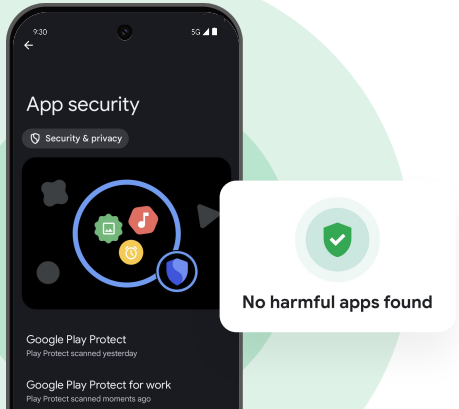
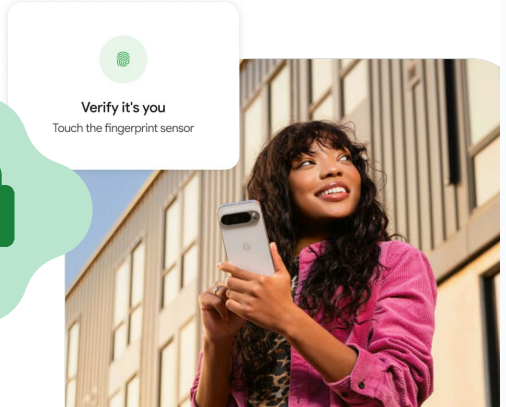
Android

Guía de seguridad móvil para pymes





Información general

Implementar medidas de seguridad de los datos sólidas es muy importante para las pequeñas empresas. Según Hiscox[1], el 25 % de las pequeñas empresas cierran tras experimentar una brecha de seguridad, ya que estas suponen de media un gasto de 200.000 USD.

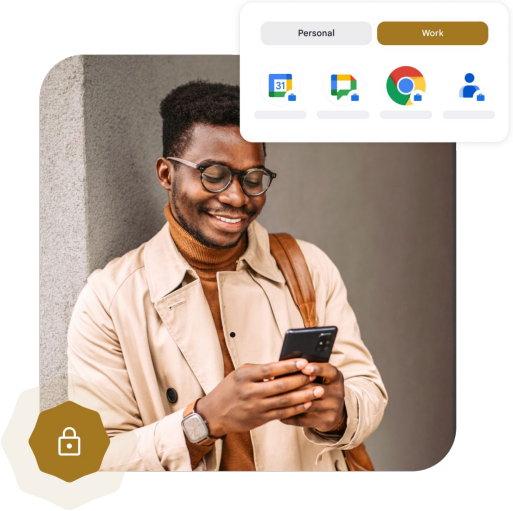
En un mundo tan hiperconectado como el actual, los smartphones y las tablets son herramientas potentes, pero también un riesgo potencial para la seguridad si no se gestionan correctamente.

El phishing es una de las mayores amenazas para los usuarios de dispositivos móviles, ya que el 83 % de los sitios de phishing[2] están dirigidos específicamente a dispositivos móviles. Los atacantes ahora utilizan la IA para lanzar ataques sofisticados que pueden engañar incluso a usuarios experimentados.

Gestionar el ciclo de vida completo de los dispositivos empresariales y asegurar la privacidad y la seguridad de los datos de los empleados y de la empresa puede parecer una tarea compleja. Sin embargo, resulta fácil y sencilla si se utilizan las herramientas adecuadas.

Android ofrece medidas de protección sencillas y discretas para mantener seguros los dispositivos y datos de la empresa, y defenderse de los ataques de phishing. Esto es esencial para las empresas que no cuentan con un equipo de TI especializado en proteger y gestionar los dispositivos.

En esta guía, compartimos prácticas recomendadas para proteger los datos de tu empresa y destacamos las características que hacen que Android sea una plataforma tan sólida y segura.



[1] Informe de Ciberpreparación de Hiscox
[2] Zimperium: informe "Global Mobile Threat Report", 2024

Información sobre los modelos de registro de dispositivos Android

Hay tres enfoques o modelos específicos que las empresas pueden implementar para proteger sus dispositivos y datos. Ofrecen varios niveles de control de los equipos de TI sobre los dispositivos.

