Políticas - Apple

- Políticas de Apple
- Apps y perfiles
- Kiosco y pantalla de inicio
- Código de acceso
- Restricciones
- Redes
- Actualizaciones de software
- macOS
- Ubicación y geocercas
- Cuentas
- Reglas de cumplimiento

Políticas de Apple

Las políticas de Apple definen los ajustes de gestión que Cerberus Enterprise aplica a los dispositivos Apple mediante MDM. Estos ajustes se configuran desde el panel de control en el editor de políticas de Apple.

Antes de empezar

La gestión de dispositivos Apple requiere que se configure la Gestión de Apple (APNs). Si es necesario, lee la página Configuración de la Gestión de Apple (APNs).

Abrir el Editor de políticas de Apple

En el panel de control, abre **Políticas** y haz clic en **Crear nueva política de Apple**. Para editar una política de Apple existente, haz clic en su fila de la tabla de políticas.

Diseño del editor

El Editor de políticas de Apple se organiza en una serie de secciones desplegables. En la parte superior de la página siempre puedes editar:

- **Nombre** (obligatorio)
- **Id** (solo lectura)
- **Descripción** (opcional)

Secciones de la política

Las secciones siguientes coinciden con los paneles disponibles actualmente en el Editor de políticas de Apple. Cuando abres una política guardada, las secciones con ajustes modificados ya están abiertas y las demás permanecen cerradas:

- **Gestión de apps**: configura las restricciones relacionadas con las apps, las apps gestionadas y los ajustes de la app Cerberus Enterprise.

- **Quiosco y pantalla de inicio**: modo de app única, apps permitidas y bloqueadas, diseño de la pantalla de inicio, clips web, ajustes de notificaciones y mensaje de la pantalla de bloqueo.
- **Seguridad**: controla funciones como Desbloqueo automático y el desbloqueo biométrico.
- **Ajustes de código de acceso**: configura los requisitos del código de acceso y las reglas relacionadas.
- **Multimedia**: permite o deniega la cámara y las funciones relacionadas.
- **Móvil**: controla los ajustes relacionados con la red móvil (ajustes de datos móviles de las apps, eSIM, cambios de plan) y el APN de datos móviles.
- **Redes**: redes Wi-Fi (también 802.1X empresarial), VPN, certificados, proxy global, DNS cifrado y filtro de contenido web, y restricciones de conectividad como AirDrop y Bluetooth.
- **Sistema e interfaz de usuario**: restringe funciones del sistema como Handoff, el nombre del dispositivo y el salvapantallas.
- **Actualizaciones de software**: exige una versión del sistema operativo antes de una fecha límite y controla cómo se descargan e instalan las actualizaciones.
- **macOS**: firewall, Gatekeeper, salvapantallas y bloqueo, almacenamiento externo y de red, Compartir pantalla, permisos de privacidad y elementos de inicio de los Mac.
- **Apps y servicios de Apple**: restringe apps y servicios de Apple como iMessage, Game Center y Buscar.
- **Siri y Apple Intelligence**: restringe Siri, el dictado y las funciones de Apple Intelligence.
- **iCloud**: permite o deniega servicios específicos de iCloud (copia de seguridad, sincronización del llavero, retransmisión privada, etc.).
- **Ubicación y geovallas**: áreas en las que los iPhone y iPad con la app Cerberus Enterprise informan cuando entran o salen, para las reglas de eventos.
- **Cuentas**: restringe la modificación de cuentas y configura cuentas de Mail, Exchange, Google, calendario, contactos y directorio.
- **Reglas de cumplimiento**: requisitos (código de acceso, versión mínima del sistema operativo, supervisión, FileVault) que hacen que los dispositivos no cumplan, con un bloqueo opcional.

> Muchas opciones del Editor de políticas de Apple incluyen una información sobre herramientas que documenta los requisitos y las versiones compatibles del sistema operativo.

Guardar, eliminar y dispositivos asociados

Usa **Guardar política** para aplicar los cambios. El botón se desactiva cuando no hay cambios pendientes o cuando la licencia ha caducado.

Al editar una política existente, la página también muestra la acción **Eliminar política**. El editor puede mostrar una lista **Dispositivos asociados** al final, para que veas cuántos dispositivos usan actualmente la política.

Páginas siguientes

- Apps y perfiles: configura las apps instaladas y los perfiles de configuración.
- Quiosco y pantalla de inicio: modo de app única, apps permitidas, diseño de la pantalla de inicio y clips web.
- Código de acceso: configura los requisitos del código de acceso y las opciones de seguridad relacionadas.
- Restricciones: define las funciones permitidas y las limitaciones a nivel de sistema operativo.
- Redes: redes Wi-Fi, VPN, certificados y restricciones de conectividad.
- Actualizaciones de software: actualizaciones obligatorias del sistema operativo y ajustes de actualización de software.
- macOS: firewall, Gatekeeper, bloqueo de pantalla, almacenamiento, permisos de privacidad y elementos de inicio de los Mac.
- Ubicación y geovallas: áreas de las que los iPhone y iPad informan al entrar y salir, y lo que necesitan para funcionar.
- Cuentas: cuentas de correo, Exchange, Google, calendario, contactos y directorio.
- Reglas de cumplimiento: requisitos para los dispositivos y bloqueo de dispositivos que no cumplen.

Apps y perfiles

Esta sección documenta cómo configurar aplicaciones gestionadas y cargas útiles de cuentas para dispositivos Apple.

Gestión de aplicaciones

El panel **Gestión de aplicaciones** contiene tanto restricciones generales relacionadas con las aplicaciones como una lista de aplicaciones gestionadas.

Restricciones generales de aplicaciones

- **Permitir clips de apps**
- **Permitir la instalación de aplicaciones**
- **Permitir la eliminación de aplicaciones**
- **Permitir descargas automáticas de aplicaciones**
- **Permitir ocultar aplicaciones**
- **Permitir bloquear aplicaciones**
- **Permitir compras dentro de la aplicación**
- **Permitir cambiar el navegador predeterminado**
- **Permitir confiar en apps empresariales**

Aplicaciones gestionadas

Usa **Añadir aplicación** para añadir una aplicación a la política. Cada aplicación gestionada se muestra como una tarjeta. Puedes expandir la tarjeta para editar sus ajustes y quitar la aplicación con la acción de eliminar.

- **ID de App Store**: el identificador de App Store de la aplicación gestionada.
- **ID de paquete**: el identificador de paquete de la aplicación.
- **Comportamiento de instalación**: controla si la aplicación debe permanecer instalada o si el usuario puede instalarla o quitarla.
- **Asignación**: el tipo de licencia que Cerberus elige para cada dispositivo: una licencia de dispositivo en dispositivos de la empresa, una licencia de usuario de la cuenta de Apple gestionada en iPhone y iPad personales (inscripción de usuario). El campo no se puede cambiar.
- **Licencia VPP**: tipo de licencia VPP usada para la instalación a través del App Store.

La lista de selección de aplicaciones muestra las licencias disponibles y totales de cada aplicación. Las aplicaciones gratuitas muestran **Ilimitadas**: Apple les da licencias ilimitadas. Una aplicación solo se puede añadir una vez a una política: se rechaza una aplicación con el mismo ID de App Store o ID de paquete que otra ya incluida en la política, y también se rechaza una política que enumera la misma aplicación dos veces al guardarla.

La lista de selección de aplicaciones muestra las aplicaciones de tu biblioteca de Apple Business. Para añadir una aplicación, en Apple Business abre **Apps & Services → Apps & Books → App Store**, busca la aplicación y haz clic en **View**. Para una aplicación gratuita, haz clic en **Add**, selecciona **All current and future** (o la unidad organizativa de tu token de Apps and Books) en **Organizational Units**, haz clic en **Add** y luego en **Review** y confirma. Para una aplicación de pago, haz clic en su precio, elige **Managed Licenses** como **License Type** (Cerberus Enterprise no puede usar códigos de canje), selecciona la **Organizational Unit** de tu token de Apps and Books, introduce el número de **Licenses** (hasta 1000 por pedido) y luego **Review** y compra. Primero se debe configurar un método de pago en **Settings → Payments & Billing → Apps & Services → Payment Methods**. Después, las aplicaciones aparecen en la lista de selección de aplicaciones.

Aplicaciones en dispositivos personales (inscripción de usuario)

Los iPhone y iPad personales inscritos con la inscripción de usuario no tienen número de serie, por lo que reciben las aplicaciones del App Store de la política con una **licencia de usuario** de la cuenta de Apple gestionada con la que se ha iniciado sesión en el dispositivo. Cerberus registra la cuenta en Apps and Books y asigna las licencias por sí mismo, incluidas las aplicaciones gratuitas. Las cuentas de Apple gestionadas y el token de Apps and Books deben pertenecer a la misma organización de Apple Business. Una aplicación de pago usa una licencia por cuenta, compartida por todos los dispositivos personales de esa cuenta.

