

Manual de Usuario

Documentación de Cerberus Enterprise MDM

- [Introducción](#)
- [Configuración](#)
 - [Configuración de Android Management](#)
 - [Configuración de Apple Management \(APNs\)](#)
- [Descripción general del aprovisionamiento de dispositivos](#)
- [Aprovisionamiento de Dispositivos - Android](#)
 - [Dispositivos compatibles](#)
 - [Tokens de inscripción](#)
 - [Dispositivos de propiedad personal](#)
 - [Dispositivos propiedad de la empresa para uso laboral y personal](#)
 - [Dispositivos propiedad de la empresa para uso laboral únicamente](#)
 - [Zero-touch](#)
 - [Inscripción mediante autenticación con Google](#)
- [Aprovisionamiento de Dispositivos - Apple](#)
 - [Resumen del aprovisionamiento de Apple](#)
 - [Inscripción manual de Apple \(Perfil de inscripción\)](#)
 - [Apple Automated Device Enrollment \(ADE\)](#)
- [Resumen de políticas](#)
- [Políticas - Android](#)
 - [Resumen](#)
 - [Gestión de aplicaciones](#)
 - [Modo quiosco](#)
 - [Seguridad](#)

- [Multimedia](#)
- [Red celular](#)
- [Redes](#)
- [Sistema](#)
- [Ubicación y geocerca](#)
- [Gestión de usuarios](#)
- [Uso personal](#)
- [Políticas entre perfiles](#)
- [Informes de estado](#)
- [Varios](#)
- [Reglas de aplicación de políticas](#)
- [Políticas - Apple](#)
 - [Políticas de Apple](#)
 - [Política de Apple: Código de acceso](#)
 - [Política de Apple: Restricciones](#)
 - [Política de Apple: Aplicaciones y perfiles](#)
- [Estado del Dispositivo](#)
 - [Resumen del dispositivo](#)
 - [Gestión de SIM](#)
 - [Comandos](#)
 - [Mapa de ubicación](#)
- [Mapa de ubicación del panel de control](#)
- [Aplicaciones privadas](#)
- [Gestión de certificados](#)
- [Reglas de eventos](#)
- [Dispositivos](#)
 - [Dispositivos](#)
- [Usuarios](#)
 - [Usuarios](#)
 - [Editor de usuarios](#)

- [Cuenta](#)
 - [Configuración](#)
- [Multitenencia](#)
 - [Resumen de multi-inquilino](#)
 - [Empresas gestionadas](#)
 - [Cambio de empresa](#)
 - [Subcuentas](#)
- [Información relevante](#)

Introducción

Cerberus Enterprise es una solución integral de EMM, diseñada para ayudarle a asegurar y gestionar sus dispositivos Android y Apple. Cuenta con todas las funciones necesarias para una gestión eficaz de los dispositivos BYOD y de propiedad de la empresa en un panel de control limpio y fácil de usar, y puede empezar a utilizarlo en cuestión de minutos.

Para utilizar Cerberus Enterprise de manera efectiva, es necesario comprender algunos conceptos clave sobre el funcionamiento del sistema.

El sistema es compatible con la gestión de dispositivos tanto Android como Apple:

En Android, Cerberus Enterprise utiliza la [API de Android Management](#) oficial de Google para gestionar dispositivos a través de la aplicación [Android Device Policy](#) (ADP). La mayoría de los ajustes se aplican directamente mediante ADP. Algunas funciones opcionales también pueden requerir la aplicación complementaria de Cerberus Enterprise, que amplía las posibilidades más allá de lo que permite solo ADP.

En los dispositivos Apple, Cerberus Enterprise gestiona los dispositivos a través de MDM (Mobile Device Management) de Apple. La gestión de Apple requiere un certificado APNs y puede integrarse opcionalmente con Apple Business Manager para la inscripción automatizada y el licenciamiento de aplicaciones.

Cada dispositivo puede ser **inscrito** en el sistema utilizando un [token de inscripción](#) o un [perfil de inscripción](#) (inscripción manual de Apple). El método de inscripción está asociado a una [política](#) que contiene las reglas que deben aplicarse a los dispositivos.

Los administradores de TI pueden cambiar la política asociada a un dispositivo después de la inscripción. Sin embargo, cada dispositivo solo puede estar asociado a una política a la vez.

Durante el proceso de inscripción (aprovisionamiento), los componentes de gestión necesarios se instalan y configuran automáticamente. En Android, esto suele incluir la aplicación Android Device Policy (y, dependiendo de su configuración, la aplicación complementaria de Cerberus Enterprise). En los dispositivos Apple, la gestión se aplica a través de MDM una vez que el dispositivo ha sido inscrito. En consecuencia, la política correspondiente se aplica automáticamente al dispositivo y todas las reglas asociadas son ejecutadas por el sistema de gestión de la plataforma.

Una política se puede aplicar a muchos dispositivos. En este caso, cuando modifique la política, todos los dispositivos asociados recibirán los cambios.

Configuración

Configuración de Android Management

Para gestionar dispositivos Android con Cerberus Enterprise, primero debe conectar su organización a Google Android Enterprise.

El proceso de configuración suele tardar unos minutos y requiere una **dirección de correo electrónico del trabajo** (por ejemplo, *nombre@empresa.com*) o, como alternativa, una **dirección de correo electrónico personal de Google**.

Qué sucede durante la configuración

- Se le redirigirá a Google Android Enterprise.
- Inicia sesión con tu dirección de correo electrónico del trabajo (o una dirección de correo electrónico personal de Google).
- Google crea la cuenta de Android Management para su organización.
- Se le redirige de nuevo a Cerberus Enterprise para completar la configuración.

Información importante

Recomendamos registrarse con una dirección de correo electrónico del trabajo, no con una cuenta personal de Gmail. Si la dirección de correo electrónico ya está asociada a una cuenta de Google Admin, se reutilizará esa cuenta existente y quedará vinculada a Cerberus Enterprise; de lo contrario, se creará una nueva cuenta gratuita de Google Admin. Una cuenta de Google Admin desbloquea el conjunto completo de funciones; por ejemplo, la inscripción de dispositivos mediante la autenticación de Google con cuentas gestionadas por su dominio de Google Admin.

¿No tiene una dirección de correo electrónico del trabajo?

Aun así, puede registrarse con una dirección de correo electrónico personal de Google (por ejemplo, una cuenta de Gmail). En este caso, Google crea una cuenta gratuita de Google Play gestionada que queda vinculada a Cerberus Enterprise.

Siguientes pasos

Tras completar la configuración, cree un [token de inscripción](#) y elija el método de aprovisionamiento adecuado para el dispositivo.

Configuración de Apple Management (APNs)

Para gestionar dispositivos Apple, Cerberus Enterprise requiere el certificado del servicio de notificaciones push de Apple (APNs).

Utilice el Apple ID asociado con su organización. El certificado APNs tiene una validez de un año y debe renovarse anualmente para continuar gestionando los dispositivos.

Paso 1: Descargar el archivo CSR

En el dashboard, inicie la configuración de Apple Management y descargue el archivo de solicitud de firma de certificado (CSR) firmado por el proveedor generado por Cerberus Enterprise.

Paso 2: Crear el certificado de notificaciones push en el portal de Apple

- Inicie sesión en el portal de certificados de Apple Push con su Apple ID.
- Haga clic en "*Create a Certificate*".
- Suba el archivo CSR del paso 1.
- Descargue el certificado de notificaciones push creado.

Enlace al portal: <https://identity.apple.com/>

Paso 3: Subir el certificado de notificaciones push

Suba el certificado de notificaciones push que descargó de Apple a Cerberus Enterprise para completar la configuración.

Si el certificado APNs caduca, la gestión de los dispositivos Apple dejará de funcionar hasta que se renueve el certificado.

Siguientes pasos

Una vez configurado el APNs, puede proceder con la inscripción de dispositivos Apple. Continúe con [Resumen del aprovisionamiento de Apple](#).

Descripción general del aprovisionamiento de dispositivos

Cerberus Enterprise es compatible con la gestión de dispositivos tanto para la plataforma Android como para la Apple. Puede configurar cada plataforma de forma independiente, según los dispositivos que necesite inscribir.

1. Complete la configuración de la plataforma en el panel de control

Antes de inscribir dispositivos, complete la configuración de la plataforma en el panel de control de Cerberus Enterprise. Si su cuenta aún no está configurada, el panel de control le guiará a través de los pasos necesarios.

Configuración de Android (Google Android Enterprise)

Para el procedimiento completo de configuración de Android, lea [Configuración de Android Management](#).

- Vaya al flujo de registro del panel de control y seleccione **Configurar Android Management**.
- Se le redirigirá a Google para iniciar sesión con una **cuenta de trabajo** y autorizar Android Enterprise.
- Tras la autorización, se le redirigirá de nuevo a Cerberus Enterprise para completar la configuración.

Configuración de Apple (certificado de notificación push APNs)

Para el procedimiento completo de configuración de Apple, lea [Configuración de Apple Management \(APNs\)](#).

- Vaya al flujo de registro del panel de control y seleccione **Configurar Apple Management**.
- Descargue el archivo CSR desde Cerberus Enterprise.
- Cree el certificado APNs en el portal de certificados push de Apple y descargue el certificado resultante.
- Suba el certificado descargado de nuevo a Cerberus Enterprise para habilitar la gestión de dispositivos Apple.

2. Inscribir dispositivos

Tras completar la configuración de la plataforma, elija el método de inscripción que se ajuste a su modelo de propiedad de dispositivos y al sistema operativo.

Inscripción de Android

Para Android, la inscripción se realiza mediante [tokens de inscripción](#). Seleccione el método adecuado según si el dispositivo es de propiedad personal o de la empresa.

- Propiedad personal (BYOD / perfil de trabajo): [siga esta guía](#).
- Propiedad de la empresa (uso laboral y personal / perfil de trabajo): [siga esta guía](#).
- Propiedad de la empresa (uso exclusivamente laboral / gestión total o dedicado): [siga esta guía](#).
- Zero-touch: [siga esta guía](#).

Inscripción de Apple

Para Apple, comience completando la configuración de APNs descrita anteriormente y luego siga las guías de aprovisionamiento de Apple: [Descripción general del aprovisionamiento de Apple](#).

Aprovisionamiento de Dispositivos - Android

Dispositivos compatibles

En general, cualquier dispositivo con Android 6 o superior que cuente con Google Play Services es compatible con Cerberus Enterprise.

Para una mejor experiencia de usuario, sugerimos utilizar dispositivos que cumplan con los requisitos de [Android Enterprise Recommended](#).

Algunas funciones están limitadas a versiones específicas de Android o pueden comportarse de manera diferente según la versión del sistema operativo. Para obtener más información sobre una función específica, consulte la sección de [Políticas](#) de la documentación.

Cerberus Enterprise es compatible tanto con dispositivos de propiedad de la empresa como de propiedad personal, y con dos modos de gestión: propietario del dispositivo (device owner) y propietario del perfil (profile owner).

Los dispositivos de **propiedad personal** pueden gestionarse mediante un **perfil de trabajo**. Esto permite una solución BYOD al mantener los datos y las aplicaciones de trabajo de los empleados separados de los datos y las aplicaciones personales, mejorando tanto la seguridad como la privacidad. Esta opción es adecuada para dispositivos que ya son propiedad de los empleados y que desea inscribir en su organización para uso laboral.

Los dispositivos **de propiedad de la empresa** también pueden gestionarse mediante un perfil de trabajo, pero también puede elegir la opción de **gestión total**, que permite un control más estricto sobre el dispositivo. Los dispositivos de propiedad de la empresa con perfil de trabajo son adecuados cuando se proporcionan dispositivos corporativos a los empleados para el trabajo, permitiendo al mismo tiempo el uso personal. Los dispositivos con gestión total son más adecuados para aquellos que deben utilizarse únicamente para el trabajo, o para **dispositivos dedicados** (COSU, dispositivos de un solo uso propiedad de la empresa), como los quioscos.

Para obtener más información sobre el aprovisionamiento de dispositivos, consulte la página [Descripción general del aprovisionamiento de dispositivos](#)).

Tokens de inscripción

Cerberus Enterprise utiliza tokens de inscripción para iniciar el proceso de inscripción (aprovisionamiento) de dispositivos Android. El token que seleccione define la política inicial aplicada a los dispositivos inscritos e influye en qué modos de aprovisionamiento están permitidos.

La pestaña de tokens de inscripción de Android solo está disponible tras completar la [**Configuración de Android Management**](#).

Dónde encontrar los tokens de inscripción

En el dashboard, abra **Tokens de inscripción**. Dependiendo de la configuración de su cuenta, la página puede mostrar varias pestañas (tokens de Android, inscripción mediante inicio de sesión de Google, inscripción manual de Apple y Apple Automated Device Enrollment).

Si su empresa de Android está respaldada por un dominio gestionado de Google (Google Workspace), el dashboard también puede mostrar una pestaña de **Autenticación mediante inscripción de Google**. Para más detalles sobre cómo habilitarla y utilizarla, consulte [**Autenticación mediante inscripción de Google**](#).

Lista de tokens de inscripción (Android)

La pestaña de tokens de Android muestra una tabla con todos los tokens. Al hacer clic en una fila, se abre la página de detalles del token.

Columnas

- **Id:** identificador interno del token.
- **Estado:** **Disponible**, **Usado** (token de un solo uso ya utilizado) o **Expirado**.
- **Expiración:** fecha/hora de expiración, o **Nunca**.
- **Política:** la política asignada al token (la descripción emergente de la interfaz también muestra el ID de la política).
- **Uso personal:** Permitido / No permitido / Dispositivo dedicado.
- **Usos permitidos:** Múltiples o de un solo uso.
- **Usuario:** usuario opcional preasignado a los dispositivos inscritos con el token.

Acciones

- Cada fila tiene una acción de eliminación (**Eliminar token de inscripción**). La eliminación está deshabilitada cuando la licencia ha expirado.
- La tabla permite la selección de varias filas: puede activar el modo de selección, seleccionar varios tokens y eliminarlos con **Eliminar tokens seleccionados**.
- Utilice la acción de actualizar para recargar la lista. La tabla está paginada (10/25/50 elementos por página).

Crear un nuevo token de inscripción

En la pestaña de tokens de Android, haga clic en **Nuevo token de inscripción** para abrir la página de creación de tokens. Si su licencia ha expirado, el botón de creación estará deshabilitado.

Opciones del token

1. Política

Obligatorio. La política que se aplica automáticamente a todos los dispositivos inscritos con este token. Seleccione una de sus [políticas de Android](#). Si aún no tiene ninguna política, cree una primero.

2. Usuario

Opcional. Si se establece, los dispositivos recién inscritos se asociarán automáticamente con este usuario.

3. Uso personal

Controla si se permite el uso personal en un dispositivo aprovisionado con este token de inscripción:

- **Permitido:** adecuado para dispositivos de propiedad personal (perfil de trabajo) y dispositivos propiedad de la empresa para uso laboral y personal.
- **No permitido:** adecuado para dispositivos propiedad de la empresa para uso laboral únicamente (gestión completa).
- **Dispositivo dedicado:** adecuado para dispositivos de quiosco o dedicados (el dispositivo no está asociado a un único usuario).

4. Usos permitidos

Seleccione si el token se puede usar varias veces (**Múltiples**) o solo una vez (**De un solo uso**).

5. Expiración

Seleccione la unidad de expiración (**Minutos, Horas, Días, o Nunca**). Cuando no se establece en Nunca, introduzca el valor de expiración. El rango permitido depende de la unidad seleccionada y puede llegar hasta los 10,000 días.

6. Autenticación de Google

Controla si el usuario debe autenticarse con una cuenta de Google durante la inscripción del dispositivo:

- **No especificado:** se utiliza el ajuste de autenticación de Google a nivel de empresa para determinar si el usuario necesita autenticarse con Google durante la inscripción.
- **Opcional:** el usuario puede optar por omitir la autenticación de Google durante la inscripción.
- **Requerido:** el usuario debe autenticarse con una cuenta de Google para continuar con la inscripción.

Cuando se selecciona **Requerido**, aparece un campo opcional de **Correo electrónico de la cuenta requerida**. Si se establece, el usuario debe autenticarse con esa cuenta de Google específica durante la inscripción.

Opciones de aprovisionamiento (solo código QR)

Estas opciones adicionales se integran en el código QR y se aplican durante el aprovisionamiento de dispositivos totalmente gestionados inscritos mediante el escaneo del código QR. No se aplican a los perfiles de trabajo ni a los dispositivos inscritos mediante la URL o el token de inscripción.

Configuración de Wi-Fi

Utilice esto para permitir que un dispositivo se conecte automáticamente a Wi-Fi durante el aprovisionamiento, de modo que pueda descargar e iniciar la aplicación de gestión. Los campos disponibles incluyen **SSID**, **SSID oculto**, **Seguridad** y (cuando sea necesario) **Frase de contraseña**.

También puede configurar un proxy HTTP (**Proxy**) y, dependiendo del modo, establecer **Host/Puerto**, **URI de PAC** y **Host de omisión de proxy**.

Otras opciones

Las opciones adicionales incluyen **Región e idioma**, **Zona horaria** y **Omitir cifrado**.

Detalles del token de inscripción

Al abrir un token, la página de detalles muestra la configuración del token y la información de uso:

- **Estado**, **Expiración**, **Uso**, **Uso personal**, **Usos permitidos** y (cuando se establece) **Autenticación de Google** con el campo opcional **Correo electrónico de la cuenta requerida**.
- **Token**: el valor bruto del token de inscripción (se puede copiar).
- **URL de inscripción**: una URL de inscripción de Google Android Enterprise (se puede copiar y enviar por correo electrónico).
- **Código QR**: se muestra en el lado derecho de la página y se utiliza para inscribir dispositivos totalmente gestionados.

Para los procedimientos de aprovisionamiento paso a paso, siga las guías de inscripción de Android: [Dispositivos de propiedad personal](#), [Dispositivos de propiedad de la empresa para uso laboral y personal](#), [Dispositivos de propiedad de la empresa para uso exclusivamente laboral](#), y [Zero-touch](#).

Dispositivos de propiedad personal

Los dispositivos propiedad de los empleados pueden configurarse con un **perfil de trabajo**. Un perfil de trabajo proporciona un espacio independiente para las aplicaciones y los datos de trabajo, separado de las aplicaciones y los datos personales. La mayoría de las políticas de gestión de aplicaciones, datos y otros elementos se aplican únicamente al perfil de trabajo, mientras que las aplicaciones y los datos personales de los empleados permanecen privados.

Para configurar un perfil de trabajo en un dispositivo de propiedad personal, utilice uno de los siguientes métodos de aprovisionamiento (asegúrese de que el [token de inscripción](#)) tenga **Uso personal** establecido como **Permitido**):

Enlace del token de inscripción

Versión de Android
6.0+

Puede proporcionar la URL de inscripción a los usuarios finales. Cuando un usuario final abra el enlace desde su dispositivo, se le guiará a través de la configuración del perfil de trabajo.

Añadir perfil de trabajo desde "Ajustes"

Versión de Android
6.0+

Para configurar un perfil de trabajo en su dispositivo, el usuario puede abrir la aplicación de **Ajustes**, luego usar la barra de búsqueda para encontrar y tocar la opción **Configurar su perfil de trabajo**.

Si la búsqueda no tiene éxito, la ubicación de esta opción puede variar. Aquí tiene algunas posibilidades:

- *Ajustes -> Servicios y preferencias de Google -> Todos los servicios -> Configure su perfil de trabajo.*
- *Ajustes -> Google -> Configurar y restaurar -> Configure su perfil de trabajo.*

Estos pasos inician un asistente de configuración que descarga *Android Device Policy* en el

dispositivo. A continuación, se le pedirá al usuario que escanee un código QR o introduzca manualmente un token de inscripción para completar la configuración del perfil de trabajo.

Descargar Android Device Policy

Versión de Android
6.0+

Para configurar un perfil de trabajo en su dispositivo, el usuario puede descargar Android Device Policy desde la Google Play Store. Una vez instalada la aplicación, se le pedirá al usuario que escanee un código QR o introduzca manualmente un token de inscripción para completar la configuración del perfil de trabajo.

Dispositivos propiedad de la empresa para uso laboral y personal

La configuración de un dispositivo propiedad de la empresa con un **perfil de trabajo** permite el uso del dispositivo tanto para fines laborales como personales. En los dispositivos propiedad de la empresa con perfiles de trabajo:

- La mayoría de las políticas de aplicaciones, datos y otras gestiones se aplican únicamente al perfil de trabajo.
- Los perfiles personales de los empleados permanecen privados. Sin embargo, las empresas pueden aplicar ciertas políticas para todo el dispositivo y políticas de uso personal.
- Las empresas pueden utilizar el *alcance de bloqueo* para aplicar acciones de cumplimiento en todo el dispositivo o solo en su perfil de trabajo.
- La desinscripción del dispositivo y los comandos del dispositivo se aplican a todo el dispositivo.

Para configurar un dispositivo propiedad de la empresa con un perfil de trabajo, utilice uno de los siguientes métodos de aprovisionamiento (asegúrese de que el [token de inscripción](#) tenga configurado el **Uso personal** como **Permitido**):

Método de código QR

Versión de Android
8.0+

En un dispositivo nuevo o restablecido de fábrica, el usuario (normalmente un administrador de TI) toca la pantalla seis veces en el mismo lugar. Esto activa que el dispositivo solicite al usuario escanear un código QR.

Dispositivos propiedad de la empresa para uso laboral únicamente

La **gestión completa del dispositivo** es adecuada para los dispositivos propiedad de la empresa destinados exclusivamente a fines laborales. Las empresas pueden gestionar todas las aplicaciones del dispositivo y aplicar todo el espectro de políticas y comandos de la API de Android Management.

También es posible restringir un dispositivo (mediante una política) a una única aplicación o a un pequeño conjunto de aplicaciones para cumplir con un propósito o caso de uso específico. Este subconjunto de dispositivos totalmente gestionados se denomina **dispositivos dedicados**. Para configurar la gestión completa en un dispositivo propiedad de la empresa, utilice uno de los siguientes métodos de aprovisionamiento (asegúrese de que el [token de inscripción](#) tenga configurado el **Uso personal** como **No permitido**):

Método de código QR

Versión de Android
7.0+

En un dispositivo nuevo o restablecido de fábrica, el usuario (normalmente un administrador de TI) toca la pantalla seis veces en el mismo lugar. Esto activa que el dispositivo solicite al usuario escanear un código QR.

Método de identificador DPC

Versión de Android
5.1+

Si no se puede añadir Android Device Policy mediante un código QR, un usuario o administrador de TI puede seguir estos pasos para aprovisionar un dispositivo totalmente gestionado o dedicado:

1. Siga el asistente de configuración en un dispositivo nuevo o restablecido de fábrica.
2. Introduzca los datos de inicio de sesión de Wi-Fi para conectar el dispositivo a Internet.

3. Cuando se le solicite iniciar sesión, introduzca **afw#setup**, lo que descargará Android Device Policy.
4. Escanee un código QR o introduzca manualmente un token de inscripción para aprovisionar el dispositivo.

Zero-touch

Los administradores de TI pueden aprovisionar dispositivos de propiedad de la empresa utilizando el método de inscripción zero-touch, descrito en [Inscripción zero-touch para administradores de TI](#). Cuando se enciende un dispositivo por primera vez, este se aplica automáticamente a la configuración definida por el administrador de TI.

Los administradores de TI pueden preconfigurar los dispositivos adquiridos a [distribuidores autorizados](#) y gestionarlos mediante el panel de control de Cerberus Enterprise. Para vincular su cuenta de Zero-touch, vaya a la sección **Zero-touch** en el panel de control y siga las instrucciones.

Versión de Android	Perfil de trabajo	Dispositivo con gestión total	Dispositivo dedicado
8.0+ (Pixel 7.1+)	✓	✓	✓

Inscripción mediante autenticación con Google

La inscripción mediante autenticación con Google (también denominada **Autenticación de Google para la inscripción**) permite a los usuarios autenticarse con su cuenta de Google Workspace durante la inscripción de dispositivos Android.

Esta función solo está disponible para empresas de Android respaldadas por un dominio gestionado de Google (Google Workspace).

Dónde encontrarlo

En el panel de control, abra **Tokens de inscripción** y seleccione la pestaña **Inscripción mediante autenticación con Google**. La pestaña solo se muestra cuando Android Management está configurado y la integración con Google Workspace está disponible para su empresa.

Activar (o desactivar) la autenticación con Google

La autenticación con Google se activa desde la **consola de administración de Google**. Tras cambiar la configuración, vuelva a Cerberus Enterprise y utilice **Actualizar estado** para recargar la configuración actual.

