Políticas - Android

Resumen

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

Puede explorar sus políticas y crear nuevas desde la sección **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 **Editor de políticas**.

Una política puede estar asociada a un token de inscripción, por lo que se aplicará automáticamente a los dispositivos durante el proceso de configuración. También puede cambiar la política asignada a un dispositivo después de la configuración.

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

> Muchas opciones de política solo se aplican a tipos de dispositivos específicos (administrados, dedicados, perfil de trabajo) y versiones de Android. Los ajustes no admitidos pueden ser ignorados por el dispositivo o informados como no conformes.

Diseño del editor de políticas

El editor de políticas está organizado en 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: administración de aplicaciones, seguridad, red, sistema, uso personal, políticas entre perfiles y más). Utilice las páginas de este manual para comprender cada panel en detalle.

Guardar, eliminar y dispositivos asociados

Utilice **Guardar política** para aplicar sus cambios. El botón está deshabilitado cuando no hay modificaciones pendientes o cuando la licencia ha expirado.

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

Gestión de aplicaciones

En esta sección, puedes configurar políticas relacionadas con la disponibilidad de aplicaciones, la instalación, las actualizaciones y la gestión de permisos.

> Las cuentas de Google Play gestionadas se crean automáticamente al aprovisionar los dispositivos.

1. Modo de la tienda de aplicaciones

Este modo controla qué aplicaciones están disponibles para el usuario en la tienda de aplicaciones y cómo se comporta el dispositivo cuando las aplicaciones se eliminan de la configuración.

Lista blanca (predeterminado): Solo las aplicaciones incluidas en la configuración estarán disponibles, y cualquier aplicación que no esté en la configuración se desinstalará automáticamente del dispositivo. La tienda de aplicaciones 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 configuración de las aplicaciones. La tienda de aplicaciones mostrará todas las aplicaciones, excepto las bloqueadas.

2. Política de aplicaciones no confiables

Política para aplicaciones no confiables (aplicaciones de fuentes desconocidas) aplicada al dispositivo. Esta opción controla la configuración del sistema Android que determina si un usuario puede instalar aplicaciones desde fuera de la Tienda Google Play (instalación manual).

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

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

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

3. Google Play Protect

¿Se aplica la verificación de aplicaciones de Google Play Protect?

Obligatorio (predeterminado): Activa forzadamente la verificación de aplicaciones.

Elección del usuario: Permite al usuario elegir si habilitar o no 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.

Otorgar: Otorgar automáticamente un permiso.

Denegar: Denegar automáticamente un permiso.

5. Funciones de la aplicación

Controla si las aplicaciones en dispositivos administrados o en perfiles de trabajo pueden mostrar sus funciones. Requiere Android 16 o superior.

Permitido (por defecto): Las aplicaciones en dispositivos totalmente administrados o en perfiles de trabajo pueden mostrar sus funciones.

No permitido: Las aplicaciones en dispositivos totalmente administrados o en perfiles de trabajo no pueden mostrar sus funciones.

6. Instalar aplicaciones desactivadas

¿Está desactivada la instalación de aplicaciones por parte del usuario?

7. Desinstalar aplicaciones: desactivado

¿Está desactivada la desinstalación de aplicaciones por parte del usuario?

8. Políticas de permisos

Permisos explícitos o concesiones/denegaciones de grupos para todas las aplicaciones. Estos valores anulan la configuración de la **política de permisos predeterminada**.

Utilice **"Agregar política de permisos"** para crear entradas y eliminarlas 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**: Permitir / Denegar / Preguntar (utiliza las mismas opciones de política que la **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 configurado en **el modo de Google Play**.

Si el **modo de Google Play** está configurado en **lista blanca**, solo estarán disponibles las aplicaciones que estén incluidas en la política, y cualquier aplicación que no esté en la política se desinstalará automáticamente del dispositivo.

Si el **modo 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 agregar una nueva aplicación, haga clic en el botón **Añadir aplicaciones** (o en el icono **Añadir aplicaciones**), y luego seleccione la aplicación desde Play Store y haga clic en el botón **Seleccionar** en la tarjeta de la aplicación.

> Todas las aplicaciones disponibles en la Play Store de su país están seleccionables de forma predeterminada. Para seleccionar sus propias aplicaciones privadas o web, debe subirlas al sistema primero. Para obtener más información, consulte la página **Aplicaciones privadas**.

Cada aplicación se puede configurar con sus propios ajustes, que se muestran visualmente en una tarjeta:

9.1. Tipo de instalación

El tipo de instalación a realizar para una aplicación.

> **Disponible**: La aplicación está disponible para su instalación.

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

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

Bloqueada: La aplicación está bloqueada y no se puede instalar. Si la aplicación se había instalado bajo una política anterior, se desinstalará.

Requerido para la configuración: La aplicación se instala automáticamente y el usuario no puede eliminarla; además, impedirá que la configuración se complete hasta que la instalación finalice.

Modo Quiosco: La aplicación se instala automáticamente en modo quiosco: se establece como la intención de inicio preferida y se incluye en la lista de aplicaciones permitidas para el modo de tarea bloqueada. La configuración del dispositivo no se completará hasta que se instale la aplicación. Después de la instalación, los usuarios no podrán eliminar la aplicación. Solo puede configurar este **tipo de instalación** para una sola aplicación por política. Cuando esta opción está presente en la política, la barra de estado se desactiva automáticamente.

Para obtener más información, consulte la página dedicada de **Modo Quiosco**.

9.2. Instalar restricciones

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

> Esta opción se muestra solo cuando el **tipo de instalación** es **preinstalada** o **instalada forzosamente**.

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

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

En espera: Instala 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 condiciones: (1) el dispositivo no se está utilizando activamente, (2) el dispositivo está conectado a una red no limitada, (3) el dispositivo se está cargando. El dispositivo recibe una notificación sobre una nueva actualización dentro de las 24 horas posteriores a su publicación por el desarrollador, momento en el cual la aplicación se actualiza la próxima vez

que se cumplen las condiciones anteriores.

Aplazado: La aplicación no se actualiza automáticamente durante un máximo de 90 días después de que la aplicación quede obsoleta. 90 días después de que la aplicación quede obsoleta, la última versión disponible se instala automáticamente con baja prioridad (consulte el modo de actualización automática **predeterminado**). Después de que la aplicación se actualiza, no se actualiza automáticamente nuevamente hasta 90 días después de que vuelva a quedar obsoleta. El usuario aún puede actualizar manualmente la aplicación desde la Play Store en cualquier momento.

Prioridad alta: La aplicación se actualiza lo antes posible. No se aplican restricciones. El dispositivo se notifica inmediatamente sobre una nueva actualización una vez que está disponible.

9.4. Versión mínima requerida

La versión mínima de la aplicación que se ejecuta en el dispositivo. Si se establece, el dispositivo intenta actualizar la aplicación a al menos esta versión. Si la aplicación no está actualizada, el dispositivo mostrará un **detalle de incumplimiento** con la **razón de incumplimiento** establecida en **APP_NOT_UPDATED**. La aplicación debe estar publicada en Google Play con un código de versión mayor o igual a este valor. Un máximo de 20 aplicaciones pueden especificar un código de versión mínima por política.

9.5. Ámbitos delegados

Los ámbitos delegados a la aplicación desde la política del dispositivo Android. Puede otorgar a otras aplicaciones una selección de permisos especiales de Android:

Instalación de certificados: Otorga acceso a la instalación y administración de certificados.

Configuraciones gestionadas: Otorga acceso a la administración de configuraciones gestionadas.

Bloquear desinstalación: Permite acceder a la función de bloqueo de desinstalación.

Permisos: Permite acceder a la configuración de las políticas de permisos y al estado de la concesión de permisos.

Acceso a paquetes: Permite acceder al estado de acceso a paquetes.

Aplicación del sistema: Permite el acceso para habilitar aplicaciones del sistema.

9.6. Red preferencial

El servicio de red preferencial a utilizar para esta aplicación. Si se especifica, la aplicación utilizará la segmentación de red empresarial definida para sus conexiones, cuando esté disponible. Debe coincidir con una segmentación de red configurada en la sección **Configuración de segmentación de red 5G** del panel **Celular**.