- **Esperando una licencia de usuario**: la aplicación se envía al dispositivo solo después de que Apple confirme su licencia, normalmente en pocos minutos. El panel **Aplicaciones** del dispositivo muestra el motivo.
- **Error en la licencia de usuario**: Apple no pudo asignar la licencia, por ejemplo porque una aplicación de pago no tiene licencias disponibles. Añade licencias en Apple Business y luego usa **Solicitar de nuevo**; Cerberus también lo vuelve a intentar por sí mismo cada día.
- **Aviso de instalación**: iOS pregunta al usuario antes de instalar cada aplicación. Si el usuario cancela, la aplicación muestra **Esperando a que el usuario apruebe la instalación**; **Solicitar de nuevo** vuelve a mostrar el aviso.
- **Liberación**: quitar la aplicación de la política, o anular la inscripción del último dispositivo personal de la cuenta, elimina la aplicación y libera su licencia, a menos que otro dispositivo inscrito de la misma cuenta aún la necesite.

Para obtener más información, consulta **Inscripción de Apple basada en la cuenta**.

Configuración gestionada

Una configuración gestionada proporciona a una aplicación sus ajustes (por ejemplo, una dirección de servidor o un nombre de cuenta), tal como los documenta el proveedor de la aplicación. Abre la aplicación en la política y haz clic en **Añadir configuración gestionada**. Se envía a iPhone y iPad con **iOS o iPadOS 18.4 o posterior** y a Mac con **macOS 27 o posterior**; aún no se envía a Apple Vision Pro. La aplicación debe admitir la configuración gestionada: una aplicación que no la lee la ignora. El panel de la aplicación muestra el número de claves junto al nombre de la aplicación.

- **Claves**: cada fila tiene una clave, un tipo y un valor. Los tipos son Texto, Entero, Número decimal, Booleano, Fecha, Lista de texto y Lista de enteros. Las claves distinguen entre mayúsculas y minúsculas y deben ser únicas. **Añadir clave** añade una fila; **Eliminar configuración** elimina todas las claves.
- **Variables**: los valores de Texto y Lista de texto pueden contener $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ y $UDID$, sustituidos por los valores de cada dispositivo y de su usuario. Una variable sin valor (por ejemplo, $EMAIL$ en un dispositivo sin usuario) se deja vacía, y los registros del sistema lo indican. Cuando cambian los datos de un usuario, los dispositivos reciben los nuevos valores; para los usuarios sincronizados desde Google Directory, los valores se actualizan en el siguiente cambio de la política o del dispositivo.
- **Importar una configuración**: abre o pega el archivo que publica el proveedor de la aplicación para MDM y luego haz clic en **Leer**. Un archivo de especificación **AppConfig specfile** (specfile.xml) enumera todas las claves que admite la aplicación con su descripción, tipo, valor predeterminado y valores permitidos: selecciona las claves que quieres importar (las que tienen un valor predeterminado ya están seleccionadas) y completa las demás después de la importación. Aparece una advertencia cuando el archivo de especificación corresponde a otra aplicación. Una **lista de propiedades** (una lista de propiedades completa o solo su <dict>) se importa tal cual. Después, elige si quieres reemplazar las claves actuales o añadirlas. Los diccionarios anidados, los valores de datos y las listas con tipos mixtos o desconocidos no son compatibles y se enumeran como omitidos. Apple no publica las claves de configuración de las aplicaciones, así que pide el archivo al proveedor cuando no esté en su documentación. **Copiar como plist** copia la configuración tal como la recibe el dispositivo, antes de que se sustituyan las variables.
- **Límites**: hasta 200 claves por aplicación; claves de hasta 255 caracteres; valores de texto de hasta 4096 caracteres; listas de hasta 200 elementos de hasta 1024 caracteres cada uno; fechas entre 1970 y 9999; 64 KB por aplicación en total.
- **No para contraseñas**: la configuración se envía solo al dispositivo para el que se crea y los registros muestran solo los nombres y tipos de las claves, pero los administradores del panel de control pueden leer los valores, y la dirección desde la que el dispositivo la descarga cambia con los valores, por lo que un valor fácil de adivinar (un booleano o un número pequeño) podría deducirse de ella. No incluyas contraseñas ni otros secretos en una configuración gestionada.

- **Estado**: cuando el dispositivo informa de que la aplicación no aceptó su configuración, el panel Aplicaciones del dispositivo muestra **Configuración no aceptada** junto a la aplicación. No marca el dispositivo como incumplidor. Una configuración que el dispositivo no puede descargar sí lo marca como incumplidor.

Opciones de la aplicación

Cada aplicación de la política (del App Store y personalizadas) tiene estas opciones. **Predeterminado del dispositivo** deja la elección al dispositivo. Los dispositivos que no admiten una opción no la reciben; la aplicación se sigue instalando.

- **Actualizaciones automáticas**: ajuste del App Store, Siempre o Nunca. iOS, iPadOS, macOS y visionOS 26 o posterior. Para las aplicaciones personalizadas, el ajuste del App Store se comporta como Nunca.
- **Descargas por red móvil**: ajuste del App Store, Siempre o Nunca, para las instalaciones y actualizaciones automáticas. Solo iPhone y iPad supervisados con iOS o iPadOS 26 o posterior.
- **Hacer copia de seguridad de los datos de la aplicación**: si los datos de la aplicación se incluyen en las copias de seguridad del dispositivo. No en Mac.
- **El usuario puede ocultar la aplicación** y **El usuario puede bloquear la aplicación**: iOS y iPadOS 18.1 o posterior, aplicado en dispositivos supervisados. No permitir el bloqueo también impide ocultarla. Las restricciones **Permitir ocultar aplicaciones** y **Permitir bloquear aplicaciones** se aplican a todas las aplicaciones.
- **Bloquear el dispositivo después de las transacciones de Tap to Pay que necesitan el PIN del cliente**: solo iPhone.
- **Dominios asociados**: los dominios a los que se asocia la aplicación (por ejemplo, para enlaces universales o autorrelleno de contraseñas), hasta 50. Introduce nombres de host simples como www.example.com, sin applinks:, comodines ni ?mode=. No en Mac.
- **Verificar los dominios directamente**: el dispositivo comprueba el archivo de asociación de sitios de los dominios directamente en lugar de a través de los servidores de Apple. Actívalo solo para dominios internos a los que no se pueda acceder desde internet.
- **Eliminación**: las aplicaciones instaladas como **Obligatorias** no las puede quitar el usuario.

Aplicaciones del Mac App Store

La lista de selección de aplicaciones muestra las plataformas de cada aplicación (iPhone/iPad, Mac, Apple TV, Vision); una aplicación que solo existe para Mac muestra su icono de Mac. Una aplicación que solo existe para Mac se aplica a los Mac cuando la añades. Una aplicación del App Store sin versión para Mac no se envía a los Mac: la política muestra "Esta aplicación no tiene versión para Mac: no se envía a los Mac" en **Se aplica a**. Los Mac reciben las aplicaciones del App Store por su ID de App Store, por lo que las aplicaciones con un ID de paquete diferente en Mac se instalan

correctamente.

Aplicación Cerberus Enterprise

Cerberus instala su app **Cerberus Enterprise** en cada iPhone y iPad con **iOS o iPadOS 18.4 o posterior**, con o sin política. La app comparte la ubicación del dispositivo y recibe notificaciones y solicitudes de seguimiento en vivo. Se instala como **Obligatoria**, con una licencia de dispositivo de Apps and Books (una licencia de usuario en dispositivos personales), así que el usuario no puede eliminarla.

- **Configuración única**: añade la aplicación gratuita a tu biblioteca una vez. En Apple Business, abre **Apps & Services** → **Apps & Books** → **App Store**, busca "Cerberus Enterprise", haz clic en **View**, luego en **Add**, selecciona **All current and future** en **Organizational Units**, haz clic en **Add** y luego en **Review** y confirma. Si la aplicación muestra **Manage**, ya está en tu biblioteca: ábrela y comprueba que sus unidades organizativas son **All current and future units**. Hasta entonces, el panel de control muestra un banner y los dispositivos muestran la aplicación como no instalada. Consulta **Configuración de la cuenta**.
- **No está en las políticas**: la aplicación no se puede añadir a una política. Está deshabilitada en la lista de selección de aplicaciones y se rechaza como aplicación personalizada (mismo ID de paquete). Una política que ya la incluye elimina la entrada cuando la abres: guarda la política para confirmar.
- **No se instala en**: dispositivos con iOS o iPadOS anterior a 18.4. El iPad compartido es compatible con la instalación, pero las funciones de la app no se han verificado en él.
- **Dispositivos personales**: en iPhone y iPad inscritos con User Enrollment, la app también se instala, con una indicación de instalación y una licencia de usuario de la Managed Apple Account. Recibe mensajes de tu organización y no accede a la ubicación a menos que la política active **Ubicación y geovallas en dispositivos personales** y el usuario lo permita.
- **Se mantiene instalada**: si el token de Apps and Books caduca o la aplicación sale de tu biblioteca, la aplicación permanece en los dispositivos y la página del dispositivo indica que Apps and Books necesita atención. Solo se elimina si la aplicación sigue faltando en tu biblioteca 24 horas después.

Aplicaciones personalizadas

Las aplicaciones personalizadas son tus propias aplicaciones para iPhone y iPad (archivos .ipa), distribuidas sin el App Store. En Xcode, exporta la aplicación para distribución **Enterprise** (Apple Developer Enterprise Program: se instala en todos los dispositivos) o para distribución **Ad Hoc** (se instala solo en los dispositivos registrados en su perfil de aprovisionamiento). Las compilaciones del App Store no se pueden subir.