01

El primer modelo no cuenta con funciones de gestión de la movilidad empresarial (EMM) y se clasifica como "Iniciado por el usuario". En este modelo, el equipo de TI de la empresa informa a los usuarios sobre las prácticas recomendadas para configurar ajustes específicos de seguridad y privacidad en sus dispositivos.

02

En la segunda opción, Device Trust from Android Enterprise ofrece un modelo de confianza cero para mejorar la seguridad. Este enfoque mejora la capacidad de los proveedores de soluciones de confianza para comprobar el estado de seguridad de un dispositivo independientemente de que esté gestionado por un sistema de EMM. Incluye un amplio conjunto de soluciones, como proveedores de identidades (IdPs), protección contra amenazas móviles, funciones de detección y respuesta (EDRs) y proveedores de redes privadas virtuales (VPNs). La integración de estas soluciones de partners con Android Enterprise permite verificar que los dispositivos cumplen determinados criterios antes de concederles acceso a los recursos de la empresa.

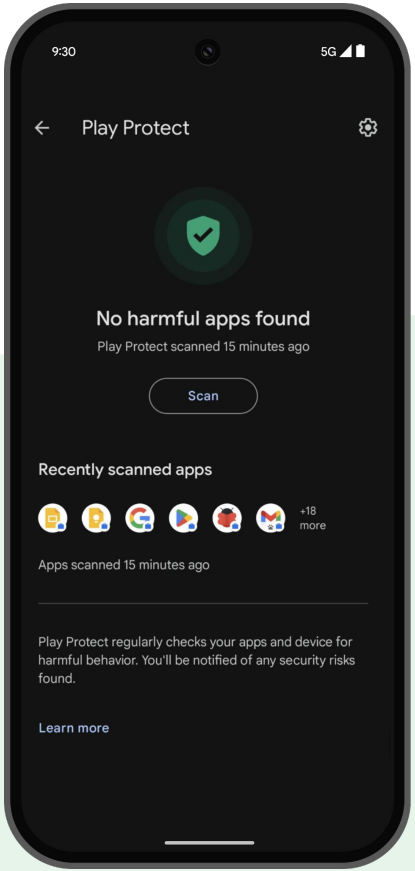
03

El tercer modelo se basa en los controles de gestión de la movilidad empresarial (EMM), que permiten a las organizaciones ejercer un mayor control sobre los dispositivos de los usuarios, ya sean propiedad de la empresa o formen parte de un programa de Bring Your Own Device (BYOD). En el caso de los dispositivos personales, la empresa da de alta un perfil de trabajo, lo que permite al equipo de TI supervisarlo de forma exhaustiva y proteger la privacidad del usuario en su área personal.

Android Enterprise ofrece varios modelos de registro de dispositivos para satisfacer las necesidades de los clientes de pymes

Para ofrecer mayor flexibilidad a las pymes, todos los modelos pueden integrarse y usarse de forma conjunta en función de las necesidades de cada empresa. Gracias a las sólidas funciones de seguridad de Android y a estas prácticas recomendadas, tu empresa podrá operar con confianza en el entorno móvil.

El compromiso de Android con los avances en materia de seguridad, además de su flexibilidad y rentabilidad, lo convierten en la mejor opción para las pequeñas y medianas empresas.



Políticas de seguridad y ajustes recomendados para los modelos de registro

Instrucciones específicas para cada modelo: Iniciado por el usuario, Device Trust y EMM.

Cada uno de estos modelos está diseñado para cumplir niveles de privacidad del usuario y de control de la empresa específicos en función de tus requisitos.

01 Configuración de seguridad iniciada por el usuario

El equipo de TI informará a los usuarios sobre cómo y por qué deben configurar manualmente los siguientes ajustes en sus dispositivos Android para proteger los datos de los usuarios y de la empresa.