9.7. Política de permisos predeterminada

La política predeterminada para todos los permisos solicitados por la aplicación. Si se especifica, esto anula la política de **permisos predeterminada** 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.

Otorgar: Otorgar automáticamente un permiso.

Denegar: Denegar automáticamente un permiso.

9.8. Trabajo conectado y aplicaciones personales

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

No permitido (por defecto): Impide que la aplicación se comunique entre perfiles.

Permitido: Permite que la aplicación se comunique entre perfiles después de recibir el consentimiento del usuario.

9.9. Exención del bloqueo VPN Always On

Especifica si la aplicación puede acceder a la red cuando la VPN no está conectada y el **modo de bloqueo** está habilitado. Solo es compatible con dispositivos que ejecutan Android 10 o superior.

Obligatorio (por defecto): La aplicación respeta la configuración de bloqueo VPN permanente.

Exento: La aplicación está exenta de la configuración de bloqueo VPN permanente.

9.10. Widgets del perfil de trabajo

Especifica si la aplicación instalada en el perfil de trabajo puede agregar widgets a la pantalla de inicio.

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

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

9.11. Configuración de controles para el 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 está deshabilitado independientemente de esta configuración. Para aplicaciones de quiosco, puedes usar **Permitido** para permitir el control del usuario.

No especificado: Utiliza el comportamiento predeterminado de la aplicación para determinar si el control del usuario está permitido o denegado.

Permitido: El control del usuario está permitido para la aplicación.

No permitido: El control del usuario no está permitido para la aplicación.

9.12. Desactivado

¿Está la aplicación desactivada? Cuando está desactivada, los datos de la aplicación se conservan.

9.13. Permitir proveedor de credenciales

Si la aplicación puede actuar como proveedor de credenciales en Android 14 y versiones posteriores.

9.14. Configuración gestionada

Para configurar la configuración gestionada de la aplicación, haga clic en el botón **Activar configuración gestionada**. Si ya existe una configuración gestionada para la aplicación, puede modificar la configuración con el botón **Configuración gestionada** o eliminarla con el botón **Eliminar configuración**.

> **La opción de configuración gestionada** solo está disponible para aplicaciones que admiten esta funcionalidad.

9.15. Políticas de permisos

Concesiones o denegaciones de permisos explícitas 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 agregar una o más reglas de permisos a la tarjeta de la aplicación y elimínelas con la acción de eliminar.

9.16. Realice un seguimiento de los ID

Lista de los ID de la rama de pruebas cerradas de la aplicación a la que un dispositivo puede acceder. Si se seleccionan varios ID de rama, los dispositivos reciben la última versión disponible entre todas las ramas accesibles. Si no se selecciona ningún ID de rama, los dispositivos solo tienen acceso a la rama de producción de la aplicación.

> **La opción de ID de rama** está disponible solo para aplicaciones que tengan al menos un ID de rama disponible para su organización. Para obtener más detalles sobre cómo agregar su organización a una rama de pruebas cerradas para una aplicación específica, consulte aquí.

10. Configuración predeterminada de la aplicación

Establecer las aplicaciones predeterminadas para los tipos admitidos. 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 una configuración de aplicación predeterminada por cada **tipo de aplicación predeterminada**]. La lista de aplicaciones predeterminadas no debe contener duplicados.

10.1. Tipo de aplicación predeterminado

Seleccione la categoría de la aplicación que desea 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 aplicación predeterminados

Seleccione dónde se aplicará la aplicación predeterminada (administración completa, perfil de trabajo o perfil personal). Solo se pueden seleccionar los ámbitos compatibles con el tipo seleccionado.

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

10.3. Aplicaciones predeterminadas

Lista de aplicaciones que se pueden establecer como predeterminadas para el tipo seleccionado. La primera aplicación instalada y que cumpla los requisitos se establece como la predeterminada.

> Si los permisos incluyen **administración completa** o **perfil de trabajo**, cada aplicación también debe existir en la lista de **aplicaciones** con el **tipo de instalación** no establecido en **bloqueado**.

11. Selección de la clave privada

Permite mostrar una interfaz en un dispositivo para que el usuario seleccione un alias de clave privada si no existen reglas coincidentes en **Reglas de selección de clave privada**.

>

> Para dispositivos con versiones de Android anteriores a la P, establecer esto podría dejar las claves empresariales vulnerables.

12. Seleccione las reglas de la clave privada

Controla el acceso de las aplicaciones a las claves privadas. La regla determina qué clave privada, si existe, otorga la política de dispositivo Android a la aplicación especificada. El acceso se concede cuando la aplicación llama a KeyChain.choosePrivateKeyAlias (o cualquier función equivalente) para solicitar un alias de clave privada para una URL determinada, o para reglas que no son específicas de una URL (es decir, si urlPattern no está definido o está vacío o es igual a ".*") en Android 11 y versiones posteriores, 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 más de una regla choosePrivateKeyRules coincide, la última regla que coincide define qué alias de clave se debe devolver.

Utilice **Agregar regla de clave privada** para crear entradas y eliminarlas 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 que se utilizará para comparar con la URL de la solicitud. Si no se establece o está vacío, se aplicará a todas las URLs. Utiliza la sintaxis de expresiones regulares de java.util.regex.Pattern.

12.3. Nombres de paquetes

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

Utilice **Añadir nombre del paquete** para agregar entradas y eliminarlas con la acción de eliminar.

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

Modo quiosco

Con el modo quiosco, puedes limitar la funcionalidad de un dispositivo a una sola aplicación o a varias aplicaciones. La elección entre el modo quiosco de una sola aplicación y el de varias aplicaciones depende de tus objetivos empresariales.

En **modo kiosco de aplicación única**, un dispositivo está configurado para una sola aplicación y no permite a los usuarios acceder a otras aplicaciones en el dispositivo. Tampoco pueden salir de la aplicación, lo que la convierte en un dispositivo dedicado para esa aplicación específica. Para habilitar este modo, especifique una aplicación en la sección **Administración de aplicaciones**, con el **tipo de instalación** establecido en **Kiosk**.

En **el modo quiosco multi-aplicaciones**, los dispositivos pueden acceder a múltiples aplicaciones. Los usuarios finales pueden navegar entre varias aplicaciones a través de un lanzador personalizado. Para habilitar este modo, active la opción de **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 la configuración del sistema y la barra de estado.

Lanzador personalizado para modo quiosco

Indica si el lanzador personalizado para quioscos está habilitado. Esto reemplaza la pantalla de inicio con un lanzador que restringe el dispositivo a las aplicaciones instaladas a través de la **gestión de aplicaciones**. Las aplicaciones aparecen en una sola página en orden alfabético.

Acciones del botón de encendido

Define el comportamiento del dispositivo en modo kiosco cuando un usuario presiona y mantiene presionado (doble toque) el botón de encendido.

> **Disponible (predeterminado)**: El menú de energía (por ejemplo, Apagar, Reiniciar) se muestra cuando un usuario presiona y mantiene presionado el botón de encendido de un dispositivo en modo kiosco.
>
> **Bloqueado**: El menú de energía (por ejemplo, Apagar, Reiniciar) no se muestra cuando un usuario presiona y mantiene presionado el botón de encendido de un dispositivo en modo kiosco. Nota: esto podría impedir que los usuarios apaguen el dispositivo.

Advertencias de errores del sistema

Especifica si los cuadros de diálogo de errores del sistema para aplicaciones que se bloquean o no responden se bloquean en el modo kiosco. Cuando están bloqueados, el sistema finalizará la aplicación como si el usuario eligiera la opción "cerrar aplicación" en la interfaz.

Bloqueado (predeterminado): Todos los cuadros de diálogo de error del sistema, como los mensajes de bloqueo y de "aplicación no responde" (ANR), están bloqueados. Cuando están bloqueados, el sistema cierra la aplicación como si el usuario la cerrara desde la interfaz de usuario.

Activado: Se muestran todos los cuadros de diálogo de error del sistema, como los mensajes de bloqueo y de "la aplicación no responde" (ANR).