Haz clic en **Añadir aplicación personalizada** para abrir las aplicaciones personalizadas de tu organización. **Subir aplicación** añade un archivo .ipa (hasta 2 GB). Selecciona una aplicación y

haz clic en **Añadir a la política**. La lista muestra la versión, el tipo de firma, el número de dispositivos del perfil de las aplicaciones ad hoc y la fecha de caducidad del perfil de aprovisionamiento.

- **Nueva versión**: sube una aplicación con el mismo ID de paquete. Reemplaza la versión anterior y los dispositivos de las políticas que la usan actualizan la aplicación.
- **Requisitos**: iPhone y iPad con iOS 17.2 o posterior. Los dispositivos que no pueden instalar la aplicación no la reciben: una aplicación solo para iPad en un iPhone, un iOS anterior al que necesita la aplicación, un dispositivo que no está en el perfil de una aplicación ad hoc o un perfil de aprovisionamiento caducado.
- **Caducidad**: cuando caduca el perfil de aprovisionamiento, la aplicación deja de abrirse. Sube una versión firmada con un nuevo perfil antes de la fecha de caducidad.
- **ID de paquete reservado**: una aplicación personalizada con el ID de paquete de la aplicación Cerberus Enterprise (com.lsdroid.Cerberus.Enterprise) no se puede añadir a una política, porque Cerberus instala esa aplicación por sí mismo.
- **Eliminar**: primero quita la app de sus políticas; después los dispositivos la eliminan.

Paquetes de Mac

Las apps personalizadas también aceptan paquetes de instalación de Mac (archivos .pkg). El paquete debe ser un paquete de distribución creado con **productbuild** (se rechaza un paquete de componentes creado solo con pkgbuild) y firmado con un certificado **Developer ID Installer**. Se recomienda notarizarlo y grapar el ticket (**notarytool** y **stapler**). Se rechazan los paquetes sin firmar, los paquetes modificados después de firmarlos y los paquetes firmados con otros certificados.

Sube el archivo .pkg con **Subir app** y agrégalo a la política: aparece en **Paquetes de Mac**. Los iPhone y iPad lo ignoran.

Los Mac con **macOS 26 o posterior** (supervisados, lo que incluye los Mac registrados manualmente, pero no User Enrollment) reciben el paquete como una **declaración**: el Mac lo descarga, lo instala, reintenta y lo actualiza por sí solo e informa su estado. Los Mac más antiguos, y los paquetes instalados como apps administradas, lo reciben con un **comando MDM**, en cualquier versión de macOS. Un Mac que se actualiza a macOS 26 pasa a la declaración por sí solo; puede instalar cada paquete una vez más. Lo mismo puede ocurrir cuando un Mac pasa a otra política que tiene el mismo paquete.

- **Nueva versión**: sube un paquete con el mismo identificador de paquete. Reemplaza la versión anterior, y los Mac de las políticas que lo usan instalan la nueva.
- **Mac omitidos**: Mac con un macOS más antiguo que el que permite el paquete, y Mac Intel para paquetes creados solo para Apple silicon. La página del dispositivo muestra el paquete como Omitido, con el motivo; la versión instalada antes permanece en el Mac.
- **Instalar**: **Obligatorio** (opción predeterminada) instala el paquete en el Mac; **Opcional** deja el paquete disponible en el Mac sin instalarlo. macOS 26 no muestra los paquetes

opcionales al usuario en Ajustes del Sistema ni en el App Store (probado en macOS 26.3), así que una app o un script del Mac tiene que instalarlos; elige Opcional solo si dispones de uno. Se aplica a los Mac con macOS 26 o posterior; los Mac más antiguos siempre instalan el paquete. La opción no está disponible para paquetes instalados como apps administradas.

- **Eliminar los archivos del paquete cuando salga de la política (macOS 27 o posterior)**: cuando el paquete se quita de la política, los Mac con macOS 27 o posterior eliminan los archivos que instaló. Está desactivado de forma predeterminada. En los Mac más antiguos, los archivos permanecen. No está disponible para paquetes instalados como apps administradas.
- **Instalar como app administrada**: actívalo para que un paquete de la política instale su app como app administrada (macOS 11 o posterior, no con la inscripción de usuarios). macOS entonces informa cuando falla la instalación, y MDM puede eliminar la app. La app debe instalarse directamente en la carpeta Aplicaciones, firmada con un certificado **Developer ID Application** y notarizada; en macOS 11 a 13 el paquete debe contener solo esa app (ningún otro archivo ni script). Las apps personalizadas muestran qué paquetes cumplen los requisitos. Cuando la opción no se puede aplicar en un Mac, el paquete se instala allí como de costumbre y la página del dispositivo indica por qué.
- **Opciones de eliminación** de una app administrada: **Eliminar la app cuando el paquete se quita de la política** (activado de forma predeterminada) y **Eliminar la app cuando el Mac deja de estar administrado**. Eliminar una app también borra sus datos. Si el usuario ya había instalado la misma app, esa copia pasa a estar administrada y también se elimina.
- **Eliminación**: el comando MDM no puede desinstalar un paquete. Para un paquete instalado como app administrada, quitarlo de la política elimina la app (cuando la opción está activada); sus otros archivos y el recibo del paquete permanecen. Los paquetes con **Eliminar los archivos del paquete** activado se eliminan de los Mac con macOS 27 o posterior. Otros paquetes: quitarlos de la política solo detiene las nuevas instalaciones, los archivos permanecen en los Mac. Un Mac que se omite (por ejemplo, tras una nueva versión que necesita un macOS más reciente) conserva la app mientras el paquete está en la política; quitarlo entonces de la política también la elimina. Elimina los archivos sobrantes del Mac (por ejemplo, con el propio desinstalador del paquete) y ejecuta `sudo pkgutil --forget <identifier>` para olvidar el recibo del paquete.
- **Estado en el dispositivo**: el panel Aplicaciones del Mac muestra cada paquete de la política como En cola, Aceptado (el Mac aceptó el comando), Descargado, Instalado (solo para paquetes que contienen apps, cuando las apps se encuentran en el Mac) o Fallido (con el error). macOS no informa la instalación de un paquete enviado con el comando, así que Descargado es el último estado para los paquetes sin apps. Un paquete instalado como app administrada también pasa a Fallido cuando macOS informa que la app no se pudo instalar o se eliminó del Mac. **Instalar de nuevo** envía el paquete al Mac otra vez.
- **Estado con la declaración**: los paquetes entregados como declaración muestran la etiqueta **Declaración** y el estado que informa el Mac: En cola, Disponible (un paquete opcional que el usuario no ha instalado), Esperando al usuario, Descargando, Instalando, Instalado o Fallido (con el motivo, por ejemplo una descarga o instalación fallida, o una declaración que el Mac rechazó). La etiqueta **Archivos eliminados con la política**

marca los paquetes cuyos archivos elimina un Mac con macOS 27 cuando salen de la política. **Instalar de nuevo** aparece solo después de un fallo y pide al Mac que lo intente otra vez; no se ofrece cuando el Mac rechazó la declaración.

Cuentas

El panel **Cuentas** te permite configurar cuentas que se aplican a los dispositivos administrados. También incluye un interruptor de restricción para la modificación de cuentas.

Restricción

- **Permitir la modificación de cuentas**: cuando está desactivado, los usuarios no pueden modificar cuentas como las cuentas de Apple y las cuentas de internet.

Añadir cuentas

Usa **Añadir cuenta de Google** o **Añadir cuenta de correo** para añadir cargas útiles de cuenta a la política. Cada cuenta aparece como una tarjeta con sus campos de configuración.

Credenciales de cuenta de los usuarios

Tanto las tarjetas de cuenta de Google como las de correo proporcionan un interruptor **Credenciales de cuenta de los usuarios**. Cuando está activado, el sistema aplica las credenciales de cuenta por usuario. Cuando está desactivado, introduces la identidad de la cuenta en la política.

Campos de la cuenta de Google

- **Nombre visible**: el nombre que se muestra al usuario para la cuenta.
- **Dirección de correo de Google**: la dirección de correo del usuario.
- **Nombre completo**: el nombre completo del usuario.

Campos de la cuenta de correo

Las cuentas de correo incluyen campos de identidad y la configuración de los servidores entrante y saliente. Los nombres de host son obligatorios.

- **Nombre visible**: el nombre que se muestra al usuario para la cuenta de correo.

- **Dirección de correo**: la dirección de correo del usuario.
- **Nombre completo**: el nombre completo del usuario.

Servidor entrante

- **Tipo de servidor**: protocolo de correo (por ejemplo, IMAP o POP).
- **Método de autenticación**: método de autenticación del servidor.
- **Prefijo de ruta de IMAP**: se muestra solo cuando el tipo de servidor es IMAP.
- **Nombre de host**: obligatorio.
- **Puerto**: puerto del servidor (1–65535).

Servidor saliente

- **Método de autenticación**
- **Nombre de host**: obligatorio.
- **Puerto**: puerto del servidor (1–65535).

Opciones de S/MIME

Para las cuentas de correo, también puedes configurar el comportamiento de cifrado y firma de S/MIME.

Cifrado

- **Cifrado S/MIME**
- **Identidad modificable por el usuario**
- **Interruptor por mensaje activado**
- **Modificable por el usuario**

Firma

- **Firma S/MIME**
- **Identidad modificable por el usuario**
- **Modificable por el usuario**

> Las opciones de cuenta y restricción incluyen información emergente en el panel de control que documenta los requisitos previos y las versiones de SO compatibles.

