

Guía de Seguridad de las TIC CCN-STIC 1637

Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 14)



Octubre de 2024





Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-198-X.

Fecha de Edición: octubre de 2024.

Samsung Electronics ha participado en el desarrollo del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1.	INTRODUCCION	1
1.1	COMPONENTES Y ESCENARIOS UNA SOLUCIÓN DE MOVILIDAD	2
1.1.1.	<i>Componentes.....</i>	2
1.1.2.	<i>Escenarios en función de la propiedad del dispositivo.....</i>	2
2.	PROCESO DE DESPLIEGUE.....	4
2.1	APIs Y SERVIDORES DE LICENCIAS DE KNOX	4
2.2	SELECCIÓN DE LA SOLUCIÓN MDM Y CONFIGURACIÓN	6
2.3	KNOX MOBILE ENROLLMENT	6
2.4	KNOX CONFIGURE	7
2.5	KNOX ASSET INTELLIGENCE.....	7
2.6	KNOX MANAGE	8
2.7	ENTERPRISE FIRMWARE OVER-THE-AIR (E-FOTA)	8
2.8	KNOX SERVICE PLUGIN (KSP)	9
2.9	SEPARATED APPS	10
2.10	SAMSUNG DEX.....	11
3.	CONFIGURACIÓN RECOMENDADA	12
3.1	DISPOSITIVOS CUALIFICADOS	12
3.1.1.	<i>Dispositivos Enterprise Edition.....</i>	13
3.2	IDENTIFICACIÓN DE VERSIÓN DE DISPOSITIVO	13
3.3	REGLAS DE CONFIGURACION GENERAL DEL DISPOSITIVO.....	14
3.3.1.	<i>Tabla de Configuración - COBO</i>	15
3.4	BORRADO DEL DISPOSITIVO	17
3.4.1.	<i>Desenrolado.....</i>	17
3.5	DIRECTIVAS A USUARIO FINAL / UBE (USER-BASED ENFORCEMENT).....	17
3.5.1.	<i>Alarma de calendario</i>	18
3.5.2.	<i>Transferencia de contenido y Duplicado de pantalla.....</i>	18
3.5.3.	<i>Uso de Accesorios (DeX Station, USB Dongle)</i>	19
4.	ABREVIATURAS	20
ANEXO A.	INTRODUCCIÓN A KNOX PLATFORM FOR ENTERPRISE (KPE).....	22
	<i>KPE como extensión de AE.....</i>	22
	<i>ARMONIZACIÓN.....</i>	22
	<i>Trusted Execution Environment</i>	23
	<i>Knox Verified Boot (KVB)</i>	23
	<i>Knox Platform for Enterprise (KPE).....</i>	23
ANEXO B.	AUDITORIA DE CONFIGURACION SEGURA.....	24
ANEXO C.	TEST DEVICE POLICY CONTROL (TEST DPC)	45

1. INTRODUCCION

El objetivo de este documento es proporcionar una guía de configuración de los dispositivos Samsung Galaxy con Android cualificados por CCN e incluidos como tales en el Catálogo de Productos CPSTIC (cpstic.ccn.es).

El siguiente procedimiento de empleo seguro es válido para dispositivos **móviles Samsung con una versión de Android 14** o superior mientras no exista una publicación más reciente que sustituya este procedimiento.

Las diferentes secciones están organizadas como sigue:

La sección [1.1](#) proporciona una visión general de los componentes y escenarios de despliegue con los que el Administrador IT de la organización debe estar familiarizado. La correcta comprensión de este punto es vital a la hora de diseñar o plantear la renovación de un sistema de comunicaciones móviles¹.

La sección [2](#) revisa aspectos a tener en cuenta por un Administrador IT a la hora de diseñar un despliegue de comunicaciones móviles o replantear el diseño de uno existente. Aspectos como la arquitectura elegida para el sistema, la política de seguridad o los detalles de la solución MDM elegida se incluyen solo de manera superficial, no siendo objeto de la presente guía.

La sección [3](#) detalla la configuración recomendada que CCN y Samsung han elaborado como referencia para el Administrador IT de la organización. La configuración recomendada se compone de tres bloques:

- Las reglas de configuración general del dispositivo mediante el establecimiento de políticas en la consola de la herramienta de gestión (MDM/UEM),
- la desactivación de aplicaciones que pueden presentar un riesgo de filtrado de datos, y finalmente
- unas políticas que deben ser establecidas a base de directivas, esto es, configuración que debe realizar o no modificar el usuario final.

La configuración incluida en esta sección es la utilizada por el CCN y es la recomendada para despliegues que utilicen este documento como referencia. No se consideran otras configuraciones y no se pueden realizar valoraciones generales sobre el impacto en la seguridad de los cambios que se introduzcan.

El [ANEXO B](#) proporciona un lote de casos de test para facilitar la auditoría del despliegue en la organización acorde a esta guía de configuración segura.

El escenario validado por el Centro Criptológico Nacional y el que debe utilizarse en los despliegues que declaren conformidad con esta guía es el conocido como COBO (Corporate Owned Business Only), en el que el dispositivo se dedica exclusivamente al

¹ El lector puede acudir a la web del CCN, donde encontrará diferentes niveles de información. Se recomienda comenzar la lectura por la CCN-STIC 496.

uso profesional. Otros escenarios no están considerados en el proceso y no se realiza ninguna declaración sobre los mismos.