- Habilitar Bloqueo Antirrobo
- Habilitar Bloqueo Remoto
- Habilitar Bloqueo del Dispositivo Sin Conexión
- Habilitar Verificación de Identidad
- Habilitar Espacio Privado
- Definir un PIN o una contraseña de al menos 6 caracteres que no se repitan
- Asegurarse de que Google Play Protect esté habilitado
- Instalar aplicaciones solo desde Google Play Store

02 Modelo de confianza cero

Además de los controles y las restricciones disponibles con Device Trust from Android Enterprise, el equipo de TI también debería enseñar a los usuarios a configurar y aprovechar todas las funciones de seguridad iniciadas por el usuario que se mencionan en la sección 1.

Modelo Device Trust:

Selecciona de la siguiente lista qué comprobaciones quieres implementar antes de permitir el acceso a los recursos de la empresa. La elección de los ajustes dependerá de los partners de Device Trust, por lo que te recomendamos que consultes la documentación correspondiente.

02 Device Trust from Android Enterprise

Selecciona de la siguiente lista qué comprobaciones quieres implementar antes de permitir el acceso a los recursos de la empresa. La elección de los ajustes dependerá de los partners de dispositivos de confianza, por lo que te recomendamos que consultes la documentación correspondiente.

Señal	Descripción
Modelo o marca del dispositivo	Muestra el modelo y la marca del dispositivo.
Estado de la gestión	Muestra el estado de la gestión y la aplicación de gestión.
Estado de la red	Muestra información sobre todas las redes activas del dispositivo.
Nivel del parche de seguridad del dispositivo	Muestra el nivel del parche de seguridad del dispositivo (incluido el nivel del parche de la actualización del sistema de Google Play).
Nivel del parche de seguridad publicado	Muestra el nivel del parche de seguridad publicado por Google para el componente actualizable correspondiente del dispositivo.*
Estado de cifrado del disco	Muestra si el almacenamiento del dispositivo está cifrado.
Versión del SO y actualizaciones OTA pendientes	Muestra la versión del SO del dispositivo y si hay alguna actualización del SO pendiente.
Bloqueo de pantalla y control de calidad	Muestra la complejidad del bloqueo de pantalla que tiene definido el usuario en ese momento.
Estado de Play Protect	Muestra si Google Play Protect está habilitado.

03 Habilitado por políticas de EMM

Los administradores de TI pueden consultar la documentación de su sistema de gestión de la movilidad empresarial sobre cómo configurar las políticas para proteger a los usuarios. Mediante este sistema, el departamento de TI puede configurar los dispositivos como perfil de trabajo, propiedad de la empresa, perfil personal (COPE) o totalmente gestionado. Tanto el perfil de trabajo como los dispositivos COPE proporcionan a la empresa opciones para gestionar un perfil de trabajo, pero solo estos últimos ofrecen un mayor control sobre todo el dispositivo. Estos son algunos ejemplos de controles de seguridad que se deben tener en cuenta:

- Longitud mínima de la contraseña: 6 caracteres
- Máximo de intentos para desbloquear el dispositivo: 10
- Habilitar Google Play Integrity
- Inhabilitar capturas de pantalla
- No permitir que se añadan cuentas en el perfil de trabajo
- Inhabilitar Opciones para desarrolladores
- No instalar aplicaciones de fuentes desconocidas
- Inhabilitar la función de copiar y pegar entre perfiles
- No permitir Android Debug Bridge (ADB)
- Usar Google Play administrado con listas de permitidos
- No inhabilitar Navegación Segura en Chrome

Prácticas recomendadas para implementar dispositivos Android en tu empresa

01 Enseñar a los empleados a habilitar funciones de seguridad integradas

Práctica recomendada

Protege tus datos frente a robos y accesos no autorizados con funciones adicionales integradas y diseñadas para proteger la información confidencial de la empresa. Por ejemplo:

A

Activa Bloqueo Antirrobo, que usa la IA, los sensores de movimiento de tu dispositivo, el Wi-Fi y el Bluetooth para detectar un movimiento brusco y bloquear el dispositivo automáticamente.