Kiosco y pantalla de inicio

La sección **Quiosco y pantalla de inicio** del Editor de políticas de Apple bloquea los dispositivos en una sola app, elige qué apps se pueden abrir, organiza la pantalla de inicio y añade iconos de sitios web. Cada ajuste se instala en los dispositivos como un perfil de configuración.

> Apple aplica la mayoría de estos ajustes solo a iPhone y iPad supervisados (dispositivos inscritos con Automated Device Enrollment o preparados con Apple Configurator). Los demás dispositivos no los reciben. Los clips web también funcionan en iPhone y iPad no supervisados. Los Mac no reciben ninguno de estos ajustes.

Elegir apps

Las apps se identifican por su ID de paquete. Escribe el nombre de una app para elegirla entre las apps integradas de Apple y las apps de la política, o escribe cualquier ID de paquete, por ejemplo `com.example.app`.

Modo de app única

El dispositivo ejecuta solo la app elegida: los usuarios no pueden volver a la pantalla de inicio ni abrir otras apps. Primero instala la app con la política. El dispositivo sale del Modo de app única cuando desactivas el ajuste o eliminas la app.

- **Opciones**: desactiva la pantalla táctil, la rotación, los botones de volumen, el interruptor Silencio/Timbre, el botón lateral o el bloqueo automático, y activa funciones de accesibilidad como VoiceOver o Zoom.
- **Funciones de accesibilidad que el usuario puede activar**: funciones que el usuario puede activar con una triple pulsación del botón lateral.

Apps permitidas y bloqueadas

- **Apps bloqueadas**: los dispositivos ocultan estas apps y no las abren. `com.apple.webapp` bloquea todos los clips web. Ajustes y, en iPhone, Teléfono no se pueden bloquear.
- **Permitir solo algunas apps**: los dispositivos muestran solo estas apps. Deja la lista vacía para permitir todas las apps. **Apps de la política** añade las apps instaladas por la

política; `com.apple.webapp` permite todos los clips web.
- **Apps que pueden iniciar el Modo de app única**: apps que pueden bloquear el dispositivo en sí mismas mientras lo necesitan, por ejemplo durante un examen.

> Con **Permitir solo algunas apps**, todas las apps que no estén en la lista desaparecen de los dispositivos, incluidas las apps de la política. Ajustes y, en iPhone, Teléfono permanecen siempre.

Diseño de la pantalla de inicio

Organiza el Dock y las páginas de la pantalla de inicio. Añade apps, carpetas de apps y los clips web de la política, eligiendo dónde con **Añadir a**, y arrastra los iconos para moverlos entre el Dock y las páginas. Haz clic en una carpeta para cambiar su nombre y sus apps.

Los usuarios no pueden mover los iconos ni eliminar apps de la pantalla de inicio. Las apps que no están en el diseño van a las páginas posteriores a las que has definido. Un iPhone muestra cuatro iconos en el Dock. Los usuarios aún pueden eliminar apps que no sean Obligatorias en la pantalla de almacenamiento de Ajustes. Para evitarlo, desactiva **Permitir eliminar apps** en Gestión de apps.

Clips web

Un clip web es un icono de la pantalla de inicio que abre un sitio web. Define la etiqueta y la URL, y opcionalmente una imagen (PNG o JPEG, recortada a un cuadrado).

- **Los usuarios pueden eliminarlo**: desactívalo para mantener el icono en los dispositivos.
- **Pantalla completa**: el sitio web se abre como una app web, sin la barra de direcciones de Safari. **Mantener la pantalla completa en otros sitios web** también abre los enlaces a otros sitios web en la app web.
- **Abrir con esta app**: una app que abre la URL en lugar de Safari.

Ajustes de notificaciones

Elige cómo muestran los dispositivos las notificaciones de algunas apps: si están permitidas, dónde aparecen (pantalla de bloqueo, Centro de notificaciones, CarPlay), las insignias, los sonidos, las alertas críticas, el estilo de los banners, la agrupación y las vistas previas. Los usuarios no pueden cambiar estos ajustes.

Mensaje de la pantalla de bloqueo

Un mensaje que se muestra en la parte inferior de la pantalla de bloqueo, por ejemplo a quién llamar si se encuentra el dispositivo, y una etiqueta de activo. Ambos pueden contener las variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ y $UDID$: una variable sin valor para el dispositivo se deja vacía.

Código de acceso

La sección **Ajustes de código de acceso** controla los requisitos de código de acceso del dispositivo y las reglas de seguridad relacionadas (por ejemplo, longitud y complejidad mínimas). En un Mac (macOS 13 o posterior, no con Inscripción de usuario) las reglas se aplican a la contraseña de inicio de sesión de los usuarios.

Opciones

En el Editor de políticas de Apple, las opciones de código de acceso se configuran con una combinación de interruptores y campos numéricos. Muchos campos incluyen información emergente que indica las versiones de SO compatibles y los requisitos de supervisión.

Interruptores de código de acceso

- **Cambiar en la próxima autenticación**: fuerza un restablecimiento del código de acceso la próxima vez que el usuario se autentique.
- **Requerir código de acceso alfanumérico**: requiere al menos un carácter alfabético y un número.
- **Requerir código de acceso complejo**: requiere un código de acceso «complejo» (sin patrones repetidos ni secuenciales y al menos un carácter no alfanumérico).
- **Requerir código de acceso**: requiere un código de acceso sin requisitos adicionales de longitud o calidad. Nota: configurar otros ajustes de código de acceso requiere implícitamente un código de acceso.

Campos numéricos

- **Restablecimiento de intentos fallidos (minutos)**: minutos antes de que se restablezca el contador de intentos fallidos (requiere Intentos fallidos máximos).
- **Máximo de intentos fallidos**: intentos fallidos permitidos antes de que se borre un iPhone o iPad, o se bloquee un Mac (intervalo: 2–11).
- **Periodo de gracia máximo (minutos)**: cuánto tiempo puede estar desbloqueado el dispositivo sin requerir el código de acceso (0 = ninguno).
- **Inactividad máxima (minutos)**: tiempo de inactividad antes de que se bloquee el dispositivo (intervalo: 0–15).
- **Antigüedad máxima del código de acceso (días)**: antigüedad máxima del código de acceso antes de un cambio forzado (intervalo: 0–730).

- **Caracteres complejos mínimos**: número mínimo de caracteres «complejos» (intervalo: 0–4).
- **Longitud mínima**: longitud mínima del código de acceso (intervalo: 0–16).
- **Límite de reutilización del código de acceso**: longitud del historial de códigos de acceso para evitar reutilizar códigos antiguos (intervalo: 1–50).

Restricciones

Las secciones de Restricciones controlan qué funciones del SO se permiten en los dispositivos Apple administrados. En el Editor de políticas de Apple, estas opciones se presentan como paneles agrupados con varios interruptores.

Los interruptores de los paneles **Gestión de apps** y **Redes** se describen en las páginas Apps y perfiles y Redes de las políticas de Apple.

> Muchas restricciones solo son compatibles con versiones específicas del SO y pueden requerir dispositivos supervisados. Usa la información emergente del panel de control para consultar los requisitos oficiales.

> En los dispositivos con User Enrollment (dispositivos personales registrados al iniciar sesión con una cuenta de trabajo), no se envían las restricciones que Apple no permite allí. Si no se aplica ninguna de las restricciones de la política, estos dispositivos no reciben perfil de restricciones. El editor de políticas muestra cuántas restricciones no se aplican a los dispositivos con User Enrollment.

Seguridad

- **Permitir el desbloqueo automático**
- **Permitir huella digital para desbloquear**
- **Permitir la modificación de huellas digitales**
- **Permitir borrar contenido y ajustes**
- **Permitir habilitar restricciones**
- **Permitir que los usuarios instalen perfiles**
- **Permitir el emparejamiento con host**
- **Permitir el envío de diagnósticos**
- **Permitir modificar el envío de diagnósticos**
- **Permitir publicidad personalizada de Apple**
- **Permitir modificar Remote Management**

Multimedia

- **Permitir cámara**
- **Permitir modificación de Compartir archivos**
- **Permitir acceso a unidades USB de Archivos**
- **Permitir la grabación de llamadas**
- **Permitir AirPrint**
- **Permitir almacenamiento de credenciales de AirPrint**
- **Permitir detección de iBeacon para AirPrint**

Red móvil

- **Permitir modificación de datos móviles por app**
- **Permitir modificación del plan móvil**
- **Permitir modificación de la eSIM**
- **Permitir transferencias salientes de eSIM**
- **Conservar la eSIM al borrar el dispositivo**
- **Permitir la actualización en segundo plano durante la itinerancia**

APN móvil

APN móvil establece el nombre de punto de acceso (APN) que te dio tu operador, por ejemplo para una red móvil privada o de empresa. Establece el **nombre de punto de acceso** y, si el operador lo solicita, la autenticación (PAP o CHAP), el nombre de usuario (se permiten variables como $EMAIL$), la contraseña, las versiones de IP (también en itinerancia), un servidor proxy con su puerto y XLAT464. Activa **Adjuntar APN** solo si el operador te da un APN independiente para conectarte a la red.

- Solo lo reciben los iPhone y los iPad con conexión móvil, también sin supervisión. Los dispositivos registrados con User Enrollment (dispositivos personales) no lo reciben.
- Se aplica solo a la SIM que se usa para datos móviles. Un dispositivo que ya tiene un perfil de APN instalado de otra forma no lo instala.
- La contraseña está protegida como las demás contraseñas de red: el perfil se envía solo al dispositivo para el que se creó y la contraseña no se escribe en los registros.