Navegación del sistema

Especifica qué funciones de navegación están habilitadas (por ejemplo, botones de "Inicio" y "Resumen") en el modo kiosco.

Deshabilitado (por defecto): Los botones de "Inicio" y "Resumen" no son accesibles.

Solo inicio: Solo el botón de "Inicio" está habilitado.

Activados: Los botones de "Inicio" y "Resumen" están habilitados.

Barra de estado

Especifica si la información del sistema y las notificaciones están desactivadas en el modo kiosco.

Desactivado (predeterminado): La información del sistema y las notificaciones están desactivadas en el modo kiosco.

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

Activado: En el modo kiosco, se muestran la información del sistema y las notificaciones en la barra de estado. Nota: Para que esta política tenga efecto, el botón de inicio del dispositivo debe estar habilitado mediante kioskCustomization.systemNavigation.

Configuración del dispositivo

Especifica si se permite la aplicación de Configuración en el modo kiosco.

Permitido (por defecto): Se permite el acceso a la aplicación de Configuración en el modo kiosco.

Bloqueado: El acceso a la aplicación de Configuración no está permitido en el modo kiosco.

Seguridad

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

Acciones de riesgo de seguridad

Elija qué hacer cuando un dispositivo informa un riesgo de seguridad en los informes de estado.

Tipos de riesgos de seguridad admitidos:

Sistema operativo desconocido: La API de Play Integrity detecta que el dispositivo está ejecutando un sistema operativo desconocido (la comprobación básica de integridad se completa, pero ctsProfileMatch falla).

Sistema operativo comprometido: La API de Play Integrity detecta que el dispositivo está ejecutando un sistema operativo comprometido (la comprobación básica de integridad falla).

La evaluación basada en hardware falló: La API de Play Integrity detecta que el dispositivo no tiene una garantía sólida de integridad del sistema, si la etiqueta MEETS_STRONG_INTEGRITY no se muestra en el campo de integridad del dispositivo.

Acciones disponibles:

Borrar datos corporativos (por defecto): Desregistrar y borrar los datos de trabajo (todo el dispositivo si está gestionado completamente, o solo el perfil de trabajo si es propiedad del perfil).

Ninguna acción: No se realiza ninguna acción y el dispositivo permanece inscrito.

Cuando selecciona **Borrar datos corporativos**, también puede configurar opciones de borrado:

Mantener la protección de restablecimiento de fábrica: Conserva los datos de la protección contra restablecimiento de fábrica (FRP) al borrar el dispositivo.

Borrar almacenamiento externo: Además, se borrará el almacenamiento externo del dispositivo (como las tarjetas SD) al realizar el borrado.

Borrar eSIMs: Para dispositivos propiedad de la empresa, esto elimina todos los eSIM del dispositivo al realizar el borrado. En dispositivos de uso personal, esto eliminará los eSIM administrados (eSIM que se agregan mediante el comando ADD_ESIM) en los dispositivos, y no se eliminarán los eSIM de propiedad personal.

1. Tiempo máximo de bloqueo

Tiempo máximo (en segundos) de inactividad del usuario antes de que el dispositivo se bloquee. Un valor de 0 indica que no hay restricción.

2. Permanecer activo durante la carga

Los modos de carga en los que el dispositivo permanece encendido. Al usar esta configuración, se recomienda borrar **Tiempo máximo de bloqueo** para evitar que el dispositivo se bloquee mientras permanece encendido.

Cargador de corriente alterna: La fuente de alimentación es un cargador de corriente alterna.

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

Cargador inalámbrico: La fuente de alimentación es inalámbrica.

3. Clave de seguridad desactivada

Si es verdadero, esto deshabilita la pantalla de bloqueo para las pantallas principal(es) y/o secundaria(s). Esta política solo se admite en el modo de gestión de dispositivos dedicado.

4. Requisitos de contraseña

Políticas de requisitos de contraseña.

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

Los requisitos de contraseña pueden usar **el ámbito "Automático"** (un único requisito) o ámbitos separados de **dispositivo** y/o **perfil de trabajo**. Los requisitos basados en la complejidad deben combinarse con requisitos basados en la calidad para el mismo ámbito.

4.1. Ámbito de aplicación

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 para los dispositivos con perfil de trabajo y a todo el dispositivo para los dispositivos gestionados o dedicados.

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

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

4.2. Longitud del historial de contraseñas

Longitud del historial de contraseñas. Después de establecer este valor, el usuario no podrá usar una contraseña nueva que sea idéntica a alguna de las contraseñas anteriores. Un valor de 0 indica que no hay restricciones.

4.3. Número máximo de intentos fallidos de contraseña antes de que se borre el dispositivo

Número de contraseñas incorrectas para desbloquear el dispositivo antes de que se borre. Un valor de 0 significa que no hay restricciones.

4.4. Tiempo de expiración de la contraseña (días)

Esta configuración obliga al usuario a actualizar su contraseña periódicamente, después del número de días especificado.

4.5. Requiere desbloqueo con contraseña

El tiempo transcurrido después de que un dispositivo o perfil de trabajo se desbloquee mediante un método de autenticación seguro (contraseña, PIN, patrón), durante el cual se puede desbloquear con cualquier otro método (por ejemplo, huella digital, agentes de confianza, reconocimiento facial). Una vez transcurrido el período de tiempo especificado, solo se pueden usar métodos de autenticación seguros para desbloquear el dispositivo o el perfil de trabajo.

Configuración predeterminada del dispositivo: El período de tiempo se establece con la configuración predeterminada del dispositivo.

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

4.6. Calidad de la contraseña

La calidad de contraseña requerida.

Alta complejidad: Defina el rango de alta complejidad de la contraseña como: En Android 12 y versiones posteriores: PIN sin secuencias repetidas (4444) ni ordenadas (1234, 4321, 2468), longitud mínima de 8; alfabético, longitud mínima de 6; alfanumérico, longitud mínima de 6.

Complejidad media: Defina el rango de complejidad media de la contraseña como: PIN sin secuencias repetidas (4444) ni ordenadas (1234, 4321, 2468), longitud mínima de 4; alfabético, longitud mínima de 4; alfanumérico, longitud mínima de 4.

Baja complejidad: Defina el nivel de complejidad baja de la contraseña como: patrón; PIN con secuencias repetidas (4444) o ordenadas (1234, 4321, 2468).

Ninguno: No se aplican requisitos de contraseña.

Débil: El dispositivo debe estar protegido con una tecnología de reconocimiento biométrico de baja seguridad, como mínimo. Esto incluye tecnologías que pueden reconocer la identidad de una persona y que son aproximadamente equivalentes a un PIN de 3 dígitos (la tasa de falsos positivos es inferior a 1 en 1000).

Cualquier: Se requiere una contraseña, pero no hay restricciones sobre su contenido.

Numérico: La contraseña debe contener caracteres numéricos.

Numérico complejo: La contraseña debe contener caracteres numéricos sin secuencias repetidas (como 4444) ni ordenadas (como 1234, 4321, 2468).

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

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

Compleja: 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

Longitud mínima de contraseña permitida. Un valor de 0 indica que no hay restricción.

4.8. Mínimo de letras

Número mínimo de letras requeridas en la contraseña.

4.9. Número mínimo de letras minúsculas

Número mínimo de letras minúsculas requeridas en la contraseña.

4.10. Número mínimo de letras mayúsculas

Número mínimo de letras mayúsculas requeridas en la contraseña.

4.11. Número mínimo de caracteres no alfabéticos

Número mínimo de caracteres no alfabéticos (dígitos o símbolos) requeridos en la contraseña.

4.12. Mínimo de dígitos numéricos

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 que ejecutan Android 9 y versiones posteriores con 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.
>
> **Requiere un bloqueo de trabajo independiente**: Se requiere un bloqueo separado para el perfil de trabajo.

5. Restablecimiento de fábrica deshabilitado

¿Está desactivada la opción de restablecimiento de fábrica desde la configuración? Solo se aplica a dispositivos completamente gestionados.