1.1 COMPONENTES Y ESCENARIOS UNA SOLUCIÓN DE MOVILIDAD

1.1.1. COMPONENTES

Para desplegar y mantener un sistema seguro basado en dispositivos móviles es necesario disponer de los siguientes bloques funcionales:

- Dispositivos móviles, con las capacidades y la configuración apropiada.
- Soluciones de gestión de dispositivos móviles (MDM-Mobile Device Management / UEM- Unified Endpoint Management / Enroll Service / Upgrade Service) apropiadas y que dispongan de las funcionalidades necesarias.
- Redes de comunicaciones, de diferentes tecnologías (3G, 4G, 5G, WiFi, ...).
- Equipo de Administradores de dispositivos móviles de la organización donde se realiza el despliegue, así como su estructura organizativa y recursos
- Política de seguridad de las TIC, en la que se reflejen la valoración de los sistemas, los riesgos a los que se enfrentan, las contramedidas utilizadas.
- Usuarios de la organización, responsables del uso diario de los dispositivos.

Todos estos elementos son necesarios y deben estar correctamente configurados y gestionados, debiendo mantenerse en todo momento una perspectiva de seguridad a nivel de sistema.

1.1.2. ESCENARIOS EN FUNCIÓN DE LA PROPIEDAD DEL DISPOSITIVO

Los tres principales escenarios en despliegue de una solución de movilidad en una organización se pueden clasificar como:

- BYOD - Bring Your Own Device
- COPE - Corporate-owned Personally Enabled
- COBO - Corporate Owned Business Only

En un escenario BYOD, el usuario final es propietario del dispositivo móvil, donde el Administrador IT de la organización genera un Workspace, también llamado contenedor o Perfil de Trabajo (WorkProfile), dentro de este espacio es donde la organización administra políticas y restricciones de seguridad, a través de una aplicación agente dentro del Workspace, mediante una aplicación Android especial llamada Profile Owner. El presente documento no aplica a este escenario, por no considerarse un escenario válido para despliegues donde los dispositivos vayan a utilizar o acceder a recursos de una organización.

En los escenarios COBO y COPE el dispositivo móvil es propiedad de la organización, y el Administrador IT tiene la posibilidad de controlar el dispositivo, implementando políticas de seguridad y restricciones.

En el escenario COPE, cuya implementación se denomina Work Profile in Company owned device (WP-C), existe una aplicación agente denominada PO (Profile Owner) con capacidad para aplicar políticas de seguridad y gestión tanto al perfil de trabajo como, limitadamente, a todo el terminal. Esta aplicación puede aplicar políticas sobre el lado personal siempre y cuando estas políticas no vulneren la privacidad del empleado. El Administrador IT de la organización, realizará una configuración de seguridad más estricta en Workspace / Contenedor de trabajo, que complementará la configuración básica del área personal del usuario. El presente documento no aplica a este escenario, por no considerarse un escenario válido para despliegues donde los dispositivos vayan a utilizar o acceder a recursos de una organización.

El escenario COBO, cuya implementación se denomina Fully managed Device, se utiliza en despliegues que requieren mayor seguridad, donde el usuario final no dispone de área personal, ya que el conjunto del dispositivo está fuertemente restringido. En un escenario COBO, existe un agente, aplicación Android especial, que se denomina DO (Device Owner), y **ningún** Workspace / Contenedor de trabajo es creado, el dispositivo en su totalidad es gestionado y securizado.

En este tipo de escenarios (COBO), la organización puede decidir aceptar la realización de ciertas comunicaciones personales esporádicas por parte del usuario final.

Los agentes MDM / UEM, tanto sean DO como PO son transparentes al Administrador IT de la organización, ya que el interfaz para el establecimiento de políticas y configuraciones es la consola de PC de la solución MDM / UEM.

El **escenario validado por el Centro Criptológico Nacional** y el que debe utilizarse en los despliegues que declaren conformidad con esta guía es el comúnmente conocido como **COBO**, en el que el dispositivo se dedica exclusivamente al uso profesional. Otros escenarios no están considerados en el proceso y no se realiza ninguna declaración sobre los mismos.

2. PROCESO DE DESPLIEGUE

El proceso, tipología y componentes utilizados en un despliegue específico de una organización dependerá de una serie de factores, entre los que se incluyen:

- Perfil de riesgo de la organización.
- Aspectos financieros.
- Legislación aplicable.
- Capacidad técnica de la organización.
- Arquitectura admitida por la solución de MDM escogida.
- Modelos de propiedad permitidos en la organización (COBO, WP-C, BYOD).

Cada organización es responsable de conocer y evaluar los factores que le son de aplicación previamente al diseño o replanteo del sistema, la reserva de recursos y la selección de componentes a incluir.

La organización que realiza el despliegue debe realizar un análisis del valor de la información que se va a manejar en los dispositivos móviles y la clasificación del sistema TIC de la organización en su conjunto según la legislación vigente antes de realizar el diseño del sistema o reservar recursos para su puesta en marcha.

A continuación, se introducen conceptos técnicos a tener en cuenta por un Administrador IT a la hora de diseñar un despliegue, así como soluciones de Samsung que pueden ser de utilidad cuando se incorpora movilidad en una organización. En este documento no se indica ni recoge el funcionamiento de ninguna solución MDM específica.

2.1 APIS Y SERVIDORES DE LICENCIAS DE KNOX

En la sección **3** de este documento, se indica la configuración recomendada para un despliegue, la cual, a nivel de dispositivo se realiza mediante el establecimiento de ciertas políticas de seguridad que se implementan en llamadas a APIs que el dispositivo móvil soporta.

