Sistema

En esta sección, puedes configurar políticas relacionadas con el sistema.

1. Nivel mínimo de API

El nivel mínimo permitido de la API de Android.

2. Política de cifrado

Indica si el cifrado está habilitado.

> **Predeterminado**: Este valor se ignora, es decir, no se requiere cifrado.
>
> **Habilitado sin contraseña**: Se requiere cifrado, pero no se requiere contraseña para arrancar.
>
> **Habilitado con contraseña**: Se requiere cifrado y se requiere contraseña para arrancar.

3. Fecha y hora automáticas

Indica si la fecha, la hora y la zona horaria automáticas están habilitadas 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.
>
> **Forzado**: Fuerza la fecha, la hora y la 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 configurarlos opcionalmente.

5. Modo Common Criteria

Controla el modo Common Criteria, el conjunto de estándares de seguridad definidos en Common Criteria for Information Technology Security Evaluation (CC). Activar el modo Common Criteria incrementa ciertos componentes de seguridad del dispositivo (por ejemplo: cifrado AES-GCM de las claves de largo plazo de Bluetooth, validación adicional de algunos certificados de red y comprobaciones de integridad criptográfica de las políticas). El modo Common Criteria solo es compatible con dispositivos propiedad de la empresa que ejecuten Android 11 o superior. Advertencia: el modo Common Criteria aplica un modelo de seguridad estricto que normalmente solo necesitan las organizaciones de alta sensibilidad. El uso estándar del dispositivo puede verse afectado; actívalo solo si es necesario.

Desactivado (predeterminado): desactiva el modo Common Criteria.

Activado: activa el modo Common Criteria.

6. Memory Tagging Extension (MTE)

Controla Memory Tagging Extension (MTE) en el dispositivo.

Elección del usuario (predeterminado): el usuario puede elegir activar o desactivar MTE en el dispositivo (si el dispositivo lo admite).

Forzado: MTE está activado y el usuario no puede cambiarlo (Android 14+; compatible con dispositivos totalmente gestionados y perfiles de trabajo en dispositivos propiedad de la empresa).

Desactivado: MTE está desactivado y el usuario no puede cambiarlo (Android 14+; solo compatible con dispositivos totalmente gestionados).

7. Protección de contenido

Controla si la protección de contenido (que analiza en busca de aplicaciones engañosas) está activada. Es compatible con Android 15 y versiones posteriores.

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

Forzado: 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 AssistContent a una aplicación privilegiada, como una aplicación de asistente (por ejemplo, Circle to Search). AssistContent incluye capturas de pantalla e información sobre una aplicación, como el nombre del paquete. Es compatible con Android 15 y versiones posteriores.

Permitido (predeterminado): se permite enviar el contenido de asistencia a una aplicación privilegiada (Android 15+).

No permitido: se bloquea el envío del contenido de asistencia a una aplicación privilegiada (Android 15+).

9. Creación de ventanas desactivada

Indica si está desactivada la creación de ventanas distintas de las de las aplicaciones. Esta opción impide que se muestren las siguientes interfaces del sistema: 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. Vía de escape de red

Indica si está activada la vía de escape de red. Si no se puede establecer una conexión de red al arrancar, la vía de escape pide al usuario que se conecte temporalmente a una red para actualizar la política del dispositivo. Después de aplicar la política, la red temporal se olvidará y el dispositivo continuará arrancando. Esto evita que no se pueda conectar a una red si no hay ninguna red adecuada en la última política y el dispositivo arranca en una aplicación en modo de bloqueo de tareas, o si el usuario no puede acceder de otro modo a la configuración del dispositivo.

11. Actividades predeterminadas

Una lista de actividades predeterminadas para gestionar intents que coinciden con un filtro de intents concreto. Por ejemplo, esta función permite a los administradores de TI elegir qué aplicación de navegador abre automáticamente los enlaces web o qué aplicación de lanzador se usa al tocar el botón de inicio.

Usa **Añadir actividad predeterminada** para crear entradas. Dentro de una entrada, usa **Añadir acción** y **Añadir categoría** para construir el filtro de intents.

11.1. Actividad receptora

La actividad que debe ser el controlador de intents predeterminado. Debe ser el nombre de un componente de Android, por ejemplo, com.android.enterprise.app/.MainActivity. Como alternativa, 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 gestionar el intent.

11.2. Acción

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

11.3. Categoría

Las categorías de intent que deben coincidir con el filtro. Un intent incluye las categorías que requiere, y todas ellas deben estar incluidas en el filtro para que coincida. En otras palabras, añadir una categoría al filtro no afecta a la coincidencia a menos que esa categoría se especifique en el intent.

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

12.1. Métodos de entrada autorizados

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

Usa **Añadir método de entrada** para añadir entradas y quítalas con la acción de eliminar.

13. Servicios de accesibilidad permitidos

Especifica los servicios de accesibilidad permitidos.

Todos permitidos: se puede usar cualquier servicio de accesibilidad.

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

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

13.1. Servicios de accesibilidad autorizados

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

Usa **Añadir servicio de accesibilidad** para añadir entradas y quítalas con la acción de eliminar.

14. Política de actualización del sistema

Configuración para gestionar 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: instala automáticamente en cuanto haya una actualización disponible.

Con ventana: 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 de kiosco, ya que es la única forma en que Play puede actualizar las aplicaciones fijadas de forma persistente en primer plano.

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

14.1. Ventana de mantenimiento (solo con ventana)

Cuando **Política de actualización del sistema** está configurada en **Con ventana**, puedes definir la ventana de mantenimiento diaria con los campos **desde** y **hasta**.

14.2. Periodos de congelación de las actualizaciones del sistema

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

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

15. Proveedores de credenciales predeterminados

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

> **No permitido (predeterminado)**: las aplicaciones con credentialProviderPolicy sin especificar no pueden actuar como proveedor de credenciales.
>
> **No permitido excepto el sistema**: las aplicaciones con credentialProviderPolicy sin especificar no pueden actuar como proveedor de credenciales, excepto los proveedores de credenciales predeterminados del OEM.

Revision #58
Created 2025-12-17 09:33:15 UTC by Admin
Updated 2026-11-12 09:54:29 UTC by Admin