6. Protección contra el restablecimiento de fábrica

Direcciones de correo electrónico de los administradores del dispositivo para la protección contra el restablecimiento de fábrica. Cuando el dispositivo experimenta un restablecimiento de fábrica no autorizado, requerirá que uno de estos administradores inicie sesión con la dirección de correo electrónico y la contraseña de la cuenta de Google para desbloquear el dispositivo. Si no se especifican administradores, el dispositivo no proporcionará protección contra el restablecimiento de fábrica. Solo se aplica a dispositivos completamente administrados.

Direcciones de correo electrónico de los administradores: utilice **Activar protección contra restablecimiento de fábrica** para comenzar a configurar los administradores. Luego, utilice **Añadir dirección de correo electrónico del administrador** para agregar direcciones y eliminarlas con la acción de eliminar.

7. Funciones de bloqueo de pantalla

Funciones de la pantalla de bloqueo que se pueden desactivar.

7.1. Desactivar todo

Desactivar todas las personalizaciones actuales y futuras de la pantalla de bloqueo.

7.2. Desactivar cámara

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

7.3. Desactivar las notificaciones

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

7.4. Desactivar notificaciones sin censura

Desactivar 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 digital

Desactivar el sensor de huellas dactilares en las pantallas de bloqueo seguras.

7.7. Desactivar la entrada de texto en las notificaciones

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

7.8. Desactivar la autenticación facial

Desactivar la autenticación facial en las pantallas de bloqueo seguras.

7.9. Desactivar la autenticación mediante el iris

Desactivar la autenticación mediante el iris en las pantallas de bloqueo seguras.

7.10. Desactivar toda la autenticación biométrica

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

7.11. Desactivar todos los atajos

Desactivar todos los atajos en la pantalla de bloqueo segura en Android 14 y versiones posteriores.

Multimedia

En esta sección, puede configurar el comportamiento de la cámara/micrófono, el acceso a datos 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 afecta a todo el dispositivo en dispositivos administrados completamente, 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 (administración total: a nivel del dispositivo; perfil de trabajo: solo para aplicaciones del perfil de trabajo). El interruptor de acceso a la cámara no tiene efecto en el ámbito administrado.
>
> **Activado**: Las cámaras están disponibles. En dispositivos con administración completa que ejecutan Android 12 o superior, el usuario no puede activar o desactivar el acceso a la cámara. En otros dispositivos o versiones, el comportamiento es similar a la opción de elección del usuario.

2. Acceso al micrófono

En dispositivos totalmente administrados, controla el uso del micrófono y si el usuario puede acceder al interruptor de acceso al micrófono (Android 12+). Esta configuración no tiene efecto en dispositivos que no están totalmente administrados.

> **Elección del usuario (predeterminado)**: Comportamiento predeterminado. El micrófono está disponible y (en Android 12 o posterior), el usuario puede activar o desactivar el acceso al micrófono.
>
> **Desactivado**: El micrófono está desactivado (a nivel del dispositivo). El interruptor de acceso al micrófono no tendrá ningún efecto.
>
> **Obligatorio**: El micrófono está disponible. En Android 12 o versiones posteriores, el usuario no puede activar o desactivar el acceso al micrófono. En Android 11 o versiones anteriores, el

comportamiento es similar a la opción de elección del usuario.

3. Acceso a datos USB

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

Deshabilitar la transferencia de archivos (predeterminado): Se deshabilitan las transferencias de archivos, pero se permiten otras conexiones de datos USB (p. ej., ratón/teclado).

Deshabilitar la transferencia de datos: Se prohíben todos los tipos de transferencias de datos USB (Android 12+ con USB HAL 1.3+). Si no es compatible, el dispositivo recurre a la opción de "Deshabilitar la transferencia de archivos".

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

4. Impresión

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

Permitido (por defecto): La impresión está permitida.

No permitido: La impresión está deshabilitada (Android 9 y versiones posteriores).

5. Configuración del brillo de la pantalla

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

Modo de brillo de la pantalla:

Elección del usuario (predeterminado): El usuario puede configurar el brillo de la pantalla.

Automático: El brillo se ajusta automáticamente y el usuario no puede modificarlo. Aún se puede establecer un valor de brillo, el cual se utiliza como parte del ajuste automático (disponible en Android 9+; 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 modificarlo. Se requiere un valor de brillo (Android 9+ con gestión completa; perfiles de trabajo en

dispositivos Android 15+ propiedad de la empresa).

Brillo de pantalla: Fijo: El brillo se establece en el valor configurado y el usuario no puede modificarlo. Se requiere un valor de brillo (Android 9+ con gestión completa; perfiles de trabajo en dispositivos Android 15+ propiedad de la empresa)

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

6. Configuración del tiempo de espera de la pantalla

Controla si el usuario puede configurar el tiempo de espera de la pantalla y, cuando está habilitado, el valor del tiempo de espera.

El campo **Modo de tiempo de espera de pantalla** permite seleccionar entre un comportamiento controlado por el usuario y uno forzado.

Elección del usuario (predeterminado): Al usuario se le permite configurar el tiempo de espera de la pantalla.

Forzado: El tiempo de espera de la pantalla se establece en el valor configurado y el usuario no puede cambiarlo (Android 9+ con gestión completa; perfiles de trabajo en dispositivos Android propiedad de la empresa, versión 15+).

Tiempo de espera de la pantalla:

Duración del tiempo de espera en segundos. El valor debe ser mayor que 0. Si es mayor que **Tiempo máximo de bloqueo**, el sistema podría limitarlo y reportar un incumplimiento.

7. Captura de pantalla desactivada

¿La captura de pantalla está desactivada?

8. Ajuste de volumen desactivado

Si el ajuste del volumen general está desactivado.

9. Montaje de medios físicos desactivado

¿Está desactivada la opción de montar medios externos físicos?

Celular

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

1. Modo avión

Controla si el usuario puede activar o desactivar el modo avión o no.

> **Elección del usuario (predeterminado)**: El usuario puede activar o desactivar el modo avión.
>
> **Desactivado**: El modo avión está desactivado. El usuario no puede activar ni desactivar el modo avión. Compatible con Android 9 y versiones posteriores.

2. Celular 2G

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

> **Elección del usuario (predeterminado)**: Al usuario se le permite activar o desactivar la red celular 2G.
>
> **Deshabilitado**: La red celular 2G está desactivada. Al usuario no se le permite activar la red celular 2G a través de la configuración. Compatible con Android 14 y versiones posteriores.

3. Anular APNs

Controla si las APNs personalizadas están habilitadas o deshabilitadas. Cuando está habilitada, solo se utilizan las APNs personalizadas configuradas y se ignoran todas las demás APNs del dispositivo.

> **Desactivado (por defecto)**: Todas las configuraciones de APN configuradas se guardan en el dispositivo, pero están desactivadas y no tienen ningún efecto. Todas las demás APNs del dispositivo permanecen activas.
>
> **Activado**: Solo se utilizan las APN de reemplazo; todas las demás APN se ignoran. Esta configuración solo se puede configurar en dispositivos administrados con Android 10 o superior.

4. Configuración de APN

Configure una o más entradas de APN. Utiliza **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 administración y la versión de Android).

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

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

Campos APN opcionales:

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

Protocolo y **Protocolo de roaming**: Configuración del protocolo IP.

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

Dirección del proxy y **Puerto del proxy**: Servidor proxy HTTP para el tráfico de datos (si es aplicable).

Dirección del servidor proxy MMS, **Puerto del servidor proxy MMS**, **MMSC (URI del centro MMS)**: Configuración relacionada con MMS.

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

Configuración de "Siempre activo": Indica si la sesión PDU activada por esta APN debe permanecer activa constantemente. Disponible en Android 15 y versiones posteriores.

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

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

5. Configuración de mensajes de celda desactivada

Si la configuración de mensajes de celda está desactivada.

6. Configuración de redes móviles deshabilitada

¿Está configurada la opción para deshabilitar las redes móviles?

7. Datos en roaming desactivados

¿Los servicios de datos en itinerancia están desactivados?

8. Las llamadas salientes están deshabilitadas

¿Están deshabilitadas las llamadas salientes?