B

Activa y usa Bloqueo Remoto.
Si pierdes tu dispositivo o te lo roban, puedes usar Bloqueo Remoto con un número de teléfono verificado para bloquear la pantalla rápidamente.

C

Activa Bloqueo del Dispositivo Sin Conexión.
Poco después de que el dispositivo se quede sin conexión, Bloqueo del Dispositivo Sin Conexión bloquea automáticamente la pantalla del dispositivo para proteger tus datos. Por ejemplo, si alguien te roba el teléfono y desactiva la conexión a Internet para que no puedas encontrarlo con Encontrar Mi Dispositivo, el dispositivo se bloqueará después de estar sin conexión durante un breve periodo.

01 Enseñar a los empleados a habilitar funciones de seguridad integradas

Práctica recomendada

Protege tus datos frente a robos y accesos no autorizados con funciones adicionales integradas y diseñadas para proteger la información confidencial de la empresa. Por ejemplo:

D

Activa Verificación de Identidad. Para verificar tu identidad, Verificación de Identidad requiere datos biométricos y otras medidas de seguridad. Tu identidad se verifica cuando llevas a cabo acciones sensibles en tu dispositivo o haces cambios en tu cuenta de Google fuera de los sitios de confianza.

E

Oculta aplicaciones sensibles con el Espacio Privado. Para proteger tus aplicaciones privadas frente a accesos no autorizados, Android ofrece la función de Espacio Privado. De esta forma, se crea un área oculta e independiente en tu dispositivo donde puedes organizar tus aplicaciones personales. Aunque te roben el teléfono desbloqueado, tus aplicaciones sensibles seguirán estando protegidas dentro del espacio privado.

F

Google también ha integrado funciones antiphishing directamente en Mensajes de Google para proteger a los usuarios frente a las técnicas de phishing más sofisticadas. Además, hay nuevas funciones que mejoran la protección de los usuarios, como la protección contra spam y el identificador de llamada de Android.

02 Usar el directorio de soluciones de Recomendado por Android Enterprise

Práctica recomendada

Crea una lista de dispositivos aprobados para usarlos en el trabajo en el directorio de soluciones de Recomendado por Android Enterprise.

Los dispositivos de nuestro directorio se someten a rigurosas pruebas de seguridad y se actualizan con regularidad.

La validación de Recomendado por Android Enterprise asegura que tu empresa reciba dispositivos con funciones y mejoras de seguridad integradas que se han optimizado para satisfacer sus necesidades.

03 Implementar una solución de gestión de dispositivos para tener un control centralizado

Práctica recomendada

Utiliza una solución de gestión de la movilidad empresarial para implementar políticas de seguridad, bloquear dispositivos o borrar sus datos de forma remota y gestionar la descarga de aplicaciones. Para ver una lista de partners de EMM validados y autorizados, puedes consultar el directorio de soluciones de EMM de Recomendado por Android Enterprise.

La completa integración de Android con las soluciones de EMM permite a las empresas de cualquier tamaño tener un control granular y una gestión de la seguridad eficiente.

04 Actualizaciones de seguridad constantes

Práctica recomendada

Usa las políticas de dispositivos de Android Enterprise mediante una solución de EMM para asegurar que todos los dispositivos cuenten con los últimos parches de seguridad de Android. Android Enterprise proporciona a los administradores opciones para aplicar políticas de actualizaciones del SO y las aplicaciones que se ajusten a las necesidades de la empresa.

Android se ha comprometido a lanzar actualizaciones de seguridad cada 30 días para que el ecosistema de los fabricantes y operadores pueda ofrecer actualizaciones a tiempo. Además, si seleccionas dispositivos del directorio de soluciones, recibirán actualizaciones al menos cada 90 días. Los fabricantes de dispositivos, como Pixel y Samsung, ahora ofrecen 7 años de actualizaciones de seguridad y del SO. De esta forma, las posibles vulnerabilidades se solucionan rápidamente.