> Un APN incorrecto deja los dispositivos sin datos móviles: prueba primero los ajustes en un dispositivo de prueba con una SIM del operador.

Sistema e interfaz de usuario

- **Permitir Handoff**
- **Permitir la autocorrección**
- **Permitir la atenuación automática**
- **Permitir el salvapantallas automático**
- **Permitir el teclado QuickPath**
- **Permitir la búsqueda de definiciones**
- **Permitir modificar el nombre del dispositivo**
- **Permitir la suspensión del dispositivo**
- **Permitir iPhone Mirroring**
- **Permitir widgets de iPhone en Mac**
- **Permitir los atajos de teclado**

Apps y servicios de Apple

- **Permitir iMessage**
- **Permitir Game Center**
- **Permitir añadir amigos en Game Center**
- **Permitir Buscar mi dispositivo**
- **Permitir Buscar amigos**
- **Permitir modificar Buscar amigos**
- **Permitir la librería**
- **Permitir contenido erótico de la librería**
- **Permitir la copia de seguridad de libros empresariales**
- **Permitir la sincronización de metadatos de libros empresariales**
- **Permitir iTunes Store**
- **Permitir contenido explícito**

Siri y Apple Intelligence

- **Permitir Siri**
- **Permitir contenido generado por el usuario en Siri**
- **Permitir Siri con el dispositivo bloqueado**
- **Permitir el dictado**
- **Permitir integraciones de inteligencia externas**
- **Permitir iniciar sesión en inteligencia externa**
- **Permitir Genmoji**
- **Permitir Image Playground**
- **Permitir Image Wand**

iCloud

- **Permitir la libreta de direcciones de iCloud**
- **Permitir la copia de seguridad de iCloud**
- **Permitir los marcadores de iCloud**
- **Permitir el calendario de iCloud**
- **Permitir el escritorio y los documentos de iCloud**
- **Permitir la sincronización de documentos de iCloud**
- **Permitir Freeform de iCloud**
- **Permitir la sincronización del llavero de iCloud**
- **Permitir Mail de iCloud**
- **Permitir Notas de iCloud**
- **Permitir Fototeca de iCloud**
- **Permitir Retransmisión privada de iCloud**
- **Permitir Recordatorios de iCloud**

Cuentas (restricción)

El panel Cuentas contiene una restricción y (opcionalmente) la configuración de cuentas. El interruptor de restricción controla si el usuario puede modificar las cuentas del sistema.

- **Permitir modificación de cuentas**

Redes

La sección **Redes** del Editor de políticas de Apple configura redes Wi-Fi y VPN en los dispositivos, instala certificados y restringe funciones de conectividad como AirDrop y Bluetooth. Cada red Wi-Fi, VPN y certificado se instala como su propio perfil de configuración, que puedes ver en el dispositivo en **Configuración > General > VPN y gestión de dispositivos** (Mac: **Configuración del Sistema > General > Gestión de dispositivos**, o **Privacidad y seguridad > Perfiles** en macOS 13 y 14) y en el panel **Perfiles, certificados y seguridad** de la página del dispositivo.

> Los certificados se toman de la página **Certificados**: primero impórtalos allí. La política solo hace referencia a ellos, así que un certificado nunca se copia en la política.

Restricciones

- **Permitir AirDrop**
- **Permitir solicitudes entrantes de AirPlay**
- **Permitir modificación de Bluetooth**
- **Permitir modificación de Compartir Bluetooth**
- **Permitir acceso a unidades de red de Archivos**
- **Permitir modificación de Compartir Internet**
- **Permitir el almacenamiento en caché de contenido**
- **Permitir compartir archivos por iTunes**

Redes Wi-Fi

Haz clic en **Añadir red Wi-Fi** y rellena:

- **Nombre de la red (SSID)**: el nombre de la red, de hasta 32 caracteres.
- **Seguridad**: ninguna (red abierta), WEP, WPA o WPA2, WPA2 o WPA3, solo WPA3, o cualquiera.
- **Contraseña**: la contraseña de una red personal.
- **Unirse automáticamente** y **Red oculta** (para las redes que no difunden su nombre).
- **Proxy**: ninguno, manual (servidor y puerto) o automático (una URL de archivo PAC, o vacío para encontrar la configuración en la red con WPAD).
- **Nombre del perfil** (opcional) y **Se aplica a**, para limitar la red a algunos tipos de dispositivo.

Redes empresariales (802.1X)

Activa **Empresarial (802.1X)** cuando los usuarios se autentican con sus propias credenciales o un certificado en lugar de una contraseña compartida.

- **Autenticación**: PEAP, TTLS (con su autenticación interna, por ejemplo MSCHAPv2) o TLS (solo certificado).
- **Credenciales del usuario del dispositivo**: cada dispositivo usa la identidad EAP, la identidad anónima y la contraseña de su usuario, configuradas en la página Usuarios. Los dispositivos sin usuario no reciben la red.
- **Identidad**, **Identidad anónima** y **Contraseña**: las mismas para todos los dispositivos. La identidad puede contener las variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ y $UDID$. Deja la contraseña vacía para que el usuario la escriba en el dispositivo.
- **Certificado de identidad**: el certificado de cliente que presenta el dispositivo (obligatorio para TLS). Consulta las opciones de certificado a continuación.
- **Certificados de confianza**: los certificados de CA que emitieron el certificado de tu servidor RADIUS. Se instalan con la red.
- **Nombres de servidor de confianza**: los nombres de los certificados del servidor RADIUS que aceptan los dispositivos, por ejemplo radius.example.com o *.example.com.

VPN

Haz clic en **Añadir VPN** para configurar una VPN IKEv2 o Cisco IPSec, integrada en iOS, iPadOS y macOS (no se necesita ninguna app de VPN).

- **Tipo** y **Servidor**. Para IKEv2, también el **Identificador remoto** (la identidad del servidor; vacío significa la dirección del servidor) y el **Identificador local**, que puede contener las variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ y $UDID$.
- **Autenticación** del dispositivo: un certificado (de la página Certificados, el certificado del usuario del dispositivo, o solicitado a un servidor SCEP), un secreto compartido (con el nombre de grupo opcional para IPSec), o ninguna para los servidores IKEv2 que solo comprueban el nombre de usuario y la contraseña.
- **Certificados de confianza**: los certificados de CA de tu servidor VPN, instalados con la VPN. Para IKEv2 también puedes establecer el emisor y el nombre del certificado de servidor esperados.
- **Nombre de usuario y contraseña**: el usuario también se autentica con un nombre de usuario (se permiten variables) y una contraseña (EAP para IKEv2, XAuth para IPSec). Deja la contraseña vacía para que el usuario la escriba en el dispositivo.
- **Nombre de la VPN** (se muestra en Configuración) y **Se aplica a**.

Conexión

- **El usuario se conecta en Configuración**: la VPN está instalada y el usuario la activa cuando es necesario.
- **Bajo demanda**: el dispositivo conecta la VPN automáticamente. Con **excepto en redes Wi-Fi de confianza** no se usa la VPN en las redes Wi-Fi que indiques, por ejemplo la red de la oficina.
- **Siempre activa** (IKEv2, solo iPhone y iPad supervisados): todo el tráfico pasa por la VPN en redes móviles y Wi-Fi, y el usuario no puede desactivarla. Los demás dispositivos no reciben esta VPN. Si la VPN usa un nombre de usuario, la contraseña debe establecerse en la política.
- **VPN por app**: solo algunas apps usan la VPN. Elige la VPN para cada app en la sección **Gestión de apps** (campo **VPN** de la app, no disponible en Mac) y, opcionalmente, indica los dominios de Safari que la usan.

> Prueba primero una VPN Siempre activa o bajo demanda en un dispositivo de prueba: si no se puede alcanzar el servidor, el dispositivo puede quedarse sin conexión.

Proxy global, DNS cifrado y filtro de contenido web

Estos ajustes se aplican a todo el tráfico del dispositivo. Actívalos con su interruptor.

- **Proxy HTTP global** (iPhone y iPad supervisados, Mac): todo el tráfico HTTP pasa por el proxy, en todas las redes. Establece el servidor y el puerto (con un nombre de usuario y una contraseña opcionales) o una configuración automática (URL de archivo PAC, o vacío para encontrarla en la red). **Permitir páginas de inicio de sesión Wi-Fi** permite al usuario iniciar sesión en redes Wi-Fi públicas sin el proxy.
- **DNS cifrado**: el dispositivo resuelve nombres con tu servidor DNS mediante DNS over HTTPS (URL del servidor) o DNS over TLS (nombre del servidor), opcionalmente solo para algunos dominios. En los dispositivos supervisados puedes impedir que el usuario lo desactive.
- **Filtro de contenido web** (iPhone y iPad supervisados): el filtro integrado en iOS limita los sitios web para adultos, con listas de sitios web siempre permitidos o siempre bloqueados, o permite solo una lista de sitios web, que se muestran como marcadores en Safari.

>

> Un proxy o servidor DNS incorrecto puede dejar los dispositivos sin conexión: pruebaprimero los ajustes en un dispositivo de prueba.