No obstante, en el ecosistema de gestión de movilidad en las organizaciones, la interface que maneja el Administrador IT es la consola de la solución MDM elegida salvo en el caso de KSP que se comenta más adelante. Dichas soluciones cuando enrojan a un dispositivo instalan un agente, que es una aplicación de Android especial, la cual llamará a las APIs necesarias en el dispositivo acorde con los perfiles y configuraciones realizadas en la consola de PC de la solución MDM. Todo este proceso de llamadas a las APIs por el agente es transparente al Administrador IT de la organización.

Es por ello que es preciso que el Administrador IT, entienda qué política o regla puede y debe configurar el dispositivo, mediante una API propuesta, para después trabajar con su proveedor de MDM en identificar qué configuración de consola la satisface.

En un dispositivo Android de Samsung se encuentran disponibles las APIs de Android Enterprise, así como las específicas de Samsung llamadas Knox, estas últimas se ofrecen para configurar características adicionales y controles de seguridad mejorados o extendidos.

Para que las APIs de Knox funcionen correctamente es necesaria la activación de una licencia Knox Platform for Enterprise (KPE). La licencia KPE se obtiene desde el portal del cliente sin ningún coste asociado y debe ser activada desde el MDM/EMM. Durante el proceso de activación, el dispositivo validará la licencia contra el servidor Samsung Knox License Management (KLM). Una vez validada la licencia, todas las características KPE y APIs estarán disponibles. Los detalles técnicos de la configuración de la licencia KPE en la consola MDM así como su obtención no se cubre en la presente guía, ya que se pretende en este asunto informar al Administrador IT e instarle a continuar la conversación con su representante de la solución MDM y Samsung para su despliegue en concreto.

En el caso de tener un requerimiento en la organización de utilizar servidores On-Premise, se utilizarán los servidores de Activación de licencias Samsung Knox On-Premise. La instalación de los paquetes está disponible tanto para Windows como para Linux, con soporte de mantenimiento desde Samsung.

El servidor On-Premise incluye:

- KLM: El sistema de gestión de licencias y compliance, usado para activar los servicios KPE.
- Global Server Load Balancing (GSLB): Un servidor diccionario para servicios KPE. Durante la activación de la licencia, el servidor devolverá las URLs para los distintos servicios KPE y los dispositivos.

La licencia KPE Estándar contiene la URL del servidor GSLB en la nube. Para usar la solución on-premise, la licencia debe estar contenida en el servidor on-premise, para conseguirlo, la URL debe ser proporcionada por el revendedor Knox, de esta forma la licencia correcta será creada.

Para organizaciones que permitan el uso de servicios cloud es altamente recomendable usar el servicio de inscripción automatizado Knox Mobile Enrollment para garantizar la inscripción obligatoria en la solución UEM y el servicio Knox E-FOTA para administrar las actualizaciones del Firmware del dispositivo. Se puede obtener más información sobre las capacidades de estos servicios en las siguientes secciones.

2.2 SELECCIÓN DE LA SOLUCIÓN MDM Y CONFIGURACIÓN

La solución MDM seleccionada debe soportar el API extendido de Samsung Knox para habilitar las funcionalidades detalladas en esta guía. Cuanto más completo sea el soporte de la solución MDM a las APIs de Samsung Knox, mayores serán la funcionalidades, configuraciones y políticas que se puedan controlar en el dispositivo móvil utilizando la solución MDM seleccionada.

Para habilitar funcionalidades tales como el borrado remoto del dispositivo, la solución MDM puede requerir estar emplazada en un área de la organización con acceso a redes externas a la organización, para que la consola MDM pueda comunicarse con el Agente MDM instalado en el dispositivo móvil. Dicha conexión a Internet deberá realizarse siguiendo las instrucciones de despliegue de la solución MDM seleccionada y siempre respetando la normativa y criterios de seguridad en lo concerniente a interconexión de redes dentro del contexto del Esquema Nacional de Seguridad en función de la categoría del sistema.

La comunicación entre la consola en el dispositivo móvil puede realizarse habilitando o no una conexión VPN. La selección de una u otra posibilidad dependerá del análisis de riesgos realizado por la organización

Cuando se seleccione una solución MDM hay que prestar especial atención que la configuración del modo Common Criteria esté soportada. En caso contrario no se podrá configurar el dispositivo móvil en el modo certificado utilizado la solución MDM seleccionada y por lo tanto no se podrá alcanzar el nivel de seguridad para el que se ha adquirido.

2.3 KNOX MOBILE ENROLLMENT

KME es un servicio gratuito que ayuda a las organizaciones a automatizar el enrolado de los terminales móviles Samsung en el MDM/EMM. El uso de KME es recomendado por el CCN.

Para utilizar KME, el IMEI o número de serie de los terminales adquiridos son asignados al cliente por el reseller a través del Knox Development Program (KDP). Una vez registrada la cuenta de KME, el Administrador IT de la organización puede configurar el registro de los terminales utilizando la consola de la solución. El enrolado ocurre automáticamente cuando el usuario enciende el dispositivo y lo conecta a internet durante los primeros pasos de la configuración del terminal.