1. Inicie sesión en su [consola de administración de Google](#) con una cuenta de administrador.
2. Abra **Dispositivos**.
3. Vaya a **Dispositivos móviles y puntos finales** → **Configuración** → **Integraciones de terceros**.
4. Busque la **integración de Android EMM** para Cerberus Enterprise y ábrala.
5. Haga clic en **Gestionar proveedores de EMM**.

6. Active o desactive **Autenticación con Google** para habilitar o deshabilitar la autenticación con Google para la inscripción.
7. Haga clic en **Guardar**.
8. Vuelva al panel de control de Cerberus Enterprise y haga clic en **Actualizar estado** en la pestaña **Inscripción mediante autenticación con Google**.

Token de inscripción mediante autenticación con Google

Cuando la autenticación con Google está activada, el panel de control muestra un token de inscripción específico utilizado para este modo de inscripción. La página puede mostrar un **código QR**, un valor de **Token de inscripción** y una **URL de inscripción** (que se puede copiar y enviar por correo electrónico).

Opciones clave

- **Permitir uso personal**: controla si el token puede inscribir dispositivos para uso laboral y personal (escenarios de perfil de trabajo) o solo para uso laboral (escenarios de gestión total / dedicados).
- **Política predeterminada de respaldo**: la política que se aplica cuando el usuario que realiza la inscripción no tiene asignada una política predeterminada de autenticación con Google específica.

Interacción con las políticas

El ajuste de política **Autenticación de la configuración de la cuenta de trabajo** (workAccountSetupConfig.authenticationType) controla cómo se autentican los usuarios durante la configuración de la cuenta de trabajo, pero el ajuste de la consola de administración de Google **Autenticación con Google** y el tipo de token de inscripción aún pueden requerir autenticación.

Para los dispositivos ya inscritos, esta política solo se aplica si el dispositivo está gestionado por una cuenta de Google Play gestionada (es decir, inscrito sin **Inscripción mediante autenticación con Google**).

Algunas acciones (por ejemplo, cambiar las opciones del token) pueden quedar deshabilitadas cuando la licencia ha caducado.

Inscribir un dispositivo

Durante la inscripción, se le pedirá al usuario que se autentique con su cuenta de Google Workspace. Tras una inscripción exitosa, el dispositivo quedará asociado al usuario autenticado.

Perfil de trabajo (dispositivos de propiedad personal)

- Comparta la **URL de inscripción** con el usuario. Cuando el usuario la abra en su dispositivo Android, se le guiará a través de la configuración del perfil de trabajo y la autenticación con Google.
- Alternativamente, el usuario puede comenzar desde los ajustes de Android y elegir el flujo de configuración del perfil de trabajo; después, podrá escanear el código QR o introducir el token de inscripción cuando se le solicite.

Dispositivos de propiedad de la empresa

- **Método de código QR:** en un dispositivo nuevo o restablecido de fábrica, pulse la pantalla varias veces en el mismo lugar hasta que aparezca el aviso del código QR y, a continuación, escanee el código QR que se muestra en el panel de control.
- **Método de identificador DPC** (cuando el escaneo de QR no está disponible): siga el asistente de configuración, conéctese a una red Wi-Fi y, cuando se le pida que inicie sesión, introduzca **afw#setup** y continúe escaneando el código QR o introduciendo el token de inscripción. Cuando se le solicite, auténtíquese con la cuenta de Google Workspace.

Para los procedimientos generales de aprovisionamiento de Android (perfil de trabajo frente a gestión total), consulte las páginas estándar de inscripción de Android en este manual.

Aprovisionamiento de Dispositivos - Apple

Resumen del aprovisionamiento de Apple

Cerberus Enterprise admite la inscripción y gestión de dispositivos Apple. El aprovisionamiento de Apple requiere un certificado APNs y puede realizarse utilizando diferentes métodos de inscripción.

Prerrequisito: configurar Apple Management (APNs)

Antes de inscribir cualquier dispositivo Apple, complete la [Configuración de Apple Management \(APNs\)](#).

Elija un método de inscripción

Inscripción manual (Perfil de inscripción)

Este método proporciona una URL de inscripción y un archivo de perfil de configuración (mobileconfig) que se instala en el dispositivo. Lea [Inscripción manual de Apple](#).

Automated Device Enrollment (ADE)

Este método se integra con Apple Business Manager para automatizar la inscripción de los dispositivos propiedad de la empresa. Lea [Apple Automated Device Enrollment \(ADE\)](#).

Puede utilizar la inscripción manual y el ADE de forma paralela, dependiendo de su flota de dispositivos y del proceso de compra.

Inscripción manual de Apple (Perfil de inscripción)

Cerberus Enterprise admite la inscripción manual de dispositivos Apple mediante una URL de inscripción y un archivo de perfil de inscripción.

La inscripción manual está disponible cuando Apple Management (APNs) está configurado. Si aún no ha completado la configuración de APNs, lea [Configuración de Apple Management \(APNs\)](#).

Obtener la URL y el perfil de inscripción

- Abra la sección de **Inscripción** en el dashboard y seleccione la pestaña **Inscripción manual de Apple (Perfil de inscripción)**.
- Copie la **URL de inscripción** o utilice la acción de enviar por correo electrónico.
- Descargue el **Perfil de inscripción** (archivo mobileconfig).

Cómo inscribir un iPhone o iPad

iOS/iPadOS 15.0+

1. Envíe el archivo del perfil de inscripción (*enroll.mobileconfig*) al dispositivo, o abra la URL de inscripción en Safari en el dispositivo.
2. En el dispositivo, abra *Ajustes* → *Perfil descargado* → *Instalar*, luego siga las instrucciones.
3. Tras la inscripción, puede verificar el estado en *Ajustes* → *General* → *VPN y gestión de dispositivos* (o *Perfiles y gestión de dispositivos*).

Instale únicamente los perfiles de inscripción que haya obtenido desde su dashboard de Cerberus Enterprise.

Apple Automated Device Enrollment (ADE)

Automated Device Enrollment (ADE) se integra con Apple Business Manager (ABM) para inscribir automáticamente los dispositivos propiedad de la empresa cuando se encienden por primera vez (o después de un restablecimiento de fábrica).

ADE requiere que primero se configure Apple Management (APNs). Si es necesario, lea [Configuración de Apple Management \(APNs\)](#).

Cómo inscribir dispositivos automáticamente

1. Añada los dispositivos a su cuenta de Apple Business Manager.
2. Tras añadir nuevos dispositivos a su cuenta de ABM, sincronícelos en Cerberus Enterprise desde la sección **Dispositivos** utilizando la acción **Sincronizar desde ABM**.
3. Cree un perfil ADE en el dashboard desde **Inscripción** → **Apple Automated Device Enrollment (ADE)** → **Nuevo perfil ADE**.
4. Asigne un perfil ADE a un dispositivo desde la página de detalles del dispositivo utilizando el campo **Perfil ADE**.

Configuración del perfil ADE (resumen)

Un perfil ADE controla cómo se inscribe el dispositivo y cómo se comporta el Asistente de configuración. En Cerberus Enterprise, un perfil ADE incluye un nombre, una política inicial opcional y algunas opciones de inscripción.

Nombre del perfil

Un nombre legible para el perfil (por ejemplo, *Perfil ADE predeterminado*).

Política

La política que se aplica inicialmente a los dispositivos inscritos. Puede asignar una política al crear un nuevo perfil ADE.

Opciones de inscripción

- **MDM eliminable:** controla si el payload de MDM se puede eliminar del dispositivo.
- **Permitir emparejamiento:** controla si se permite el emparejamiento (obsoleto por Apple en iOS 13).
- **Avance automático de la configuración:** avanza automáticamente a través de las pantallas del Asistente de configuración.
- **Esperar a que el dispositivo esté configurado:** bloquea el Asistente de configuración hasta que el servidor marque el dispositivo como configurado.
- **Obligatorio:** evita que se pueda omitir la aplicación del perfil durante la configuración.
- **Multiusuario (iPad compartido):** configura el dispositivo para iPad compartido.
- **Supervisado:** solicita la supervisión del dispositivo.

Una vez que se ha asignado un perfil ADE a un dispositivo, este está listo para ser inscrito automáticamente.

Resumen de políticas

La sección de **Políticas** del panel (*Panel* → *Políticas*) enumera todas las políticas de su cuenta y le permite crearlas, copiarlas, editarlas y eliminarlas.

Lista de políticas

Las políticas se muestran en una tabla. Al hacer clic en una fila, se abre el editor de la política correspondiente.

Columnas

- **ID**: identificador interno de la política.
- **MDM**: la plataforma de la política (Android o Apple).
- **Nombre**: nombre de la política.
- **Descripción**: descripción de la política.
- **Dispositivos**: número de dispositivos inscritos asignados actualmente a la política.

Filtros y búsqueda

- Si tanto la gestión de Android como la de Apple están configuradas, puede filtrar la lista por **Todo**, **Android** o **Apple**.
- Puede activar **Búsqueda** y buscar por nombre o descripción de la política.

Actualización y paginación

- Utilice la acción de actualizar para recargar la lista.
- La tabla está paginada (10/25/50 elementos por página).

Crear una nueva política

En la parte inferior de la página de Políticas, puede crear una nueva política. Dependiendo de qué plataforma esté configurada en su cuenta, es posible que vea una o ambas acciones:

- **Crear nueva política de Android**
- **Crear nueva política de Apple**

Si su licencia ha caducado, la creación de políticas (y otras acciones de escritura) están deshabilitadas.

Copiar y eliminar políticas

Cada fila de política tiene un menú de acciones que incluye **Copiar política** y **Eliminar política**.

Advertencias para eliminar la política

Al eliminar una política, el panel de control puede mostrar advertencias adicionales dependiendo de cómo se utilice la política.

- Si la política está asignada a dispositivos inscritos, eliminarla desinscribirá los dispositivos asociados y borrará sus aplicaciones y datos.
- Si la política está asignada a tokens de inscripción, es posible que esos tokens ya no puedan completar la inscripción.
- Si la política está establecida como predeterminada para la inscripción mediante Google Authentication (a nivel global o para algunos usuarios), eliminarla puede causar fallos en las inscripciones.

Eliminar varias políticas

La lista de políticas permite la selección de varias filas para su eliminación masiva. En el modo de selección múltiple, puede seleccionar varias políticas y eliminarlas en una sola acción.

La eliminación masiva solo se habilita cuando todas las políticas seleccionadas pertenecen a la misma plataforma (todo Android o todo Apple).

Siguiente: editar la configuración de la política

La lista de políticas es el punto de entrada. Para configurar la configuración de las políticas, utilice la documentación del editor correspondiente: [Políticas → Android](#) y [Políticas → Apple](#).

Las políticas referenciadas por los tokens de inscripción se aplican automáticamente durante la inscripción del dispositivo.

Políticas - Android

Resumen

Las políticas de Android son las entidades principales del sistema: definen las reglas que se aplican y ejecutan en los dispositivos gestionados.

Puede explorar sus políticas y crear nuevas desde la sección de **Políticas** del panel. Para abrir una política de Android, haga clic en la fila de la política en la tabla: el sistema abrirá la página del **Editor de políticas**.

Una política puede asociarse con un [token de registro](#), de modo que se aplicará automáticamente a los dispositivos durante el proceso de aprovisionamiento. También puede cambiar la política asignada a un dispositivo después del aprovisionamiento.

Cada dispositivo solo puede estar asociado con una política a la vez.

Muchas opciones de política solo se aplican a tipos de dispositivos específicos (gestión completa, dedicados, perfil de trabajo) y versiones de Android. Es posible que el dispositivo ignore los ajustes no compatibles o que estos se informen como no conformes.

Diseño del editor de políticas

El Editor de políticas está organizado como un conjunto de secciones expandibles. En la parte superior de la página, siempre puede editar:

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

Las secciones a continuación corresponden a los paneles del Editor de políticas (por ejemplo: Gestión de aplicaciones, Seguridad, Redes, Sistema, Uso personal, Políticas entre perfiles y más). Utilice las páginas de los capítulos de este manual para comprender cada panel en detalle.

Guardar, eliminar y dispositivos asociados

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

Si ha abierto una política existente (que tiene un Id), la página mostrará una acción de **Eliminar política** y una lista de **Dispositivos asociados** en la parte inferior, para que pueda ver cuántos dispositivos están utilizando la política actualmente.

Gestión de aplicaciones

En esta sección, puede establecer políticas relacionadas con la disponibilidad de aplicaciones, su instalación, actualizaciones y la gestión de permisos.

Las cuentas de Managed Google Play se crean automáticamente cuando se realiza el aprovisionamiento de los dispositivos.

1. Modo de Play Store

Este modo controla qué aplicaciones están disponibles para el usuario en la Play Store y el comportamiento del dispositivo cuando se eliminan aplicaciones de la política.

Lista blanca (predeterminado): Solo las aplicaciones que están en la política estarán disponibles y cualquier aplicación que no esté en la política se desinstalará automáticamente del dispositivo. La Play Store solo mostrará las aplicaciones disponibles.

Lista negra: Todas las aplicaciones están disponibles y cualquier aplicación que no deba estar en el dispositivo debe marcarse explícitamente como **bloqueada** en la política de aplicaciones. La Play Store mostrará todas las aplicaciones, excepto las bloqueadas.

2. Política de aplicaciones no confiables

La política para aplicaciones no confiables (aplicaciones de fuentes desconocidas) aplicada en el dispositivo. Esta opción controla el ajuste del sistema Android que determina si un usuario puede instalar aplicaciones fuera de la Play Store (sideloading).

Deshabilitar (predeterminado): Deshabilitar la instalación de aplicaciones no confiables en todo el dispositivo.

Solo perfil personal: Para dispositivos con perfiles de trabajo, permite la instalación de aplicaciones no confiables únicamente en el perfil personal del dispositivo.

Permitir: Permitir la instalación de aplicaciones no confiables en todo el dispositivo.

3. Google Play Protect

Si se aplica la verificación de aplicaciones de Google Play Protect.

Obligatorio (predeterminado): Habilita de forma obligatoria la verificación de aplicaciones.

Elección del usuario: Permite que el usuario elija si desea habilitar la verificación de aplicaciones.

4. Política de permisos predeterminada

La política para conceder solicitudes de permisos en tiempo de ejecución a las aplicaciones.

Solicitar (predeterminado): Solicitar al usuario que conceda un permiso.

Conceder: Conceder un permiso automáticamente.

Denegar: Denegar un permiso automáticamente.

5. Funciones de la aplicación

Controla si se permite que las aplicaciones en dispositivos totalmente gestionados o en perfiles de trabajo expongan funciones de la aplicación. Requiere Android 16 o superior.

Permitido (predeterminado): Las aplicaciones en dispositivos totalmente gestionados o en perfiles de trabajo pueden exponer funciones de la aplicación.

No permitido: Las aplicaciones en dispositivos totalmente gestionados o en perfiles de trabajo no pueden exponer funciones de la aplicación.

6. Instalación de aplicaciones deshabilitada

Si la instalación de aplicaciones por parte del usuario está deshabilitada.

7. Desinstalación de aplicaciones deshabilitada

Si la desinstalación de aplicaciones por parte del usuario está deshabilitada.

8. Políticas de permisos

Concesiones o denegaciones explícitas de permisos individuales o grupales para todas las aplicaciones. Estos valores anulan el ajuste de **Política de permisos predeterminada**.

Utilice **Añadir política de permisos** para crear entradas y elimínelas con la acción de eliminar.

Cada entrada incluye:

Permiso/grupo de Android: El permiso o grupo de Android (obligatorio), por ejemplo **android.permission.READ_CALENDAR** o **android.permission_group.CALENDAR**.

Política: Conceder / Denegar / Solicitar (utiliza las mismas opciones de política que **Política de permisos predeterminada**).

9. Aplicaciones

Lista de aplicaciones que deben incluirse en la política. El comportamiento del contenido de la lista depende del valor establecido en **Modo de Play Store**.

Si el **Modo de Play Store** está configurado como **lista blanca**, solo las aplicaciones que están en la política estarán disponibles y cualquier aplicación que no esté en la política se desinstalará automáticamente del dispositivo.

Si el **Modo de Play Store** está configurado como **lista negra**, todas las aplicaciones están disponibles y cualquier aplicación que no deba estar en el dispositivo debe marcarse explícitamente como **bloqueada** en la política de aplicaciones.

Para añadir una nueva aplicación, haz clic en el botón **Añadir aplicaciones** (o en el icono de **Añadir aplicaciones**), selecciona **Desde Managed Google Play**, luego elige la aplicación de Play Store y haz clic en el botón **Seleccionar** de la tarjeta de la aplicación.

Para añadir una aplicación que no está publicada en Google Play pero que ya está presente en el dispositivo (por ejemplo, una aplicación del sistema o del fabricante), pulsa en **Añadir aplicaciones**, selecciona **Por nombre de paquete (aplicaciones preinstaladas)**, escribe el nombre del paquete de la aplicación (por ejemplo, **com.example.app**) y pulsa en **Añadir**. La aplicación se añade con el tipo de instalación **Instalación forzada**. Para mostrar la aplicación en el lanzador personalizado del kiosco, su **Tipo de instalación** debe ser **Preinstalada** o **Instalación forzada**: con **Disponible** la aplicación no se muestra.

Las aplicaciones que no están disponibles en Managed Google Play se marcan con un icono de Android en la lista de aplicaciones. No se pueden instalar desde Google Play, por lo que

ya deben estar presentes en el dispositivo: los dispositivos que no tengan la aplicación no podrán instalarla.

Todas las aplicaciones publicadas en la Play Store de su país están disponibles para su selección de forma predeterminada. Para seleccionar sus propias aplicaciones privadas o web, primero debe cargarlas en el sistema. Para más información, lea la página de

Aplicaciones privadas.

Cada aplicación puede configurarse con sus propios ajustes, los cuales se encuentran contenidos visualmente en una tarjeta:

9.1. Tipo de instalación

El tipo de instalación que se realizará para una aplicación.

Disponible: La aplicación está disponible para su instalación.

Preinstalada: La aplicación se instala automáticamente y puede ser eliminada por el usuario.

Instalación forzada: La aplicación se instala automáticamente y no puede ser eliminada por el usuario.

Bloqueada: La aplicación está bloqueada y no se puede instalar. Si la aplicación se instaló bajo una política anterior, será desinstalada.

Requerida para la configuración: La aplicación se instala automáticamente, no puede ser eliminada por el usuario y evitará que se complete la configuración hasta que la instalación finalice.

Quiosco: La aplicación se instala automáticamente en modo quiosco: se establece como la intención de inicio preferida y se incluye en la lista blanca para el modo de tarea bloqueada. La configuración del dispositivo no se completará hasta que la aplicación esté instalada. Tras la instalación, los usuarios no podrán eliminar la aplicación. Solo puede establecer este **tipo de instalación** para una aplicación por política. Cuando esto esté presente en la política, la barra de estado se deshabilitará automáticamente. Para más información, lea la página dedicada al **Modo quiosco**.

9.2. Restricciones de instalación

Define un conjunto de restricciones para la instalación de la aplicación. Cuando se seleccionan varias restricciones, deben cumplirse todas ellas para que la aplicación pueda instalarse.

Esta opción se muestra solo cuando el **Tipo de instalación** es **Preinstalada o Instalación forzada**.

Red sin límites de datos: Instale la aplicación solo cuando el dispositivo esté conectado a una red sin límites de datos (por ejemplo, Wi-Fi).

Cargando: Instale la aplicación solo cuando el dispositivo se esté cargando.

Inactivo: Instale la aplicación solo cuando el dispositivo esté inactivo.

9.3. Modo de actualización automática

Controla el modo de actualización automática de la aplicación.

Predeterminado: La aplicación se actualiza automáticamente con baja prioridad para minimizar el impacto en el usuario. La aplicación se actualiza cuando se cumplen todas las siguientes restricciones: (1) el dispositivo no se está utilizando activamente, (2) el dispositivo está conectado a una red sin límites de datos, (3) el dispositivo se está cargando. El dispositivo recibe la notificación de una nueva actualización dentro de las 24 horas posteriores a su publicación por parte del desarrollador, tras lo cual la aplicación se actualizará la próxima vez que se cumplan las restricciones anteriores.

Aplazado: La aplicación no se actualiza automáticamente durante un máximo de 90 días después de que la aplicación quede desactualizada. Transcurridos los 90 días desde que la aplicación queda desactualizada, se instalará automáticamente la versión más reciente disponible con baja prioridad (consulte el **Modo de actualización automática predeterminado**). Una vez actualizada la aplicación, no se volverá a actualizar automáticamente hasta 90 días después de que vuelva a quedar desactualizada. El usuario aún puede actualizar la aplicación manualmente desde la Play Store en cualquier momento.

Prioridad alta: La aplicación se actualiza lo antes posible. No se aplican restricciones. El dispositivo recibe una notificación inmediata sobre la nueva actualización en cuanto esté disponible.

9.4. Código de versión mínimo

La versión mínima de la aplicación que se ejecuta en el dispositivo. Si se establece, el dispositivo intentará actualizar la aplicación al menos a este código de versión. Si la aplicación no está actualizada, el dispositivo mostrará un **Detalle de incumplimiento** con el **Motivo de incumplimiento** establecido como **APP_NOT_UPDATED**. La aplicación ya debe estar publicada en Google Play con un código de versión mayor o igual a este valor. Se pueden especificar un máximo de 20 aplicaciones con código de versión mínimo por política.

9.5. Ámbitos delegados

Los ámbitos delegados a la aplicación desde Android Device Policy. Puede conceder a otras aplicaciones una selección de permisos especiales de Android:

Instalación de certificados: Concede acceso a la instalación y gestión de certificados.

Configuraciones gestionadas: Concede acceso a la gestión de configuraciones gestionadas.

Bloquear desinstalación: Concede acceso para bloquear la desinstalación.

Permisos: Concede acceso a la política de permisos y al estado de concesión de permisos.

Acceso a paquetes: Concede acceso al estado de acceso a paquetes.

Aplicación del sistema: Concede acceso para habilitar aplicaciones del sistema.

9.6. Red preferente

El servicio de red preferente que se utilizará para esta aplicación. Si se establece, la aplicación utilizará el segmento de red empresarial especificado para sus conexiones cuando esté disponible. Esto debe coincidir con un segmento de red configurado en la sección **Configuración de segmentación de red 5G** del panel de **Red celular**.

9.7. Política de permisos predeterminada

La política predeterminada para todos los permisos solicitados por la aplicación. Si se especifica, esta anula la **Política de permisos predeterminada** a nivel de política que se aplica a todas las aplicaciones. No anula las **Políticas de permisos** que se aplican a todas las aplicaciones.

Solicitar (predeterminado): Solicitar al usuario que conceda un permiso.

Conceder: Conceder un permiso automáticamente.

Denegar: Denegar un permiso automáticamente.

9.8. Aplicación conectada entre perfiles de trabajo y personales

Controla si la aplicación puede comunicarse entre los perfiles de trabajo y personales del dispositivo, sujeto al consentimiento del usuario (Android 11+).

No permitido (predeterminado): Evita que la aplicación se comuniquen entre perfiles.

Permitido: Permite que la aplicación se comuniquen entre perfiles tras recibir el consentimiento del usuario.

9.9. Exención de bloqueo de Always On VPN

Especifica si se permite que la aplicación tenga acceso a la red cuando la VPN no está conectada y el **bloqueo activado** está activo. Solo es compatible con dispositivos que ejecutan Android 10 o superior.

Obligatorio (predeterminado): La aplicación respeta el ajuste de bloqueo de Always On VPN.

Exento: La aplicación está exenta del ajuste de bloqueo de Always On VPN.

9.10. Widgets del perfil de trabajo

Especifica si se permite que la aplicación instalada en el perfil de trabajo añada widgets a la pantalla de inicio.

Permitido: La aplicación puede añadir widgets a la pantalla de inicio.

No permitido: La aplicación no puede añadir widgets a la pantalla de inicio.

9.11. Ajustes de control del usuario

Especifica si se permite el control del usuario para una aplicación determinada. El control del usuario incluye acciones como forzar la detención y borrar los datos de la aplicación (Android 11+). Si **extensionConfig** está habilitado para una aplicación, el control del usuario queda deshabilitado independientemente de este ajuste. Para las aplicaciones de quiosco, puede usar **Permitido** para permitir el control del usuario.

No especificado: Utiliza el comportamiento predeterminado de la aplicación para determinar si se permite o no el control del usuario.

Permitido: Se permite el control del usuario para la aplicación.

No permitido: No se permite el control del usuario para la aplicación.

9.12. Deshabilitada

Si la aplicación está deshabilitada. Cuando se deshabilita, los datos de la aplicación se conservan.

9.13. Permitir proveedor de credenciales

Si se permite que la aplicación actúe como proveedor de credenciales en Android 14 y versiones superiores.