9. SMS deshabilitado

¿Está desactivado el envío y la recepción de mensajes SMS?

10. Configuración de segmentación de red 5G

Configura los ajustes del servicio de red preferencial para habilitar la segmentación de red 5G empresarial. Puedes configurar hasta 5 segmentos empresariales y asignar aplicaciones a redes específicas para una optimización del enrutamiento del tráfico.

10.1. Red Preferencial Predeterminada

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

Nota: Aplicaciones críticas como **com.google.android.apps.work.clouddpc** y **com.google.android.gms** están excluidas de esta configuración predeterminada.

10.2. Configuraciones del servicio de red

Utiliza **Añadir configuración de red** para crear una configuración de segmentación. Puedes añadir hasta 5 configuraciones. Cada configuración tiene:

ID de red preferida (asignado automáticamente): El ID de la red se asigna automáticamente y no se puede modificar.

Conexión alternativa predeterminada: Define si se debe recurrir a la conexión predeterminada del dispositivo. Si está desactivado, las aplicaciones no podrán acceder a Internet si la red 5G no está disponible.

Redes incompatibles: Indica si las aplicaciones sujetas a esta configuración pueden utilizar redes distintas al servicio preferente. Si se establece en **No permitido**, también debe estar configurada como **Conexión alternativa predeterminada** en **No permitido**. Requiere Android 14 y versiones posteriores.

Redes

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

> Las configuraciones de Wi-Fi pueden ser aprovisionadas y administradas por el sistema a través de **configuraciones de Wi-Fi**. Dependiendo del valor configurado en **Configurar Wi-Fi**, los usuarios pueden tener control limitado o nulo sobre la adición/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 cambiarlo.

Elección del usuario (predeterminado): Al usuario se le permite activar o desactivar Wi-Fi.

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

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

2. Nivel mínimo de seguridad de Wi?Fi

El nivel mínimo de seguridad de redes Wi-Fi al que el dispositivo puede conectarse. Compatible con Android 13 y versiones posteriores, 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: Deshabilita las redes Wi-Fi abiertas; requiere al menos seguridad personal (por ejemplo, WPA2-PSK).

Red corporativa: Requiere redes EAP empresariales; desactiva las redes Wi-Fi con un nivel de seguridad inferior.

Red corporativa de 192 bits: Requiere redes corporativas de 192 bits; opción más segura.

3. Estado de banda ultranancha (UWB)

Controla el estado de la configuración de banda ultranancha y si el usuario puede activarla o desactivarla.

Elección del usuario (predeterminado): El usuario puede activar o desactivar UWB.

Desactivado: UWB está desactivado y el usuario no puede activarlo o desactivarlo a través de la configuración (Android 14+).

Gestión de la conectividad de los dispositivos

4. Compartir vía Bluetooth

Controla si se permite o no el uso de Bluetooth para compartir.

Permitido: Compartir mediante Bluetooth está permitido (activado de forma predeterminada en dispositivos gestionados completamente, Android 8+).

No permitido: El uso de Bluetooth para compartir archivos no está permitido (configuración predeterminada en perfiles de trabajo, Android 8+).

5. Configure Wi-Fi

Controla los privilegios de configuración de Wi-Fi. Según la opción seleccionada, el usuario tiene control total, limitado o nulo para configurar redes Wi-Fi.

Permitir la configuración de Wi-Fi (predeterminado): Al usuario se le permite configurar Wi-Fi.

No permitir la adición de configuraciones de Wi-Fi: Se impide agregar nuevas configuraciones de Wi-Fi. El usuario puede cambiar entre las redes ya configuradas (Android 13+; perfiles de trabajo administrados y propiedad de la empresa).

No permitir la configuración de Wi-Fi: Impide la configuración de redes Wi-Fi. Para dispositivos totalmente gestionados, elimina las redes configuradas por el usuario y conserva solo las configuradas a través de **configuraciones de Wi-Fi**. Para perfiles de trabajo propiedad de la empresa, las redes existentes no se ven afectadas, pero los usuarios no

pueden agregar, eliminar ni modificar redes Wi-Fi.

> Cuando la configuración de Wi-Fi está desactivada y el dispositivo no puede conectarse al inicio, el sistema puede mostrar la **opción de conexión alternativa** para permitir al usuario conectarse temporalmente y actualizar la configuración.

6. Configuración de Wi-Fi Direct

Controles para configurar y usar la configuración de Wi-Fi Direct. Disponible en dispositivos propiedad de la empresa con Android 13 o superior.

Permitir (por defecto): El usuario puede utilizar Wi-Fi Direct.

No permitir: Al usuario no se le permite utilizar Wi-Fi Direct.

7. Configuración de conexión a Internet

Controla la configuración de conexión a Internet. Según el valor establecido, se permite o se prohíbe completamente al usuario utilizar diferentes métodos de conexión.

Permitir todas las opciones de conexión (predeterminado): Permite la configuración y el uso de todas las formas de conexión.

Deshabilitar la conexión Wi-Fi: Impide que el usuario utilice la conexión Wi-Fi (dispositivos Android 13 o superior propiedad de la empresa).

Desactivar todas las conexiones de acceso a internet: Impide todas las formas de conexión a internet (dispositivos administrados completamente y perfiles de trabajo propiedad de la empresa).

8. Política de SSID de Wi-Fi

Restricciones sobre a qué SSIDs de Wi-Fi puede conectarse el dispositivo (esto no afecta a qué redes se pueden configurar en el dispositivo). Disponible en dispositivos propiedad de la empresa que ejecuten Android 13 o superior.

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

Lista de SSIDs permitidos: El dispositivo solo puede conectarse a las redes Wi-Fi cuyos nombres (SSIDs) estén en la lista. La lista de SSIDs no debe estar vacía.

Utilice **Agregar SSID** para agregar entradas. Dependiendo del tipo de política seleccionado, la lista se interpreta como una lista de SSIDs 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 de acceso y **SSID de Wi-Fi denegados** para las listas de denegación.

9. Configuración de roaming Wi-Fi

Configura el modo de roaming Wi-Fi para cada SSID. Usa **Añadir configuración de roaming Wi-Fi** para crear entradas.

Cada entrada incluye:

> **SSID**: El SSID al que se aplica la configuración de roaming (obligatorio).
>
> **Modo de roaming Wi-Fi**: Predeterminado / Deshabilitado / Agresivo. Deshabilitado y Agresivo requieren Android 15 o superior y solo son compatibles con dispositivos totalmente administrados y perfiles administrados en dispositivos propiedad de la empresa.

Restricciones de red

Bluetooth desactivado

¿Está desactivado el Bluetooth? (Priorizar esta opción sobre "Configuración de Bluetooth desactivada" porque esta última puede ser modificada por el usuario).

11. Compartir contactos por Bluetooth desactivado

Si compartir contactos por Bluetooth está desactivado.

12. Configuración de Bluetooth desactivada

¿Está desactivada la configuración de Bluetooth?

13. Restablecimiento de red desactivado

¿Está desactivada la opción de restablecer la configuración de red?

14. Transmisión saliente desactivada

¿Está desactivada la opción de usar NFC para transmitir datos desde las aplicaciones?

VPN

Aplicación VPN de conexión permanente

Especifique un nombre de paquete VPN de conexión permanente para garantizar que los datos de las aplicaciones administradas configuradas siempre se transmitan a través de una VPN configurada.

> Nota: Esta función requiere la implementación de un cliente VPN que admita tanto la conexión permanente como las funciones de VPN por aplicación.

16. Bloqueo VPN

Impide la conexión de red cuando la VPN no está conectada.

17. Configuración de VPN desactivada

Si la configuración de VPN está deshabilitada.

Servicios de proxy y de red

18. Servicio de red preferente

Controla si el servicio de red preferente está habilitado en el perfil de trabajo. Por ejemplo, una organización puede tener un acuerdo con un proveedor de servicios que permita que los datos de trabajo se transmitan a través de una red dedicada para uso empresarial (por ejemplo, una red empresarial en redes 5G). Esto no tiene efecto en los dispositivos totalmente administrados.