Las características básicas de KME incluyen:

- Retener el Control de Activos de la organización
 - Los terminales quedarán ligados a KME incluso tras realizar un Factory Data Reset

- Bypass del Factory Reset Protection de Google
- Inicio automático en el MDM/ EMM
 - A través de las credenciales de usuario controladas por el equipo de IT
- Proceso de configuración de dispositivos optimizado y personalizable
- Instalación automática de certificados raíz o intermedios

Para más información, visite [Knox Mobile Enrollment | Inscripción masiva de dispositivos empresariales \(samsungknox.com\)](https://www.samsungknox.com/es-419/solutions/it-solutions/knox-enrollment)

2.4 KNOX CONFIGURE

Es un servicio Cloud disponible para terminales Samsung que permite aplicar un perfil de configuración de manera remota, consiguiendo personalizar los terminales para las necesidades del caso de negocio específico. Se puede aplicar un perfil de configuración donde se apliquen restricciones sobre los ajustes, se instalen aplicaciones, se defina una animación al encender o apagar el terminal, el fondo de pantalla como la imagen de la compañía, además de otro tipo de contenido. Los dispositivos registrados recibirán la configuración una vez que el terminal tenga conexión a internet, ya sea vía WiFi o datos móviles.

Para más información, consultar el enlace del producto:

<https://www.samsungknox.com/es-419/solutions/it-solutions/knox-configure>

Así como la Admin guide: <https://docs.samsungknox.com/admin/knox-configure/welcome.htm>

2.5 KNOX ASSET INTELLIGENCE

Es un servicio Cloud disponible para algunos modelos Samsung que nos permitirá consultar el estado de estos terminales para realizar una administración inteligente de los mismos en términos de batería, información de aplicaciones, información de conectividad y conocer la ubicación del terminal y comunicarnos con el mismo.

Para más información sobre el servicio y terminales, consultar los enlaces:
<https://www.samsungknox.com/es-419/solutions/it-solutions/knox-asset-intelligence>
<https://www.samsungknox.com/en/knox-platform/supported-devices>

2.6 KNOX MANAGE

Servicio Cloud que permite administrar tanto terminales Samsung como cualquier terminal Android, iOS o Windows 10 ofreciendo un extra de políticas de seguridad y gestión para los terminales Samsung gracias a las APIs de Knox Platform.

Para más información sobre el servicio, consultar el enlace:

<https://www.samsungknox.com/es-419/solutions/it-solutions/knox-manage>

Así como la guía de administración, con información más técnica:
<https://docs.samsungknox.com/admin/knox-manage/welcome.htm>

2.7 ENTERPRISE FIRMWARE OVER-THE-AIR (E-FOTA)

E-FOTA controla las versiones del Sistema Operativo en los dispositivos Samsung Galaxy, para garantizar que los últimos parches de seguridad se implementan en los terminales. Los administradores de IT pueden probar las actualizaciones antes de implementar una campaña de actualización de terminales, asegurando la compatibilidad entre las aplicaciones internas y las nuevas versiones del Sistema Operativo. E-FOTA está recomendado por el CCN para su uso en la Organización.

Las características básicas incluyen:

- Actualización selectiva de versiones del Sistema Operativo
- Asignación de múltiples dispositivos a diferentes versiones del Sistema Operativo en una misma campaña
- Carga automatizada de identificadores de dispositivos por medio de los revendedores (registrados en el servicio de Knox Deployment Program)
- Instalación automática del cliente E-FOTA
- Flexibilidad a la hora de añadir licencias
- No es necesaria la interacción del usuario
- Actualizaciones programadas
- Actualizaciones forzadas
- Bypass de las restricciones FOTA del Carrier

Para más información, visite https://www.samsungknox.com/es-419/solutions/it-solutions/samsung_e-fota

2.8 KNOX SERVICE PLUGIN (KSP)

Como se ha comentado en el apartado 2.1 la implementación de las políticas de seguridad en el dispositivo se realiza mediante APIs, y que el interfaz con el Administrador IT es la consola de la solución MDM.

Es por esto que nativamente cada solución MDM ofrece al Administrador IT un subconjunto de las políticas/APIs soportadas en el dispositivo móvil. Además, cuando Samsung diseña nuevas políticas/APIs es decisión de la solución MDM si la implementa y la pone a disposición del Administrador IT en la consola y cuándo lo hace.

Es por esta razón que Samsung ha creado la solución Knox Service Plugin (KSP) para proporcionar al Administrador IT de la organización un mecanismo para configurar ciertas políticas/APIs de Knox como extensión a la funcionalidad ofrecida por la consola MDM.

Knox Service Plugin (KSP) es una aplicación disponible en Google Play, que se puede incorporar como aplicación a desplegar en los dispositivos de la organización igual que cualquier otra, siguiendo el procedimiento de incorporar una aplicación al Catálogo de Aplicaciones permitidas y aprobadas en el MDM.

Al igual que otras aplicaciones de Google Play, Knox Service Plugin (KSP) permite realizar una configuración de la aplicación en el MDM, que se instalará al mismo tiempo que la aplicación es instalada en el dispositivo, es lo que se denomina Managed Configuration.

Knox Service Plugin

Samsung Electronics Co., Ltd.

4.0 ★
523 reviews

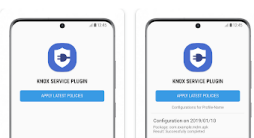
50K+
Downloads

Everyone

Install

Share

Add to wishlist



https://play.google.com/store/apps/details?id=com.samsung.android.knox.kpu&hl=en_GB&gl=US

De esta manera mediante la configuración de la aplicación en el MDM podemos realizar llamadas específicas a APIs para implementar políticas no soportadas nativamente en nuestro MDM.