Certificados

Haz clic en **Añadir certificado** para instalar un certificado por separado: una autoridad de certificación en la que Safari y las apps deben confiar, o una identidad que usan las apps. Los certificados de una red Wi-Fi o una VPN no necesitan añadirse aquí.

Opciones de certificado

- **Un certificado de la página Certificados**: el mismo certificado en todos los dispositivos. Haz clic en **Elegir un certificado** para seleccionarlo.
- **El certificado del usuario del dispositivo**: cada dispositivo recibe el certificado de cliente vinculado a su usuario. Los dispositivos cuyo usuario no tiene certificado no lo reciben. Cuando vinculas otro certificado al usuario, los dispositivos se actualizan.
- **Solicitado a un servidor SCEP**: cada dispositivo solicita su propio certificado a tu servidor SCEP (por ejemplo Microsoft NDES), así que la clave privada nunca sale del dispositivo. Establece la URL del servidor, el desafío si el servidor lo requiere, el sujeto (por ejemplo CN=$EMAIL$), los nombres alternativos, el tamaño de la clave y el uso de la clave.

> Los certificados de cliente (.p12) protegidos con el antiguo cifrado RC2 no se pueden instalar en dispositivos Apple. Vuelve a exportarlos con cifrado 3DES o AES antes de importarlos.

Seguridad

Los perfiles que contienen contraseñas o claves privadas se envían solo al dispositivo para el que se crearon: el dispositivo debe firmar su solicitud con su certificado de gestión. Las contraseñas y los certificados no se escriben en los registros.

Actualizaciones de software

La sección **Actualizaciones de software** del Editor de políticas de Apple mantiene los dispositivos actualizados: puede exigir una versión concreta del sistema operativo antes de una fecha límite y controlar cómo los dispositivos descargan e instalan las actualizaciones.

Actualizaciones del sistema operativo obligatorias

Toca **Añadir actualización obligatoria** para exigir una versión del sistema operativo. El dispositivo descarga la actualización, informa al usuario de la fecha límite y la instala en esa fecha si el usuario no lo ha hecho antes. Los dispositivos que ya ejecutan esa versión o una posterior la ignoran. Requiere iOS y iPadOS 17 o macOS 14.

- **Se aplica a** (obligatorio): iPhone y iPad, o Mac. Cada sistema operativo tiene sus propios números de versión, así que añade una actualización obligatoria para cada uno.
- **Versión del sistema operativo**: la versión que se va a instalar, por ejemplo 18.5 o 15.4.1.
- **Compilación** (opcional): una compilación concreta, por ejemplo una beta o una Mejora de seguridad en segundo plano.
- **Instalar antes de**: la fecha límite, en la hora local de cada dispositivo. Una fecha en el pasado hace que los dispositivos instalen la actualización lo antes posible.
- **URL de detalles** (opcional): una página web sobre la actualización que se muestra al usuario.

> El dispositivo informa del progreso de la actualización (descarga, instalación, fallos) en el panel **Estado del dispositivo** de la página del dispositivo.

Ajustes de actualización de software

Activa **Ajustes de actualización de software para iPhone y iPad** o **Ajustes de actualización de software para Mac** para controlar las actualizaciones en esos dispositivos. Cuando un

interruptor está desactivado, los dispositivos mantienen sus propios ajustes. Requiere iOS y iPadOS 18 o macOS 15: los dispositivos más antiguos ignoran estos ajustes.

- **Aplazar actualizaciones**: las nuevas actualizaciones solo se muestran al usuario después del número de días indicado (del 1 al 90). En un Mac puedes establecer periodos distintos para las actualizaciones principales, las secundarias y otras actualizaciones del sistema.
- **Actualizaciones mostradas al usuario** (iPhone y iPad): cuando haya más de una actualización disponible, muestra todas, solo la actualización secundaria más antigua o solo la más reciente.
- **Los usuarios estándar pueden instalar actualizaciones** (Mac): los usuarios sin derechos de administrador pueden instalar actualizaciones de macOS.
- **Notificar al usuario las actualizaciones obligatorias**: muestra las notificaciones sobre las actualizaciones obligatorias y su fecha límite.
- **Descarga automática**, **Instalación automática** y **Actualizaciones de seguridad automáticas**: deja que el usuario decida (valor predeterminado de Apple) o mantenlas siempre activadas o siempre desactivadas.
- **Mejoras de seguridad en segundo plano**: ofrece al usuario las correcciones de seguridad rápidas de Apple y elige si el usuario puede eliminarlas.
- **Programas beta**: permite que el usuario se una a los programas beta de Apple, o quita el dispositivo de ellos y bloquéalos (en iPhone y iPad, solo dispositivos supervisados).

Instalar una actualización desde la página del dispositivo

El panel **Estado del dispositivo** de un dispositivo muestra las actualizaciones disponibles para él. Usa **Buscar actualizaciones** para pedir al dispositivo la lista e **Instalar** para instalar una ahora o descargarla y dejar que el usuario la instale. Esto funciona en iPhone y iPad supervisados y en Mac. Apple elimina estos comandos en iOS, iPadOS y macOS 27: en esas versiones, usa las actualizaciones obligatorias de la política.

macOS

La sección **macOS** del Editor de políticas de Apple gestiona los ajustes de seguridad, privacidad e inicio de sesión de los Mac: FileVault, Firewall, Gatekeeper, salvapantallas y bloqueo, almacenamiento externo y de red, Compartir pantalla, permisos de privacidad, elementos de inicio y las extensiones de sistema y de kernel que se permite cargar. También instala archivos de configuración de servicios del sistema y tareas en segundo plano. Los demás dispositivos de la política no reciben estos ajustes. Activa un ajuste para gestionarlo; mientras está desactivado, los usuarios conservan sus propias opciones.

> La mayoría de los ajustes se instalan en el Mac como perfiles de configuración, visibles en Ajustes del Sistema > General > Gestión de dispositivos. FileVault, los permisos de privacidad, los elementos de inicio y los ajustes de extensiones necesitan un MDM aprobado por el usuario: en un Mac registrado con la URL de inscripción o el código QR, el usuario aprueba el perfil de inscripción en Ajustes del Sistema. La página del dispositivo lo muestra en el campo **MDM aprobado por el usuario**. Cuando el usuario lo aprueba más tarde, el Mac recibe estos ajustes automáticamente.

FileVault

FileVault cifra el disco del Mac. Con este ajuste activado, se pide a los usuarios que activen FileVault con su contraseña, y el Mac envía su clave de recuperación personal a Cerberus Enterprise, cifrada con una clave que pertenece solo a tu organización. La clave se muestra y se cambia desde el campo **FileVault** de la página del dispositivo (consulta Comandos de dispositivo). El ajuste necesita macOS 13 o posterior y un MDM aprobado por el usuario; sin un MDM aprobado por el usuario no se pide al Mac que active FileVault, pero si un usuario lo activa, su clave se almacena.

- **Obligatorio al iniciar sesión**: en el siguiente inicio de sesión, tras un número de omisiones (se vuelve a preguntar al usuario en cada inicio y cierre de sesión), o solo cuando el usuario cierra la sesión.
- **No preguntar al cerrar sesión**: se pregunta al usuario solo al iniciar sesión. No se puede combinar con «Solo se pregunta al cerrar sesión».
- **Mostrar la clave de recuperación al usuario**: desactivado de forma predeterminada, así que solo los administradores conocen la clave, desde la página del dispositivo.
- **Impedir desactivar FileVault**: activado de forma predeterminada.
- **Eliminar la clave de la memoria en modo de espera**: el usuario vuelve a escribir la contraseña cuando el Mac se despierta del modo de espera.

- **Dónde se guarda la clave**: texto que se muestra al usuario en la ventana de inicio de sesión, por ejemplo a quién llamar para recuperar el Mac (predeterminado «Cerberus Enterprise»).

> Un Mac que ya estaba cifrado cuando recibió el ajuste conserva su clave actual, que Cerberus Enterprise no recibe: la clave se almacena solo después de que el usuario desactive y vuelva a activar FileVault (con «Impedir desactivar FileVault» desactivado). Desactivar el ajuste, o quitar el Mac de la gestión, no desactiva FileVault, y la clave almacenada sigue funcionando. El ajuste no se puede guardar cuando el servidor no está configurado para almacenar claves de recuperación.

Firewall

- **Activar el Firewall**: cuando está desactivado, el Firewall permanece desactivado y los usuarios no pueden activarlo.
- **Bloquear todas las conexiones entrantes**: solo los servicios de red básicos (DHCP, Bonjour, IPSec) pueden recibir conexiones.
- **Modo sigiloso**: el Mac no responde a las solicitudes de ping ni a las conexiones a puertos cerrados.
- **Permitir software integrado** y **Permitir apps firmadas descargadas** para recibir conexiones sin preguntar al usuario (macOS 12.3 o posterior).
- **Reglas para apps específicas**: permite o bloquea las conexiones entrantes de una app, por ID de paquete.

Gatekeeper

Gatekeeper comprueba las apps antes de abrirlas. Elige si los Mac abren solo apps del App Store, o también las apps de desarrolladores identificados. Con Gatekeeper desactivado, se puede abrir cualquier app, también las que no están firmadas o están dañadas. En macOS 15 o posterior también puedes elegir si se pregunta a los usuarios si desean enviar el malware bloqueado a Apple.