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 el corte de red empresarial, también configure **Configuración de corte de red 5G** en el panel de la política **Celular** y asigne aplicaciones a un corte utilizando su configuración de **Red Preferencial**.

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.

Deshabilitado

Proxy directo

Proxy de configuración automática (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 utilizada para configurar el proxy.

19.4. Hosts excluidos

Para un proxy directo, se especifican aquí los hosts para los que el proxy no se aplica. Los nombres de los hosts pueden incluir comodines como ***.example.com**.

Utilice **Agregar host excluido** para agregar entradas (disponible solo para proxy directo).

Configuraciones de red 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 eliminar.

20. Campos de configuración de Wi?Fi

Cada configuración incluye:

Nombre de la configuración: Obligatorio.

SSID: Obligatorio.

Conexión automática: Indica si la red debe conectarse automáticamente cuando esté disponible.

Transición rápida: Indica si el dispositivo debe intentar utilizar la transición rápida (IEEE 802.11r-2008) con la red.

SSID oculto: Indica si el SSID se transmitirá.

Modo de aleatorización de la dirección 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**. Se requiere la frase de contraseña.

20.3. Método EAP (Enterprise)

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 la fase 2

Mostrado para el túnel de métodos externos (**EAP-TTLS** y **PEAP**).

MSCHAPv2

PAP

20.5. Credenciales EAP proporcionadas por los usuarios

Cuando está habilitada, 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**, puedes asignar un certificado de cliente que se utiliza para la autenticación Wi-Fi.

Para obtener más información, consulta la página de **Administración 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 que permite la autenticación Wi-Fi.

> Si tanto el **certificado de cliente** como el **alias del par de claves del certificado de cliente** están configurados, el alias del par de claves se ignora.

20.7. Identidad

Identidad del usuario. Para el túnel de protocolos externos (PEAP, EAP-TTLS), esto se utiliza para autenticarse dentro del túnel, y **la identidad anónima** se utiliza para la identidad EAP fuera del túnel. Para 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 presentada al protocolo externo.

20.9. Contraseña

Contraseña del usuario. Si no se especifica, se solicita al usuario.

20.10. Certificados CA del servidor

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

Utilice **Añadir certificado CA del servidor** para agregar entradas y eliminarlas con la acción de eliminar.

20.11. Coincidencia del 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 los nombres DNS del nombre alternativo del certificado del servidor de autenticación.

Sistema

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

1. Nivel mínimo de la API

El nivel mínimo de la API de Android permitido.

2. Política de cifrado

¿Está habilitado el cifrado?

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

Activado sin contraseña: Se requiere cifrado, pero no se necesita contraseña para iniciar.

Activado con contraseña: Se requiere cifrado y se necesita una contraseña para iniciar.

3. Fecha y hora automáticas

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

Opción del usuario (por defecto): La fecha, la hora y la zona horaria se configuran según la elección del usuario.

Obligatorio: Aplicar automáticamente la fecha, la hora y la zona horaria en el dispositivo.

4. Opciones para desarrolladores

Controla el acceso a la configuración para desarrolladores: opciones para desarrolladores y modo de arranque seguro.

Desactivado (por defecto): Desactiva todas las opciones para desarrolladores y evita que el usuario acceda a ellas.

Permitido: Permite todas las opciones para desarrolladores. El usuario puede acceder y, opcionalmente, configurar estas opciones.

5. Modo de Cumplimiento de Estándares Comunes

Modo de Criterios Comunes: estándares de seguridad definidos en el Common Criteria para la Evaluación de la Seguridad de la Información Tecnológica (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 a largo plazo de Bluetooth, validación adicional para algunos certificados de red y verificaciones 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 superior. Advertencia: el Modo de Criterios Comunes impone un modelo de seguridad estricto, normalmente requerido solo para organizaciones con información altamente sensible. El uso normal del dispositivo puede verse afectado; actívelo solo si es necesario.

Deshabilitado (por defecto): Desactiva el Modo de Criterios Comunes.

Activado: Habilita 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 habilitar o deshabilitar MTE en el dispositivo (si el dispositivo lo admite).

Obligatorio: MTE está habilitado y el usuario no puede cambiarlo (Android 14 o superior; compatible con dispositivos totalmente administrados y perfiles de trabajo en dispositivos propiedad de la empresa).

Deshabilitado: MTE está desactivado y el usuario no puede modificarlo (Android 14 o superior; compatible solo con dispositivos totalmente administrados).

7. Protección de contenido

Controla si la protección de contenido (que escanea en busca de aplicaciones engañosas) está habilitada. Esto es compatible en Android 15 y versiones posteriores.

Desactivado (por defecto): La protección de contenido está desactivada y el usuario no puede cambiar esta configuración.

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

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

8. Asistencia para contenido

Controla si se permite enviar contenido de asistencia a una aplicación privilegiada, 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 está disponible en Android 15 y versiones posteriores.

Permitido (por defecto): Se permite enviar contenido de asistencia a una aplicación privilegiada (Android 15 y versiones posteriores).

No permitido: El contenido de asistencia está bloqueado y no se puede enviar a una aplicación privilegiada (Android 15 y versiones posteriores).

9. Crear ventanas deshabilitadas

¿Se desactiva la creación de ventanas además de las ventanas de la aplicación? Esta opción evita que se muestren las siguientes interfaces de usuario del sistema: notificaciones y barras de estado, actividades del teléfono (como llamadas entrantes) y actividades prioritarias del teléfono (como llamadas en curso), alertas del sistema, errores del sistema y superposiciones del sistema.

10. Salida de emergencia de la red

¿Está habilitada la opción de "salida de emergencia de la red"? Si no se puede establecer una conexión de red al iniciar el dispositivo, la opción de "salida de emergencia" solicita al usuario que se conecte temporalmente a una red para actualizar la configuración del dispositivo. Una vez aplicada la configuración, la conexión temporal se eliminará y el dispositivo continuará arrancándose. Esto evita que el dispositivo no pueda conectarse a una red si no hay una red adecuada en la configuración y el dispositivo se inicia en un modo de tarea bloqueada, o si el usuario no puede acceder a la configuración del dispositivo.

11. Actividades predeterminadas

Una lista de actividades predeterminadas para gestionar los intents que coinciden con un filtro de intents específico. Por ejemplo, esta función permitiría a los administradores de TI elegir qué

aplicación de navegador se abre automáticamente para los enlaces web, o qué aplicación de inicio se utiliza al pulsar el botón de inicio.

Utilice "**Agregar actividad predeterminada**" para crear entradas. Dentro de una entrada, utilice "**Agregar acción**" y "**Agregar categoría**" para crear el filtro de intents.

11.1. Actividad del receptor

La actividad que debe ser el manejador de intenciones predeterminado. Este debe ser el nombre de un componente de Android, por ejemplo, com.android.enterprise.app/.MainActivity. Alternativamente, el valor puede ser el nombre del paquete de una aplicación, lo que hace que Android Device Policy elija una actividad adecuada de la aplicación para manejar la intención.

11.2. Acción

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

11.3. Categoría

Las categorías de intención que se deben incluir en el filtro. Una intención incluye las categorías que requiere, y todas deben estar incluidas en el filtro para que coincida. En otras palabras, agregar una categoría al filtro no afecta la coincidencia a menos que esa categoría se especifique en la intención.

12. Métodos de entrada permitidos

Especifica los métodos de entrada permitidos.

> **Todos permitidos**: No se aplica ninguna restricción. Se permiten todos los métodos de entrada.
>
> **Solo métodos del sistema**: Solo se permiten los métodos de entrada integrados en el sistema.
>
> **Solo métodos del sistema y proporcionados**: Solo se permiten los métodos de entrada integrados en el sistema y los proporcionados.

12.1. Métodos de entrada permitidos

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

Utilice **el método de entrada "Añadir"** para agregar elementos y elimínelos con la acción de eliminar.

13. Servicios de accesibilidad permitidos

Especifica los servicios de accesibilidad permitidos.

Permitidos todos: Se puede utilizar cualquier servicio de accesibilidad.

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

Solo los servicios de accesibilidad proporcionados y los integrados: 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 **el servicio de accesibilidad "Agregar"** para añadir elementos y eliminarlos con la acción de eliminar.