Para más información, visite

<https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/welcome/>

2.9 SEPARATED APPS

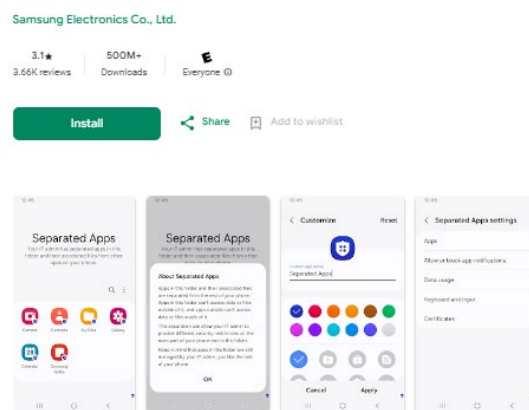
Como se ha explicado en la sección 1.1.2, en los escenarios de despliegue COBO, cuya implementación se denomina Fully Managed Device, donde solamente existe un agente administrador (aplicación APK especial de Android) en el dispositivo llamado Device Owner (DO), las aplicación disponibles en el escritorio principal del dispositivo están muy limitadas por las políticas de seguridad de la organización.

Es por esta razón, que en los dispositivos Samsung existe una funcionalidad llamada Separated Apps que permite la creación de una nueva carpeta en el dispositivo donde el Administrador IT permitirá ciertas aplicaciones de conveniencia para el usuario, pero que está aisladas del resto de aplicaciones corporativas.

Separated Apps es una solución alternativa a usar un perfil de trabajo para aplicaciones y datos aislados del grupo principal. Se aprueban aplicaciones separadas para su uso en la Organización.

Separated Apps se habilita en los dispositivos mediante una configuración a realizar en KSP explicada en la sección 2.8, o en dispositivos con Android 14 Knox 3.10 o superiores alternativamente se puede realizar asignado y configurando, al igual se hace con KSP, la aplicación Separated Apps.

Separated Apps



https://play.google.com/store/apps/details?id=com.samsung.android.appseparation&hl=en_GB&gl=US

En el caso de utilizar la configuración utilizando KSP, note el Administrador IT, que la aplicación Separated Apps se proporciona de serie en los binarios de Android, estando ya presente en el dispositivo móvil antes realizar habilitación alguna. En este caso la aplicación/paquete se actualiza automáticamente de Google Play igualmente.

Separated Apps permite especificar la lista de aplicaciones que se aislarán en la carpeta de aplicaciones separadas. Hay dos opciones para separar aplicaciones:

- Interna: Aísla una lista de aplicaciones que se instalarán y ejecutarán dentro de este espacio
- Externa: Aísla aplicaciones y datos dentro de la carpeta, excepto una lista específica de aplicaciones

Para utilizar esta funcionalidad, implemente dispositivos en el modo de gestión COBO (totalmente gestionado), luego use KSP/SeparatedApps en la consola del MDM para aplicar las siguientes configuraciones:

- Separación de las aplicaciones
- Políticas de separación de aplicaciones [Allow List Policy] >> CONFIGURE
- Habilitar políticas de separación de aplicaciones [Habilitar]
- Ubicación para la instalación de aplicaciones separadas [Interna / Externa] según sea necesario
- Lista de aplicaciones a instalar en un grupo separado >> Lista con los nombres de los paquetes de las aplicaciones separadas por comas

Se puede encontrar más información en el siguiente enlace:

<https://docs.samsungknox.com/admin/knox-platform-for-enterprise/migrate-to-android-14/separated-apps-for-android-14/>

2.10 SAMSUNG DeX

DeX permite el uso del dispositivo como si fuera un ordenador portátil u ordenador de escritorio, simulando una experiencia Windows. DeX está recomendado para su uso en la Organización.

DeX admite tres modos diferentes:

- Modo DeX: La pantalla del dispositivo aparece en el monitor conectado. También se puede conectar un teclado y un ratón.
- Screen Mirroring: La pantalla del dispositivo se duplica en el monitor conectado.
- Modo Dual: La pantalla del dispositivo y el monitor conectados se pueden usar al mismo tiempo.

El uso de Samsung DeX requiere uno de los siguientes accesorios:

- DeX station
- DeX pad
- Adaptador multipuerto
- Adaptador USB tipo C a HDMI
- Cable DeX
- Cable USB con la aplicación DeX Companion

3. CONFIGURACIÓN RECOMENDADA

Samsung, en colaboración con el Centro Criptológico Nacional, ha elaborado una configuración que permite que la solución cumpla los requisitos del marco de seguridad detallados en este documento, permitiendo a los Administradores gestionar y mitigar los riesgos de forma óptima para el despliegue de sistemas con los requisitos del Esquema Nacional de Seguridad en su Nivel Alto.

Los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia Dispositivos Móviles para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN, se detallan en la guía CCN-STIC-140 y su anexo F.1.

Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia, debe implementar para un determinado caso de uso, los cuales, para la generación de esta configuración segura recomendada, se han expandido basándose en guías de controles de seguridad ampliamente reconocidas y aceptadas, como son NIST SP 800-53, NIST SP 800-53A, NIST SP 800-53 Revisión 4.