9.14. Configuración gestionada

Para configurar los ajustes gestionados de la aplicación, haga clic en el botón **Habilitar configuración gestionada**. Si ya se ha establecido una configuración gestionada para la aplicación, puede modificarla con el botón **Configuración gestionada** o eliminarla con el botón

Eliminar configuración.

La opción de **Configuración gestionada** solo está disponible para las aplicaciones que admiten esta funcionalidad.

9.15. Políticas de permisos

Concesiones o denegaciones explícitas de permisos para la aplicación. Estos valores anulan la **Política de permisos predeterminada** y las **Políticas de permisos** que se aplican a todas las aplicaciones.

Utilice **Añadir política de permisos** para añadir una o más reglas de permisos a la tarjeta de la aplicación y elimínelas con la acción de eliminar.

9.16. ID de las pistas

Lista de los ID de las pistas de prueba cerrada de la aplicación a las que un dispositivo puede acceder. Si se seleccionan varios ID de pistas, los dispositivos recibirán la versión más reciente entre todas las pistas accesibles. Si no se selecciona ningún ID de pista, los dispositivos solo tendrán acceso a la pista de producción de la aplicación.

La opción de IDs de seguimiento solo está disponible para aplicaciones que tengan al menos un ID de seguimiento disponible para su organización. Para obtener más detalles sobre cómo añadir su organización a una vía de pruebas cerradas para una aplicación específica, lea [aquí](#).

10. Ajustes predeterminados de aplicaciones

Establezca las aplicaciones predeterminadas para los tipos compatibles. Cuando se establece una aplicación predeterminada para al menos un tipo, se impide que los usuarios cambien las aplicaciones predeterminadas en ese perfil.

Solo se permite un ajuste de aplicación predeterminada por **Tipo de aplicación predeterminada**. La lista de aplicaciones predeterminadas no debe contener duplicados.

10.1. Tipo de aplicación predeterminada

Seleccione la categoría de aplicación para configurar (por ejemplo, Navegador, Marcador, SMS, Billetera o Asistente). La disponibilidad depende de la versión de Android y del modo de gestión.

10.2. Ámbitos de la aplicación predeterminada

Seleccione dónde debe aplicarse la aplicación predeterminada (Totalmente gestionado, Perfil de trabajo o Perfil personal). Solo se pueden elegir los ámbitos compatibles con el tipo seleccionado.

Si ninguno de los ámbitos seleccionados es aplicable al modo de gestión del dispositivo, el dispositivo informará un detalle de incumplimiento.

10.3. Aplicaciones predeterminadas

Lista de aplicaciones que pueden establecerse como predeterminadas para el tipo seleccionado. La primera aplicación instalada y elegible se establece como la predeterminada.

Si los ámbitos incluyen **Totalmente gestionado** o **Perfil de trabajo**, cada aplicación también debe existir en la lista de **Aplicaciones** con el **Tipo de instalación** que no esté establecido como **Bloqueada**.

11. Selección de clave privada

Permite mostrar la interfaz de usuario en un dispositivo para que el usuario pueda elegir un alias de clave privada si no hay reglas coincidentes en **Elegir reglas de clave privada**.

Para dispositivos con una versión anterior a Android P, establecer esto puede dejar las claves empresariales vulnerables.

12. Elegir reglas de clave privada

Controla el acceso de las aplicaciones a las claves privadas. La regla determina qué clave privada, si la hay, Android Device Policy concede a la aplicación especificada. El acceso se concede cuando la aplicación llama a `KeyChain.choosePrivateKeyAlias` (o cualquier sobrecarga) para solicitar un alias de clave privada para una URL determinada, o en el caso de reglas que no son específicas de una URL (es decir, si `urlPattern` no está establecido, o se establece como una cadena vacía o `.*`) en Android 11 y versiones superiores, directamente para que la aplicación pueda llamar a `KeyChain.getPrivateKey` sin tener que llamar primero a `KeyChain.choosePrivateKeyAlias`. Cuando una aplicación llama a `KeyChain.choosePrivateKeyAlias` y coinciden más de una regla de `choosePrivateKeyRules`, la última regla que coincida define qué alias de clave devolver.

Utilice **Añadir regla de clave privada** para crear entradas y elimínelas con la acción de eliminar.

12.1. Alias de clave privada

El alias de la clave privada que se utilizará.

12.2. Patrón de URL

El patrón de URL para comparar con la URL de la solicitud. Si no se establece o está vacío, coincidirá con todas las URLs. Esto utiliza la sintaxis de expresiones regulares de `java.util.regex.Pattern`.

12.3. Nombres de paquetes

Los nombres de paquetes a los que se aplica esta regla. El hash del certificado de firma de cada aplicación se verifica con el hash proporcionado por Play. Si no se especifican nombres de paquetes, el alias se proporcionará a todas las aplicaciones que llamen a `KeyChain.choosePrivateKeyAlias` o cualquier sobrecarga (pero no sin llamar a `KeyChain.choosePrivateKeyAlias`, incluso en Android 11 y versiones superiores). Cualquier aplicación con el mismo UID de Android que un paquete especificado aquí tendrá acceso cuando llamen a `KeyChain.choosePrivateKeyAlias`.

Utilice **Añadir nombre de paquete** para añadir entradas y elimínelas con la acción de eliminar.

Para eliminar una aplicación, haga clic en el icono de **papelera** en la parte inferior de la tarjeta de la aplicación.

Modo quiosco

Con el modo quiosco, puede restringir la funcionalidad de un dispositivo a una sola aplicación o a varias aplicaciones. La elección entre el modo quiosco de una sola aplicación o de múltiples aplicaciones dependerá de sus objetivos empresariales.

En el **modo quiosco de una sola aplicación**, el dispositivo se configura para una única aplicación y no permite que los usuarios finales accedan a otras aplicaciones del dispositivo. Tampoco pueden salir de la aplicación, lo que la convierte en un dispositivo dedicado a esa aplicación específica. Para habilitar este modo, especifique una aplicación en la sección de

[Gestión de aplicaciones](#) con el **Tipo de instalación** establecido como **Quiosco**.

En el **modo quiosco de múltiples aplicaciones**, se permite el acceso a múltiples aplicaciones en los dispositivos. Los usuarios finales pueden navegar entre varias aplicaciones a través de un lanzador personalizado. Para habilitar este modo, active la opción **Lanzador personalizado de quiosco**.

Cuando el modo quiosco está habilitado, también puede configurar si los usuarios finales pueden acceder a ciertas funciones del sistema, como los ajustes del sistema y la barra de estado.

Lanzador personalizado de quiosco

Indica si el lanzador personalizado de quiosco está habilitado. Este reemplaza la pantalla de inicio por un lanzador que bloquea el dispositivo para las aplicaciones instaladas a través del ajuste de [Gestión de aplicaciones](#). Las aplicaciones aparecen en una única página en orden alfabético.

Acciones del botón de encendido

Establece el comportamiento de un dispositivo en modo quiosco cuando un usuario mantiene pulsado (pulsación larga) el botón de encendido.

Disponible (predeterminado): El menú de encendido (por ejemplo, Apagar, Reiniciar) se muestra cuando un usuario mantiene pulsado el botón de encendido en un dispositivo en modo quiosco.

Bloqueado: El menú de encendido (por ejemplo, Apagar, Reiniciar) no se muestra cuando un usuario mantiene pulsado el botón de encendido en un dispositivo en modo quiosco. Nota:

esto puede impedir que los usuarios apaguen el dispositivo.

Advertencias de errores del sistema

Especifica si se bloquean los diálogos de error del sistema por aplicaciones que se han cerrado inesperadamente o no responden en el modo quiosco. Cuando están bloqueados, el sistema forzará la detención de la aplicación como si el usuario eligiera la opción "cerrar aplicación" en la interfaz.

Bloqueado (predeterminado): Se bloquean todos los diálogos de error del sistema, como los de cierre inesperado y de la aplicación no responde (ANR). Cuando están bloqueados, el sistema fuerza la detención de la aplicación como si el usuario cerrara la aplicación desde la interfaz.

Habilitado: Se muestran todos los diálogos de error del sistema, como los de cierre inesperado y de la aplicación no responde (ANR).

Navegación del sistema

Especifica qué funciones de navegación están habilitadas (por ejemplo, los botones de Inicio y de Vista general) en el modo quiosco.

Deshabilitado (predeterminado): Los botones de Inicio y Vista general no son accesibles.

Solo inicio: Solo se habilita el botón de inicio.

Habilitado: Los botones de inicio y vista general están habilitados.

Barra de estado

Especifica si la información del sistema y las notificaciones están deshabilitadas en el modo quiosco.

Deshabilitado (predeterminado): La información del sistema y las notificaciones están deshabilitadas en el modo quiosco.

Solo sistema: Solo se muestra la información del sistema en la barra de estado.

Habilitado: La información del sistema y las notificaciones se muestran en la barra de estado en el modo quiosco. Nota: Para que esta política surta efecto, el botón de inicio del dispositivo debe estar habilitado mediante `kioskCustomization.systemNavigation`.

Ajustes del dispositivo

Especifica si se permite la aplicación de Ajustes en el modo quiosco.

Permitido (predeterminado): Se permite el acceso a la aplicación de Ajustes en el modo quiosco.

Bloqueado: No se permite el acceso a la aplicación de Ajustes en el modo quiosco.

Seguridad

En esta sección, puede configurar las políticas relacionadas con la seguridad.

Acciones ante riesgos de seguridad

Elija qué hacer cuando un dispositivo informe de un riesgo de seguridad (SecurityRisk) en los informes de estado.

Tipos de riesgo de seguridad (SecurityRisk) compatibles:

SO desconocido: La API de Play Integrity detecta que el dispositivo ejecuta un SO desconocido (la comprobación basicIntegrity es correcta, pero ctsProfileMatch falla).

SO comprometido: La API de Play Integrity detecta que el dispositivo ejecuta un SO comprometido (la comprobación basicIntegrity falla).

Fallo en la evaluación basada en hardware: La API de Play Integrity detecta que el dispositivo no cuenta con una garantía sólida de integridad del sistema, si la etiqueta MEETS_STRONG_INTEGRITY no aparece en el campo de integridad del dispositivo.

Acciones disponibles:

Eliminar datos corporativos (predeterminado): Eliminar el registro y borrar los datos de trabajo (todo el dispositivo si es de gestión completa, o solo el perfil de trabajo si es propiedad del perfil).

Sin acción: Mantener el dispositivo registrado y no realizar ninguna acción de forma automática.

Al seleccionar **Eliminar datos corporativos**, también puede configurar las opciones de eliminación:

Conservar la protección contra restablecimiento de fábrica: Conservar los datos de la protección contra restablecimiento de fábrica (FRP) al eliminar el dispositivo.

Eliminar almacenamiento externo: Eliminar también el almacenamiento externo del dispositivo (como tarjetas SD) al realizar la eliminación.

Eliminar eSIM: En dispositivos propiedad de la empresa, esto elimina todas las eSIM del dispositivo al realizar la eliminación. En dispositivos de propiedad personal, se eliminarán las eSIM gestionadas (las eSIM que se agregaron mediante el comando ADD_ESIM) y no se eliminarán las eSIM de propiedad personal.

1. Tiempo máximo para el bloqueo

Tiempo máximo (en segundos) de actividad del usuario hasta que el dispositivo se bloquee. Un valor de 0 significa que no hay restricciones.

2. Mantener encendido al cargar

Los modos de conexión a la batería en los que el dispositivo permanece encendido. Al usar este ajuste, se recomienda borrar **el tiempo máximo para el bloqueo** para que el dispositivo no se bloquee mientras permanece encendido.

Cargador de CA: La fuente de alimentación es un cargador de CA.

Puerto USB: La fuente de alimentación es un puerto USB.

Cargador inalámbrico: La fuente de alimentación es inalámbrica.

3. Bloqueo de pantalla desactivado

Si se activa, esto desactiva la pantalla de bloqueo para las pantallas principales y/o secundarias. Esta política solo es compatible con el modo de gestión de dispositivos dedicados.

4. Requisitos de contraseña

Políticas de requisitos de contraseña.

Utilice **Configurar requisitos de contraseña** para añadir uno o más bloques de requisitos de contraseña. Utilice **Borrar todo** para eliminar todos los requisitos de contraseña configurados.

Los requisitos de contraseña pueden utilizar el ámbito **Auto** (requisito único) o ámbitos independientes de **Dispositivo/Perfil de trabajo**. Los requisitos basados en la complejidad deben combinarse con requisitos basados en la calidad para el mismo ámbito.

4.1. Ámbito

El ámbito al que se aplica el requisito de contraseña.

Auto: El ámbito no está especificado. Los requisitos de contraseña se aplican al perfil de trabajo en los dispositivos con perfil de trabajo, y a todo el dispositivo en los dispositivos de gestión completa o dedicados.

Dispositivo: Los requisitos de contraseña se aplican únicamente al dispositivo.

Perfil de trabajo: Los requisitos de contraseña se aplican únicamente al perfil de trabajo.

4.2. Longitud del historial de contraseñas

La longitud del historial de contraseñas. Tras configurar este campo, el usuario no podrá introducir una contraseña nueva que sea igual a cualquiera de las contraseñas del historial. Un valor de 0 significa que no hay restricciones.

4.3. Máximo de contraseñas fallidas para la eliminación

Número de contraseñas incorrectas para desbloquear el dispositivo que se pueden introducir antes de que se realice la eliminación del mismo. Un valor de 0 significa que no hay restricciones.

4.4. Tiempo de expiración de la contraseña (días)

Este ajuste obliga al usuario a actualizar su contraseña periódicamente, tras el número de días especificado.

4.5. Requerir desbloqueo con contraseña

El periodo de tiempo tras el cual un dispositivo o perfil de trabajo, habiendo sido desbloqueado mediante una forma de autenticación fuerte (contraseña, PIN, patrón), puede ser desbloqueado utilizando cualquier otro método de autenticación (por ejemplo: huella dactilar, agentes de confianza, rostro). Una vez transcurrido el periodo de tiempo especificado, solo se podrán utilizar formas de autenticación fuertes para desbloquear el dispositivo o perfil de trabajo.

Predeterminado del dispositivo: El periodo de tiempo de espera se establece según el valor predeterminado del dispositivo.

Cada día: El periodo de tiempo de espera se establece en 24 horas.

4.6. Calidad de la contraseña

La calidad de contraseña requerida.

Complejidad alta: Define el nivel de complejidad alta de la contraseña como: En Android 12 y versiones superiores: PIN sin secuencias repetitivas (4444) o de orden (1234, 4321, 2468), con una longitud de al menos 8 caracteres; alfabética, con una longitud de al menos 6 caracteres; alfanumérica, con una longitud de al menos 6 caracteres.

Complejidad media: Define el nivel de complejidad media de la contraseña como: PIN sin secuencias repetitivas (4444) o de orden (1234, 4321, 2468), con una longitud de al menos 4 caracteres; alfabética, con una longitud de al menos 4 caracteres; alfanumérica, con una longitud de al menos 4 caracteres.

Complejidad baja: Define el nivel de complejidad baja de la contraseña como: patrón; PIN con secuencias repetitivas (4444) o de orden (1234, 4321, 2468).

Ninguno: No hay requisitos de contraseña.

Débil: El dispositivo debe asegurarse, como mínimo, con una tecnología de reconocimiento biométrico de baja seguridad. Esto incluye tecnologías que pueden reconocer la identidad de un individuo y que son aproximadamente equivalentes a un PIN de 3 dígitos (la detección falsa es inferior a 1 entre 1.000).

Cualquiera: Se requiere una contraseña, pero no hay restricciones sobre lo que debe contener.

Numérico: La contraseña debe contener caracteres numéricos.

Numérico complejo: La contraseña debe contener caracteres numéricos sin secuencias repetitivas (4444) o de orden (1234, 4321, 2468).

Alfabético: La contraseña debe contener caracteres alfabéticos (o símbolos).

Alfanumérico: La contraseña debe contener tanto caracteres numéricos como alfabéticos (o símbolos).

Complejo: La contraseña debe cumplir con los requisitos mínimos especificados en `passwordMinimumLength`, `passwordMinimumLetters`, `passwordMinimumSymbols`, etc. Por ejemplo, si `passwordMinimumSymbols` es 2, la contraseña debe contener al menos dos símbolos.

4.7. Longitud mínima

La longitud mínima permitida para la contraseña. Un valor de 0 significa que no hay restricciones.

4.8. Mínimo de letras

Número mínimo de letras requeridas en la contraseña.

4.9. Mínimo de letras minúsculas

Número mínimo de letras minúsculas requeridas en la contraseña.

4.10. Mínimo de letras mayúsculas

Número mínimo de letras mayúsculas requeridas en la contraseña.

4.11. Mínimo de caracteres que no sean letras

Número mínimo de caracteres que no sean letras (dígitos numéricos o símbolos) requeridos en la contraseña.

4.12. Mínimo de dígitos numéricos

Número mínimo de dígitos numéricos requeridos en la contraseña.

4.13. Mínimo de símbolos

Número mínimo de símbolos requeridos en la contraseña.

4.14. Bloqueo unificado

Controla si se permite un bloqueo unificado para el dispositivo y el perfil de trabajo en dispositivos con Android 9 o superior que tengan un perfil de trabajo. Esto no tiene efecto en otros dispositivos.

Permitir bloqueo unificado: Se permite un bloqueo común para el dispositivo y el perfil de trabajo.

Requerir bloqueo de trabajo independiente: Se requiere un bloqueo independiente para el perfil de trabajo.

5. Restablecimiento de fábrica desactivado

Si se desactiva el restablecimiento de fábrica desde los ajustes. Solo se aplica a dispositivos con gestión completa.

6. Protección contra restablecimiento de fábrica

Direcciones de correo electrónico de los administradores del dispositivo para la protección contra restablecimiento de fábrica. Si el dispositivo sufre un restablecimiento de fábrica no autorizado, se requerirá que uno de estos administradores inicie sesión con su dirección de correo electrónico y contraseña de la cuenta de Google para desbloquear el dispositivo. Si no se especifican

administradores, el dispositivo no ofrecerá protección contra restablecimiento de fábrica. Solo se aplica a dispositivos con gestión completa.

Correos electrónicos de administradores: use **Activar la protección contra restablecimiento de fábrica** para empezar a configurar los administradores. Luego, use **Añadir correo electrónico de administrador** para añadir direcciones y elimínelas con la acción de borrar.

7. Funciones de bloqueo de pantalla

Funciones de bloqueo de pantalla (pantalla de bloqueo) que se pueden desactivar.

7.1. Desactivar todo

Desactiva todas las personalizaciones actuales y futuras del bloqueo de pantalla.

7.2. Desactivar cámara

Desactiva la cámara en las pantallas de bloqueo seguras (por ejemplo, PIN).

7.3. Desactivar notificaciones

Desactiva la visualización de todas las notificaciones en las pantallas de bloqueo seguras.

7.4. Desactivar notificaciones sin censura

Desactiva las notificaciones sin censura en las pantallas de bloqueo seguras.

7.5. Ignorar el estado del agente de confianza

Ignorar el estado del agente de confianza en las pantallas de bloqueo seguras.

7.6. Desactivar huella dactilar

Desactiva el sensor de huella dactilar en las pantallas de bloqueo seguras.

7.7. Desactivar entrada de texto en notificaciones

Desactiva la entrada de texto en las notificaciones en las pantallas de bloqueo seguras.

7.8. Desactivar autenticación facial

Desactiva la autenticación facial en las pantallas de bloqueo seguras.

7.9. Desactivar autenticación de iris

Desactiva la autenticación de iris en las pantallas de bloqueo seguras.

7.10. Desactivar toda la autenticación biométrica

Desactiva toda la autenticación biométrica en las pantallas de bloqueo seguras.

7.11. Desactivar todos los accesos directos

Desactiva todos los accesos directos en la pantalla de bloqueo segura en Android 14 y versiones superiores.

Multimedia

En esta sección, puede configurar el comportamiento de la cámara/micrófono, el acceso a datos por USB, la impresión y las restricciones relacionadas con la pantalla.

1. Acceso a la cámara

Controla el uso de la cámara y si el usuario puede acceder al interruptor de acceso a la cámara (Android 12+). En general, desactivar la cámara se aplica a todo el dispositivo en dispositivos totalmente gestionados y solo dentro del perfil de trabajo en dispositivos con perfil de trabajo.

Elección del usuario (predeterminado): Comportamiento predeterminado del dispositivo. Las cámaras están disponibles y (en Android 12+) el usuario puede activar o desactivar el acceso a la cámara.

Desactivado: Todas las cámaras están desactivadas (en dispositivos totalmente gestionados: en todo el dispositivo; en perfiles de trabajo: solo para las aplicaciones del perfil de trabajo). El interruptor de acceso a la cámara no tiene efecto en el ámbito gestionado.

Obligatorio: Las cámaras están disponibles. En dispositivos totalmente gestionados con Android 12 o superior, el usuario no puede activar o desactivar el acceso a la cámara. En otros dispositivos/versiones, este comportamiento es como la elección del usuario.

2. Acceso al micrófono

En dispositivos totalmente gestionados, controla el uso del micrófono y si el usuario puede acceder al interruptor de acceso al micrófono (Android 12+). Este ajuste no tiene efecto en dispositivos que no son totalmente gestionados.

Elección del usuario (predeterminado): Comportamiento predeterminado. El micrófono está disponible y (en Android 12+) el usuario puede activar o desactivar el acceso al micrófono.

Desactivado: El micrófono está desactivado (en todo el dispositivo). El interruptor de acceso al micrófono no tiene efecto.

Obligatorio: El micrófono está disponible. En Android 12 o superior, el usuario no puede activar o desactivar el acceso al micrófono. En Android 11 o versiones anteriores, este comportamiento es como la elección del usuario.

3. Acceso a datos por USB

Controla qué archivos y/o datos se pueden transferir a través de USB. Solo es compatible con dispositivos propiedad de la empresa.

No permitir la transferencia de archivos (predeterminado): No se permiten las transferencias de archivos, pero se permiten otras conexiones de datos por USB (por ejemplo, ratón/teclado).

No permitir la transferencia de datos: Se prohíben todos los tipos de transferencia de datos por USB (Android 12+ con USB HAL 1.3+). Si no es compatible, el dispositivo utilizará la opción de No permitir la transferencia de archivos.

Permitir la transferencia de datos: Se permiten todos los tipos de transferencia de datos por USB.

4. Impresión

Controla si se permite la impresión (Android 9+).

Permitido (predeterminado): Se permite la impresión.

No permitido: No se permite la impresión (Android 9+).

5. Ajustes de brillo de la pantalla

Controla el modo de brillo de la pantalla y (opcionalmente) el valor del brillo.

Modo de brillo de la pantalla:

Elección del usuario (predeterminado): Se permite al usuario configurar el brillo de la pantalla.

Automático: El brillo es automático y el usuario no puede cambiarlo. Aún así, se puede establecer un valor de brillo, que se utiliza como parte del ajuste automático (dispositivos Android 9+ totalmente gestionados; perfiles de trabajo en dispositivos Android 15+ propiedad de la empresa).

Fijo: El brillo se establece en el valor configurado y el usuario no puede cambiarlo. Se requiere un valor de brillo (dispositivos Android 9+ totalmente gestionados; perfiles de trabajo en dispositivos Android 15+ propiedad de la empresa).

Brillo de la pantalla:

Valor de 1 a 255 (1 = mínimo, 255 = máximo). Un valor de 0 significa que no se ha establecido ningún valor de brillo.

6. Ajustes de tiempo de espera de la pantalla

Controla si el usuario puede configurar el tiempo de espera de la pantalla y, cuando se aplica de forma obligatoria, el valor del tiempo de espera.

El campo **Modo de tiempo de espera de la pantalla** permite elegir entre un comportamiento controlado por el usuario o uno obligatorio.

Elección del usuario (predeterminado): Se permite al usuario configurar el tiempo de espera de la pantalla.

Obligatorio: El tiempo de espera de la pantalla se establece en el valor configurado y el usuario no puede cambiarlo (dispositivos Android 9+ totalmente gestionados; perfiles de trabajo en dispositivos Android 15+ propiedad de la empresa).

Tiempo de espera de la pantalla:

Duración del tiempo de espera en segundos. El valor debe ser superior a 0. Si es superior al **tiempo máximo de bloqueo**, el sistema puede ajustarlo y notificar un incumplimiento.

7. Captura de pantalla desactivada

Si se desactiva la captura de pantalla.

8. Ajuste de volumen desactivado

Si se desactiva el ajuste del volumen maestro.

9. Montaje de medios físicos desactivado

Si se desactiva el montaje de medios físicos externos.

Red celular

En esta sección, puede configurar las políticas relacionadas con la red celular.

1. Modo avión

Controla si el usuario puede activar o desactivar el modo avión.

Elección del usuario (predeterminado): Se permite al usuario activar o desactivar el modo avión.

