UNIVERSIDAD DE EL SALVADOR FACULTAD MULTIDISCIPLINARIA PARACENTRAL
DEPARTAMENTO DE INFORMÁTICA

Tarea de MDM: Seguridad informática

Nombre: Edgar Giovanni Gómez Cerón. **Carnet:** GC21028

Nombre: Javier Eduardo Hernández Sánchez. **Carnet:** HS21002

San Vicente, 17 de noviembre 2025

Análisis de la situación actual

Identificar los riesgos de seguridad móvil existentes.

- Pérdida o robo de dispositivos.
- Accesos no autorizados a aplicaciones y correos corporativos.
- Ausencia de controles de seguridad.
- Uso de apps no autorizadas.
- Falta de actualizaciones.
- Conexión a redes wifi inseguras.
- Imposibilidad de borrar dispositivos de forma remota en caso de incidentes.

Definir requerimientos de la empresa

- Administrar Android, IOS, IPadOs y laptops.
- Permitir borrado remoto y ubicación.
- Gestionar instalación y bloqueo de aplicaciones.
- Aplicar políticas de seguridad.
- Integrase con correo corporativos.
- Proveer reportes y monitoreos.

Investigación de soluciones MDM

Describir características, ventajas, desventajas y costos.

Microsoft Intune

Características	Ventajas	Desventajas
• Gestiona Android, iOs, macOS, y Windows. • Integración nativa con Microsoft 365 y Azure AD. • Aplicación de políticas, borrado, remoto, control de apps.	• Muy seguro y robusto. • Buen sistema de reportes. • Se integra con identidad corporativa.	• Configuración compleja. • Requiere suscripción.

VMware Workspace ONE

Características	Ventajas	Desventajas
• Plataforma unificada para movilidad y escritorios virtuales. • Control granular de políticas y apps. • Automatización avanzada.	• Muy personalizable. • Soporta BYOD y dispositivos corporativos.	• Costosa. • Requiere conocimientos técnicos altos.

ManageEngine Mobile Device Manager Plus

Características	Ventajas	Desventajas
• Consola administrativa centralizada. • Control de apps, perfiles, seguridad básica.	• Tiene versión gratuita permitiendo un máximo de 25 dispositivos. • Más sencillo de implementar.	• Menos robusto que Intune. • Integraciones limitadas.

Elaborar una tabla corporativa entre las soluciones investigadas.

Solución	Seguridad	Facilidad	Costo	Integración	Ideal para
Microsoft Intune	Muy alta	Media	Medio	Excelente con M365	Empresas de software
Workspace ONE	Muy alta	Baja	Alto	Alta	Empresas grandes
Mobile Device Manager Plus	Media	Alta	Bajo	Media	PYMEs

Selección y justificación.

Elegir la solución más adecuada para el caso.

Solución elegida: Microsoft Intune.

Argumentar con base en criterios técnicos y de seguridad.

Elegimos Microsoft Intune por motivos técnicos y de seguridad concretos y prácticos. Desde el punto de vista técnico, Intune ofrece gestión unificada de endpoints para Windows, iOS, Android y macOS, simplificando el inventario, el despliegue de aplicaciones y la aplicación de actualizaciones. Su integración nativa con Azure Active Directory permite políticas de acceso condicional basadas en identidad y riesgo, autenticación multifactor y SSO, reduciendo la superficie de ataque. Además, su modelo de configuración por plantillas acelera la automatización de tareas repetitivas.

En materia de seguridad, Intune facilita el cifrado forzado de dispositivos, la gestión de parches, el control de aplicaciones y restricciones de datos por medio del bloqueo de copiado o sincronización en aplicaciones no gestionadas. Las políticas de cumplimiento y las acciones remediadoras automáticas impiden el acceso a recursos corporativos desde equipos no conformes. Su integración con Microsoft Defender y SIEM mejora la detección, el análisis y la respuesta ante incidentes. Finalmente, la telemetría centralizada y los informes ayudan en auditorías y cumplimiento normativo.

Por su escalabilidad, compatibilidad con ecosistemas heterogéneos y robustez en controles de identidad y datos, Intune resulta una opción técnica y segura para proteger la información y facilitar la operación diaria en organizaciones modernas y resilientes.