Salvapantallas y bloqueo

Inicia el salvapantallas tras un tiempo de inactividad y pide la contraseña cuando se inicia el salvapantallas o se duerme la pantalla, de inmediato o tras un retraso. Un ajuste que se deja como **Sin gestionar** sigue siendo elección del usuario.

Almacenamiento externo y de red

Permite, pon en solo lectura o bloquea el almacenamiento externo (unidades USB, tarjetas SD, discos externos) y el almacenamiento de red (recursos compartidos de archivos) de los Mac. Necesita macOS 15 o posterior.

Compartir pantalla

Límites de las personas que se conectan a estos Mac con Compartir pantalla: copiar archivos desde o hacia el Mac, las conexiones de alto rendimiento y el número de pantallas virtuales. Activar Compartir pantalla sigue siendo elección del usuario. Necesita macOS 14 o posterior.

Permisos de privacidad

Concede o deniega a las apps el acceso que los usuarios permitirían en Ajustes del Sistema > Privacidad y seguridad, por ejemplo Acceso total al disco para una app de copia de seguridad, o deniega la cámara a una app. Para cada permiso, elige:

- **Permiso**: Acceso total al disco, Accesibilidad, Automatización, las carpetas, los contactos, los calendarios, las fotos, la cámara, el micrófono, la grabación de pantalla y los demás de Privacidad y seguridad.
- **Acceso**: permitir o denegar. La cámara, el micrófono, la grabación de pantalla y la monitorización de entrada no se pueden permitir con un perfil, solo denegar; para la grabación de pantalla y la monitorización de entrada, puedes permitir que los usuarios las permitan también sin derechos de administrador.
- **App**: el ID de paquete de una app, o la ruta de un programa (por ejemplo, una herramienta de línea de comandos).
- **Requisito de código**: identifica la app por su firma. Obtenlo en Terminal con `codesign -dr - /Applications/Example.app` y copia el texto que aparece después de `designated =>`.
- **Automatización** también necesita la app controlada (por ejemplo, el Finder) y su requisito de código.

Elementos de inicio y en segundo plano

Los elementos de inicio y de fondo que coinciden con las reglas se gestionan: se ejecutan sin preguntar, y los usuarios no pueden desactivarlos en Ajustes del Sistema > General > Elementos de inicio. Una regla coincide con el ID de equipo de desarrollador de una app, su ID de paquete o la etiqueta de un daemon o agente de launchd (también por su primera parte). Necesita macOS 13 o posterior.

Extensiones del sistema

Las extensiones del sistema son la forma moderna de que las apps amplíen macOS: filtros de red y VPN, agentes de seguridad de endpoints y controladores. Con este ajuste activado, las extensiones del sistema de los equipos de desarrolladores indicados se cargan sin preguntar al usuario. Necesita macOS 10.15 o posterior y un MDM aprobado por el usuario.

- **ID de equipo**: el ID de equipo de 10 caracteres del desarrollador (por ejemplo, en los detalles «Firmado por» de la app, o con `codesign -dv`). Cada equipo puede aparecer solo una vez.
- **Permitir**: todas las extensiones del equipo, o solo las extensiones con los ID de paquete indicados.
- **Tipos**: limita el equipo a extensiones de controladores, de red o de seguridad de endpoints. Si no se elige ninguno, se permiten todos los tipos.
- **Eliminación** (solo para extensiones indicadas): la app puede eliminar su extensión sin un administrador (macOS 12 o posterior), la extensión no se puede desactivar ni eliminar mientras la Protección de integridad del sistema está activada, o no se puede eliminar en Ajustes del Sistema ni en el Finder (macOS 15 o posterior). Los Mac con un macOS más antiguo siguen permitiendo la extensión, sin la opción de eliminación.
- **Los usuarios pueden aprobar otras extensiones del sistema**: activado de forma predeterminada. Cuando está desactivado, solo se pueden cargar las extensiones permitidas por un perfil; si algún perfil del Mac lo desactiva, queda desactivado.

> En macOS 11.3 o posterior, eliminar este ajuste desactiva las extensiones del sistema que permitía, por ejemplo un agente de seguridad o un filtro de red. Esto ocurre cuando se desactiva el ajuste, cuando se elimina la política y cuando el Mac pasa a una política sin él. El editor pide confirmación antes de desactivar el ajuste.

Extensiones del kernel (heredadas)

Las extensiones del kernel son la forma más antigua y obsoleta de ampliar macOS: prefiere las extensiones del sistema cuando el proveedor las ofrezca. Las extensiones del kernel de los equipos indicados (todas las extensiones de un equipo, o solo los ID de paquete indicados) se cargan sin preguntar al usuario, tras un reinicio. Necesita macOS 10.13.2 o posterior y un MDM aprobado por

el usuario.

- **Los usuarios pueden aprobar otras extensiones del kernel**: desactivado de forma predeterminada, así que solo los equipos indicados pueden cargar extensiones del kernel.
- **Los usuarios estándar también pueden aprobarlas**: con las aprobaciones de usuarios activadas, los usuarios sin derechos de administrador también pueden aprobarlas (macOS 11 o posterior).

> En los Mac con Apple silicon, un perfil por sí solo no basta: alguien debe iniciar el Mac en recoveryOS, elegir Seguridad reducida en la Utilidad de Seguridad de Arranque y permitir la gestión por el usuario de extensiones del kernel de desarrolladores identificados. El Mac también puede necesitar un Bootstrap Token custodiado en Cerberus Enterprise para aprobarlas (consulta el campo Bootstrap Token de la página del dispositivo).

Archivos de Mac

Los archivos de configuración de servicios y las tareas en segundo plano usan archivos que subes a los **Archivos de Mac** de tu organización: archivos zip y listas de propiedades (.plist) de hasta 20 MB. Súbelos, comprueba dónde se usan o elimínalos con el botón **Archivos de Mac** de la sección macOS, o con **Elegir archivo** en un ajuste. Un archivo usado por una política no se puede eliminar. Para cambiar un archivo, sube la nueva versión y elígela en la política: los Mac lo descargan de nuevo.

Archivos de configuración de servicios

Instala los archivos de configuración de un servicio del sistema desde un archivo zip. Los servicios integrados son el servidor SSH (sshd), sudo, PAM, la impresión (CUPS), el servidor web Apache, bash, zsh, el inicio de sesión con tarjeta inteligente y la autorización. También puedes usar tu propio servicio, con un identificador DNS inverso como `com.example.service`: encuentra los archivos con la biblioteca de archivos de configuración gestionados de macOS. Cada servicio puede tener un ajuste. Necesita macOS 14 o posterior.

> Un servicio integrado usa solo los archivos del archivo zip e ignora sus propios archivos, por ejemplo /etc/ssh para sshd: pon toda la configuración en el archivo zip, en carpetas que empiecen desde la raíz del disco (por ejemplo `etc/ssh/sshd_config`). Los archivos son de solo lectura en el Mac y se eliminan con el ajuste. Prueba el archivo zip primero en un Mac: una

> configuración incorrecta de sudo o PAM puede impedir que los usuarios inicien sesión o usen los derechos de administrador.

Tareas en segundo plano

Programas y scripts que se ejecutan en segundo plano, iniciados por launchd. Los usuarios no pueden desactivarlos, y se eliminan con el ajuste. Necesita macOS 15 o posterior. Para cada tarea, elige:

- **Identificador de tarea**: un identificador DNS inverso, como `com.example.task`, distinto para cada tarea.
- **Programas y scripts** (opcional): un archivo zip que el Mac descomprime en `/var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/` seguido del identificador de tarea. Conserva el permiso de ejecución de los archivos y no incluyas listas de propiedades en él.
- **Listas de propiedades de launchd**: los trabajos que inician los programas, cargados como daemon (para todo el sistema, como root) o como agente (en cada sesión de usuario). Haz referencia a los programas con su ruta en la carpeta anterior.

Una tarea necesita los programas o al menos una lista de propiedades. Cuando cambian los archivos, los Mac reinician la tarea.

Ubicación y geocercas

La sección **Ubicación y geocercas** del Editor de políticas de Apple define áreas, por ejemplo una sede o un almacén. Los iPhone y iPad con la app Cerberus Enterprise notifican cuándo entran o salen de una de estas áreas, y las reglas de eventos pueden reaccionar: enviar un correo electrónico, bloquear o deshabilitar el dispositivo, o volver a habilitarlo. Los Mac no usan geocercas.

Campos de la geocerca

Usa **Añadir geocerca** para crear una entrada nueva. Una política puede contener hasta **10 geocercas**, y sus nombres deben ser únicos dentro de la política. Cada geocerca contiene estos campos:

- **Nombre**: obligatorio y único.
- **Latitud** y **Longitud**: el centro del área. También puedes hacer clic en el mapa para establecerlo.
- **Radio (m)**: obligatorio, de **200** a **10000** metros.
- **Descripción**: notas opcionales para los administradores.
- **Informar entrada** y **Informar salida**: elige qué eventos se generan. Al menos uno debe permanecer activado.
- **Activa**: activa o desactiva la geocerca sin eliminarla.

Cada geocerca tiene una vista previa del mapa. El centro y el radio de una geocerca guardada están bloqueados: usa el botón de bloqueo del mapa para cambiarlos. Los demás botones centran el mapa en el área o en tu ubicación actual.