Deshabilitado: El modo avión está deshabilitado. No se permite al usuario activar el modo avión. Compatible con Android 9 y versiones superiores.

2. Red celular 2G

Controla si el usuario puede activar o desactivar el ajuste de red celular 2G.

Elección del usuario (predeterminado): Se permite al usuario activar o desactivar la red celular 2G.

Deshabilitado: La red celular 2G está deshabilitada. No se permite al usuario activar la red celular 2G a través de los ajustes. Compatible con Android 14 y versiones superiores.

3. Anular APN

Controla si se habilitan o deshabilitan los APN de anulación. Cuando está habilitado, solo se utilizan los APN de anulación configurados y se ignoran todos los demás APN del dispositivo.

Deshabilitado (predeterminado): Todos los ajustes de APN configurados se guardan en el dispositivo, pero están deshabilitados y no tienen efecto. Todos los demás APN del dispositivo permanecen en uso.

Habilitado: Solo se utilizan los APN de anulación; todos los demás APN se ignoran. Este ajuste solo puede configurarse en dispositivos totalmente gestionados con Android 10 o superior.

4. Ajustes de APN

Configure una o más entradas de APN. Utilice **Añadir APN** para crear una entrada y **Eliminar APN** para eliminarla.

Cada APN tiene campos obligatorios:

Tipos de APN: Seleccione uno o más tipos de tráfico para este APN (la disponibilidad depende del modo de gestión y de la versión de Android).

Nombre de APN: El identificador de APN proporcionado por su operador.

Nombre de visualización: Nombre amigable que se muestra en la interfaz de usuario.

Campos de APN opcionales:

Tipo de autenticación, Nombre de usuario, Contraseña: Configure la autenticación del operador (si es necesario).

Protocolo y Protocolo de roaming: Configuración del protocolo IP.

Tipos de red: Restringe las tecnologías celulares que el APN puede utilizar (por ejemplo, LTE/5G NR).

Dirección del proxy y Puerto del proxy: Proxy HTTP para el tráfico de datos (si corresponde).

Dirección del proxy MMS, Puerto del proxy MMS, MMSC (URI del centro MMS): Ajustes relacionados con MMS.

ID de operador numérico (MCC+MNC) y ID del operador: Campos de identificación del operador.

Ajuste de Always On: Indica si la sesión PDU activada por este APN debe estar siempre activa. Compatible con Android 15 y versiones superiores.

Tipo de MVNO: Tipo de identificador del operador de red móvil virtual.

MTU IPv4 y MTU IPv6: Unidad máxima de transmisión para las rutas IPv4/IPv6. Compatible con Android 13 y versiones superiores.

5. Configuración de difusión celular deshabilitada

Si la configuración de difusión celular está deshabilitada.

6. Configuración de redes móviles deshabilitada

Si la configuración de redes móviles está deshabilitada.

7. Datos de roaming deshabilitados

Si los servicios de datos de roaming están deshabilitados.

8. Llamadas salientes deshabilitadas

Si las llamadas salientes están deshabilitadas.

9. SMS deshabilitados

Si el envío y la recepción de mensajes SMS están deshabilitados.

10. Configuración de segmentación de red 5G

Configure los ajustes del servicio de red preferente para habilitar la segmentación de red 5G empresarial. Puede configurar hasta 5 segmentos empresariales y asignar aplicaciones a redes específicas para un enrutamiento de tráfico optimizado.

10.1. Red preferente predeterminada

ID de la red preferente predeterminada para las aplicaciones que no están en la lista de aplicaciones, o si la **Red preferente** de una aplicación no está establecida. Debe tener una configuración para el ID de red especificado (a menos que se establezca como **Sin red preferente**).

Nota: Las aplicaciones críticas como **com.google.android.apps.work.clouddpc** y **com.google.android.gms** están excluidas de este ajuste predeterminado.

10.2. Configuraciones de servicio de red

Utilice **Añadir configuración de red** para crear una configuración de segmento. Puede añadir hasta 5 configuraciones. Cada configuración tiene:

ID de red preferente (asignado automáticamente): El ID de red se asigna automáticamente y no se puede cambiar.

Reversión a la conexión predeterminada: Indica si se permite la reversión a la red predeterminada de todo el dispositivo. Si no se permite, las aplicaciones no podrán acceder a Internet si el segmento 5G no está disponible.

Redes no coincidentes: Indica si las aplicaciones sujetas a esta configuración pueden utilizar redes distintas al servicio preferente. Si se establece como **No permitido**, la **Reversión a la conexión predeterminada** también debe estar en **No permitido**. Requiere Android 14 o superior.

Redes

En esta sección, puede configurar las políticas relacionadas con la red.

Las configuraciones de Wi-Fi pueden ser aprovisionadas y gestionadas por el sistema a través de **configuraciones de Wi-Fi**. Dependiendo del valor establecido en **Configurar Wi-Fi**, los usuarios pueden tener un control limitado o nulo sobre la adición o modificación de redes.

Estado de la radio del dispositivo

1. Estado de Wi-Fi

Controla el estado actual de Wi-Fi y si el usuario puede cambiar su estado.

Elección del usuario (predeterminado): Se permite al usuario activar o desactivar el Wi-Fi.

Activado: El Wi-Fi está activado y el usuario no puede desactivarlo (Android 13+).

Desactivado: El Wi-Fi está desactivado y el usuario no puede activarlo (Android 13+).

2. Nivel mínimo de seguridad de Wi-Fi

El nivel de seguridad mínimo requerido de las redes Wi-Fi a las que el dispositivo puede conectarse. Compatible con Android 13 y versiones superiores, para dispositivos totalmente gestionados y perfiles de trabajo en dispositivos propiedad de la empresa.

Red abierta (predeterminado): El dispositivo puede conectarse a todo tipo de redes Wi-Fi.

Red personal: No permite redes Wi-Fi abiertas; requiere al menos seguridad de tipo personal (por ejemplo, WPA2-PSK).

Red de empresa: Requiere redes EAP de empresa; no permite redes Wi-Fi con un nivel de seguridad inferior a este.

Red de empresa de 192 bits: Requiere redes de empresa de 192 bits; la opción más estricta.

3. Estado de banda ultraancha (UWB)

Controla el estado del ajuste de banda ultraancha y si el usuario puede activarlo o desactivarlo.

Elección del usuario (predeterminado): Se permite al usuario activar o desactivar la UWB.

Desactivado: La UWB está desactivada y el usuario no puede activarla a través de los ajustes (Android 14+).

Gestión de la conectividad del dispositivo

4. Uso compartido de Bluetooth

Controla si se permite el uso compartido de Bluetooth.

Permitido: Se permite el uso compartido de Bluetooth (predeterminado en dispositivos totalmente gestionados, Android 8+).

No permitido: No se permite el uso compartido de Bluetooth (predeterminado en perfiles de trabajo, Android 8+).

5. Configurar Wi-Fi

Controla los privilegios de configuración de Wi-Fi. Dependiendo de la opción seleccionada, el usuario tendrá un control total, limitado o nulo sobre la configuración de las redes Wi-Fi.

Permitir la configuración de Wi-Fi (predeterminado): Se permite al usuario configurar el Wi-Fi.

No permitir la adición de configuraciones de Wi-Fi: No se permite añadir nuevas configuraciones de Wi-Fi. El usuario puede cambiar entre las redes ya configuradas (Android 13+; dispositivos totalmente gestionados y perfiles de trabajo en dispositivos propiedad de la empresa).

No permitir la configuración de Wi-Fi: No permite la configuración de redes Wi-Fi. En dispositivos totalmente gestionados, esto elimina las redes configuradas por el usuario y mantiene únicamente las redes configuradas a través de **configuraciones de Wi-Fi**. En perfiles de trabajo en dispositivos propiedad de la empresa, las redes existentes no se ven afectadas, pero los usuarios no pueden añadir, eliminar ni modificar redes Wi-Fi.

Cuando la configuración de Wi-Fi está desactivada y el dispositivo no puede conectarse durante el arranque, el sistema puede mostrar la **válvula de escape de red** para permitir que el usuario se conecte temporalmente y actualice la política.

6. Ajustes de Wi-Fi Direct

Controla la configuración y el uso de los ajustes de Wi-Fi Direct. Compatible con dispositivos propiedad de la empresa que ejecuten Android 13 o versiones superiores.

Permitir (predeterminado): Se permite al usuario utilizar Wi-Fi Direct.

No permitir: No se permite al usuario utilizar Wi-Fi Direct.

7. Ajustes de anclaje a red

Controla los ajustes de anclaje a red. Según el valor establecido, se le prohíbe al usuario, de forma parcial o total, el uso de diferentes formas de anclaje a red.

Permitir todo el anclaje a red (predeterminado): Permite la configuración y el uso de todas las formas de anclaje a red.

No permitir el anclaje por Wi-Fi: Impide que el usuario utilice el anclaje por Wi-Fi (dispositivos Android 13+ propiedad de la empresa).

No permitir ningún anclaje a red: Prohíbe todas las formas de anclaje a red (dispositivos totalmente gestionados + perfiles de trabajo en dispositivos propiedad de la empresa).

8. Política de SSID de Wi-Fi

Restricciones sobre a qué SSID de Wi-Fi puede conectarse el dispositivo (esto no afecta a qué redes pueden configurarse en el dispositivo). Compatible con dispositivos propiedad de la empresa que ejecuten Android 13 o versiones superiores.

Lista negra de SSID (predeterminado): El dispositivo no puede conectarse a ninguna red Wi-Fi cuyo SSID figure en la lista, pero sí puede conectarse a otras redes.

Lista blanca de SSID: El dispositivo solo puede conectarse a los SSID de la lista. La lista de SSID no debe estar vacía.

Utilice **Añadir SSID** para añadir entradas. Dependiendo del tipo de política seleccionada, la lista se interpretará como SSID permitidos o denegados.

En la interfaz de usuario del Editor de políticas, la lista de SSID se etiqueta como **SSID de Wi-Fi permitidos** para las listas blancas y **SSID de Wi-Fi denegados** para las listas negras.

9. Ajustes de itinerancia de Wi-Fi

Configure el modo de itinerancia de Wi-Fi por SSID. Utilice **Añadir ajuste de itinerancia de Wi-Fi** para crear entradas.

Cada entrada incluye:

SSID: El SSID al que se aplica el ajuste de itinerancia (obligatorio).

Modo de itinerancia de Wi-Fi: Predeterminado / Desactivado / Agresivo. Las opciones Desactivado y Agresivo requieren Android 15+ y solo son compatibles con dispositivos totalmente gestionados y perfiles de trabajo en dispositivos propiedad de la empresa.

Restricciones de red

10. Bluetooth desactivado

Si se desactiva el Bluetooth. Se prefiere este ajuste sobre "Desactivar configuración de Bluetooth", ya que la desactivación de la configuración de Bluetooth puede ser eludida por el usuario.

11. Uso compartido de contactos por Bluetooth desactivado

Si se desactiva el uso compartido de contactos por Bluetooth.

12. Desactivar configuración de Bluetooth

Si se desactiva la configuración de Bluetooth.

13. Restablecimiento de red desactivado

Si se desactiva el restablecimiento de los ajustes de red.

14. Beam de salida desactivado

Si se desactiva el uso de NFC para enviar datos mediante Beam desde las aplicaciones.

VPN

15. Aplicación de VPN siempre activa

Especifique el nombre del paquete de la aplicación para VPN siempre activa para garantizar que los datos de las aplicaciones gestionadas especificadas pasen siempre a través de una VPN configurada.

Nota: Esta función requiere el despliegue de un cliente VPN que admita tanto las funciones de VPN siempre activa como las de VPN por aplicación.

16. Bloqueo de red por VPN

Impide el uso de la red cuando la VPN no está conectada.

17. Desactivar configuración de VPN

Si se desactiva la configuración de VPN.

Proxy y servicios de red

18. Servicio de red preferente

Controla si el servicio de red preferente está activado en el perfil de trabajo. Por ejemplo, una organización puede tener un acuerdo con un operador para que los datos de trabajo se envíen a través de un servicio de red del operador dedicado al uso empresarial (por ejemplo, una partición de red o *slice* empresarial en redes 5G). Esto no tiene efecto en los dispositivos totalmente gestionados.

Desactivado: El servicio de red preferente está desactivado en el perfil de trabajo.

Activado: El servicio de red preferente está activado en el perfil de trabajo.

Si utiliza la partición de red empresarial, configure también la **Configuración de partición de red 5G** en el panel de políticas de **Red celular** y asigne las aplicaciones a una partición utilizando el ajuste de **Red preferente**.

19. Proxy global recomendado

El proxy HTTP global independiente de la red. Normalmente, los proxies deben configurarse por red en las configuraciones de Wi-Fi. Un proxy global puede ser útil para configuraciones inusuales, como el filtrado interno general. El proxy global es solo una recomendación y algunas aplicaciones pueden ignorarlo.

Desactivado

Proxy directo

Proxy de autoconfiguración (PAC)

19.1. Host

El host del proxy directo.

19.2. Puerto

El puerto del proxy directo.

19.3. URI de PAC

La URI del script PAC utilizado para configurar el proxy.

19.4. Hosts excluidos

Para un proxy directo, los hosts para los cuales se omite el proxy. Los nombres de host pueden contener comodines como ***.example.com**.

Utilice **Añadir host excluido** para añadir entradas (disponible solo para proxy directo).

Configuraciones de Wi-Fi

Defina las configuraciones de red Wi-Fi que el sistema aplicará en los dispositivos. Utilice **Añadir configuración de Wi-Fi** para crear una entrada y elimínela con la acción de borrar.

20. Campos de configuración de Wi-Fi

Cada configuración incluye:

Nombre de la configuración: Obligatorio.

SSID: Obligatorio.

Conexión automática: Si la red debe conectarse automáticamente cuando esté dentro del alcance.

Transición rápida: Si el cliente debe intentar utilizar la transición rápida (IEEE 802.11r-2008) con la red.

SSID oculto: Si el SSID se transmitirá.

Modo de aleatorización de MAC: Hardware o Automático (Android 13+).

20.1. Seguridad

Opciones de seguridad de Wi-Fi:

WEP-PSK: WEP (clave precompartida).

WPA-PSK: WPA/WPA2/WPA3-Personal (clave precompartida).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Protocolo de autenticación extensible).

Modo WPA3 de 192 bits: Red WPA-EAP que permite únicamente el modo WPA3 de 192 bits.

20.2. Frase de contraseña (clave precompartida)

Se muestra cuando la seguridad es **WEP-PSK** o **WPA-PSK**. La frase de contraseña es obligatoria.

20.3. Método EAP (Empresa)

Se muestra cuando la seguridad es **WPA-EAP** o **Modo WPA3 de 192 bits**. Seleccione un método EAP externo:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Autenticación de fase 2

Se muestra para los métodos externos de túnel (**EAP-TTLS** y **PEAP**).

MSCHAPv2

PAP

20.5. Credenciales EAP de los usuarios

Cuando está activado, el sistema aplica automáticamente las credenciales EAP en los dispositivos de forma individual por usuario. Puede configurar las credenciales de usuario en la sección **Usuarios**.

20.6. Certificado de cliente

Para **EAP-TLS**, puede asignar un certificado de cliente utilizado para la autenticación Wi-Fi. Para obtener más información, lea la página de [Gestión de certificados](#).

Si ya se ha asignado un certificado, puede usar **Abrir certificado** para verlo o **Cambiar certificado** para seleccionar uno diferente.

Alternativamente, puede especificar el **Alias del par de claves del certificado de cliente**, que hace referencia a un certificado de cliente almacenado en el llavero de Android y permitido para la autenticación Wi-Fi.

Si se establecen tanto el **Certificado de cliente** como el **Alias del par de claves del certificado de cliente**, se ignorará el alias del par de claves.

20.7. Identidad

Identidad del usuario. Para los protocolos de túnel externos (PEAP, EAP-TTLS), esto se utiliza para la autenticación dentro del túnel, y la **Identidad anónima** se utiliza para la identidad EAP fuera del túnel. Para los protocolos externos que no utilizan túnel, esto se utiliza para la identidad EAP.

20.8. Identidad anónima

Solo para protocolos de túnel, esto indica la identidad del usuario que se presenta al protocolo externo.

20.9. Contraseña

Contraseña del usuario. Si no se especifica, el valor predeterminado es solicitarla al usuario.

20.10. Certificados de la CA del servidor

Lista de certificados de la CA que se utilizarán para verificar la cadena de certificados del host. Al menos un certificado de la CA debe coincidir. Para obtener más información, lea la página de

[Gestión de certificados](#).

Utilice **Añadir certificado de la CA del servidor** para añadir entradas y elimínelas con la acción de borrar.

20.11. Coincidencias de sufijo de dominio

Una lista de restricciones para el nombre de dominio del servidor. Las entradas se utilizan como requisitos de coincidencia de sufijo con el nombre (o nombres) DNS del nombre alternativo del sujeto de un certificado de servidor de autenticación.

Sistema

En esta sección, puede configurar las políticas relacionadas con el sistema.

1. Nivel de API mínimo

El nivel de API de Android mínimo permitido.

2. Política de cifrado

Si el cifrado está activado.

Predeterminado: Este valor se ignora, es decir, no se requiere cifrado.

Activado sin contraseña: Se requiere cifrado, pero no se requiere contraseña para el arranque.

Activado con contraseña: Se requiere cifrado y contraseña para el arranque.

3. Fecha y hora automáticas

Si la fecha, la hora y la zona horaria automáticas están activadas en un dispositivo propiedad de la empresa.

Elección del usuario (predeterminado): La fecha, la hora y la zona horaria automáticas quedan a elección del usuario.

Obligatorio: Obliga al uso de fecha, hora y zona horaria automáticas en el dispositivo.

4. Ajustes de desarrollador

Controla el acceso a los ajustes de desarrollador: opciones de desarrollador y arranque seguro.

Desactivado (predeterminado): Desactiva todos los ajustes de desarrollador y evita que el usuario acceda a ellos.

Permitido: Permite todos los ajustes de desarrollador. El usuario puede acceder a ellos y, opcionalmente, configurarlos.

5. Modo de criterios comunes

Controla el modo de criterios comunes (Common Criteria Mode), que son estándares de seguridad definidos en la Evaluación de Seguridad de Criterios Comunes para la Tecnología de la Información (CC). Al activar el modo de criterios comunes, se incrementan ciertos componentes de seguridad en el dispositivo (por ejemplo: cifrado AES-GCM de las claves de largo plazo de Bluetooth, validación adicional para algunos certificados de red y comprobaciones de integridad de la política criptográfica). El modo de criterios comunes solo es compatible con dispositivos propiedad de la empresa que ejecuten Android 11 o versiones superiores. Advertencia: el modo de criterios comunes impone un modelo de seguridad estricto que normalmente solo se requiere para organizaciones con información altamente sensible. El uso estándar del dispositivo puede verse afectado; actívalo únicamente si es necesario.

Desactivado (predeterminado): Desactiva el modo de criterios comunes.

Activado: Activa el modo de criterios comunes.

6. Extensión de etiquetado de memoria (MTE)

Controla la Extensión de etiquetado de memoria (MTE) en el dispositivo.

Elección del usuario (predeterminado): El usuario puede elegir activar o desactivar MTE en el dispositivo (si el dispositivo es compatible).

Obligatorio: Se activa MTE y no se permite al usuario cambiarlo (Android 14+; compatible con dispositivos de gestión completa y perfiles de trabajo en dispositivos propiedad de la empresa).

Desactivado: Se desactiva MTE y no se permite al usuario cambiarlo (Android 14+; compatible solo con dispositivos de gestión completa).

7. Protección de contenido

Controla si se activa la protección de contenido (que busca aplicaciones engañosas). Esto es compatible con Android 15 y versiones superiores.

Desactivado (predeterminado): La protección de contenido está desactivada y el usuario no puede cambiar esto.

Obligatorio: La protección de contenido está activada y el usuario no puede cambiar esto (Android 15+).

Elección del usuario: La protección de contenido no está controlada por la política; el usuario puede elegir (Android 15+).

8. Contenido de asistencia

Controla si se permite enviar el contenido de asistencia (AssistContent) a una aplicación con privilegios, como una aplicación de asistente (por ejemplo, Circle to Search). El contenido de asistencia incluye capturas de pantalla e información sobre una aplicación, como el nombre del paquete. Esto es compatible con Android 15 y versiones superiores.

Permitido (predeterminado): Se permite el envío de contenido de asistencia a una aplicación con privilegios (Android 15+).

No permitido: Se bloquea el envío de contenido de asistencia a una aplicación con privilegios (Android 15+).

9. Creación de ventanas desactivada

Si se desactiva la creación de ventanas que no sean de aplicaciones. Esta opción evita que se muestren las siguientes interfaces de usuario del sistema: mensajes emergentes (toasts y snackbars), actividades telefónicas (como llamadas entrantes) y actividades telefónicas prioritarias (como llamadas en curso), alertas del sistema, errores del sistema y superposiciones del sistema.

10. Salida de emergencia de red

Si se activa la salida de emergencia de red. Si no se puede establecer una conexión de red en el momento del arranque, la salida de emergencia solicita al usuario que se conecte temporalmente a una red para actualizar la política del dispositivo. Tras aplicar la política, la red temporal se olvidará y el dispositivo continuará con el arranque. Esto evita que no se pueda conectar a una red si no hay una red adecuada en la última política y el dispositivo arranca directamente en una aplicación en modo de tarea bloqueada (lock task mode), o si el usuario no puede acceder a los ajustes del dispositivo por otros motivos.

11. Actividades predeterminadas

Una lista de actividades predeterminadas para gestionar los intents que coincidan con un filtro de intent específico. Por ejemplo, esta función permitiría a los administradores de TI elegir qué aplicación de navegador abre automáticamente los enlaces web, o qué aplicación de lanzador se utiliza al pulsar el botón de inicio.

Utilice **Añadir actividad predeterminada** para crear entradas. Dentro de una entrada, utilice **Añadir acción** y **Añadir categoría** para crear el filtro de intent.

11.1. Actividad receptora

La actividad que debe ser el gestor de intents predeterminado. Debe ser un nombre de componente de Android, por ejemplo: `com.android.enterprise.app/.MainActivity`. Alternativamente, el valor puede ser el nombre del paquete de una aplicación, lo que hará que Android Device Policy elija la actividad adecuada de dicha aplicación para gestionar el intent.

11.2. Acción

Las acciones de intent que deben coincidir en el filtro. Si se incluyen acciones en el filtro, la acción del intent debe ser uno de esos valores para que coincida. Si no se incluyen acciones, la acción del intent se ignora.

11.3. Categoría

Las categorías de intent que deben coincidir en el filtro. Un intent incluye las categorías que requiere, y todas ellas deben estar incluidas en el filtro para que haya coincidencia. En otras palabras, añadir una categoría al filtro no tiene impacto en la coincidencia a menos que esa categoría esté especificada en el intent.

12. Métodos de entrada permitidos

Especifica los métodos de entrada permitidos.

Todos los permitidos: No se aplica ninguna restricción. Se permiten todos los métodos de entrada.

Solo los del sistema: Solo se permiten los métodos de entrada integrados del sistema.

Solo los del sistema y los proporcionados: Solo se permiten los métodos de entrada proporcionados y los integrados del sistema.

12.1. Métodos de entrada permitidos

Nombres de paquetes de métodos de entrada permitidos. Solo se aplica cuando **Métodos de entrada permitidos** está configurado como **Solo los del sistema y los proporcionados**.

Utilice **Añadir método de entrada** para añadir entradas y elimínelas con la acción de borrar.

13. Servicios de accesibilidad permitidos

Especifica los servicios de accesibilidad permitidos.

Todos los permitidos: Se puede utilizar cualquier servicio de accesibilidad.

Solo los del sistema: Solo se pueden utilizar los servicios de accesibilidad integrados del sistema.

Solo los del sistema y los proporcionados: Solo se pueden utilizar los servicios de accesibilidad proporcionados y los integrados del sistema.

13.1. Servicios de accesibilidad permitidos

Servicios de accesibilidad permitidos. Solo se aplica cuando **Servicios de accesibilidad permitidos** está configurado como **Solo los del sistema y los proporcionados**.

Utilice **Añadir servicio de accesibilidad** para añadir entradas y elimínelas con la acción de borrar.

14. Política de actualización del sistema

Configuración para la gestión de las actualizaciones del sistema.

Predeterminado: Sigue el comportamiento de actualización predeterminado del dispositivo, que normalmente requiere que el usuario acepte las actualizaciones del sistema.

Automático: Instalar automáticamente en cuanto haya una actualización disponible.

En ventana de tiempo: Instalar automáticamente dentro de una ventana de mantenimiento diaria. Esto también configura las aplicaciones de Play para que se actualicen dentro de la ventana. Se recomienda encarecidamente para dispositivos de quiosco, ya que es la única forma en que las aplicaciones fijadas permanentemente en primer plano pueden ser actualizadas por Play.