Implementación simulada

Describir la instalación

Pasos para instalar Microsoft Intune

- Creamos una cuenta en Microsoft Intune en su página oficial con nuestro correo electrónico.
- Elegimos el plan gratuito para la práctica.
- En dispositivos, elegimos Android, dentro de inscripción vinculamos nuestra cuenta para Google Play Administrado ya que es una preinscripción.
- Dentro de Android nos vamos a inscripción, dispositivos de usuarios totalmente administrados de propiedad corporativa, creamos una nueva directiva del tipo staging.
- En administración de inquilinos, filtros de asignación creamos uno nuevo para Android interprese, en propiedad ponemos el nombre de la directiva creada.
- Luego asignamos los filtros a cada aplicación que instalaremos.
- Dentro de dispositivos, Android, en configuración creamos las políticas para Android interprece, restricciones del dispositivo.
- Dentro de dispositivos, Android, en cumplimientos creamos políticas de cumplimiento para que los dispositivos Android puedan acceder a Microsoft 365, seleccionamos un tipo de política totalmente administrada.
- Dentro de las políticas de cumplimiento ciframos el almacenamiento del dispositivo.
- En dispositivo, Android, inscripción, seleccionamos dispositivo de usuario totalmente administrado de propiedad corporativa.
- Abrimos el perfil de ensayo y seleccionamos el token que generar un código QR que luego escanearemos.
- Ahora reseteamos un teléfono Android en mi caso seria Samsun A30, lo volvemos a estado de fábrica.
- Cuando el teléfono este iniciando y salga la pantalla de Samsung presionamos 7 veces o en mi caso solo dos veces para activar cámara para escanear el QR.
- Una vez escaneo el QR se iniciará el proceso de instalación y asociación de mi teléfono con Miscrost Intune.
- Cuando inicie el teléfono tendremos un dispositivo totalmente gestionado por Intune y verificamos que estén correctamente aplicadas las políticas definidas.

Definir políticas de seguridad

Política de contraseña y bloqueo de pantalla.

Descripción: Requiere PIN o Contraseña segura, bloqueo automático y límite de intentos fallidos.

Objetivo: Evitar acceso no autorizados a datos corporativos.

Controles ISO 27001

Segregación de acceso lógico: asegura que los usuarios autorizados accedan al sistema.

Control de acceso: Establece autentificación fuerte en dispositivos.

Gestión de credenciales: Protege la configuración de autentificación.

Cifrado obligatorio de dispositivos

Descripción: Obligar a cifrar la memoria interna.

Objetivo: Proteger datos en caso de robo o pérdida.

Controles ISO 27001

Protección de datos en tránsito y reposo: protege datos almacenados.

Protección de información en dispositivos: requisito directo.

Eliminación segura o apropiada de información: se complementa con borrado remoto.

Restricción o Bloqueo de Aplicaciones No Autorizadas

Descripción: Usar políticas de restricción de software para bloquear apps no corporativas.

Objetivo: Reducir malware, fugas de información y apps de riesgo.

Controles ISO 27001

Protección frente a software malicioso: evita apps riesgosas.

Política de uso aceptable: regula uso permitido.

Control de acceso: limita accesos no autorizados a información.

Control de Redes: Wifi, VPN y APN Seguros

Descripción: Configura Wifi corporativa, VPN obligatorio o bloquea redes inseguras.

Objetivo: Asegurar comunicaciones y evitar ataques MITM.

Controles ISO 27001

Protección de datos en tránsito: protege comunicaciones móviles.

Seguridad de redes: garantiza redes seguras.

Uso seguro de servicios externos: evita redes no controladas.

Deshabilitar Funciones de Riesgo

Funciones típicas bloqueadas: Limitar USB externo deshabilitar instalación de software no autorizado, bloquear opciones de administrador.

Objetivo: Evitar manipulación del dispositivo o fuga de información.

Controles ISO 27001

Restricción de funciones: control de capacidades no necesarias.

Protección contra software malicioso.

Protección de dispositivos móviles.

Geolocalización y Borrado Remoto

Descripción: Borrado remoto y bloqueo.

Objetivo: Minimizar impacto de incidentes.

Controles ISO 27001

Gestión de incidentes de seguridad: respuesta ante pérdida/robo.

Eliminación segura de información: borrado remoto seguro.

Continuidad del negocio: reduce afectación de incidentes.

Políticas de Inventario y Gestión del Ciclo de Vida

Descripción: Registrar dispositivos, verificar estado de seguridad y mantener inventario actualizado.