Cuando guardas la política, Cerberus Enterprise pide a los iPhone y iPad de la política que obtengan las nuevas geocercas. Esto suele tardar unos minutos, pero iOS puede retrasarlo, por ejemplo en el Modo de bajo consumo o sin conexión de red. La página del dispositivo muestra cuándo la app aún no ha aplicado las últimas geocercas.

Requisitos

Las geocercas funcionan en los iPhone y iPad con la app Cerberus Enterprise. Los Mac las ignoran. En el dispositivo:

- la app Cerberus Enterprise está instalada (Cerberus la instala) y el usuario la ha abierto al menos una vez;
- el acceso a la ubicación de la app está configurado en **Siempre**;
- **Ubicación precisa** está activada para la app;
- **Actualización en segundo plano** está activada.

> **Ubicación y geocercas en dispositivos personales**, en la parte superior de la sección, está desactivado de forma predeterminada. Mientras está desactivado, Cerberus no recopila la ubicación de los dispositivos personales (User Enrollment), sus eventos de geocerca no se generan y su página de dispositivo no ofrece Localizar ni seguimiento en tiempo real. Cuando lo activas, los dispositivos personales de la política comparten su ubicación y sus eventos de geocerca como los dispositivos de empresa, pero solo si el usuario permite la ubicación para la app Cerberus Enterprise; la app se lo explica al usuario antes de que iOS lo solicite. Tu organización es responsable de informar a los usuarios y de cumplir las normas locales sobre la ubicación de los empleados. El modo perdido y la solicitud de ubicación de MDM nunca están disponibles en los dispositivos personales (Apple no lo permite).

En el **Modo de bajo consumo**, las geocercas siguen funcionando, pero iOS informa de la salida de un área más tarde y con una ubicación menos precisa, y puede retrasar la obtención de nuevas geocercas tras un cambio de política durante horas, hasta que la app se ejecute de nuevo (por ejemplo, en el siguiente cruce o cuando el usuario la abre).

Cómo llegan los eventos

iOS vigila las áreas de la app y la activa cuando el dispositivo cruza un límite, incluso cuando la app no está abierta. Los eventos pueden llegar unos minutos después del cruce, y se puede pasar por alto un área pequeña o una visita breve: iOS necesita que el dispositivo se aleje cierta distancia más allá del límite y permanezca allí un tiempo.

Si la app no puede ejecutarse, por ejemplo tras un reinicio antes de desbloquear el dispositivo, el servidor también detecta el cruce a partir de las ubicaciones que envía la app, más tarde. Cada cruce activa las reglas de evento una vez, tanto si lo detecta la app como el servidor.

Cuando la app no se ha comunicado con el servidor durante varias horas, el servidor pide a iOS que la active para que pueda comprobar sus geocercas de nuevo. iOS no garantiza estas solicitudes.

Página del dispositivo

En la página del dispositivo, la pestaña **Geocerca** del panel **Mapa de ubicaciones** muestra las transiciones del dispositivo. Cuando la política tiene geocercas activas, una línea de estado indica si las geocercas funcionan en el dispositivo o por qué no pueden hacerlo: la app no se ha

comunicado con el servidor o debe actualizarse, el acceso a la ubicación no está en **Siempre**, **Ubicación precisa** o **Actualización en segundo plano** está desactivado, el **Modo de bajo consumo** estaba activado cuando la app informó por última vez de sus ajustes, o la app aún no ha aplicado las últimas geocercas.

> Las transiciones de geocercas y las ubicaciones se conservan durante **90 días** y los datos más antiguos se eliminan automáticamente cada noche. La última ubicación de cada dispositivo inscrito se conserva siempre, por lo que sigue en los mapas.

Limitaciones

- Copiar una política no copia sus geocercas: vuelve a añadirlas en la copia.
- Los eventos de geocerca en los iPhone y iPad no están garantizados: iOS decide cuándo puede ejecutarse la app.

> Para reaccionar a los eventos de geocerca, crea una regla de evento para **El dispositivo entra en una geocerca** o **El dispositivo sale de una geocerca**. Consulta **Reglas de evento**.

Cuentas

La sección **Cuentas** del Editor de políticas de Apple añade cuentas de correo, Exchange, Google, calendario, contactos y directorio a iPhone, iPad y Mac. Haz clic en **Añadir cuenta** y elige el tipo. La sección también contiene la restricción **Permitir la modificación de cuentas** (dispositivos supervisados).

> En un Mac (macOS 13 o posterior), las cuentas se instalan en la sesión de los usuarios inscritos en la gestión, normalmente el usuario que inscribió el Mac, cuando inician sesión. La página del dispositivo enumera estos usuarios en **Usuarios de Mac**, con el estado de sus cuentas. Las cuentas que toman la dirección de correo electrónico del usuario del dispositivo usan el usuario asignado al Mac en Cerberus Enterprise.

Ajustes comunes

- **Nombre y correo electrónico del usuario del dispositivo** (Correo, Exchange, Google): cada dispositivo usa el nombre y la dirección de correo electrónico de su usuario, configurados en la página Usuarios (para Google, la cuenta de Google del usuario). Los dispositivos sin usuario, o cuyo usuario no tiene dirección de correo electrónico, no reciben la cuenta. En caso contrario, establece una dirección de correo electrónico y un nombre completo fijos.
- **Nombre de la cuenta** (opcional): el nombre de la cuenta en Configuración y en las aplicaciones.
- **Nombre de usuario** y **Contraseña** (opcional): el nombre de usuario puede contener las variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ y $UDID$. Deja la contraseña vacía para que el usuario la escriba en el dispositivo, o deja ambas vacías para que las escriba.
- **Se aplica a**: limita la cuenta a algunos tipos de dispositivo.

Tipos de cuenta

- **Cuenta de correo**: servidor entrante IMAP o POP y servidor saliente, con sus puertos y autenticación. El servidor saliente puede usar el mismo nombre de usuario y contraseña que el entrante.
- **Cuenta de Exchange** (Exchange ActiveSync): el servidor, o vacío para encontrarlo a partir de la dirección de correo electrónico. Elige los servicios (correo, contactos,

calendarios, recordatorios, notas) y si el usuario puede cambiarlos. Con **Autenticación moderna (OAuth)**, el usuario inicia sesión con la página de tu proveedor de identidad, por ejemplo Microsoft 365. Un **Certificado de autenticación** (iOS 17 o posterior) autentica el dispositivo con un certificado.
- **Cuenta de Google**: el usuario inicia sesión en la cuenta de Google con la dirección de correo electrónico indicada.
- **Cuenta de calendario (CalDAV)** y **Cuenta de contactos (CardDAV)**: el servidor, el puerto y la ruta.
- **Directorio (LDAP)**: el servidor y el puerto, y las búsquedas (base de búsqueda, alcance y descripción) usadas para buscar contactos.
- **Calendario suscrito**: la URL del calendario (https, http o webcal).

S/MIME

Las cuentas de correo y Exchange pueden firmar y cifrar mensajes con S/MIME (iOS 17 o posterior). Para cada una, elige el certificado: uno de la página Certificados, el certificado del usuario del dispositivo o uno solicitado a un servidor SCEP. Puedes permitir que el usuario lo desactive, elija otro certificado y, para el cifrado, mostrar un interruptor para cada mensaje.

Seguridad

Las contraseñas y los certificados no forman parte de los ajustes enviados a los dispositivos: cada dispositivo descarga sus propias credenciales desde Cerberus Enterprise y firma la solicitud con su certificado de gestión. No se escriben en los registros.

Reglas de cumplimiento

La sección **Reglas de cumplimiento** del Editor de políticas de Apple establece requisitos para los dispositivos de la política. Un dispositivo que incumple una regla queda no conforme de inmediato: la página del dispositivo muestra por qué, en **Por qué el dispositivo no cumple**, y la lista de dispositivos lo muestra como no conforme. Un dispositivo también queda no conforme cuando un ajuste de la política no se puede aplicar en él.

Reglas

- **Código de acceso**: el dispositivo tiene un código de acceso y cumple los ajustes de código de acceso de la política.
- **Versión mínima del SO**: para iPhone y iPad, o para Mac. Para actualizar los dispositivos, añade una actualización obligatoria en Actualizaciones de software.
- **Dispositivo supervisado**: los dispositivos registrados con el perfil de inscripción o con User Enrollment no están supervisados.
- **FileVault activado (Mac)**: el disco del Mac está cifrado con FileVault. Los demás dispositivos no se ven afectados.

Una regla se comprueba cuando el dispositivo envía su estado, cuando se guarda la política y cada hora. Un dispositivo cuyo estado es desconocido (por ejemplo, un Mac que aún no ha informado de FileVault) no incumple la regla.

Bloquear el dispositivo

Activa **Bloquear el dispositivo si sigue sin cumplir** e indica tras cuántos días (0 bloquea de inmediato). Los iPhone y iPad supervisados entran en modo perdido con el mensaje que configures. Los demás dispositivos se bloquean una vez; un Mac se reinicia y pide un PIN, que se muestra en los detalles del comando en el historial de comandos.

- **Desbloquear**: cuando el dispositivo vuelve a cumplir, el modo perdido se desactiva automáticamente.
- **Desactivar el modo perdido por tu cuenta**: el dispositivo no se vuelve a bloquear hasta que vuelva a cumplir e incumpla otra regla. Úsalo para permitir que el usuario repare el dispositivo.

> Para recibir notificaciones o reaccionar de otras formas, crea una regla de evento para **El dispositivo deja de cumplir**: también recibe los motivos.