3.1 DISPOSITIVOS CUALIFICADOS

Los dispositivos móviles cualificados que cumplen los requisitos de seguridad exigidos para manejar información Sensible ENS ALTA, son aquellos incluidos en la última edición publicada de Guía de Seguridad de las TIC CCN-STIC 105, CPSTIC Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación que se puede consultar en el siguiente link:

<https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file?format=html>

Así como en su versión online:

https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic?pid=26:samsung-electronics&search=&order=i.ordering&dir=asc&f_familia=&f_nivel_ens=&f_nivel_clasificacion=&f_tipo=&cm=0#tlb

El Administrador IT de la Organización debe asegurar que los modelos desplegados se encuentran recogidos en el CPSTIC.

3.1.1. DISPOSITIVOS ENTERPRISE EDITION

Samsung Galaxy Enterprise Edition añade al dispositivo móvil una serie de características exclusivas pensadas para ofrecer una seguridad mejorada, mayor personalización, simplicidad en el licenciamiento y soporte técnico. Una gran selección de dispositivos incluidos en CPSTIC Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación se ofrecen en versión Enterprise Edition, a través de canales de venta específicos. Estos dispositivos ofrecen hasta 7 años de actualizaciones de seguridad, ofrecen un ciclo de vida de al menos dos años en el mercado e incluyen licencia de Knox Suite para usar los servicios B2B, que se puede renovar tras el primer año.

Para más información: www.samsung.com/es/business/mobile/enterprise-edition/ y www.samsungknox.com

3.2 IDENTIFICACIÓN DE VERSIÓN DE DISPOSITIVO

Para identificar el número de modelo, y la versión de Android, en la aplicación “Ajustes”, seleccionar Acerca del teléfono/tableta para ver el Número de Modelo, y pulsando la opción “Información de software” se pueden identificar la Versión de Android.

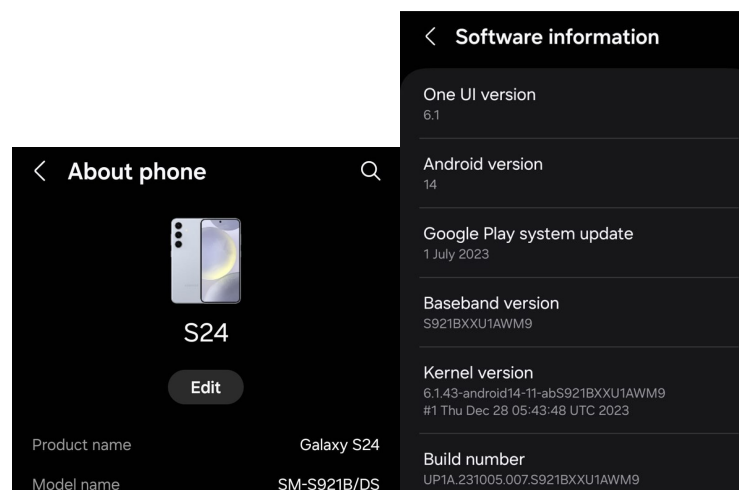


Figura 1

3.3 REGLAS DE CONFIGURACION GENERAL DEL DISPOSITIVO

En este apartado se incluyen los parámetros y funcionalidades sobre los que se establecerá una recomendación. Se compone de una tabla que detalla la configuración de diversas funcionalidades del dispositivo, la cual se puede auditar ejecutando los casos de test indicados en el [ANEXO B](#) de esta guía. El Administrador IT de la Organización deberá entender el sentido de cada regla y la aplicación en su Organización para dar cumplimiento del Esquema Nacional de Seguridad.

Las reglas de configuración del dispositivo están detalladas desde un punto de vista de la plataforma del dispositivo, siendo éstas las políticas ofrecidas por el API de AE (Android Enterprise) o por el API de Samsung Knox. Tal como se ha explicado en el capítulo [2](#) de esta guía, el interfaz del Administrador IT de la organización será la consola MDM, la cual se comunica de manera propietaria con su agente (DO) en el dispositivo, el cuál ejecuta las llamadas a la API, todo ello de manera transparente para el Administrador IT.

En varias reglas de configuración se ofrece al Administrador IT de la organización más de un método para realizar la configuración requerida. En este caso se indica #1, para el método número 1, #2, para el método número 2 y así sucesivamente. En el campo comentario se encontrará “Choose Method #1 or #2” para indicar que se elija el método 1 o 2.

Es de destacar que cada solución MDM implementa su propio interfaz de usuario, por lo que la tabla de configuración indicada en el punto [3.3.1](#) debe tomarse como conceptual, necesitando el Administrador IT conocer la opción específica de su solución MDM elegida para efectuar la configuración deseada.

Para un entrenamiento y mejor conocimiento de la configuración de políticas en un dispositivo, el Administrador IT de la organización puede utilizar un dispositivo de test y provisionarlo con la aplicación de Test DPC según se detalla en el [ANEXO B](#).