Objetivo: Asegurar control del hardware que accede a datos corporativos.

Controles ISO 27001

Inventario de activos: mantiene registro del dispositivo.

Gestión de activos: asignación y control del dispositivo.

Configuración segura: asegurar dispositivos conforme a estándares.

Actualizaciones Automáticas y Parcheo

Descripción: Forzar Windows Update automáticas, aplicaciones corporativas actualizadas.

Objetivo: Reducir vulnerabilidades explotables.

Controles ISO 27001

Gestión de vulnerabilidades técnicas: implica parcheo.

Gestión de configuración: asegurar versiones correctas.

Protección frente a malware: evita explotación de fallos.

Separación de Datos Personales y Corporativos

Descripción: Configura contenedores o perfiles de trabajo para aislar datos.

Objetivo: Separar información corporativa de información personal.

Controles ISO 27001

Clasificación de la información: separa datos sensibles.

Manejo de información: protege datos corporativos.

Protección de datos personales: cumplimiento de privacidad.

Control de Copias y Compartición de Datos

Descripción: Bloquear copias de archivos sensibles a dispositivos externos o carpetas no corporativas.

Objetivo: Evitar fugas de información.

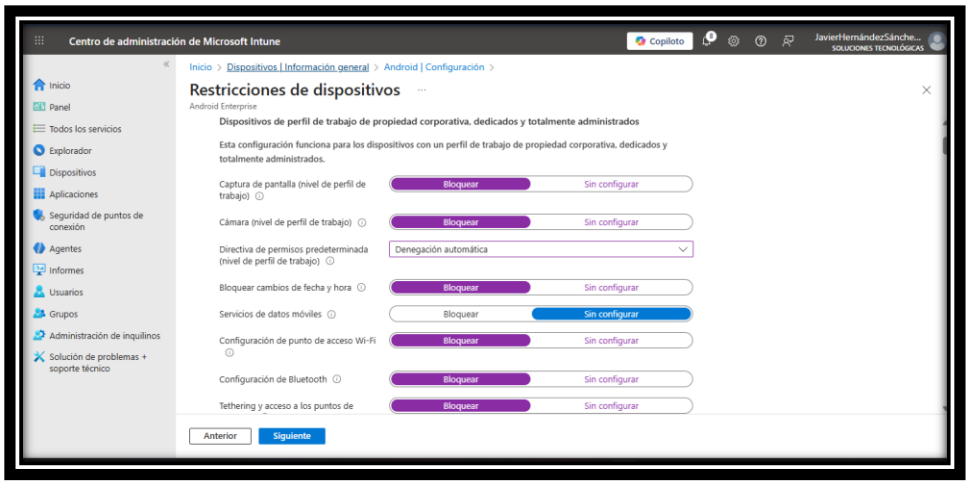
Controles ISO 27001

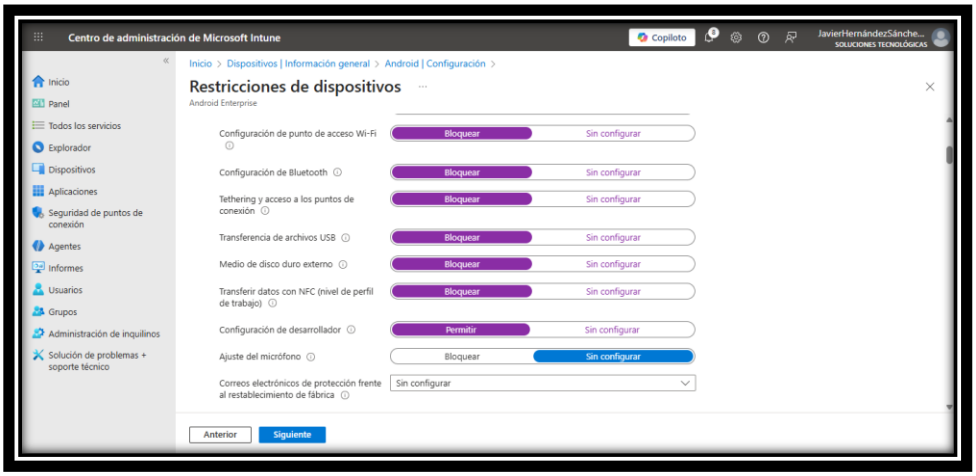
Manejo de información: protege datos.

