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.

Revision #7
Created 2026-11-10 15:14:49 UTC by Admin
Updated 2026-11-12 09:54:42 UTC by Admin