Posponer: Posponer la instalación automática hasta un máximo de 30 días.

14.1. Ventana de mantenimiento (Solo en modo ventana)

Cuando la **Política de actualización del sistema** se establece en **En ventana de tiempo**, puede definir la ventana de mantenimiento diaria utilizando los campos **desde** y **hasta**.

14.2. Periodos de congelación de actualizaciones del sistema

Un periodo de tiempo que se repite anualmente en el cual las actualizaciones del sistema por aire (OTA) se posponen para congelar la versión del SO que se ejecuta en un dispositivo. Para evitar la congelación indefinida del dispositivo, cada periodo de congelación debe estar separado por al menos 60 días. Cada periodo de congelación no debe exceder los 90 días.

Utilice **Añadir periodo de congelación de actualizaciones del sistema** para crear entradas.

15. Proveedores de credenciales predeterminados

Controla qué aplicaciones tienen permitido actuar como proveedores de credenciales en Android 14 y versiones superiores.

No permitido (predeterminado): Las aplicaciones con la política credentialProviderPolicy no especificada no tienen permitido actuar como proveedores de credenciales.

No permitido excepto el sistema: Las aplicaciones con la política credentialProviderPolicy no especificada no tienen permitido actuar como proveedores de credenciales, excepto los proveedores de credenciales predeterminados del fabricante (OEM).

Ubicación y geocerca

Este panel agrupa los ajustes de la política de Android que controlan el informe de ubicación del dispositivo, la aplicación de la ubicación y las definiciones de geocercas. Utilícelo cuando desee que Cerberus Enterprise recopile la ubicación de los dispositivos o detecte cuándo los dispositivos entran o salen de las áreas configuradas.

Informe de ubicación

Informar ubicación

Habilita el informe de geolocalización del dispositivo. Los datos de ubicación recopilados a través de este ajuste se utilizan en el [mapa de ubicación del panel de control](#), el historial de ubicación del resumen del dispositivo y el procesamiento de geocercas.

En los dispositivos que no están totalmente gestionados, los datos de ubicación pueden seguir dependiendo de que la aplicación Cerberus Enterprise tenga los permisos de ubicación requeridos y de que los servicios de ubicación estén habilitados en el dispositivo.

Modo de ubicación

Controla el ajuste de ubicación del dispositivo en los dispositivos propiedad de la empresa.

- **Elección del usuario:** los servicios de ubicación no están restringidos por la política.
- **Obligatorio:** los servicios de ubicación están activados en el dispositivo.
- **Desactivado:** los servicios de ubicación están desactivados en el dispositivo.

Ubicación compartida desactivada

Desactiva el uso compartido de la ubicación para las aplicaciones de trabajo. En dispositivos con propietario de perfil, esto afecta al perfil de trabajo. En dispositivos totalmente gestionados, desactiva la ubicación en todo el dispositivo y anula el modo de ubicación del mismo.

Comportamiento automático con perímetros virtuales activos

Los perímetros virtuales activos requieren el envío de informes de ubicación para funcionar. Cuando al menos un perímetro virtual está activo, Cerberus Enterprise mantiene automáticamente la coherencia de los ajustes de ubicación relacionados.

- **El informe de ubicación** se activa obligatoriamente mientras existan perímetros virtuales activos.
- **El modo de ubicación** se fuerza a **Obligatorio**.
- **La opción de ubicación compartida desactivada** se desactiva obligatoriamente.

Si intenta desactivar **el informe de ubicación** mientras uno o más perímetros virtuales estén activos, Cerberus Enterprise mostrará un cuadro de diálogo de confirmación. Si continúa, se desactivarán todos los perímetros virtuales activos en la política.

Lista de perímetros virtuales

Una política puede contener hasta **10 perímetros virtuales**. Los nombres de los perímetros virtuales deben ser únicos dentro de la política.

Utilice **Añadir perímetro virtual** para crear una nueva entrada. Cada perímetro virtual contiene estos campos principales:

- **Nombre:** obligatorio y único.
- **Latitud y Longitud:** el centro del área.
- **Radio (m):** obligatorio, de **100** a **10000** metros.
- **Descripción:** notas opcionales para los administradores.
- **Informe de entrada** e **Informe de salida:** elija qué eventos de transición deben generarse.
- **Activo:** activa o desactiva el perímetro virtual sin eliminarlo.

Al menos una de las opciones **Informe de entrada** o **Informe de salida** debe permanecer activada para cada perímetro virtual.

Herramientas de edición del mapa

Cada tarjeta de perímetro virtual incluye una vista previa del mapa del área. Puede editar la geometría desde el mapa o desde los campos numéricos.

- Haga clic en el mapa para mover el centro del perímetro virtual cuando la edición del área esté desbloqueada.
- Utilice el botón **Ubicación actual** para centrar el mapa en su posición actual del navegador.
- Utilice el botón **Recentrar mapa** para restaurar el área de visualización preferida para ese perímetro virtual.
- Utilice el botón de bloqueo para evitar cambios accidentales en la geometría del perímetro virtual.

Dónde aparecen los datos de los perímetros virtuales

Las transiciones de los perímetros virtuales pueden revisarse en la página de [Información general del dispositivo](#) de Android, dentro de la pestaña **Perímetro virtual** del panel de ubicación. Esa pestaña muestra las transiciones en un mapa dedicado junto con herramientas de filtrado y la lista de transiciones.

Gestión de usuarios

Desactivar la adición de usuarios

Si se desactiva la adición de nuevos usuarios y perfiles. En los dispositivos donde el modo de gestión es **DEVICE_OWNER**, este campo se ignora y al usuario nunca se le permite añadir o eliminar usuarios.

Desactivar la modificación de cuentas

Si se desactiva la adición o eliminación de cuentas.

Desactivar la configuración de credenciales de usuario

Si se desactiva la configuración de las credenciales de usuario.

Desactivar la eliminación de usuarios

Si se desactiva la eliminación de otros usuarios.

Desactivar el ajuste del icono de usuario

Si se desactiva el cambio del icono de usuario.

Desactivar el ajuste del fondo de pantalla

Si se desactiva el cambio del fondo de pantalla.

Autenticación de la configuración de la cuenta de trabajo

Controla cómo se autentican los usuarios durante la configuración de la cuenta de trabajo. Esta opción solo está disponible para empresas de Android respaldadas por un dominio gestionado de Google (Google Workspace).

Durante el aprovisionamiento o registro del dispositivo, esta política influye en si se requiere el inicio de sesión con una cuenta de trabajo, pero el ajuste **Autenticar mediante Google** de la Consola de administración de Google y el tipo de token de registro aún pueden requerir autenticación.

Para los dispositivos ya registrados, esta política solo se aplica si el dispositivo es gestionado por una cuenta de Google Play gestionada (es decir, registrado sin **el registro mediante autenticación con Google**).

Para más detalles y resolución de problemas, consulte [el registro mediante autenticación con Google](#).

Tipos de cuentas bloqueados

Tipos de cuentas que el usuario no puede gestionar. Esta opción evita que los usuarios del dispositivo añadan cuentas no aprobadas.

Utilice **Añadir tipo de cuenta bloqueada** para añadir uno o más tipos de cuenta.

Cada entrada tiene un campo de **Tipo de cuenta** (obligatorio). Introduzca una cadena como **com.google**. Elimine una entrada utilizando la acción de borrar.

Uso personal

Al [aprovisionar un dispositivo propiedad de la empresa para uso laboral y personal](#), puede especificar algunas reglas para limitar cómo el usuario puede operar el dispositivo para uso personal, fuera del perfil de trabajo.

Esta sección solo se aplica a los dispositivos propiedad de la empresa con perfil de trabajo. No tendrá ningún efecto en los dispositivos totalmente gestionados o de propiedad personal.

1. Cámara desactivada

Si se desactiva la cámara.

2. Captura de pantalla desactivada

Si se desactiva la captura de pantalla.

3. Máximo de días con el perfil de trabajo desactivado

Controla cuánto tiempo puede permanecer desactivado el perfil de trabajo.

4. Uso compartido de Bluetooth

Controla si se permite el uso compartido de Bluetooth en el perfil personal de un dispositivo propiedad de la empresa con perfil de trabajo.

5. Espacio privado

Controla si se permite un espacio privado en el dispositivo.

6. Modo de Play Store

Este modo controla qué aplicaciones se permiten o bloquean al usuario en la Play Store del perfil personal.

Lista de bloqueos (predeterminado): Todas las aplicaciones están disponibles y cualquier aplicación que no deba estar en el dispositivo debe marcarse explícitamente como **Bloqueada** en la sección de **Aplicaciones**.

Lista blanca: Solo las aplicaciones especificadas explícitamente en la sección de **Aplicaciones** con el **Tipo de instalación** establecido como **Disponible** pueden instalarse en el perfil personal.

7. Aplicaciones

Lista de aplicaciones que deben permitirse o bloquearse en el perfil personal. El comportamiento del contenido de la lista depende del valor establecido en **Modo de Play Store**.

Para añadir una nueva aplicación desde Play Store, haga clic en el icono +.

7.1. Tipo de instalación

Tipos de comportamientos de instalación que puede tener una aplicación del perfil personal.

Bloqueada: La aplicación está bloqueada y no se puede instalar en el perfil personal.

Disponible: La aplicación está disponible para instalarse en el perfil personal.

8. Tipos de cuentas bloqueadas

Tipos de cuentas que el usuario no puede gestionar. Esta opción evita que los usuarios del dispositivo añadan cuentas no aprobadas en su perfil personal.

Políticas entre perfiles

Solo se aplica a dispositivos con perfiles personales y de trabajo.

Copiar y pegar entre perfiles

Si el texto copiado de un perfil (personal o de trabajo) se puede pegar en el otro perfil.

No permitido (predeterminado): Evita que los usuarios peguen en el perfil personal el texto copiado desde el perfil de trabajo. El texto copiado desde el perfil personal se puede pegar en el perfil de trabajo.

Permitido: El texto copiado en cualquiera de los perfiles se puede pegar en el otro perfil.

Intercambio de datos entre perfiles

Si los datos de un perfil (personal o de trabajo) se pueden compartir con las aplicaciones del otro perfil. Controla específicamente el intercambio de datos sencillo a través de intents. La gestión de otros canales de comunicación entre perfiles, como la búsqueda de contactos, copiar/pegar, o las aplicaciones de trabajo y personales conectadas, se configura por separado.

No permitido: Evita que se compartan datos tanto del perfil personal al de trabajo como del perfil de trabajo al personal.

De trabajo a personal deshabilitado (predeterminado): Evita que los usuarios compartan datos desde el perfil de trabajo hacia las aplicaciones del perfil personal. Los datos personales se pueden compartir con las aplicaciones de trabajo.

Permitido: Los datos de cualquiera de los perfiles se pueden compartir con el otro perfil.

Ajustes predeterminados de los widgets del perfil de trabajo

Comportamiento predeterminado para los widgets del perfil de trabajo. Si una aplicación específica no define una política de widgets, seguirá el ajuste predeterminado establecido aquí.

Funciones de aplicaciones entre perfiles

Controla si las aplicaciones del perfil personal pueden invocar funciones de las aplicaciones del perfil de trabajo. Esto requiere Android 16 o superior.

Este ajuste depende de la opción de **Funciones de aplicaciones** a nivel de política (en la sección de Gestión de aplicaciones). Si las Funciones de aplicaciones están configuradas como **No permitido**, la API rechazará las Funciones de aplicaciones entre perfiles configuradas como **Permitido**.

Contactos de trabajo en el perfil personal

Si los contactos almacenados en el perfil de trabajo pueden mostrarse en las búsquedas de contactos y llamadas entrantes del perfil personal.

Permitido (predeterminado): Permite que los contactos del perfil de trabajo aparezcan en el perfil personal.

No permitido: Evita que las aplicaciones del perfil personal accedan a los contactos del perfil de trabajo y busquen contactos de trabajo.

No permitido excepto sistema: Evita que la mayoría de las aplicaciones personales accedan a los contactos del perfil de trabajo, excepto las aplicaciones predeterminadas del fabricante (OEM) como Marcador, Mensajes y Contactos (Android 14+).

Cuando se configura "Contactos de trabajo en el perfil personal", puede definir opcionalmente una lista de entradas de **Nombre de paquete exento**. Dependiendo del modo seleccionado, estas exenciones funcionarán como una lista blanca o una lista negra para las aplicaciones personales.

Informes de estado

En esta sección, puede configurar qué datos deben recuperarse del dispositivo. Los datos de estado se pueden ver en la página del panel de [Estado del dispositivo](#).

Informes de aplicaciones

Si los informes de aplicaciones están activados. (Información reportada sobre una aplicación instalada)

Esta opción es requerida por el sistema (para la integración con aplicaciones complementarias) y siempre está activada; no se puede desactivar.

Incluir aplicaciones eliminadas

Si las aplicaciones eliminadas se incluyen en los informes de aplicaciones.

Ajustes del dispositivo

Si la notificación de los ajustes del dispositivo está activada. (Información sobre los ajustes del dispositivo relacionados con la seguridad en el dispositivo)

Información de software

Si la notificación de información de software está activada. (Información sobre el software del dispositivo)

Información de memoria

Si la notificación de información de memoria está activada. (Un evento relacionado con las mediciones de memoria y almacenamiento)

Información de red

Si la notificación de información de red está activada. (Información de red del dispositivo)

Información de pantalla

Si la notificación de información de pantalla está activada. Los datos del informe no están disponibles para dispositivos de propiedad personal con perfiles de trabajo. (Información de la pantalla del dispositivo)

Eventos de gestión de energía

Si la notificación de eventos de gestión de energía está activada. Los datos del informe no están disponibles para dispositivos de propiedad personal con perfiles de trabajo.

Estado del hardware

Si la notificación de estado del hardware está activada. Los datos del informe no están disponibles para dispositivos de propiedad personal con perfiles de trabajo.

Propiedades del sistema

Si la notificación de propiedades del sistema está activada.

Modo de criterios comunes

Si la notificación del modo de criterios comunes está activada.

Varios

1. Juego de easter egg desactivado

Si el juego de easter egg en Ajustes está desactivado.

2. Omitir consejos de primer uso

Indicador para omitir los consejos en el primer uso. El administrador de la empresa puede habilitar la recomendación del sistema para que las aplicaciones omitan sus tutoriales de usuario y otros consejos introductorios en el primer inicio.

3. Mensaje de soporte breve

Un mensaje que se muestra al usuario en la pantalla de ajustes cuando el administrador ha desactivado alguna funcionalidad. Si el mensaje tiene más de 200 caracteres, es posible que se trunque.

4. Mensaje de soporte extenso

Un mensaje que se muestra al usuario en la pantalla de ajustes de administradores del dispositivo.

5. Información de la pantalla de bloqueo del propietario

La información del propietario del dispositivo que se mostrará en la pantalla de bloqueo.

6. Acciones de configuración

Acciones a realizar durante el proceso de configuración. Durante el registro, puede requerir que el usuario abra una o más aplicaciones necesarias para la configuración del dispositivo.

Utilice **Añadir acción de configuración** para crear entradas y elimínelas con la acción de borrar.

6.1. Iniciar aplicación

Nombre del paquete de la aplicación que se iniciará

6.2. Título

Proporciona un mensaje para el usuario con el fin de explicarle por qué es necesario iniciar la aplicación.

6.3. Descripción

Proporciona un mensaje para el usuario con el fin de explicarle por qué es necesario iniciar la aplicación.

7. Visibilidad del nombre de la empresa en pantalla

Controla si el nombre de la empresa es visible en el dispositivo (por ejemplo, como un mensaje en la pantalla de bloqueo en dispositivos propiedad de la empresa).

Visible (predeterminado): El nombre de la empresa es visible en el dispositivo (compatible con perfiles de trabajo en Android 7+ y dispositivos totalmente gestionados en Android 8+).

Oculto: El nombre de la empresa se oculta en el dispositivo.

Reglas de aplicación de políticas

Si un dispositivo o perfil de trabajo no cumple con cualquiera de los ajustes de política que se enumeran a continuación, Android Device Policy bloquea inmediatamente el uso del dispositivo o perfil de trabajo de forma predeterminada:

- **Requisitos de contraseña**
- **Política de cifrado**
- **Bloqueo de pantalla desactivado**
- **Métodos de entrada permitidos**
- **Servicios de accesibilidad permitidos**

Si el dispositivo o perfil de trabajo sigue sin cumplir con las políticas después de 10 días, Android Device Policy restablecerá el dispositivo a los valores de fábrica o eliminará el perfil de trabajo.

En esta sección, puede anular las reglas de cumplimiento predeterminadas o añadir nuevas.

Reglas

Lista de reglas que definen el comportamiento cuando una política específica no se puede aplicar a un dispositivo.

Utilice **Añadir regla** para crear una nueva regla. Cada tarjeta de regla se puede eliminar con la acción de borrar.

Nombre del ajuste

La política de nivel superior a aplicar. Por ejemplo, **Aplicaciones** o **Requisitos de contraseña**.

Obligatorio. El valor debe coincidir con un nombre de política de nivel superior compatible; de lo contrario, el campo se marcará como no válido.

Bloquear tras X días

Número de días que la política es no conforme antes de que el dispositivo o el perfil de trabajo se bloqueen. Para bloquear el acceso inmediatamente, establezca 0. El valor de **Bloquear tras X días** debe ser inferior al de **Borrar tras X días**. Solo es aplicable a dispositivos propiedad de la empresa.

Rango permitido: 0–300.

Ámbito de bloqueo

Especifica el ámbito de la acción de bloqueo. Solo es aplicable a dispositivos propiedad de la empresa.

Predeterminado (nueva regla): **Perfil de trabajo**.

Perfil de trabajo: La acción de bloqueo solo se aplica a las aplicaciones del perfil de trabajo. Las aplicaciones del perfil personal no se ven afectadas.

Todo el dispositivo: La acción de bloqueo se aplica a todo el dispositivo, incluidas las aplicaciones del perfil personal.

Borrar tras X días

Número de días que la política es no conforme antes de que el dispositivo o el perfil de trabajo se borren.

Borrar tras X días debe ser superior a **Bloquear tras X días**. Solo es aplicable a dispositivos propiedad de la empresa.

Obligatorio. Predeterminado (nueva regla): **1**.

Rango permitido: 1–300.

Preservar la protección de restablecimiento de fábrica

Si se conservan los datos de protección contra restablecimiento de fábrica en el dispositivo. Este ajuste no se aplica a los perfiles de trabajo.

Predeterminado (nueva regla): activado.

Políticas - Apple

Políticas de Apple

Las políticas de Apple definen los ajustes de gestión que Cerberus Enterprise aplica a los dispositivos Apple a través de MDM. Estos ajustes se configuran desde el panel 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, lea la página de [Configuración de la gestión de Apple \(APNs\)](#).

Abra el editor de políticas de Apple

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

Diseño del editor

El editor de políticas de Apple está organizado como un conjunto de secciones expandibles. En la parte superior de la página, siempre puede editar:

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

Secciones de la política

Las siguientes secciones corresponden a los paneles disponibles actualmente en el editor de políticas de Apple:

- **Gestión de aplicaciones:** configure las restricciones relacionadas con aplicaciones y las aplicaciones gestionadas.

- **Ajustes de código de acceso:** configure los requisitos del código de acceso y las reglas relacionadas.
- **Seguridad:** controle funciones como el desbloqueo automático y el desbloqueo biométrico.
- **iCloud:** permite o prohíbe servicios específicos de iCloud (copia de seguridad, sincronización del llavero, relé privado, etc.).
- **Multimedia:** permite o prohíbe la cámara y funciones relacionadas.
- **Celular:** controla los ajustes relacionados con la red celular (ajustes de datos celulares de aplicaciones, eSIM, cambios de plan).
- **Redes:** controla AirDrop/AirPrint/AirPlay y otros ajustes de conectividad.
- **Cuentas:** restringe la modificación de cuentas y (opcionalmente) configura las cuentas de Google y de correo electrónico.

Muchas opciones en el Editor de políticas de Apple incluyen una descripción emergente que documenta los requisitos y las versiones de SO compatibles.

Guardar, eliminar y dispositivos asociados

Utilice **Guardar política** para aplicar sus cambios. El botón se desactiva cuando no hay ediciones 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 de **Dispositivos asociados** en la parte inferior, para que pueda ver cuántos dispositivos están utilizando la política actualmente.

Páginas siguientes

- **Código de acceso:** configure los requisitos del código de acceso y las opciones de seguridad relacionadas.
- **Restricciones:** defina las funciones permitidas y las limitaciones a nivel de SO.
- **Aplicaciones y perfiles:** configure las aplicaciones instaladas y los perfiles de configuración.

Política de Apple: Código de acceso

La sección de **Ajustes de código de acceso** controla los requisitos del código de acceso del dispositivo y las reglas de seguridad relacionadas (por ejemplo, longitud mínima y complejidad).

Opciones

En el Editor de políticas de Apple, las opciones del código de acceso se configuran mediante una combinación de interruptores y campos numéricos. Muchos campos incluyen descripciones emergentes que indican las versiones de SO compatibles y los requisitos de supervisión.

Interruptores de código de acceso

- **ChangeAtNextAuth:** obliga a restablecer la contraseña la próxima vez que el usuario se autentique.
- **RequireAlphanumericPasscode:** requiere al menos un carácter alfabético y un número.
- **RequireComplexPasscode:** requiere un código de acceso "complejo" (sin patrones repetitivos o secuenciales y al menos un carácter no alfanumérico).
- **RequirePasscode:** requiere un código de acceso sin requisitos adicionales de longitud o calidad. Nota: configurar otras claves de código de acceso requiere implícitamente un código de acceso.

Campos numéricos

- **FailedAttemptsResetInMinutes:** minutos antes de que se restablezca el contador de intentos fallidos (requiere MaximumFailedAttempts).
- **MaximumFailedAttempts:** intentos fallidos permitidos antes de que el dispositivo se borre o se bloquee (rango: 2-11).
- **MaximumGracePeriodInMinutes:** cuánto tiempo puede permanecer desbloqueado el dispositivo sin requerir el código de acceso (0 = ninguno).
- **MaximumInactivityInMinutes:** tiempo de inactividad antes de que el dispositivo se bloquee (rango: 0-15).

- **MaximumPasscodeAgeInDays:** edad máxima del código de acceso antes de un cambio forzado (rango: 0-730).
- **MinimumComplexCharacters:** número mínimo de caracteres "complejos" (rango: 0-4).
- **MinimumLength:** longitud mínima del código de acceso (rango: 0-16).
- **PasscodeReuseLimit:** longitud del historial de códigos de acceso para evitar la reutilización de códigos antiguos (rango: 1-50).

Política de Apple: Restricciones

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

Muchas restricciones solo son compatibles con versiones específicas del SO y pueden requerir dispositivos supervisados. Utilice las descripciones emergentes en el panel para conocer los requisitos oficiales.

Seguridad

- **Permitir desbloqueo automático**
- **Permitir huella dactilar para desbloqueo**
- **Permitir la modificación de huella dactilar**

iCloud

- **Permitir la libreta de direcciones de iCloud**
- **Permitir copia de seguridad en iCloud**
- **Permitir marcadores de iCloud**
- **Permitir el calendario de iCloud**
- **Permitir Escritorio y Documentos de iCloud**
- **Permitir la sincronización de documentos de iCloud**
- **Permitir Freeform de iCloud**
- **Permitir la sincronización de Llavero de iCloud**
- **Permitir Mail de iCloud**
- **Permitir Notas de iCloud**
- **Permitir la Fototeca de iCloud**
- **Permitir el Relé privado de iCloud**
- **Permitir Recordatorios de iCloud**

Multimedia

- **Permitir la cámara**
- **Permitir la modificación de uso compartido de archivos**
- **Permitir el acceso de la aplicación Archivos a unidades USB**

Celular

- **Permitir la modificación de datos celulares de la aplicación**
- **Permitir la modificación del plan celular**
- **Permitir la modificación de eSIM**
- **Permitir transferencias salientes de eSIM**

Redes

- **Permitir AirDrop**
- **Permitir solicitudes entrantes de AirPlay**
- **Permitir AirPrint**
- **Permitir el almacenamiento de credenciales de AirPrint**
- **Permitir el descubrimiento de iBeacon para AirPrint**
- **Permitir la modificación de Bluetooth**
- **Permitir la modificación del uso compartido de Bluetooth**
- **Permitir el acceso de la aplicación Archivos a unidades de red**
- **Permitir la modificación del uso compartido de Internet**

Cuentas (restricción)

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

- **Permitir la modificación de cuentas**

Política de Apple: Aplicaciones y perfiles

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

Gestión de aplicaciones

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

Restricciones generales de aplicaciones

- **Permitir App Clips**
- **Permitir la instalación de aplicaciones**
- **Permitir la eliminación de aplicaciones**
- **Permitir descargas automáticas de aplicaciones**
- **Permitir que se oculten las aplicaciones**
- **Permitir que se bloqueen las aplicaciones**
- **Permitir compras integradas**

Aplicaciones gestionadas

Utilice **Añadir aplicación** para añadir una aplicación a la política. Cada aplicación gestionada se muestra como una tarjeta. Puede ampliar la tarjeta para editar su configuración y eliminar la aplicación mediante la acción de eliminar.