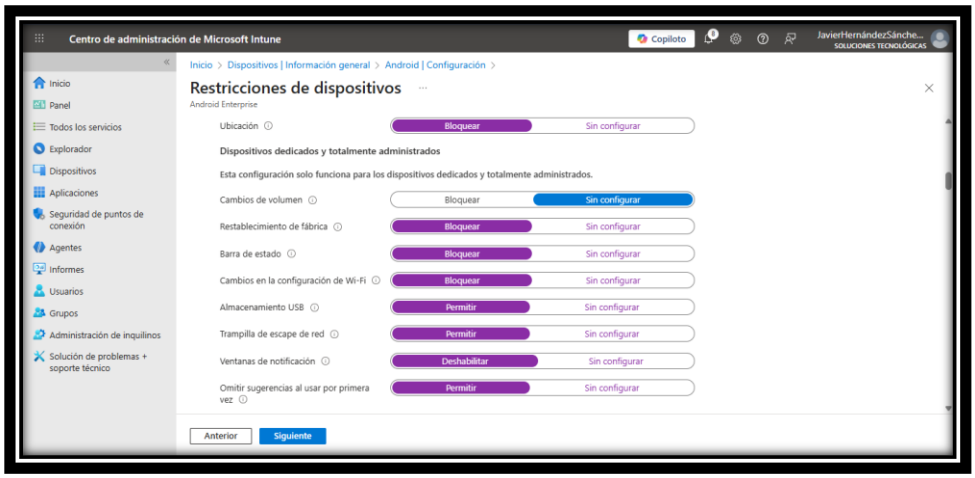
Protección de datos personales

Protección de dispositivos móviles

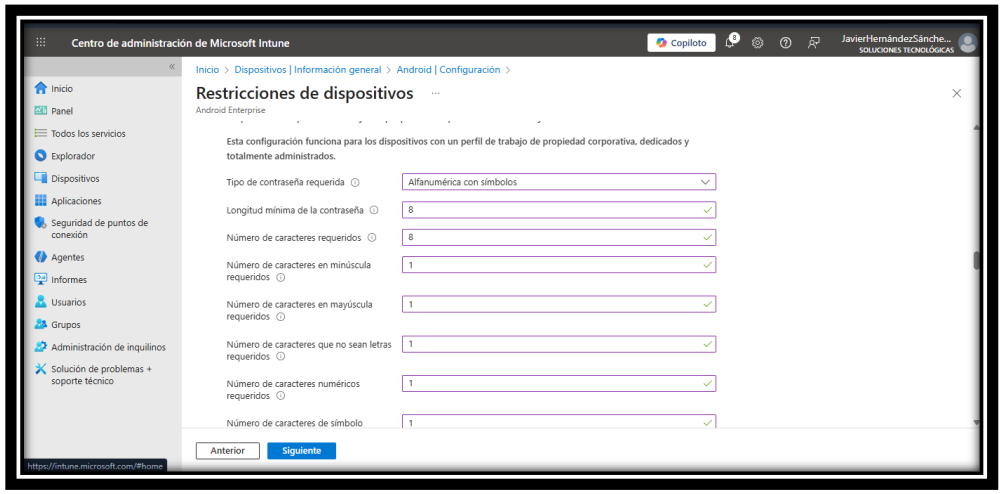
Evidencias

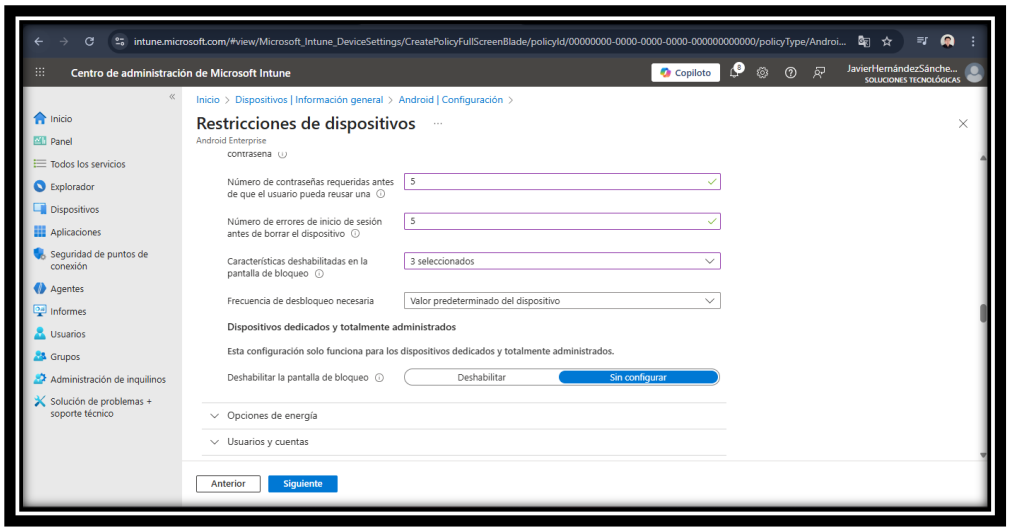


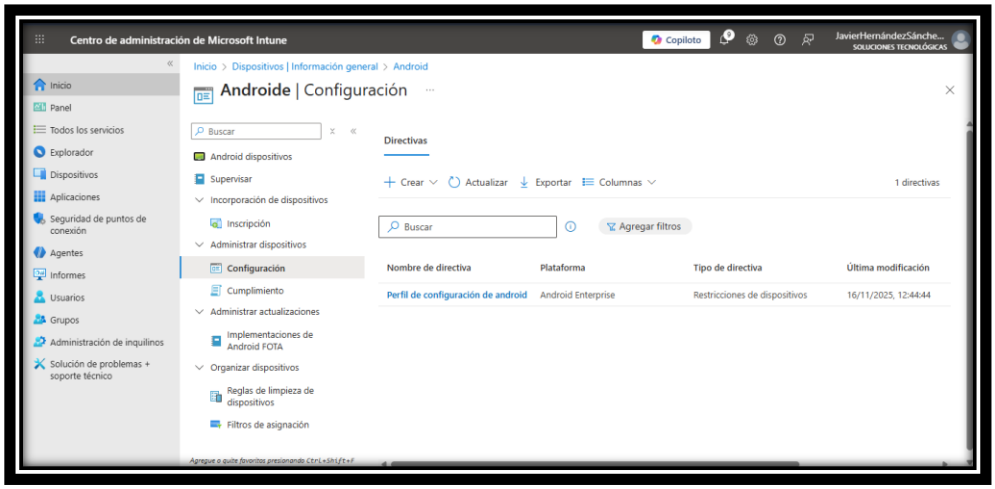


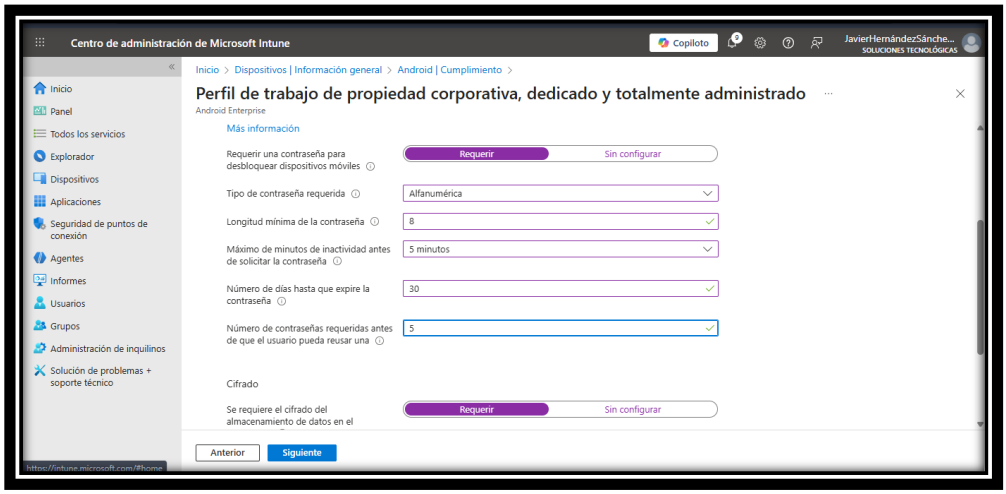

Centro de administración de Microsoft Intune
Copiloto
JavierHernándezSánche...
SOLUCIONES TECNOLÓGICAS
Inicio > Dispositivos | Información general > Android | Configuración >
Restricciones de dispositivos
Android Enterprise
Ubicación
Bloquear
Sin configurar
Dispositivos dedicados y totalmente administrados
Esta configuración solo funciona para los dispositivos dedicados y totalmente administrados.
Cambios de volumen
Restablecimiento de fábrica
Barra de estado
Cambios en la configuración de Wi-Fi
Almacenamiento USB
Permitir
Trampilla de escape de red
Ventanas de notificación
Deshabilitar
Omitir sugerencias al usar por primera vez
Anterior
Siguiente