3.3.1. TABLA DE CONFIGURACIÓN - COBO

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Password Policies	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex	Numeric(Complex)	This allows for PIN code. API: setPasswordQuality * Or setRequiredPasswordComplexity If the management tool does not support "Numeric(Complex)" but does support "Numeric", KPE can be used to achieve CCN-STIC compliance. In this case, configure this policy with value "Numeric" and use an additional KPE policy, (innately by management tool or via KSP) "Maximum Numeric Sequence Length" with value "4".
Nota aclaratoria acerca del requerimiento de contraseña	La política de Android Enterprise Password Complexity segmenta la complejidad de las claves de bloqueo de pantalla en tres niveles, complejidad baja, media y alta, con los siguientes criterios. Baja / Low: Un patrón o PIN que repite (4444) o sigue una secuencia ordenada (1234, 4321, 2468). Media / Mid: Un PIN que no repite números (4444) o secuencias ordenadas (1234, 4321, 2468) o una contraseña alfanumérica con una longitud de, al menos, 4 caracteres. Alta / High: Un PIN que no repite números (4444) o secuencias ordenadas (1234, 4321, 2468) y con una longitud de, al menos, 8 caracteres, o una contraseña alfanumérica con una longitud de, al menos, 6 caracteres.			
Device Password Policies	Minimum password length	0+ characters	8 characters	API: setPasswordMinimumLength *
Device Password Policies	Max password failures for local wipe	0+ attempts	10 attempts	API: setMaximumFailedPasswordsForWipe *
Device Password Policies	Max time to screen lock	0+ minutes	5 minutes	API: setMaximumTimeToLock *
Device Restrictions	Face recognition	Enable/Disable	Enable	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE
Device Restrictions	Trust agents	Enable/Disable	Disable	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS Or setTrustAgentConfiguration
Device Restrictions	Backup service	Enable/Disable	Disable	API: setBackupServiceEnabled *
Device Restrictions	Debugging features	Allow/Disallow	Disallow	API: addUserRestriction, DISALLOW_DEBUGGING_FEATURES *
Device Restrictions	Bluetooth	Allow/Disallow	IT Admin decision	Guidance is provided for the IT Admin to approve Bluetooth. API: addUserRestriction, DISALLOW_BLUETOOTH *

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Restrictions	Mount physical media	Allow/Disallow	Disallow	Not applicable for devices that do not support removable storage media. Disables use of all removable storage, e.g., SD cards, USB thumb drives. API: addUserRestriction, DISALLOW_MOUNT_PHYSICAL_MEDIA *
Device Restrictions	USB file transfer	Allow/Disallow	Disallow	DeX drag and drop file transfer capabilities will be prohibited, but all other DeX capabilities remain useable. API: addUserRestriction, DISALLOW_USB_FILE_TRANSFER *
Device Restrictions	Config tethering	Allow/Disallow	Disallow	API: addUserRestriction, DISALLOW_CONFIG_TETHERING * If deployment requires the use of Mobile Hotspot & Tethering, KPE can be used to allow its usage in a CCN-STIC-approved configuration. In this case, do not configure this policy, and instead replace with KPE policy (innately by management tool or via KSP) "Allow open Wi-Fi connection" with value "disable" and add Training Topic "Don't use Wi-Fi Sharing"
Device Restrictions	Config date/time	Allow/Disallow	Disallow	API: addUserRestriction, DISALLOW_CONFIG_DATE_TIME *
Device Policy Management	Certificates		Device Policy Management	API: installCaCert *
Device Restrictions	List of approved apps listed in managed Google Play	List of apps	List only approved work apps	
Device Restrictions	Unredacted notifications	Allow/Disallow	Disallow	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS
Device Restrictions	Security logging	Enable/Disable	Enable	Management tool must provide means to read the Log in the console. API: setSecurityLoggingEnabled *
Device Restrictions	Modify accounts	Allow/Disallow	Disallow	API: addUserRestriction, DISALLOW_MODIFY_ACCOUNTS *
Device Restrictions	Config credentials	Allow/Disallow	Disallow	API: addUserRestriction, DISALLOW_CONFIG_CREDENTIALS *

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Restrictions	Install from unknown sources globally	Allow/Disallow	Disallow	API: addUserRestriction, DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY *
Device Restrictions	CC mode	Enable/Disable	Enable	API: setCommonCriteriaModeEnabled *

Tabla 1 - Reglas Configuración para un despliegue COBO

3.4 BORRADO DEL DISPOSITIVO

Los dispositivos Samsung pueden ser borrados mediante un reseteo a valores de fábrica, o a través del MDM o si se alcanza el número máximo de intentos de autenticación fallida, establecida por configuración de política/API de seguridad.

3.4.1. DESENROLADO

Como parte del desenrolado de dispositivos Samsung o para transferir un terminal a un nuevo usuario, estos dispositivos deben de ser borrados por el administrador a través de la opción de borrado que proporcione su MDM. No se recomienda utilizar la opción de “recovery menu” porque puede dar lugar a incidencias como por ejemplo el Factory Reset Protection (FRP) de Google.

3.5 DIRECTIVAS A USUARIO FINAL / UBE (USER-BASED ENFORCEMENT)

Hay varias funciones disponibles en el dispositivo que, cuando son habilitadas por el usuario final, pueden ocasionar que personas no autorizadas obtengan acceso a información confidencial del dispositivo. Para las funciones que las herramientas de Gestión no pueden desactivar, la mitigación debe incluir la **formación adecuada de los usuarios finales**.

Para poder articular estos mecanismos y directivas, la organización que quiera hacer uso de estos dispositivos y alcanzar el nivel de seguridad al que se orienta este documento **debe** elaborar o dotarse de una Política de seguridad TIC para trasladar al usuario final estos conocimientos y responsabilidades. Esta Política de seguridad TIC debe ser coherente para las diferentes tecnologías (movilidad, PCs “tradicionales”, ...)

Entre los conceptos más importantes a incluir en esta formación es la necesidad de **mantener una custodia positiva del dispositivo y de no utilizar servicios y/o periféricos que no estén expresamente autorizados** por el Administrador IT del sistema.