- **ID de la App Store:** el identificador de la App Store de la aplicación gestionada.
- **ID del paquete:** el identificador del paquete de la aplicación.
- **Comportamiento de instalación:** controla si la aplicación debe permanecer instalada o si puede ser instalada/eliminada por el usuario.
- **Asignación:** tipo de asignación de licencia.
- **Licencia VPP:** tipo de licencia VPP utilizada para la instalación a través de la App Store.

Cuentas

El panel de **Cuentas** le permite configurar las cuentas que se aplican a los dispositivos gestionados. 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 de Apple o cuentas de internet.

Añadir cuentas

Utilice **Añadir cuenta de Google** o **Añadir cuenta de correo electrónico** 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 electrónico ofrecen un interruptor de **Credenciales de cuenta de los usuarios**. Cuando está habilitado, el sistema aplica las credenciales de la cuenta por cada usuario. Cuando está desactivado, usted introduce la identidad de la cuenta en la política.

Campos de la cuenta de Google

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

Campos de la cuenta de correo electrónico

Las cuentas de correo electrónico incluyen campos de identidad además de la configuración del servidor de entrada/salida. Los nombres de host son obligatorios.

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

Servidor de entrada

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

Servidor de salida

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

Opciones de S/MIME

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

Cifrado

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

Firma

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

Las opciones de cuenta y restricción incluyen descripciones emergentes en el panel que documentan los requisitos previos y las versiones de SO compatibles.

Estado del Dispositivo

Resumen del dispositivo

Abra un dispositivo desde **Dashboard** → **Dispositivos** haciendo clic en la fila del dispositivo. El título de la página muestra el **Modelo** del dispositivo (cuando está disponible) y su **Id** interno.

Datos históricos frente a inscripción actual

Cuando un dispositivo tiene múltiples inscripciones, Cerberus Enterprise puede mostrar un registro histórico de solo lectura. En ese caso, la página muestra un banner de **Datos históricos** y un botón para volver a los datos de la inscripción actual.

Campos superiores

La sección superior resume la identidad, asignación y el estado de gestión del dispositivo. Algunos campos son específicos de la plataforma y aparecen solo para dispositivos Android o Apple.

- **Id** y **Modelo**: identificadores de solo lectura.
- **Usuario**: muestra el usuario asignado actualmente (si lo hay). Desde el menú de usuario, puede **Abrir usuario** o **Cambiar usuario**, o asignar un usuario cuando no haya ninguno establecido.
- **Modo de gestión** y **Propiedad**: se muestran con descripciones emergentes en la interfaz de usuario.
- **Estado**: estado actual del dispositivo (con icono y detalles en la descripción emergente).
- **Perfil ADE** (solo Apple): muestra el perfil de inscripción automática de dispositivos asignado (si lo hay) y le permite abrirlo o cambiarlo.
- **Política**: muestra la política asignada y le permite abrirla o cambiarla, o asignar una cuando no haya ninguna establecida.
- **Estado de cumplimiento de la política** (cuando hay una política asignada): indica si el dispositivo cumple con la política.
- **Versión de la política** (cuando hay una política asignada): indica si el dispositivo tiene aplicada la versión más reciente de la política.
- **Inscrito el** y **Último informe de estado**: marcas de tiempo de la inscripción y del último estado reportado.
- **Dese inscrito el**: se muestra cuando el dispositivo ha sido desinscrito.

Algunos datos y paneles están disponibles solo cuando la categoría correspondiente está habilitada en la política del dispositivo. Para más información, lea las páginas de [Informes de estado](#) y [Ubicación y geocerca](#).

Paneles

El editor de dispositivos está organizado en secciones expandibles. Dependiendo de la plataforma y el estado, es posible que vea uno o más de los siguientes paneles:

- **Mapa de ubicación:** un panel con pestañas que contiene el historial de **Ubicación** del dispositivo actual y, en dispositivos Android, una pestaña de **Geocerca** para las transiciones de geocercas cuando los datos de la misma están disponibles.
- **Gestión de SIM** (solo Android): EID del dispositivo, SIM y eSIM instaladas e historial de comandos eSIM. Consulte la página dedicada de [Gestión de SIM](#).
- **Comandos:** envíe comandos al dispositivo y vea el historial de comandos (específico de la plataforma).
- **Estado de seguridad** (solo Android): postura, veredicto de Play Integrity y riesgos de seguridad.
- **Informes de aplicaciones** (solo Android): aplicaciones instaladas e informes de comentarios/errores.
- **Aplicaciones gestionadas** (solo Apple): estado de las aplicaciones gestionadas y detalles de instalación.
- **Detalles de incumplimiento:** se muestra cuando un dispositivo no cumple con la política; enumera los ajustes de la política que presentan incumplimiento.
- **Informes de estado:** datos adicionales reportados por el dispositivo, mostrados como un árbol de categorías y valores.
- **Historial de inscripción:** inscripciones anteriores para este mismo dispositivo físico, mostradas como una lista.

Pestañas del panel de ubicación

El panel de **Mapa de ubicación** ahora utiliza pestañas para que el historial de ubicación y las transiciones de geocerca se mantengan separados.

- **Ubicación:** muestra los filtros de historial, una búsqueda por rango de fechas, marcadores de ubicación, el círculo de precisión y los controles de seguimiento en vivo para el dispositivo actual.
- **Geocerca** (solo Android): muestra el historial de transiciones de geocercas en un mapa dedicado, con filtros de período, un interruptor opcional para geocercas archivadas y una lista lateral de transiciones.

Para conocer el comportamiento completo de estas pestañas, consulte [Mapa de ubicación](#).

Acciones

En la parte inferior de la página, puede actualizar los datos y realizar acciones dependiendo de la plataforma, el estado del dispositivo y el estado de la licencia.

- **Actualizar datos:** recarga el registro del dispositivo.
- **Deshabilitar dispositivo / Habilitar dispositivo** (solo Android): disponible en estados compatibles.
- **Desinscribir dispositivo:** elimina la gestión del dispositivo. El comportamiento exacto depende de la plataforma y la propiedad (por ejemplo, en Android se puede eliminar el perfil de trabajo o realizar un restablecimiento de fábrica).
- **Eliminar dispositivo:** disponible cuando el dispositivo ya ha sido desinscrito y su registro puede ser eliminado.

Gestión de SIM

En los dispositivos Android, el editor de Dispositivos ofrece un panel de **Gestión de SIM** para gestionar los perfiles de SIM y eSIM instalados en el dispositivo, añadir o eliminar perfiles eSIM y ver el historial de comandos eSIM enviados al dispositivo. Este panel solo está disponible para dispositivos Android.

Los dispositivos totalmente gestionados informan la información de la SIM cuando el reporte de **Información de red** está habilitado en la política del dispositivo (esta opción siempre está habilitada por Cerberus Enterprise). Consulte la página de [Reporte de estado](#).

EID del dispositivo

El EID (identificador eUICC) identifica el hardware de la eSIM del dispositivo. Los operadores lo utilizan para vincular los perfiles eSIM al dispositivo, por lo que recuperarlo suele ser el primer paso de un flujo de trabajo de aprovisionamiento de eSIM.

- **Dispositivos propiedad de la empresa** (Android 13 y versiones superiores): el EID se informa automáticamente con el estado del dispositivo y no requiere interacción del usuario.
- **Dispositivos de propiedad personal** (Android 13 y versiones superiores): utiliza el botón **Solicitar EID**. El usuario verá una notificación en el dispositivo solicitando compartir el EID, y podrá aprobar o rechazar la solicitud. El EID se muestra solo si el usuario lo aprueba. Mientras la solicitud esté pendiente, el botón permanecerá desactivado.

Al enviar una solicitud de EID se muestra primero un cuadro de diálogo de confirmación, ya que el usuario verá una notificación en el dispositivo.

SIM instaladas

La tabla de **SIM instaladas** enumera las SIM que se conocen actualmente para el dispositivo, incluidos los perfiles de SIM física y eSIM. En dispositivos de propiedad personal, los perfiles eSIM instalados con el comando **Añadir eSIM** se muestran incluso cuando el dispositivo no informa la

información de la SIM.

- **Operador:** el nombre del operador asociado a la SIM (cuando se informa).
- **Número de teléfono:** el número de teléfono asociado a la SIM (cuando se informa).
- **ICCID:** el Identificador de Tarjeta de Circuito Integrado de la SIM.
- **Estado de activación:** si la eSIM está activada o no. Se informa solo para las eSIM en Android 15 y versiones superiores.
- **Modo de configuración:** si la eSIM fue configurada por un administrador o por el usuario. Se informa solo para las eSIM en Android 15 y versiones superiores.
- **Tipo de SIM:** muestra si el dispositivo informa la entrada como una eSIM.

Las eSIM con un comando de eliminación en curso o ejecutado (que no haya fallado) muestran un estado de activación temporal de **Eliminando**. La entrada desaparece de la lista cuando el dispositivo informa la lista de SIM actualizada. Mientras una eliminación esté en curso, el botón de eliminar no estará disponible para evitar enviar el mismo comando dos veces.

Eliminar eSIM

Utilice el botón de eliminar junto a una eSIM instalada para eliminar su perfil del dispositivo. Un cuadro de diálogo le pedirá que confirme el ICCID de la eSIM que se va a eliminar antes de enviar el comando. La eliminación de una eSIM es compatible con Android 15 y versiones superiores.

Añadir eSIM

La sección **Añadir eSIM** instala un nuevo perfil eSIM en el dispositivo (compatible con Android 15 y versiones superiores). Requiere:

- **Validez:** cuánto tiempo es válido el comando si no puede ejecutarse inmediatamente.
- **Código de activación:** el código de activación para el perfil eSIM, proporcionado por el operador. Puede introducir el código completo o solo la dirección SM-DP+ para permitir que el dispositivo descubra un perfil que el operador ya haya vinculado a su EID.
- **Estado de activación:** si el perfil eSIM debe activarse automáticamente tras la descarga o si debe dejarse sin activar para que el usuario realice una activación manual.

Historial de comandos

Debajo de la sección Añadir eSIM, el panel muestra el historial de los comandos eSIM enviados al dispositivo: **Añadir eSIM**, **Eliminar eSIM** y **Solicitar EID**. La tabla se puede ordenar y admite

paginación. Algunas filas se pueden expandir para ver los parámetros del comando (por ejemplo, el código de activación o el ICCID) y el estado de ejecución, incluidos los detalles del error de la eSIM cuando una operación falla en el dispositivo.

- **Fecha de creación**
- **Comando**
- **Validez**
- **Estado**
- **Error:** muestra el estado de error de la eSIM (por ejemplo, *Usuario denegó*, *Código de activación no válido* o *ICCID no encontrado*) cuando la ejecución del comando lo informa.
- **Fecha de ejecución**

Borrar eSIM al borrar y desvincular

Cuando borras el dispositivo desde el panel de Comandos, la opción **Borrar eSIM** controla si los perfiles eSIM se eliminan con el borrado. En dispositivos de propiedad personal con un perfil de trabajo, esta opción está habilitada por defecto (se eliminan las eSIM gestionadas, pero no se ven afectadas las eSIM de propiedad personal). La misma opción está disponible en el cuadro de diálogo de confirmación **Desvincular dispositivo**.

Comandos

El editor de dispositivos proporciona un panel de **Comandos** para enviar comandos remotos a un dispositivo gestionado. Los comandos disponibles dependen de la plataforma (Android o Apple) y del estado del dispositivo.

Si el dispositivo no está conectado en este momento, el comando se enviará y ejecutará tan pronto como el dispositivo se conecte a Internet. Para los comandos de Android, puede configurar el parámetro **Validez** para determinar durante cuánto tiempo permanece válido un comando no entregado.

Comandos de Android (AMAPI)

Para los dispositivos Android, el panel de Comandos incluye un campo de **Validez** (valor + unidad) y un selector de **Comando**. Algunos comandos requieren parámetros adicionales, que aparecen dinámicamente al seleccionar el comando.

Parámetros comunes

- **Validez:** cuánto tiempo es válido el comando si no puede ejecutarse inmediatamente.
- **Comando:** elija qué acción enviar al dispositivo.

Comandos con campos adicionales

- **Restablecer contraseña:** requiere **Nueva contraseña** y **Confirmar nueva contraseña**. Los interruptores opcionales incluyen **Bloquear ahora**, **Requerir entrada** y **No solicitar credenciales al arrancar**.
- **Borrar datos de la aplicación:** requiere el **Nombre del paquete** de destino.
- **Iniciar modo de pérdida:** requiere un **Mensaje de pérdida** y admite campos de contacto opcionales (dirección, organización, número de teléfono, correo electrónico).
- **Borrar:** admite un **mensaje de motivo de borrado** (que se muestra a los usuarios en dispositivos personales) y marcadores de borrado opcionales, incluyendo **Borrar eSIM**.

Los comandos de eSIM (**Añadir eSIM**, **Eliminar eSIM**, **Solicitar EID**) están disponibles en el panel dedicado de **Gestión de SIM**.

Historial de comandos

Debajo de los controles de envío, el panel de control muestra una tabla con el historial de comandos. La tabla permite la ordenación y es paginada. Algunas filas se pueden expandir para ver parámetros adicionales o detalles de ejecución.

Columnas del historial de Android

- **Fecha de creación**
- **Comando**
- **Validez**
- **Estado**
- **Error**
- **Fecha de ejecución**

Comandos de Apple (MDM)

Para los dispositivos Apple, el panel de Comandos proporciona un selector de **Comando**. Algunos comandos requieren entradas adicionales. Al igual que con Android, se muestra una tabla de historial de comandos a continuación.

Comandos con campos adicionales

- **Instalar aplicación:** requiere el **ID del paquete** de la aplicación.
- **Enviar notificación:** requiere un **Mensaje de notificación** (longitud máxima de 200 caracteres).

Columnas del historial de Apple

- **Fecha de creación**
- **Comando**
- **Estado**
- **Hora de estado**

Actualizar

Utilice la acción de actualizar en el panel de Comandos para recargar el historial de comandos.

Mapa de ubicación

Esta página documenta las herramientas de ubicación específicas para dispositivos disponibles en [Información general del dispositivo](#). El panel contiene una pestaña de **Ubicación** para el historial de posición y, en dispositivos Android, una pestaña de **Geocerca** para las transiciones de geocerca.

Requisitos previos

Los datos de ubicación del dispositivo se muestran solo cuando el reporte de ubicación está habilitado en la política del dispositivo. Para habilitarlo, abra la política y active **Ubicación y geocerca** → **Reportar ubicación**. Para más detalles, consulte [Ubicación y geocerca](#).

En los dispositivos que no están totalmente gestionados, los datos de ubicación pueden seguir dependiendo de que la aplicación Cerberus Enterprise tenga los permisos de ubicación requeridos y de que los servicios de ubicación estén habilitados en el dispositivo.

Para el mapa global de múltiples dispositivos disponible desde el panel de control, consulte [Mapa de ubicación del panel de control](#).

Estado de carga y sin datos

- Mientras se cargan los datos de ubicación, el panel muestra una superposición de carga en el mapa.
- Si el dispositivo no tiene datos de ubicación disponibles, el panel muestra un mensaje que indica **No hay datos de ubicación disponibles** junto con un recordatorio para habilitar el reporte de ubicación en la política asignada.
- Si un filtro de fecha está activo y no hay muestras que coincidan, el panel muestra **No hay datos disponibles en el rango de fechas seleccionado**.

Pestaña de ubicación

Abra la pestaña de **Ubicación** para inspeccionar el historial de un solo dispositivo. Los filtros disponibles incluyen la última ubicación conocida, rangos de historial reciente, un rango de fechas personalizado y seguimiento en vivo.

- **Última:** muestra la última ubicación conocida.
- **Hoy, Últimos 7 días y Últimos 30 días:** muestran las ubicaciones registradas para el periodo seleccionado.
- **Buscar:** le permite elegir un rango de fechas personalizado.
- **En vivo:** inicia o detiene el seguimiento en vivo para el dispositivo actual.

Detalles del marcador

Al hacer clic en un marcador de ubicación, se abre una ventana de información con:

- La marca de tiempo del registro de ubicación.
- La **precisión** reportada (en metros).
- La **velocidad** reportada, cuando el dispositivo la proporciona.
- El **rumbo** o dirección reportada, cuando el dispositivo la proporciona.

Círculo de precisión

Cuando la ventana de información está abierta, se muestra un círculo de precisión alrededor del marcador. El radio del círculo corresponde a la precisión reportada (en metros). Al cerrar la ventana de información, el círculo se oculta.

Seguimiento en vivo

En la vista de historial del dispositivo, al seleccionar el filtro **En vivo** se inicia una solicitud de seguimiento en tiempo real para ese dispositivo específico. Cerberus Enterprise solicita confirmación antes de iniciar la solicitud.

- El seguimiento en vivo dura hasta **15 minutos**.
- El dispositivo muestra una notificación mientras el seguimiento en vivo está activo.
- Mientras el seguimiento en vivo está activo, el panel sigue actualizando la última ubicación y el indicador de en vivo permanece visible.
- Al seleccionar el filtro de en vivo nuevamente, puede detener el seguimiento en vivo antes de que finalice el tiempo de espera.

Pestaña de geocerca

En los dispositivos Android, la segunda pestaña muestra las transiciones de geocerca generadas a partir de las geocercas definidas en la política asignada. Esta pestaña está disponible cuando existen datos de geocerca para el dispositivo.

- El mapa muestra las áreas de geocerca actuales junto con los puntos de transición registrados.
- La lista de transiciones a la derecha le permite inspeccionar los eventos de **entrada** y **salida**.
- Los filtros disponibles son **Hoy**, **Últimos 7 días**, **Últimos 30 días** y una búsqueda personalizada por rango de fechas.
- **Incluir archivados** también muestra las transiciones relacionadas con definiciones de geocercas antiguas que ya no están presentes en la política actual.

Detalles de la transición de geocerca

Al seleccionar una transición se abren sus detalles en el mapa y se resalta la entrada correspondiente en la lista. Cuando está disponible, Cerberus Enterprise también muestra las coordenadas del dispositivo y la precisión reportada para esa transición.

Mapa de ubicación del panel de control

El mapa de ubicación del panel de control proporciona una vista global de la última posición conocida de los dispositivos que informan datos de ubicación. Ábralo desde **Panel de control** para revisar múltiples dispositivos en el mismo mapa de Google.

Requisitos previos

Un dispositivo aparece en este mapa solo cuando el reporte de ubicación está habilitado en su política asignada. Para habilitarlo, abra la política y active **Ubicación y geocerca** → **Reportar ubicación**. Para más detalles, consulte [Ubicación y geocerca](#).

En los dispositivos que no están totalmente gestionados, los datos de ubicación pueden seguir dependiendo de que la aplicación Cerberus Enterprise tenga los permisos de ubicación requeridos y de que los servicios de ubicación estén habilitados en el dispositivo.

Para el historial por dispositivo y las transiciones de geocerca disponibles en el editor de dispositivos, consulte [Mapa de ubicación](#).

Estado de carga y sin datos

- Mientras se cargan los datos de ubicación, el mapa muestra una superposición de carga.
- Si actualmente ningún dispositivo tiene datos de ubicación disponibles, la página muestra un mensaje de **No hay datos de ubicación disponibles**.

Marcadores y grupos

Cada dispositivo con datos de ubicación disponibles se muestra como un marcador. Cuando muchos dispositivos están cerca unos de otros, los marcadores se agrupan automáticamente para

mantener la legibilidad del mapa.

Los dispositivos que se encuentran actualmente en seguimiento en vivo se resaltan con un marcador animado para que sean más fáciles de localizar en el mapa.

Controles del mapa

Cuando el mapa contiene ubicaciones de dispositivos, Cerberus Enterprise muestra botones de acción en la esquina superior derecha del mapa.

- **Ubicación actual:** utiliza la ubicación de su navegador para mover el mapa a su posición actual y ajustar el área de precisión reportada.
- **Recentrar mapa:** ajusta el mapa nuevamente alrededor de los marcadores de dispositivos que se muestran actualmente.
- **Rastreado** indicador de seguimiento en vivo: aparece cuando uno o más dispositivos están siendo rastreados en vivo y muestra cuántos están activos actualmente.
- **Detener todo el seguimiento en vivo:** el botón de icono dentro del indicador de seguimiento en vivo detiene el seguimiento en vivo de todos los dispositivos rastreados actualmente tras la confirmación.

Detalles del marcador

Al hacer clic en un marcador se abre una ventana de información con:

- El **Modelo** y el **ID** interno del dispositivo.
- La marca de tiempo de la última ubicación reportada.
- La **precisión** reportada en metros.
- La **velocidad** reportada, cuando está disponible.
- El **rumbo** o dirección reportada, cuando está disponible.

El identificador del dispositivo en la ventana de información es un enlace que abre la página de [Información general del dispositivo](#).

Acciones de la ventana de información

Cada ventana de información también incluye botones de acción para el dispositivo seleccionado.

- **Enlace del dispositivo:** el nombre y el ID del dispositivo en la parte superior de la ventana de información abren la página de información general correspondiente del dispositivo.
- **Acercar zoom:** centra el mapa en el dispositivo seleccionado y ajusta el círculo de precisión reportada más estrechamente alrededor de este.
- **En vivo:** inicia el seguimiento en vivo para ese dispositivo. Si el seguimiento en vivo ya está activo, el mismo botón lo detiene tras la confirmación.
- **Seguimiento en vivo activo:** cuando está presente, esta línea de estado indica que el dispositivo seleccionado ya se está rastreando en tiempo real.

Círculo de precisión

Cuando se selecciona un marcador, el mapa muestra un círculo de precisión alrededor de la ubicación. El radio del círculo coincide con la precisión reportada.

Comportamiento del seguimiento en vivo

Iniciar el seguimiento en vivo desde una ventana de información envía una solicitud de seguimiento en tiempo real a ese dispositivo. Cerberus Enterprise refresca entonces el mapa automáticamente mientras la sesión esté activa.

- Cada sesión de seguimiento en vivo dura hasta **15 minutos**.
- El dispositivo muestra una notificación mientras el seguimiento en vivo está activo.
- El seguimiento en vivo se puede detener ya sea desde la ventana de información del dispositivo seleccionado o desde el botón global de **Detener todo el seguimiento en vivo** en el mapa.

Aplicaciones privadas

Desde esta sección del panel, puede cargar sus propias aplicaciones privadas de Android o crear aplicaciones web para distribuirlas en sus dispositivos.

Los únicos detalles que debe proporcionar son el título de la aplicación y su APK. Las aplicaciones privadas se aprueban automáticamente para su organización y suelen estar listas para su distribución en 10 minutos. Puede cargar un total de 15 aplicaciones privadas al día. Tenga en cuenta que las aplicaciones web también cuentan para este total.

La primera vez que publique una aplicación privada, deberá proporcionar una dirección de correo electrónico para recibir notificaciones de la Play Console sobre sus aplicaciones y su cuenta de desarrollador de Google Play. Además, Managed Play crea automáticamente una cuenta de desarrollador de Play en nombre de su organización. No es necesario pagar ninguna cuota de registro por esta cuenta.

Aplicaciones privadas publicadas desde el iframe:

- No están sujetas a los mismos controles que otras aplicaciones. Como resultado, no pueden convertirse en aplicaciones públicas.
- No son transferibles. No puede transferir la propiedad de una aplicación a una cuenta de desarrollador de Play diferente.

Para más detalles, visite la [Ayuda de Managed Google Play](#)

Gestión de certificados

El panel de control incluye una sección de **Certificados** para importar, ver y eliminar certificados. Al hacer clic en una fila de certificado se abre el editor de certificados.

Lista de certificados

Los certificados se muestran en una tabla paginada y con capacidad de ordenación. La lista incluye tanto certificados de cliente como Autoridades de Certificación (CA).

Filtros

En la parte superior de la página, puede activar los filtros utilizando la lista de chips. Algunos filtros son mutuamente excluyentes.

- **Todos:** muestra todos los certificados.
- **Cliente:** muestra solo los certificados de cliente.
- **Autoridad de certificación (CA):** muestra solo los certificados de CA.
- **Buscar:** muestra un campo de texto (etiqueta **Nombre o nombre de archivo**) para buscar por el nombre del certificado o el nombre de archivo importado.
- **Sin usuario:** muestra los certificados de cliente que no están asociados a ningún usuario.