14. Política de actualización del sistema

Configuración para administrar las actualizaciones del sistema.

Predeterminado: Sigue el comportamiento predeterminado de las actualizaciones para el dispositivo, lo que generalmente requiere que el usuario acepte las actualizaciones del sistema.

Automático: Instala automáticamente tan pronto como esté disponible una actualización.

En ventana de mantenimiento: Instala 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 tipo quiosco, ya que esta es la única forma en que las aplicaciones fijadas permanentemente en primer plano pueden actualizarse mediante Play.

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

14.1. Ventana de mantenimiento (Solo ventana)

Cuando "**Política de actualización del sistema**" está configurada como "**Interfaz gráfica**", puedes definir la ventana de mantenimiento diaria utilizando los campos "**desde**" y "**hasta**".

14.2. Periodos de suspensión de actualización del sistema

Un período anual en el que las actualizaciones del sistema enviadas de forma inalámbrica (OTA) se posponen para mantener la versión del sistema operativo que se ejecuta en un dispositivo. Para evitar que el dispositivo quede bloqueado indefinidamente, cada período de suspensión debe estar separado por al menos 60 días. Cada período de suspensión no debe exceder los 90 días.

Utilice **Definir período de suspensión de actualizaciones del sistema** para crear registros.

15. Proveedores de credenciales predeterminados

Controla qué aplicaciones pueden actuar como proveedores de credenciales en Android 14 y versiones posteriores.

> **No permitidas (por defecto)**: Las aplicaciones que no tienen especificada la política credentialProviderPolicy no están permitidas para actuar como proveedor de credenciales.
>
> **No permitidas (excepto para el sistema)**: Las aplicaciones que no tienen especificada la política credentialProviderPolicy no están permitidas para actuar como proveedor de credenciales, excepto para los proveedores de credenciales predeterminados del fabricante.

Ubicación y vallas geográficas

Este panel agrupa la configuración de políticas de Android que controlan el envío de informes de ubicación, la aplicación de la ubicación y las definiciones de vallas geográficas. Úsalo cuando quieras que Cerberus Enterprise recopile ubicaciones de dispositivos o detecte cuándo los dispositivos entran o salen de áreas configuradas.

Informes de ubicación

Reportar ubicación

Habilita el reporte de geolocalización del dispositivo. Los datos de ubicación recopilados a través de esta configuración se utilizan en el **mapa de ubicación del panel**, el historial de ubicación en la vista general del dispositivo y el procesamiento de cercas geográficas.

> En dispositivos que no están completamente gestionados, los datos de ubicación aún pueden depender de que la aplicación Cerberus Enterprise tenga los permisos de ubicación necesarios y de que los servicios de ubicación estén habilitados en el dispositivo.

Modo de ubicación

Controla la configuración de ubicación del dispositivo en dispositivos propiedad de la empresa.

- **Elección del usuario**: los servicios de ubicación no están restringidos por la política.
- **Aplicada**: los servicios de ubicación están habilitados en el dispositivo.
- **Deshabilitado**: los servicios de ubicación están desactivados en el dispositivo.

Compartir ubicación desactivado

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

Comportamiento automático con vallas geográficas activas

Las vallas geográficas activas requieren informes de ubicación para funcionar. Cuando al menos una valla geográfica está activa, Cerberus Enterprise mantiene automáticamente consistentes los ajustes de ubicación relacionados.

- **El reporte de ubicación** se activa obligatoriamente mientras existen vallas geográficas activas.
- **Modo de ubicación** se fuerza a **Activado**.
- **Compartir ubicación desactivada** se fuerza a desactivar.

Si intenta desactivar **Reportar ubicación** mientras una o más vallas geográficas están activas, Cerberus Enterprise muestra un diálogo de confirmación. Si continúa, todas las vallas geográficas activas en la directiva se desactivan.

Lista de cercas geográficas

Una política puede contener hasta **10 cercas geográficas**. Los nombres de las cercas geográficas deben ser únicos dentro de la política.

Usa **Añadir valla geográfica** para crear una nueva entrada. Cada valla geográfica 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 administradores.
- **Informe de entrada** y **Informe de salida**: elija qué eventos de transición deben generarse.
- **Activo**: habilita o deshabilita la cerca geográfica sin eliminarla.

> Al menos uno de **Report entrar** o **Report salir** debe permanecer habilitado para cada cerca geográfica.

Herramientas de edición de mapas

Cada tarjeta de valla perimetral incluye una vista previa del mapa del área. Puedes editar la geometría desde el mapa o desde los campos numéricos.

- Haz clic en el mapa para mover el centro de la valla perimetral cuando la edición de área esté desbloqueada.
- Usa el botón **Ubicación actual** para centrar el mapa en tu posición de navegador actual.
- Usa el botón **Volver a centrar mapa** para restaurar la vista preferida para esa geocerca.

- Usa el botón de bloqueo para evitar cambios accidentales en la geometría de la geocerca.

Dónde aparecen los datos de la geocerca

Las transiciones de la geocerca se pueden revisar en la página de **Visión general del dispositivo** , dentro de la pestaña **Geocercas** 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

Agregar usuario deshabilitado

Indica si la adición de nuevos usuarios y perfiles está deshabilitada. Para dispositivos donde managementMode es **DEVICE_OWNER**, este campo se ignora y al usuario nunca se le permite agregar o eliminar usuarios.

Modificar cuentas desactivadas

¿Se ha desactivado la opción de agregar o eliminar cuentas?

La configuración de credenciales de usuario está desactivada

¿Está desactivada la configuración de las credenciales del usuario?

Eliminar usuario deshabilitado

Si la opción para eliminar otros usuarios está desactivada.

Establecer icono de usuario deshabilitado

Si cambiar el icono de usuario está deshabilitado.

Establecer fondo de pantalla: Deshabilitado

Si cambiar el fondo de pantalla está deshabilitado.

Configuración de la autenticación de la cuenta de trabajo

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

Durante la configuración/inscripción del dispositivo, esta directiva influye en si se requiere un inicio de sesión en la cuenta de trabajo, pero la configuración de la Consola de administración de Google **Autenticar con Google** y el tipo de token de inscripción aún pueden requerir autenticación.

Para dispositivos ya registrados, esta directiva solo se aplica si el dispositivo está administrado por una cuenta de Google administrada (es decir, registrado sin **autenticación mediante la inscripción de Google**).

Para obtener más detalles y solucionar problemas, consulte **Autenticación mediante la inscripción de Google**.

Tipos de cuenta bloqueados

Tipos de cuenta que el usuario no puede gestionar. Esta opción evita que los usuarios del dispositivo agreguen cuentas no autorizadas.

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

Cada entrada tiene un campo de **Tipo de cuenta** (obligatorio). Ingrese una cadena como **com.google**. Elimine una entrada usando la acción de eliminar.

Uso personal

Al configurar un dispositivo propiedad de la empresa para uso laboral y personal, puede especificar algunas reglas para limitar cómo el usuario puede usar el dispositivo para uso personal, fuera del perfil de trabajo.

> Esta sección solo se aplica a los dispositivos propiedad de la empresa que tienen un perfil de trabajo. No tendrá ningún efecto en los dispositivos completamente gestionados o en los dispositivos de propiedad personal.

1. Cámara desactivada

¿Está la cámara desactivada?

2. Captura de pantalla desactivada

¿La captura de pantalla está desactivada?

3. Máximo número de días de permiso

Controla cuánto tiempo puede permanecer inactivo el perfil de trabajo.

4. Compartir vía Bluetooth

Controla si se permite el uso de Bluetooth para compartir archivos en el perfil personal de un dispositivo propiedad de la empresa y que tiene un perfil de trabajo.

5. Espacio privado

Controla si se permite un espacio privado en el dispositivo.

6. Modo de la tienda de aplicaciones

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

Lista de bloqueo (predeterminada): 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 de aplicaciones permitidas: Solo las aplicaciones especificadas explícitamente en la sección de **Aplicaciones** y con el tipo de **instalación** configurado como **Disponible** pueden ser instaladas en el perfil personal.