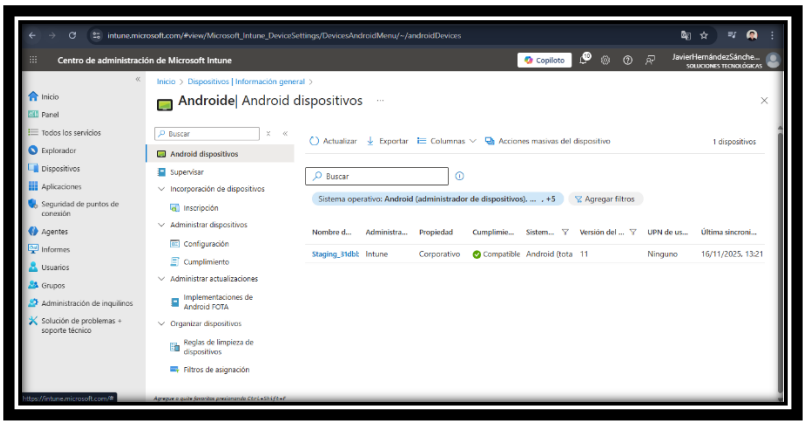

Centro de administración de Microsoft Intune
Copiloto
JavierHernándezSánche...
SOLUCIONES TECNOLÓGICAS
Inicio > Dispositivos | Información general > Android | Configuración >
Restricciones de dispositivos
Android Enterprise
Dispositivos de perfil de trabajo de propiedad corporativa y totalmente administrados
Esta configuración solo funciona para dispositivos de perfil de trabajo de propiedad corporativa y totalmente administrados.
Buscar dispositivo
Permitir
Sin configurar
Dispositivos totalmente administrados y dedicados (solo en modo de pantalla completa)
Esta configuración solo funciona para dispositivos totalmente administrados y dedicados que funcionan con una directiva de pantalla completa.
Menú de botón de encendido
Bloquear
Advertencias de errores del sistema
Características de navegación del sistema habilitadas
Información y notificaciones del sistema
Anterior
Siguiente

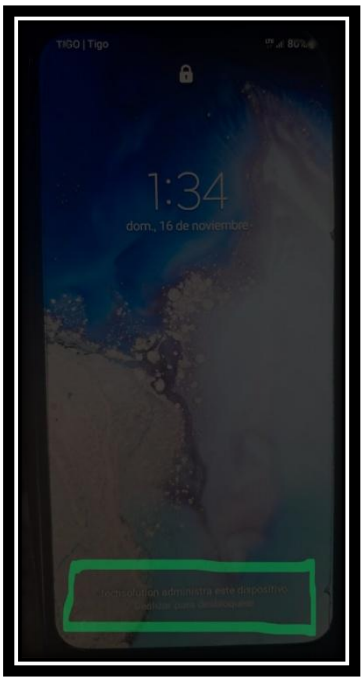

Centro de administración de Microsoft Intune
Copiloto
JavierHernándezSánche...
SOLUCIONES TECNOLÓGICAS
Inicio > Dispositivos | Información general > Android | Configuración >
Restricciones de dispositivos
Android Enterprise
Esta configuración funciona para los dispositivos con un perfil de trabajo de propiedad corporativa, dedicados y totalmente administrados.
Tipo de contraseña requerida
Alfanumérica con símbolos
Longitud mínima de la contraseña
8
Número de caracteres requeridos
Número de caracteres en minúscula requeridos
1
Número de caracteres en mayúscula requeridos
Número de caracteres que no sean letras requeridos
Número de caracteres numéricos requeridos
Número de caracteres de símbolo
Anterior
Siguiente
https://intune.microsoft.com/#home