05 Implementar una autenticación segura

Práctica recomendada

Los controles de Android Enterprise ofrecen la posibilidad de configurar requisitos para los códigos de desbloqueo de los dispositivos. Estas opciones incluyen PINs, patrones y contraseñas, que se pueden combinar con opciones de desbloqueo facial y por huella digital. Los administradores pueden exigir a los usuarios que configuren requisitos que se ajusten a las necesidades de la organización. De acuerdo con las directrices más recientes de NIST SP 800-53, se requieren al menos 6 dígitos con caracteres que no se repitan.

La compatibilidad con la biometría de Android y el almacenamiento seguro de claves ofrecen a los usuarios una experiencia óptima y protegen el dispositivo mediante una autenticación segura y respaldada por hardware.

06 Implementar y gestionar aplicaciones de forma segura

Práctica recomendada

Permite que los usuarios solo instalen aplicaciones de Google Play Store y exige que Google Play Protect esté siempre habilitado. Con Google Play administrado, los administradores pueden elaborar una lista de aplicaciones aprobadas y configurar permisos.

Google Play Administrado impide que se instalen aplicaciones de fuentes desconocidas que no se hayan aprobado y Google Play Protect analiza de forma activa todas las aplicaciones instaladas en busca de malware.

07 Proteger los datos en tránsito

Práctica recomendada

Usa VPNs para establecer conexiones seguras con los servicios de tu empresa cuando estés fuera de la oficina, asegúrate de que todos los servicios usan HTTPS y configura correctamente las conexiones Wi-Fi de la red de tu empresa.

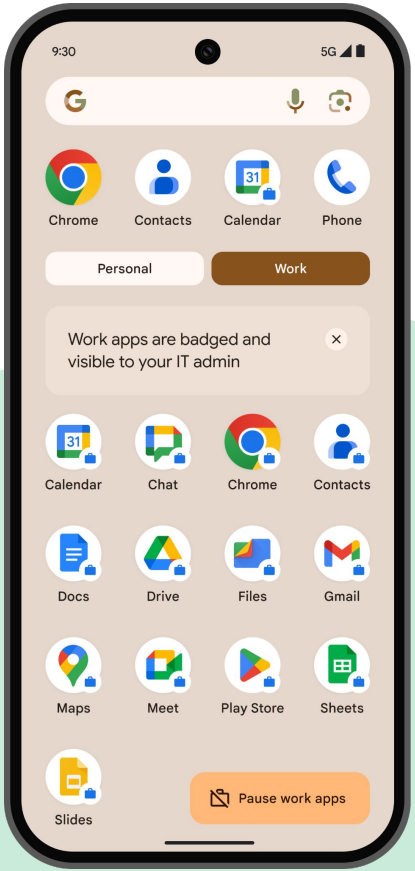
El sistema de cifrado integrado de Android y la compatibilidad con VPNs ayudan a proteger tus datos, tanto si están almacenados en el dispositivo como si se transmiten a través de la red.

08 Utilizar el perfil de trabajo de Android

Práctica recomendada

Si los empleados usan dispositivos personales (BYOD), los administradores deberían implementar un perfil de trabajo para separar los datos personales de los de la empresa en un mismo dispositivo.

El perfil de trabajo de Android es una función exclusiva de Android que permite crear un entorno seguro y aislado para proteger los datos empresariales y mantener la privacidad de los datos personales.



Conclusiones clave

Para minimizar las llamadas al centro de asistencia o al departamento de TI, es fundamental formar a los usuarios y ofrecerles una guía sencilla para configurar cada uno de los tres modelos.

Consulta el directorio de soluciones de Android Enterprise para ver una selección de dispositivos y partners aprobados. Este recurso puede ayudarte a elegir los productos más adecuados en función de tus necesidades.

Prioriza la implementación de medidas de seguridad, por muy básicas que sean. Todos los modelos de protección de dispositivos conllevan unos costes. Selecciona un modelo que te permita equilibrar las medidas de seguridad y los gastos de implementación y mantenimiento.

Android

Más información en

www.android.com/enterprise/security