7. Aplicaciones

Lista de aplicaciones que deben estar permitidas o bloqueadas en el perfil personal. El comportamiento del contenido de la lista depende del valor configurado en **el modo de Google Play**.

Para agregar una nueva aplicación desde la Play Store, haga clic en el icono **+**.

7.1. Tipo de instalación

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

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

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

8. Tipos de cuenta bloqueados

Tipos de cuenta que el usuario no puede gestionar. Esta opción evita que los usuarios del dispositivo agreguen cuentas no autorizadas 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 (por defecto)**: Evita que los usuarios peguen texto en el perfil personal que se haya copiado desde el perfil de trabajo. El texto copiado del perfil personal se puede pegar en el perfil de trabajo.
>
> **Permitido**: El texto copiado en cualquier perfil puede pegarse en el otro perfil.

Compartir datos entre perfiles

Define si los datos de un perfil (personal o de trabajo) pueden compartirse con las aplicaciones del otro perfil. Esto controla específicamente el intercambio de datos básico a través de intenciones. La gestión de otros canales de comunicación entre perfiles, como la búsqueda de contactos, la copia y pegado,
o las aplicaciones de trabajo y personales conectadas, se configuran por separado.

> **No permitido**: Evita que los datos se compartan entre el perfil personal y el perfil de trabajo, y viceversa.
>
> **No se permite compartir** datos del perfil de trabajo al perfil personal (por defecto): Evita que los usuarios compartan datos desde el perfil de trabajo a aplicaciones en el perfil personal. Los datos personales pueden compartirse con aplicaciones de trabajo.
>
> **Permitido**: Los datos de cualquier perfil pueden compartirse con el otro perfil.

Los widgets del perfil de trabajo tienen un comportamiento predeterminado

Comportamiento predeterminado para los widgets del perfil de trabajo. Si una aplicación específica no define una política de widgets, se aplica el valor predeterminado configurado aquí.

Funciones de aplicaciones entre perfiles

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

> Esta configuración depende de la opción de política de nivel **Funciones de la aplicación** (en la sección de administración de aplicaciones). Si las funciones de la aplicación están configuradas como **No permitidas**, la API rechazará las funciones de aplicaciones entre perfiles configuradas como **Permitidas**.

Contactos laborales en el perfil personal

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

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

No permitido: Impide que las aplicaciones personales accedan a los contactos del perfil de trabajo ni que busquen contactos laborales.

No permitido, excepto para aplicaciones del sistema: Impide que la mayoría de las aplicaciones personales accedan a los contactos del perfil de trabajo, excepto para las aplicaciones predeterminadas del fabricante (OEM) como el marcador, los mensajes y la aplicación de contactos (Android 14 y versiones posteriores).

Cuando los contactos de trabajo están configurados en el perfil personal, puede definir opcionalmente una lista de entradas de **nombres de paquetes excluidos**. Dependiendo del modo seleccionado, estas exclusiones funcionan como una lista de aplicaciones permitidas o una lista de aplicaciones bloqueadas para las aplicaciones personales.

Informes de estado

En esta sección, puede configurar qué datos se deben recuperar del dispositivo. Los datos de estado se pueden ver en la página del panel de control de **estado del dispositivo**.

Informes de aplicaciones

¿Se habilitan los informes de aplicaciones? (Información reportada sobre una aplicación instalada)

> Esta opción es obligatoria para el sistema (para la integración con la aplicación complementaria) y siempre está habilitada; no se puede deshabilitar.

Incluir aplicaciones eliminadas

¿Se incluyen las aplicaciones eliminadas en los informes de aplicaciones?

Configuración del dispositivo

¿Está habilitado el informe de la configuración del dispositivo? (Información sobre la configuración del dispositivo relacionada con la seguridad)

Información del software

¿Está habilitado el informe de información del software? (Información sobre el software del dispositivo)

Información de memoria

¿Está habilitado el informe de memoria? (Un evento relacionado con las mediciones de memoria y almacenamiento)

Información de la red

¿Está habilitada la recopilación de información de la red? (Información de la red del dispositivo)

Mostrar información

¿Está habilitada la visualización de informes? Los datos de los informes no están disponibles para los dispositivos de uso personal con perfiles de trabajo. (Información de visualización del dispositivo)

Eventos de administración de energía

¿Está habilitada la función de reporte de eventos de administración de energía? Los datos de reporte no están disponibles para dispositivos de propiedad personal con perfiles de trabajo.

Estado del hardware

¿Está habilitado el informe del estado del hardware? Los datos del informe no están disponibles para dispositivos de propiedad personal con perfiles de trabajo.

Propiedades del sistema

¿Está habilitada la función de informes de propiedades del sistema?

Modo de Cumplimiento de Estándares Comunes

¿Está habilitado el informe del Modo de Cumplimiento de Estándares Comunes?

Varios

1. Juego oculto desactivado

Si el juego oculto en la configuración está desactivado.

2. Omitir las sugerencias de la primera ejecución

Marcar para omitir las sugerencias en el primer uso. Los administradores de la empresa pueden activar la recomendación del sistema para que las aplicaciones omitan su tutorial y otras sugerencias introductorias al iniciarse por primera vez.

3. Mensaje de soporte breve

Un mensaje que se muestra al usuario en la pantalla de configuración cuando una funcionalidad ha sido desactivada por el administrador. Si el mensaje es más largo de 200 caracteres, podría ser truncado.

4. Mensaje de soporte extenso

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

5. Información de la pantalla de bloqueo para el 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 la inscripción, puede requerir que el usuario abra una o más aplicaciones necesarias para la configuración del dispositivo.

Utiliza **Añadir acción de configuración** para crear entradas y eliminarlas con la acción de eliminar.

6.1. Iniciar aplicación

Nombre del paquete de la aplicación a ejecutar

6.2. Título

Proporciona un mensaje visible para el usuario, explicando por qué la aplicación necesita iniciarse.

6.3. Descripción

Proporciona un mensaje visible para el usuario, explicando por qué la aplicación necesita iniciarse.

7. Visibilidad del nombre para empresas

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

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

Oculto: El nombre de la empresa no se muestra en el dispositivo.

Reglas de aplicación de políticas

Si un dispositivo o perfil de trabajo no cumple con alguno de los parámetros de configuración indicados a continuación, Android Device Policy bloquea automáticamente el uso del dispositivo o perfil de trabajo de forma predeterminada:

- **Requisitos de contraseña**
- **Política de cifrado**
- **Clave de seguridad desactivada**
- **Métodos de entrada permitidos**
- **Servicios de accesibilidad permitidos**

Si el dispositivo o el perfil de trabajo siguen sin cumplir los requisitos después de 10 días, la política de dispositivo Android restablecerá el dispositivo a su configuración de fábrica o eliminará el perfil de trabajo.

En esta sección, puede anular las reglas de cumplimiento predeterminadas o agregar 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 utilizando la acción de eliminar.

Nombre del ajuste

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

Requerido. El valor debe coincidir con un nombre de política de nivel superior válido; de lo contrario, el campo se marcará como inválido.

Bloquear después de X días

Número de días que la política no cumple con los requisitos antes de que se bloquee el dispositivo o el perfil de trabajo. Para bloquear el acceso de inmediato, establezca en 0. **Bloquear después de X días** debe ser menor que **Borrar después de X días**. Solo aplicable a dispositivos propiedad de la empresa.

Rango permitido: 0–300.

Ámbito de bloqueo

Especifica el alcance de la acción bloqueada. Solo 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.
>
> **Dispositivo completo**: La acción de bloqueo se aplica a todo el dispositivo, incluidas las aplicaciones del perfil personal.

Borrar datos después de X días

Número de días en que la directiva no cumple con los requisitos antes de que se elimine el dispositivo o el perfil de trabajo.
Días antes de la eliminación debe ser mayor que **Días antes del bloqueo**. Solo aplicable a dispositivos propiedad de la empresa.

Requerido. Valor predeterminado (nueva regla): **1**.

Rango permitido: de 1 a 300.

Mantener la protección de restablecimiento de fábrica

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

Predeterminado (nueva regla): activado.