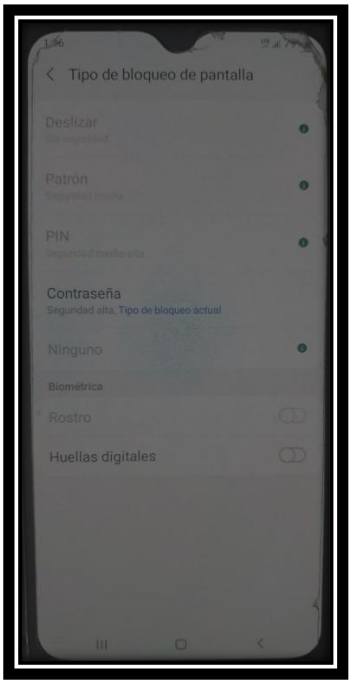

Centro de administración de Microsoft Intune
Copiloto
Inicio > Dispositivos | Información general > Android | Configuración >
Restricciones de dispositivos
Android Enterprise
contrasena
Número de contraseñas requeridas antes de que el usuario pueda reusar una
5
Número de errores de inicio de sesión antes de borrar el dispositivo
5
Características deshabilitadas en la pantalla de bloqueo
3 seleccionados
Frecuencia de desbloqueo necesaria
Valor predeterminado del dispositivo
Dispositivos dedicados y totalmente administrados
Esta configuración solo funciona para los dispositivos dedicados y totalmente administrados.
Deshabilitar la pantalla de bloqueo
Deshabilitar
Sin configurar
Opciones de energía
Usuarios y cuentas
Anterior
Siguiente

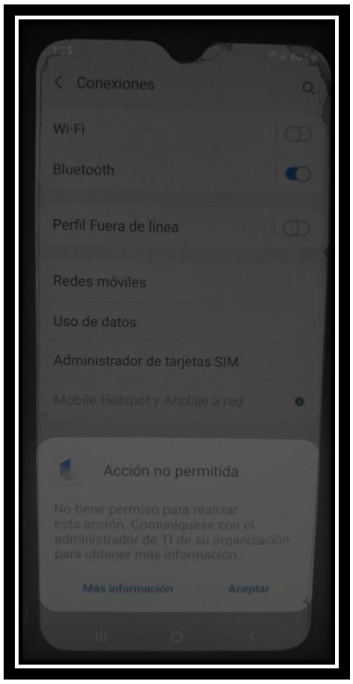

Centro de administración de Microsoft Intune
Copiloto
Inicio > Dispositivos | Información general > Android
Androide | Configuración
Directivas
Crear
Actualizar
Exportar
Columnas
1 directivas
Buscar
Agregar filtros
Nombre de directiva
Plataforma
Tipo de directiva
Última modificación
Perfil de configuración de android
Android Enterprise
Restricciones de dispositivos
16/11/2025, 12:44:44


Centro de administración de Microsoft Intune
Copiloto
Inicio > Dispositivos | Información general > Android | Cumplimiento
Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado
Android Enterprise
Más información
Requerir una contraseña para desbloquear dispositivos móviles
Requerir
Sin configurar
Tipo de contraseña requerida
Alfanumérica
Longitud mínima de la contraseña
8
Máximo de minutos de inactividad antes de solicitar la contraseña
5 minutos
Número de días hasta que expire la contraseña
30
Número de contraseñas requeridas antes de que el usuario pueda reusar una
5
Cifrado
Se requiere el cifrado del almacenamiento de datos en el
Requerir
Sin configurar
Anterior
Siguiente









Conclusión

Después de realizar toda la práctica con Microsoft Intune, pudimos entender de manera mucho más concreta cómo funciona un entorno MDM en un escenario real. El proceso de inscripción del dispositivo, la creación de políticas y la aplicación de configuraciones nos permitió ver cómo un teléfono puede pasar de ser un equipo común a convertirse en un dispositivo totalmente gestionado y seguro. Aunque algunos pasos requieren precisión como la creación de directivas o la asignación de filtros, el sistema en general resulta ordenado y lógico una vez que se comprende su estructura.

Lo más valioso fue comprobar en la práctica cómo cada política de seguridad realmente se aplica en el dispositivo y cómo esto ayuda a cumplir estándares como ISO 27001. Desde el cifrado, las restricciones de aplicaciones, el control de redes y el borrado remoto, cada medida se puede vincular claramente a un riesgo que se busca mitigar. En conjunto, la experiencia nos dejó una visión más completa de cómo una organización puede mantener sus dispositivos bajo control y proteger la información sin depender únicamente del usuario final. Intune demostró ser una herramienta robusta, flexible y alineada con buenas prácticas de seguridad modernas.