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.

Revision #37
Created 2025-12-17 09:33:15 UTC by Admin
Updated 2026-04-22 15:49:31 UTC by Admin