Columnas de la tabla

- **Nombre**
- **Tipo**
- **Vencimiento**
- **Usuario** (se muestra para los certificados de cliente)
- **Nombre de archivo importado**
- **Fecha de importación**

Acciones

- **Abrir certificado:** haga clic en una fila para abrir el editor de certificados.
- **Eliminar certificado:** disponible solo cuando el certificado no está asociado a usuarios/políticas y no es utilizado por dispositivos. La acción también puede estar

deshabilitada cuando la licencia ha vencido.

- **Selección de varias filas:** puede activar la selección de varias filas para eliminar múltiples certificados a la vez. Solo se pueden seleccionar los certificados que se pueden eliminar.
- **Actualizar:** recarga la lista de certificados.

Importar certificados

Para importar certificados, haga clic en **Importar certificado** y seleccione uno o más archivos. Los formatos compatibles se muestran en la descripción emergente del botón de importación.

Clientes

Formato compatible: PKCS#12 codificado en Base64 (.p12 / .pfx).

Los certificados de cliente identifican a un usuario o a un dispositivo en la red de la empresa. Los certificados de cliente pueden estar asociados a un usuario específico.

Cada certificado de cliente puede asignarse opcionalmente a un usuario específico: esto permite implementar la misma configuración de Wi-Fi EAP en muchos dispositivos. Puede hacerlo en la sección de [configuración de red](#) de la política, utilizando la opción **credenciales EAP de los usuarios**.

Alternativamente, puede asignar un certificado a un usuario desde la página de **Usuarios**.

Autoridades de certificación (CA)

Formatos compatibles: X.509 codificado en Base64 (.crt / .pem / .cer / .der).

Los certificados de CA identifican a una Autoridad de Certificación e indican al dispositivo que debe confiar en cualquier certificado emitido por dicha CA. El panel de control valida que un certificado X.509 importado sea una CA.

Editor de certificados

Cuando abre un certificado, el editor muestra sus campos principales y un panel de **Información del certificado** de solo lectura.

Campos principales

- **Nombre** (obligatorio)
- **ID** (solo lectura)
- **Tipo** (solo lectura)
- **Vencimiento** (solo lectura)
- **Fecha de importación** (solo lectura)
- **Nombre de archivo importado** (solo lectura)

Asociación de usuario (certificados de cliente)

Para los certificados de **Cliente**, el editor muestra un campo de **Usuario**. Si hay un usuario asignado, un menú le permite **Abrir usuario**, **Cambiar usuario** o **Desasociar usuario**. Si no hay ningún usuario asignado, puede asignar uno utilizando el botón de acción de usuario.

Eliminar certificado

La acción de eliminar se deshabilita cuando el certificado está asociado actualmente a un usuario o se utiliza en políticas. También puede estar deshabilitada cuando la licencia ha vencido.

Reglas de eventos

Las reglas de eventos le permiten automatizar las reacciones ante eventos de dispositivos compatibles. Abra **Panel de control** → **Reglas de eventos** para crear reglas que supervisen los eventos de inscripción, desinscripción, incumplimiento y geovalla de Android, para luego activar una o más acciones automáticamente.

Qué puede hacer una regla de eventos

Cada regla combina un **sujeto**, un **evento** y una o dos **acciones**. Los sujetos compatibles son **Todos los dispositivos**, **Dispositivo específico** y **Política**.

- **Eventos:** inscripción de dispositivo, desinscripción de dispositivo, el dispositivo deja de cumplir con las políticas, entrada en la geovalla y salida de la geovalla.
- **Acciones del dispositivo:** deshabilitar dispositivo, habilitar dispositivo, bloquear dispositivo.
- **Acción de correo electrónico:** enviar un correo electrónico de notificación a los administradores y, cuando esté habilitado, a los gestores delegados.

Una regla puede contener únicamente una acción de correo electrónico, únicamente una acción del dispositivo, o bien una acción del dispositivo más una acción de correo electrónico. Si se configuran ambas acciones, Cerberus Enterprise ejecutará primero la acción del dispositivo y después la acción de correo electrónico.

Reglas de plataforma y compatibilidad

Los eventos y las acciones disponibles dependen del sujeto seleccionado y de la plataforma que se aplique a dicho sujeto.

- **Android** admite eventos de inscripción, desinscripción, incumplimiento y geovalla.
- **Apple** admite eventos de inscripción, desinscripción e incumplimiento.

- **Deshabilitar dispositivo** y **Habilitar dispositivo** son acciones exclusivas de Android.
- **Bloquear dispositivo** y **Enviar correo electrónico** están disponibles tanto en Android como en Apple, cuando el evento seleccionado los permite.
- **Desinscripción de dispositivo** solo admite acciones de correo electrónico.

Lista de reglas

La lista de reglas de eventos es la página principal de gestión para esta función. Incluye una tabla con buscador que contiene el nombre de la regla, el sujeto, el evento, las acciones, la plataforma, el estado de activación y la hora de actualización.

- Utilice las etiquetas de filtro para alternar entre todas las reglas, reglas activadas, reglas deshabilitadas y búsqueda de texto.
- Utilice el botón **Actualizar** para recargar la vista actual de la tabla.
- Utilice el interruptor de activación en cada fila para habilitar o deshabilitar temporalmente una regla.
- Utilice el modo de selección de varias filas para eliminar varias reglas a la vez.
- Utilice **Crear regla de eventos** para abrir el editor de una nueva regla.

Editor de reglas

El editor se divide en las secciones de **General**, **Alcance**, **Activador** y **Acciones**. En la parte inferior de la página, una barra de acciones fija mantiene visibles los botones principales mientras se desplaza.

General

- **Nombre:** obligatorio, hasta 150 caracteres.
- **Descripción:** opcional, hasta 2000 caracteres.
- **Regla activada:** guarda la regla en estado activado o deshabilitado.

Alcance

El alcance define a qué dispositivos puede aplicarse la regla. El editor también muestra la plataforma resuelta y, cuando está disponible, el contexto de política efectivo.

- **Todos los dispositivos:** la regla puede aplicarse a todos los dispositivos compatibles en la empresa.

- **Dispositivo específico:** seleccione un dispositivo gestionado en el cuadro de diálogo de selección.
- **Política:** seleccione una plantilla de política en el cuadro de diálogo de selección.

Activador

La sección de activador filtra automáticamente los eventos disponibles basándose en el alcance y la plataforma seleccionados.

Activadores de geovalla

Las reglas de entrada y salida de geovalla solo son compatibles con Android y requieren un contexto de política de Android válido. Para información sobre el informe de ubicación y las definiciones de geovalla, consulte [Ubicación y geovalla](#).

- Si el sujeto es **Todos los dispositivos**, la regla siempre se aplica a **Cualquier geovalla**.
- Si el sujeto es un dispositivo o una política, puede elegir **Cualquier geovalla** o una **Geovalla específica**.
- La lista de geovallas específicas se carga desde el contexto de política efectivo del dispositivo o la política seleccionados.

Acciones

La sección de acciones le permite elegir una acción del dispositivo opcional y una notificación por correo electrónico opcional. La interfaz oculta automáticamente las combinaciones no compatibles.

- Si no hay ninguna acción de dispositivo disponible para el evento y el alcance seleccionados, aún puede guardar una regla que consista únicamente en un correo electrónico.
- Si el correo electrónico está deshabilitado para el evento y la plataforma seleccionados, el interruptor de correo electrónico no estará disponible.
- Una regla sin ninguna acción no es válida y no se puede guardar.

Destinatarios del correo electrónico

Las acciones de correo electrónico siempre incluyen a los usuarios de la empresa con el rol de **ADMIN**. Si la empresa se gestiona mediante multiinquilinato, puede ampliar los destinatarios para incluir a los gestores de MT.

- **Solo gestores principales:** incluye a los administradores de la empresa y a los contactos principales de gestión de MT.
- **Gestores principales y gestores de subcuentas:** añade también a los gestores de subcuentas asignados.
- La lista de vista previa muestra las direcciones de correo electrónico reales que se utilizarán cuando se ejecute la regla.
- Solo se incluyen en la lista de destinatarios finales los gestores delegados que tengan acceso concedido a la empresa.

Comportamiento de ejecución

Las reglas de eventos se ejecutan inmediatamente cuando Cerberus Enterprise recibe un evento compatible de las integraciones del backend. Las reglas deshabilitadas se omiten automáticamente.

Las ejecuciones exitosas y fallidas se registran en el registro del sistema con mensajes legibles para los humanos.

Dispositivos

Dispositivos

La sección de **Dispositivos** del panel de control (*Panel de control* → *Dispositivos*) muestra todos los dispositivos inscritos en su cuenta. Desde esta página, puede filtrar la lista, abrir el registro de un dispositivo y realizar acciones como deshabilitarlo o desinscribirlo.

Filtros

En la parte superior de la página, puede activar uno o más filtros utilizando la lista de etiquetas. Las etiquetas seleccionadas representan los filtros que están activos actualmente.

Filtros disponibles

- **Todos:** muestra todos los dispositivos.
- **Android:** muestra solo dispositivos Android.
- **Apple:** muestra solo dispositivos Apple.
- **De propiedad de la empresa:** muestra solo dispositivos de propiedad de la empresa.
- **De propiedad personal:** muestra solo dispositivos de propiedad personal.
- **Propietario del perfil:** muestra solo dispositivos con perfil de trabajo de Android.
- **Propietario del dispositivo:** muestra solo dispositivos Android con gestión total.
- **Activo:** muestra los dispositivos en estado activo.
- **Cumple con las políticas:** muestra los dispositivos que cumplen con las políticas.
- **No cumple con las políticas:** muestra los dispositivos que no cumplen con las políticas.
- **Seguro:** muestra los dispositivos con una postura de seguridad.
- **No seguro:** muestra los dispositivos con una postura de seguridad no satisfactoria.
- **Política no actualizada:** muestra los dispositivos que tienen cambios de política pendientes.
- **Estado no actualizado:** muestra los dispositivos que no han informado su estado en las últimas 72 horas.
- **Error de aplicaciones:** muestra los dispositivos cuyas aplicaciones han enviado comentarios de error.
- **Buscar:** activa un campo de búsqueda de texto.

Buscar

Cuando activa el filtro de **Buscar**, aparece un campo de texto con la etiqueta **ID, modelo o usuario**. La lista se actualiza automáticamente tras dejar de escribir.

Tabla de dispositivos

Los dispositivos se muestran en una tabla paginada y con capacidad de ordenación. Al hacer clic en una fila, se abrirá el editor del dispositivo.

Columnas

- **ID**: identificador interno del dispositivo.
- **MDM**: plataforma (Android o Apple).
- **Modelo**: modelo del dispositivo.
- **Propiedad**: de la empresa o personal (con detalles en el cuadro informativo).
- **Modo de gestión**: modo de gestión (con detalles en el cuadro informativo).
- **Política**: política asignada actualmente.
- **Usuario**: usuario asociado (nombre, correo electrónico o ID, según disponibilidad).
- **Último informe de estado**: marca de tiempo del informe de estado más reciente (cuando esté disponible).
- **Estado**: estado del dispositivo (con detalles en el cuadro informativo).
- **Cumplimiento**: indicador del estado de cumplimiento.
- **Seguridad**: postura de seguridad (con detalles en el cuadro informativo).
- **Error de aplicaciones**: indicador de errores en las aplicaciones.

Actualización y paginación

- Utilice la acción de actualizar para recargar la lista.
- La tabla está paginada (10/25/50 elementos por página).

Acciones de los dispositivos

Cada fila de dispositivo puede ofrecer acciones, dependiendo de la plataforma y el estado del dispositivo. Algunas acciones se deshabilitan cuando su licencia ha caducado o ha sido rescindida.

Acciones por dispositivo

- **Deshabilitar dispositivo / Habilitar dispositivo:** disponible para dispositivos Android en estados compatibles.
- **Desinscribir dispositivo:** elimina la gestión. En Android, esto puede borrar el perfil de trabajo o restablecer los valores de fábrica (según la propiedad); en Apple, esto elimina los ajustes de las políticas.
- **Eliminar dispositivo:** disponible para dispositivos que ya han sido desinscritos (elimina el registro del sistema).

Selección de varias filas

Puede activar la selección de varias filas desde la barra de acciones situada debajo de la tabla. Cuando esté activada, podrá seleccionar varias filas y aplicar acciones masivas (deshabilitar, habilitar, desinscribir o eliminar), dependiendo de qué dispositivos se seleccionen.

Sincronización con Apple Business Manager

Si la gestión de Apple está configurada y existe un token de inscripción automática de dispositivos, es posible que la página muestre la acción **Sincronizar desde ABM** para importar dispositivos desde Apple Business Manager.

Inscribir un dispositivo

Utilice **Inscribir un dispositivo** para abrir la sección de tokens de inscripción y comenzar a inscribir un nuevo dispositivo.

Usuarios

Usuarios

La sección **Usuarios** del dashboard (*Dashboard* → *Usuarios*) enumera todos los usuarios configurados en su cuenta. Desde esta página, puede buscar usuarios, abrir el editor de usuarios, crear nuevos usuarios y eliminar usuarios que no estén asociados actualmente con dispositivos.

Buscar

En la parte superior de la página hay un campo de búsqueda con la etiqueta **Buscar** y el marcador de posición **Nombre, nombre de usuario o correo electrónico**. La lista se actualiza automáticamente después de dejar de escribir.

Tabla de usuarios

Los usuarios se muestran en una tabla paginada y con capacidad de ordenación. Al hacer clic en una fila, se abre el editor de usuarios.

Columnas

- **ID**: identificador interno de usuario.
- **Nombre**: nombre del usuario.
- **Apellido**: apellido del usuario.
- **Nombre de usuario**: nombre de usuario (a menudo el nombre de usuario del directorio).
- **Correo electrónico**: dirección de correo electrónico del usuario.
- **Dispositivos**: número de dispositivos asociados actualmente con el usuario.
- **Certificado Wi-Fi**: indicador que muestra si se ha asignado un certificado Wi-Fi al usuario.

Actualización y paginación

- La acción de actualizar recarga la lista.
- La tabla está paginada (10/25/50 elementos por página).

Acciones de usuario

Crear nuevo usuario

Utilice **Crear nuevo usuario** para abrir el cuadro de diálogo de creación de usuario. Esta acción se deshabilita cuando su licencia ha caducado.

Sincronizar desde Google Workspace

Si la sincronización de directorios de Google Workspace está disponible para su cuenta, la página muestra **Sincronizar desde Google Workspace**. Cuando inicia una sincronización, se muestra un indicador de progreso mientras la solicitud se está ejecutando.

Eliminar un usuario

Puede eliminar un usuario solo cuando este no esté asociado a ningún dispositivo (la columna **Dispositivos** debe ser 0). La acción de eliminar se deshabilita cuando su licencia ha caducado o ha sido cancelada.

Selección de varias filas y eliminación masiva

Desde la barra de acciones debajo de la tabla, puede habilitar la selección de varias filas. En este modo, puede seleccionar varios usuarios y eliminarlos de forma masiva.

- **Elegibilidad:** solo los usuarios con **Dispositivos** = 0 pueden seleccionarse para su eliminación.
- **Seleccionar todo:** la casilla de verificación **Todo** selecciona todas las filas elegibles en la página actual.
- **Eliminación masiva:** **Eliminar usuarios seleccionados** se deshabilita cuando no hay filas seleccionadas, o cuando su licencia ha caducado o ha sido cancelada.

Certificados Wi-Fi y EAP

La columna **Certificado Wi-Fi** muestra si actualmente hay un certificado asignado a un usuario. Los certificados de usuario se utilizan normalmente para configuraciones de Wi-Fi EAP (por

ejemplo, EAP-TLS). Para la asignación y gestión de certificados, consulte [Gestión de certificados](#).

Editor de usuarios

El editor de usuarios está disponible desde *Dashboard* → *Usuarios* al hacer clic en una fila de usuario. Permite editar los detalles del usuario, configurar las credenciales EAP de Wi-Fi por usuario y ver los dispositivos asociados al usuario.

Detalles del usuario

La sección superior contiene los campos principales del usuario. Algunos campos son obligatorios y el editor muestra errores de validación cuando faltan o no son válidos.

- **ID:** identificador de solo lectura.
- **Nombre:** obligatorio.
- **Apellido:** obligatorio.
- **Nombre de usuario:** obligatorio.
- **Correo electrónico:** obligatorio y debe ser una dirección de correo electrónico válida.
- **Número de teléfono:** opcional.
- **Cuenta de Google:** opcional y debe ser una dirección de correo electrónico válida cuando se proporcione.

Política predeterminada de autenticación de Google

En entornos de Google Workspace con la autenticación de Google habilitada, el editor puede mostrar **Política predeterminada de autenticación de Google**. Esta es la política aplicada a los dispositivos registrados mediante la autenticación de Google por este usuario.

- **Cambiar política:** abre el cuadro de diálogo de selección de política.
- **Abrir política:** abre la política seleccionada en el editor de políticas (cuando hay una política establecida).
- Después de seleccionar una nueva política predeterminada, debe guardar al usuario para aplicar el cambio. El editor muestra una notificación recordándole que debe guardar.

Credenciales EAP de Wi-Fi

La sección **Credenciales EAP de Wi-Fi** se utiliza para configurar credenciales por usuario que se instalan automáticamente en los dispositivos del usuario cuando su política asignada contiene una configuración de Wi-Fi EAP que las requiere. La configuración de Wi-Fi EAP es parte de la [configuración de red](#) de la política de Android.

Certificado de cliente

Puede asignar opcionalmente un certificado de cliente a un usuario. Cuando se asigna un certificado, este aparece en el campo **Certificado de cliente** y un menú ofrece acciones. Cuando no se ha asignado ningún certificado, el campo muestra **Sin certificado asignado** y puede asignar uno.

- **Asignar certificado:** abre el cuadro de diálogo de selección de certificado.
- **Abrir certificado:** abre el editor de certificados.
- **Cambiar certificado:** selecciona un certificado de cliente diferente.
- **Desasociar certificado:** elimina el certificado del usuario. El sistema también elimina el certificado de todos los dispositivos asociados con este usuario.

Para la importación y gestión de certificados, consulte [Gestión de certificados](#).

Identidad, identidad anónima y contraseña

- **Identidad:** identidad del usuario. Para protocolos de túnel externos (PEAP, EAP-TTLS), esta se utiliza dentro del túnel.
- **Identidad anónima:** se utiliza para protocolos de túnel externos como la identidad presentada fuera del túnel. Cuando no se especifica, el valor predeterminado es una cadena vacía.
- **Contraseña:** la contraseña del usuario para los métodos EAP que la requieran. Si no se especifica, el dispositivo puede solicitarla al usuario. Una acción de mostrar/ocultar alterna la visibilidad de la contraseña.

Dispositivos asociados

La sección **Dispositivos asociados** muestra la lista de dispositivos vinculados actualmente al usuario. Si el usuario tiene uno o más dispositivos asociados, no se podrá eliminar al usuario.

Guardar y eliminar

- **Guardar usuario:** se habilita solo cuando el formulario es válido, hay cambios pendientes y la licencia está activa. Se muestra un indicador de progreso durante el guardado.
- **Eliminar usuario:** se deshabilita cuando el usuario está asociado a dispositivos o cuando la licencia ha caducado o ha sido cancelada. Cuando se permite la eliminación, se muestra un cuadro de diálogo de confirmación. Si el usuario está asignado a tokens de registro, el cuadro de diálogo advierte que los dispositivos registrados con esos tokens ya no estarán asignados a un usuario.

Advertencia de cambios no guardados

Si tiene cambios sin guardar e intenta salir de la página, el dashboard le preguntará si desea descartar los cambios.

Cuenta

Configuración

La página de **Configuración** (*Dashboard* → *Configuración*) resume la información de la cuenta y de las licencias, y ofrece acciones para gestionar la facturación, la configuración de la plataforma (Android Management y Apple Management) e integraciones opcionales de directorios o tokens.

Banner de licencia (por vencer / vencida)

Cuando su licencia esté **por vencer**, **vencida** o **cancelada**, se mostrará un banner destacado en la parte superior de la página. Dependiendo del estado de su suscripción, ofrecerá una acción de **Gestionar facturación** (portal de clientes de Stripe) o una acción de **Comprar licencia**.

Cuando la licencia ha vencido, el acceso de la cuenta se limita únicamente a la desvinculación de dispositivos. Tras el periodo de gracia, la cuenta puede ser cancelada y los dispositivos pueden desvincularse automáticamente.

Acceso de administrador de la empresa

La tarjeta **Acceso de administrador de la empresa** solo se muestra para las empresas gestionadas por una cuenta multi-tenancy (por ejemplo, un proveedor de servicios gestionados). Permite ver qué cuentas de administrador pueden operar en tu empresa y controlar su acceso.

La tarjeta muestra:

- El **propietario** de la empresa. El propietario siempre tiene acceso y su acceso no se puede revocar.
- Cada cuenta de administrador de la cuenta multi-tenancy, indicada como **Administrador principal** o **Subcuenta**, con su nombre, nombre de usuario y estado de acceso (**Otorgado**, **Revocado** o **No otorgado**).

Otorgar y revocar el acceso

Usa **Otorgar** para permitir que una cuenta de administrador acceda a tu empresa y la gestione, y **Revocar** para retirar ese acceso. Cada acción solicita confirmación. Un administrador cuyo acceso se ha revocado ya no puede operar en la empresa, aunque esté trabajando en ella en ese momento.

- Como administrador de la empresa, puedes otorgar o revocar el acceso a cualquier cuenta de administrador de la lista.
- El administrador principal puede otorgar o revocar el acceso a sus propias subcuentas, pero solo mientras su propio acceso esté otorgado. No puede otorgarse acceso a sí mismo ni revocar su propio acceso.

Revocar el acceso al **Administrador principal** también revoca el acceso de todas sus subcuentas. En ese caso, el diálogo de confirmación muestra las subcuentas que perderán el acceso.

Información de la cuenta

La tarjeta de **Información de la cuenta** muestra campos de solo lectura:

- **Nombre de usuario**
- **Nombre de la empresa**
- **ID de la empresa**

Cambiar contraseña

Si no has iniciado sesión con Google, Apple o Microsoft, la tarjeta también muestra una acción de **Cambiar contraseña**. Esto abre un cuadro de diálogo para continuar con el flujo de cambio de contraseña.

También puedes cambiar tu contraseña en cualquier momento desde el menú de usuario de la barra superior, con **Cambiar contraseña**. Esto es útil para las cuentas multi-tenancy, que pueden cambiar su contraseña sin entrar en una empresa.

Si un administrador creó tu cuenta o restableció tu contraseña, inicias sesión con una contraseña temporal y debes elegir una nueva contraseña antes de continuar.

Información de la licencia

La tarjeta de **Información de la licencia** muestra el estado actual de la licencia y su límite de dispositivos. También ofrece acciones para contactar con ventas, gestionar la facturación o comprar una licencia.

- **Estado de la licencia:** se muestra como **Activa** o **Caducada** (con un icono de insignia y descripción emergente).
- **Prueba gratuita:** se muestra cuando la cuenta se encuentra actualmente en modo de prueba.
- **Dispositivos con licencia:** número máximo de dispositivos permitidos por la licencia. El enlace *¿necesita más dispositivos?* abre un mensaje para contactar con soporte.
- **Próxima renovación programada:** se muestra para las suscripciones activas que se renuevan automáticamente. De lo contrario, la tarjeta muestra la **fecha de vencimiento**.

Gestión de Android

La tarjeta de **Gestión de Android** muestra el estado de la gestión de Android para su empresa. Si aún no se ha configurado la Gestión de Android, la tarjeta ofrece una acción de **Configurar la gestión de Android** que abre el flujo de configuración.

Estado configurado

Cuando la Gestión de Android está configurada, la tarjeta puede mostrar:

- **ID de gestión**
- **Tipo de vinculación:** identifica si la empresa utiliza una **cuenta de Managed Google Play** o un **dominio de Managed Google**.
- **Sincronizado con Google Workspace** (distintivo que se muestra cuando la sincronización del directorio está activa)
- **Sincronizar con Google Workspace** (se muestra cuando la sincronización del directorio no está configurada; abre el panel de instrucciones en la parte inferior de la página)

Vinculación de Android Enterprise

Android Management puede asociarse con una **cuenta de Managed Google Play** o un **dominio de Managed Google**. El campo **Tipo de vinculación** muestra qué opción está asociada actualmente con su empresa.

Una **cuenta de Managed Google Play** es una cuenta ligera de Android Enterprise. Es adecuada para gestionar dispositivos y aplicaciones Android a través de Cerberus Enterprise, pero es independiente de una organización de Google Workspace o Cloud Identity. No proporciona la experiencia de administración centralizada de Google que está disponible con un dominio de Managed Google.

Un **dominio de Managed Google** asocia Android Enterprise con la identidad de Google de su organización. Los administradores de TI pueden gestionar productos de Google como Google Workspace, Cloud Identity y Gemini desde la consola de administración de Google, mientras continúan gestionando aplicaciones y políticas de Android en Cerberus Enterprise. Esto proporciona un enfoque más ágil e integrado para la gestión de Android y permite flujos de trabajo de inscripción y gestión de usuarios basados en Google Workspace.

Cuando la empresa utiliza una cuenta de Managed Google Play, la tarjeta de Ajustes ofrece **Actualizar a un dominio de Managed Google** y una acción de información. La actualización abre el proceso guiado de Google para trasladar la cuenta de Android Enterprise existente a un dominio gestionado.

Durante la actualización, Google puede vincular una cuenta de Google Admin existente asociada a su dirección de correo electrónico de trabajo o crear automáticamente una nueva cuenta gratuita de Google Admin. Utilice una dirección de correo electrónico de trabajo como *nombre@empresa.com* para continuar con la configuración guiada de Google.

Gestión de dispositivos Apple

La tarjeta de **Gestión de dispositivos Apple** muestra el estado de la gestión de dispositivos Apple (MDM) para su empresa. Si la gestión de Apple aún no se ha configurado, la tarjeta ofrece la acción **Configurar gestión de Apple** que abre el flujo de configuración.

Estado configurado

Cuando la gestión de Apple está configurada, la tarjeta puede mostrar:

- **ID de Apple**
- **Vencimiento del certificado de Apple Push:** muestra la fecha de vencimiento y un distintivo con icono. Si el certificado está próximo a vencer o ya ha vencido, el distintivo es clicable y abre las instrucciones de renovación.
- **Vencimiento del token de ABM:** muestra el vencimiento del token de Apple Business Manager (con un distintivo clicable cuando se requiere una acción).
- **Token VPP:** muestra el nombre de la organización y el vencimiento del token del Apple Volume Purchase Program (con un distintivo clicable cuando se requiere una acción).

- **Portal de Apple Business Manager:** enlace que se muestra cuando hay un token de ABM presente.
- **Sincronizar con Apple Business Manager y Sincronizar con Apple Volume Purchase Program:** se muestran cuando faltan tokens.

La gestión de Apple requiere la configuración del certificado APNs. Si es necesario, consulte [Configuración de la gestión de Apple \(APNs\)](#).

Preferencias y privacidad

La tarjeta de **Preferencias y privacidad** contiene un interruptor de preferencias de marketing y enlaces a las Condiciones del servicio y la Política de privacidad. Utilice **Guardar preferencias** para aplicar los cambios (se mostrará un indicador de progreso mientras se guarda).

Enviar comentarios

Cuando las suscripciones están habilitadas para la cuenta, la página puede mostrar una tarjeta de **Enviar comentarios** con enlaces a: **Solicitar una función** y plataformas de reseñas externas.

Instrucciones de configuración y renovación integradas

En la parte inferior de la página, el panel de control puede mostrar paneles de instrucciones expandibles según el estado actual (por ejemplo, cuando falta un certificado/token o está próximo a vencer).

Renovar el certificado de Apple Push (APNs)

Cuando el certificado APNs está próximo a vencer o ya ha vencido, la página muestra un panel con los pasos para descargar un CSR, renovar el certificado en el portal de Apple y cargar el nuevo certificado en Cerberus Enterprise.

Sincronizar con Apple Business Manager (ABM)

Cuando el token de ABM falta, ha vencido o está próximo a vencer, la página muestra un panel con los pasos para descargar un token de Apple Business Manager y cargarlo en Cerberus Enterprise.

Sincronizar con Apple Volume Purchase Program (VPP)

Cuando el token VPP falta, ha vencido o está próximo a vencer, la página muestra un panel con los pasos para descargar un token de contenido de Apple Business Manager y cargarlo en Cerberus Enterprise.

Sincronizar con Google Workspace

Cuando la sincronización del directorio de Google Workspace no está configurada, la página muestra un panel que explica la integración y proporciona un botón de autorización. También enumera el alcance de Google OAuth requerido:

<https://www.googleapis.com/auth/admin.directory.user.readonly>.

Para la configuración inicial de Android, consulte [Configuración de la gestión de Android](#)

Multitenencia

Resumen de multi-inquilino

La sección de **Multi-inquilino** está disponible para las cuentas de MSP y de gestores de empresas que gestionan múltiples empresas de clientes desde un único inicio de sesión. Este capítulo explica el modelo de alcance de la empresa, el cambio de empresa, la administración de empresas gestionadas y las subcuentas.

Para solicitar una cuenta multi-inquilino, póngase en contacto con enterprise@cerberusapp.com.

Conceptos básicos

- **Cuenta principal multi-inquilino:** la cuenta de gestión principal que puede acceder al espacio de trabajo global multi-inquilino.
- **Subcuenta:** una cuenta de gestor delegada creada por la cuenta principal, con asignaciones de empresas seleccionables.
- **Contexto de empresa seleccionado:** la empresa activa que está abierta actualmente en el panel para las operaciones diarias.
- **Delegación:** permiso otorgado por el propietario de una empresa que permite a una cuenta de gestor entrar y administrar dicha empresa.

Modelo de navegación

Cuando no hay un contexto de empresa seleccionado, la navegación lateral muestra áreas multi-inquilino como **Empresas** y, para las cuentas principales, **Subcuentas**. Tras entrar en una empresa, el panel cambia a la navegación estándar de una sola empresa (Inicio, Usuarios, Dispositivos, Inscripción, Políticas y más).

Propiedad y delegación

Cada empresa gestionada tiene un propietario. El propietario siempre puede acceder a esa empresa. Las cuentas de gestor que no son propietarias solo pueden acceder a una empresa cuando se ha otorgado la delegación.

- Cuando una empresa tiene su propio usuario administrador, ese administrador es el propietario y decide qué cuentas de administrador pueden acceder a la empresa.
- Cuando una empresa no tiene su propio usuario administrador, el propietario es la cuenta multi-tenancy principal.
- En las empresas cuyo propietario es un administrador del cliente, la cuenta principal puede otorgar o revocar el acceso a sus propias subcuentas mientras su propio acceso esté otorgado, pero no puede otorgarse acceso a sí misma.
- Si el administrador de la empresa revoca el acceso de la cuenta principal, también se revoca el acceso de sus subcuentas.
- Quitar una empresa de las asignaciones de una subcuenta también elimina el acceso de esa subcuenta a la empresa. Si la vuelves a asignar más adelante, habrá que otorgar el acceso de nuevo.

Los administradores de la empresa gestionan el acceso desde la tarjeta **Acceso de administrador de la empresa** en la página **Configuración**.

El estado de propiedad y delegación se muestra directamente en las tarjetas de empresa para que el alcance del acceso sea explícito antes de entrar en una empresa.

Acciones de licencia y facturación

Las vistas multi-inquilino muestran el estado de la licencia, los límites de dispositivos y las acciones de facturación de la empresa. Dependiendo del estado de la suscripción de la empresa y de sus permisos, la tarjeta puede mostrar **Gestionar facturación** o **Comprar licencia**.

Para las empresas creadas por una cuenta multi-inquilino, la gestión de licencias es realizada por los usuarios multi-inquilino. La cuenta principal siempre puede gestionar las licencias, mientras que las subcuentas solo pueden gestionarlas cuando la cuenta principal habilita el permiso **Puede gestionar licencias** para esa subcuenta.

Páginas de este capítulo

- [Empresas gestionadas](#): búsqueda, filtros, detalles de las tarjetas y creación de empresas.
- [Cambio de empresa](#): comportamiento del selector superior y transiciones de alcance.
- [Subcuentas](#): operadores delegados, asignaciones y gestión de credenciales.

Empresas gestionadas

La página de **Empresas** (*Panel* → *Empresas*) es el centro de control para el acceso a las empresas gestionadas. Enumera todas las empresas visibles para su cuenta multi-inquilino y le permite filtrar, inspeccionar la propiedad/delegación, entrar en un contexto de empresa y crear nuevas empresas gestionadas (solo cuentas principales).

Búsqueda y filtros

- **Buscar empresa:** filtra por nombre de empresa o ID de empresa.
- **Delegación:** **Todo**, **Delegada**, o **No delegada**.
- **Estado de la licencia:** **Todo**, **Válida**, **Por vencer**, **Caducada**, o **Terminada**.

Tarjetas de empresa

Cada tarjeta de empresa muestra metadatos clave de gestión:

- **Estado de la licencia** con insignia de icono y descripción emergente contextual.
- **Dispositivos con licencia** (límite de dispositivos de la empresa).
- **Próxima renovación programada** o **Fecha de vencimiento**, según el estado de la suscripción.
- Estado de **delegación** (**Propietario**, **Concedida**, o **No concedida**).
- Nombre de visualización y nombre de usuario del **propietario**.

Empresas seleccionadas recientemente

Las empresas a las que accedió recientemente están fijadas en una sección de **Seleccionadas recientemente** para acelerar los cambios de contexto repetidos.

Acciones de la empresa

- **Entrar en la empresa:** abre el contexto de la empresa seleccionada cuando la delegación/propiedad permite el acceso.

- **Gestionar facturación:** abre la gestión de facturación de la empresa cuando está disponible y permitida.
- **Comprar licencia:** abre el flujo de compra de la empresa cuando la facturación no está activa.

Quién puede gestionar licencias

Para las empresas creadas por una cuenta multi-inquilino, la gestión de licencias es controlada por los usuarios multi-inquilino. La cuenta principal siempre puede gestionar la facturación y las acciones de licencia para esas empresas.

Las subcuentas pueden gestionar la facturación y las acciones de licencia solo si la cuenta principal otorga el permiso **Puede gestionar licencias** en la página de [Subcuentas](#).

Crear empresa gestionada

Las cuentas principales multi-inquilino pueden ampliar **Crear empresa gestionada** desde el área de acciones inferior.

- Se requiere el **nombre de la empresa**.
- **Crear usuario administrador por empresa** controla el modo de propiedad.
- Cuando está habilitado, se requieren el **nombre de usuario del administrador** (en formato de correo electrónico) y el **nombre del administrador**.
- Antes de la creación, un cuadro de diálogo de confirmación resume la operación y, cuando corresponde, advierte que se enviarán credenciales temporales por correo electrónico al nuevo usuario administrador.

El nuevo usuario administrador debe elegir una nueva contraseña la primera vez que inicie sesión con la contraseña temporal.

Modo de propiedad

- **Administrador por empresa habilitado:** el nuevo usuario administrador es el propietario de la empresa y puede delegar la gestión a su cuenta multi-inquilino.
- **Administrador por empresa deshabilitado:** la empresa es propiedad directa de su cuenta multi-inquilino.

Cuota de empresa

Si la cuenta alcanza la cuota de empresas configurada, la creación se bloqueará y el formulario mostrará un mensaje de contacto de soporte con el recuento actual y máximo de empresas.

Cuando se alcance la cuota de empresas, no podrá crear más empresas gestionadas hasta que se aumente su límite.

Cambio de empresa

El selector de empresas en la barra de herramientas superior permite que los usuarios de entornos multi-inquilino se desplacen entre empresas delegadas sin necesidad de cerrar sesión. Está disponible cuando se puede seleccionar al menos un contexto de empresa.

Comportamiento del selector

- El activador muestra el nombre de la empresa actual (o el ID de la empresa si no hay un nombre disponible).
- El menú enumera las empresas delegadas/accesibles y marca la empresa actual como ya seleccionada.
- Durante el cambio, las acciones del selector se desactivan temporalmente para evitar cambios de alcance simultáneos.

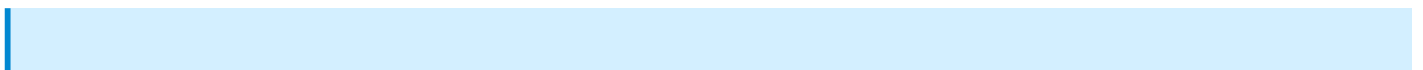
Salir de la empresa

El menú del selector incluye **Salir de la empresa**, lo que limpia el contexto de la empresa actual y le devuelve al espacio de trabajo global multi-inquilino.

Reglas de restablecimiento de contexto

El cambio de empresa o la salida de la empresa restablecen el alcance del panel. Las páginas específicas de la empresa y los datos se actualizan para el nuevo contexto seleccionado, y la visibilidad del menú se adapta según si hay una empresa seleccionada actualmente.

La empresa seleccionada se aplica a todas las pestañas abiertas del navegador. Si cambias de empresa o sales de ella en una pestaña, las demás pestañas recargan el panel en su siguiente acción, de modo que nunca operan sobre una empresa distinta de la mostrada.



Utilice el selector para realizar cambios rápidos de contexto operativo, pero verifique el nombre de la empresa seleccionada antes de ejecutar acciones sensibles, como actualizaciones de políticas o comandos a dispositivos.

Subcuentas

La página de **Subcuentas** (*Panel* → *Subcuentas*) está disponible para las cuentas principales multi-inquilino. Le permite crear usuarios administradores delegados, asignar empresas gestionadas, controlar los permisos de facturación y mantener las credenciales de las subcuentas.

Lista de subcuentas

Cada tarjeta de subcuenta muestra los controles de identidad y gestión:

- **Nombre y nombre de usuario/correo electrónico.**
- Asignación de selección múltiple de **empresas gestionadas**.
- Interruptor de permiso **Puede gestionar licencias**.
- Acciones de **Restablecer contraseña** y **Eliminar**.

Asignación de empresas gestionadas

Las asignaciones de empresas se editan a través del campo de selección múltiple **Empresas gestionadas**. Al cerrar el selector tras realizar los cambios, el panel solicitará una confirmación antes de guardar las actualizaciones.

Asignar una empresa la pone a disposición de la subcuenta, pero la subcuenta solo puede entrar en ella después de que se le otorgue el acceso. Quitar una empresa de las asignaciones también elimina el acceso de la subcuenta a ella.

Permiso de gestión de licencias

El interruptor **Puede gestionar licencias** controla si una subcuenta puede acceder a las acciones de gestión de facturación/licencias de la empresa.

Para las empresas creadas por la cuenta multi-inquilino, la cuenta principal siempre tiene derechos de gestión de licencias. Las subcuentas reciben derechos de gestión de licencias solo cuando la cuenta principal habilita este interruptor.

Restablecimiento de contraseña

Restablecer contraseña genera una nueva contraseña temporal y la envía a la subcuenta por correo electrónico tras la confirmación.

Al iniciar sesión con una contraseña temporal, ya sea tras un restablecimiento o con una subcuenta recién creada, el usuario debe elegir una nueva contraseña antes de continuar.

Eliminar subcuenta

Eliminar una subcuenta requiere confirmación y elimina permanentemente el acceso delegado para esa cuenta.

Crear subcuenta

Utilice el panel de acciones inferior **Crear subcuenta** para añadir un nuevo administrador delegado.

- **Correo electrónico:** obligatorio y validado con formato de correo electrónico.
- **Nombre:** nombre de visualización obligatorio.
- **Puede gestionar licencias:** permiso de facturación inicial opcional.
- Antes de la creación, un cuadro de diálogo de confirmación advierte que se enviará un correo electrónico con una contraseña temporal a la dirección proporcionada.

Información relevante

Aquí tiene algunos artículos que profundizan en cómo el MDM puede ayudar a su empresa:

[¿Qué es el modo quiosco? Una guía para bloquear dispositivos Android y Apple para empresas](#)

El modo quiosco convierte los teléfonos y tabletas estándar en herramientas empresariales especializadas. Cerberus Enterprise ayuda a las organizaciones a bloquear los dispositivos para que solo utilicen una aplicación o un pequeño conjunto de aplicaciones aprobadas, para casos de uso como puntos de venta (POS) minoristas, registro de clientes o navegación de flotas, al tiempo que facilita la seguridad, el soporte y la gestión a escala de estos dispositivos especializados.

[Cómo elegir la solución de MDM adecuada: una lista de comprobación de 7 puntos para pequeñas empresas](#)

Elegir un MDM en una etapa avanzada del proceso de compra es más sencillo cuando la comparativa se mantiene práctica. Esta lista de comprobación ayuda a las pequeñas empresas a

evaluar a los proveedores basándose en los siete criterios que suelen ser más importantes en los despliegues reales: seguridad, soporte para Android y Apple, facilidad de uso para equipos reducidos, escalabilidad, límites de privacidad, coste total de propiedad y capacidad de soporte diario.

Creación de un aula digital segura y enfocada: una guía de MDM para escuelas K-12

Los dispositivos gestionados por la escuela funcionan mejor cuando se centran en el aprendizaje. Cerberus Enterprise ayuda a las organizaciones de K-12 a mantener los dispositivos de los estudiantes enfocados mediante aplicaciones gestionadas, restricciones de estilo quiosco, configuraciones estandarizadas para dispositivos compartidos o prestados, y acciones de recuperación remota que reducen las pérdidas, el desvío de uso y las interrupciones en el aula.

Equipar a sus técnicos de campo: Cómo el MDM potencia la eficiencia y la seguridad en el lugar de trabajo

Los técnicos de campo dependen de los dispositivos móviles para consultar horarios, notas de servicio, referencias técnicas, el historial de clientes y actualizaciones de tareas mientras trabajan en el lugar. Cerberus Enterprise ayuda a mantener esos dispositivos listos mediante aplicaciones gestionadas, modelos de dispositivos estandarizados, comandos de soporte remoto y visibilidad basada en la ubicación que puede mejorar la coordinación de los envíos mientras se refuerza la

seguridad en el terreno.

Más allá del mapa: Cómo utilizar el MDM para una gestión de flotas y seguridad de conductores más inteligentes

Las operaciones de flota dependen de los dispositivos móviles para la navegación, el despacho, la mensajería, el registro y la ejecución en campo. Cerberus Enterprise ayuda a mantener esos dispositivos enfocados en los flujos de trabajo aprobados mediante aplicaciones gestionadas, controles de quiosco y dispositivos dedicados, políticas de comunicación segura, resolución de problemas remota y supervisión basada en la ubicación que puede reducir el tiempo de inactividad y apoyar operaciones de conducción más seguras.

Cómo las geovallas, el seguimiento en tiempo real y los mapas de ubicación mejoran las operaciones empresariales

Las funciones con conocimiento de ubicación en Cerberus Enterprise ayudan a las organizaciones a pasar de una simple visibilidad de los dispositivos a un control operativo más práctico. Los informes periódicos de ubicación, el seguimiento en tiempo real, las transiciones de geovalla y los

mapas interactivos pueden dar soporte a la logística, el servicio de campo, la atención sanitaria, el comercio minorista, la construcción y otros equipos distribuidos que necesitan una mejor visión de dónde se está realizando el trabajo y cuándo los dispositivos entran o salen de áreas importantes.

Cómo el multiinquilinato ayuda a los MSP a escalar los servicios de MDM y crear nuevas vías de ingresos

El multiinquilinato permite que los MSP, revendedores y organizaciones de múltiples empresas gestionen varias entidades desde una única cuenta de Cerberus Enterprise, manteniendo cada entorno separado. Este modelo reduce la fricción operativa, mejora la escalabilidad del servicio y permite el acceso delegado mediante subcuentas y una administración explícita controlada por el cliente. También crea oportunidades de negocio más sólidas para los proveedores que desean combinar el licenciamiento de software con servicios de incorporación, soporte, cumplimiento y gestión de movilidad.

Mejorar la operatividad empresarial con soluciones de MDM

La gestión de dispositivos móviles (MDM) centraliza el control de los dispositivos de la empresa, simplificando la inscripción, la configuración y el mantenimiento. El aprovisionamiento automatizado y las operaciones masivas reducen el trabajo manual de TI y garantizan políticas consistentes en todos los dispositivos. Las funciones de seguridad, como el cifrado, la supervisión

del cumplimiento y el borrado remoto, protegen los datos corporativos. En general, el MDM mejora la productividad al tiempo que reduce los costes de soporte y la complejidad operativa.

Seguridad avanzada en la gestión de Android Enterprise

Android Enterprise utiliza un perfil de trabajo para aislar las aplicaciones y los datos corporativos del contenido personal en el mismo dispositivo. Esta contenedorización crea entornos cifrados independientes gestionados de forma autónoma por los administradores de TI. Las políticas de seguridad pueden controlar el intercambio de datos corporativos sin afectar a las aplicaciones personales. La arquitectura protege los datos empresariales incluso si las aplicaciones personales se ven comprometidas.

MDM para Apple iPhone e inscripción automatizada

El marco de trabajo MDM de Apple permite la gestión centralizada de los iPhone en entornos empresariales. Combinado con Apple Business Manager, los dispositivos pueden inscribirse y configurarse automáticamente al activarse por primera vez. Los administradores pueden implementar y configurar aplicaciones corporativas de forma silenciosa, aplicar ajustes de seguridad y supervisar el cumplimiento. Esta automatización garantiza una configuración coherente de los dispositivos y reduce los errores de configuración.

Comprendiendo la gestión de dispositivos móviles

La gestión de dispositivos móviles (MDM) proporciona una plataforma centralizada para supervisar, asegurar y controlar los dispositivos móviles que acceden a los sistemas corporativos. Sus capacidades principales incluyen la aplicación de políticas de seguridad, la gestión de aplicaciones y el bloqueo o borrado remoto de dispositivos extraviados. El MDM ayuda a proteger los datos corporativos al tiempo que mantiene el cumplimiento de los dispositivos. Permite que organizaciones de cualquier tamaño gestionen de forma segura fuerzas de trabajo móviles en constante crecimiento.

Modelos de despliegue de dispositivos empresariales

Las organizaciones pueden adoptar múltiples modelos de propiedad de dispositivos, como BYOD, CYOD, COPE, COBO y COSU. Cada modelo equilibra de forma distinta el coste, la flexibilidad del usuario y el control de seguridad. El BYOD prioriza la comodidad del usuario, mientras que el COBO y el COSU maximizan el control corporativo y la seguridad. La elección del modelo correcto depende de los requisitos normativos, las necesidades de la fuerza laboral y la capacidad de gestión de TI.

MDM frente a EMM frente a UEM

El MDM se centra en la gestión y seguridad de los dispositivos móviles mediante la aplicación de políticas, el control de la configuración y la gestión remota. El EMM amplía este alcance para incluir la gestión de aplicaciones y contenidos, mientras que el UEM intenta gestionar todos los puntos finales, incluidos ordenadores portátiles y de sobremesa. Para muchas pymes, las suites completas de EMM o UEM añaden una complejidad innecesaria. En la práctica, las capacidades sólidas de MDM suelen satisfacer la mayoría de los requisitos de gestión móvil.

MDM en teléfonos personales y privacidad de los empleados

Los sistemas de MDM modernos utilizan la contenedorización para separar los datos personales de los de trabajo en dispositivos propiedad de los empleados. Los empleadores solo pueden gestionar y supervisar el entorno de trabajo, incluyendo las aplicaciones corporativas y la información sobre el cumplimiento del dispositivo. Los datos personales, como fotos, mensajes e historial de navegación, permanecen inaccesibles para la empresa. Esta separación técnica permite programas BYOD seguros al tiempo que preserva la privacidad de los empleados.

ROI del MDM y valor empresarial

El MDM debe evaluarse como una inversión estratégica en lugar de un simple gasto de seguridad. Genera retornos financieros mediante la reducción de la pérdida de dispositivos, menores costes de soporte de TI y una mayor eficiencia operativa. La gestión automatizada también aumenta la productividad de los empleados y reduce el tiempo de inactividad. Además, una seguridad más sólida reduce el riesgo y el impacto financiero de las brechas de datos.

Gestión de dispositivos conforme a

HIPAA

Las organizaciones de atención médica deben proteger los datos electrónicos de los pacientes de acuerdo con los requisitos de seguridad de HIPAA. El MDM ayuda a aplicar el cifrado, los controles de autenticación, la transmisión segura de datos y registros de auditoría detallados. También permite el borrado remoto y la aplicación centralizada de políticas para los dispositivos que acceden a sistemas médicos. Estos controles reducen los riesgos de cumplimiento al tiempo que permiten flujos de trabajo móviles en entornos sanitarios.

MDM para operaciones y seguridad en el sector minorista

Las organizaciones minoristas dependen de los dispositivos móviles para los sistemas de punto de venta (POS), la gestión de inventarios y las operaciones en tienda. El MDM garantiza que estos dispositivos permanezcan seguros, actualizados y conformes con estándares como PCI-DSS. La gestión centralizada reduce el tiempo de inactividad y simplifica el despliegue de dispositivos en

múltiples ubicaciones. El resultado es una mayor eficiencia operativa y un menor riesgo de incidentes de seguridad relacionados con los pagos.