3.5.1. ALARMA DE CALENDARIO

La aplicación predeterminada de Calendario preinstalada por Samsung permite a los usuarios crear eventos que incluyen el título del evento, la ubicación, la fecha y la hora, así como las alarmas de notificación del evento. Cuando se configura la alarma, a la hora especificada, los detalles del evento se muestran en la pantalla del dispositivo, incluso cuando el dispositivo está en estado de bloqueo. Los usuarios deben estar formados para no configurar esta opción o para no incluir información confidencial en el título y la ubicación del evento.

3.5.2. TRANSFERENCIA DE CONTENIDO Y DUPLICADO DE PANTALLA

Los dispositivos Samsung incluyen varios mecanismos que permiten al usuario transferir archivos de su dispositivo a otros dispositivos y mostrar el contenido de su dispositivo en ciertas Smart TV de Samsung.

Se accede a las funciones "Smart View" (depende del modelo del dispositivo) desde la barra de notificaciones y se muestra una lista de dispositivos escaneados a los que se puede conectar el dispositivo del usuario. El usuario puede seleccionar un dispositivo de esta lista para transferir los archivos seleccionados (a través de WiFi Direct o Bluetooth) o para realizar la duplicación de pantalla. Dependiendo de las posibilidades del dispositivo seleccionado, se utilizará la tecnología Miracast o DLNA para proporcionar el reflejo de la pantalla. Tanto Miracast como DLNA funcionarán a través de una conexión WiFi Direct o con dispositivos conectados al mismo punto de acceso WiFi. Mientras que Miracast presenta lo que está en la pantalla del dispositivo al dispositivo de destino, DLNA requiere la reproducción en el dispositivo de destino.

El duplicado de pantalla también se puede iniciar seleccionando el archivo y luego seleccionando "Compartir" y "Vista inteligente" o habilitando "Vista inteligente" en el panel de Configuración rápida.

El usuario puede habilitar "MirrorLink" para permitir la integración del dispositivo con los sistemas de información y entretenimiento de automóviles, conectados a través de USB. Esto brinda al usuario la posibilidad de acceder y controlar aplicaciones en el dispositivo a través del sistema de información y entretenimiento del automóvil. Esto se habilita seleccionando "Conexiones", "Más conexiones" y "MirrorLink" en la aplicación Configuración.

La opción "Visibilidad del teléfono" permite al usuario hacer que el dispositivo sea visible para otros dispositivos a través de interfaces inalámbricas como Bluetooth o WiFi Directo, lo que significa que otros dispositivos pueden intentar iniciar transferencias de datos.

Los usuarios deben estar formados para no habilitar estas opciones a menos que estén autorizados para hacerlo y verifiquen visualmente el dispositivo receptor. Los usuarios deben recibir formación para no habilitar estas opciones a menos que utilicen una tecnología de duplicación de pantalla con FIPS 140-2 WiFi validado o superior. Miracast solo debe utilizarse con televisores, monitores y dongles Miracast con clientes WiFi validados FIPS 140-2 o superior.

Nota: El Administrador IT de la organización también puede restringir el método de conexión subyacente (Bluetooth, WiFi Direct, etc.) a través de los controles de MDM, o el Administrador puede desactivar explícitamente el paquete de la aplicación que implementa el servicio.

3.5.3. USO DE ACCESORIOS (DEX STATION, USB DONGLE)

La funcionalidad Samsung DeX ofrece la posibilidad de conectar el dispositivo Android de Samsung a un monitor externo, portátil, televisión utilizando un cable o mediante WiFi. La idea es transformar la experiencia de usuario Android a una interfaz Windows en una pantalla más grande y mejorar esta experiencia añadiendo teclado y ratón. Los adaptadores / dongles de USB a Ethernet también ofrecen posibilidad de red por cable para dispositivos Samsung de Android.

Se debe gestionar el riesgo de seguridad que supone, de acuerdo a la política de seguridad de la empresa, la conexión de un dispositivo Samsung con Android a una red de la organización a través de cualquier accesorio que proporcione capacidades de red por cable.

4. ABREVIATURAS

AE	<i>Solución liderada por Google para habilitar el uso empresarial en dispositivos Android (Android Enterprise)</i>
API	<i>Interfaz de programación de aplicación (Application Programming Interface)</i>
BYOD	<i>Política «Traiga su propio dispositivo» (Bring-Your-Own-Device)</i>
CA	<i>Autoridad de certificación (Certification Authority)</i>
CC	<i>Criterios Comunes (Common Criteria)</i>
CCN	<i>Centro Criptológico Nacional</i>
COBO	<i>Política «Uso solo profesional» (Corporate Owned Business Only)</i>
COPE	<i>Política «Uso profesional con área personal» Corporate Owned Personal Enabled)</i>
CPSTIC	<i>Catálogo de Productos de Seguridad Tecnologías de la Información y Comunicaciones</i>
DO	<i>Agente(aplicación) MDM para establecer políticas de seguridad (Device Owner)</i>
DPC	<i>Aplicación de test (DO o PO) para probar políticas AE (Device Policy Control)</i>
EAS	<i>Microsoft Exchange ActiveSync</i>
ENS	<i>Esquema Nacional de Seguridad</i>
EMM	<i>Enterprise Mobility Management</i>
FIPS	<i>Federal Information Processing Standards</i>
GSLB	<i>Global Server Load Balancing</i>
ISV	<i>Independent Software Vendor</i>
KIES	<i>Samsung Kies es un programa que permite transferir archivos y sincronizar datos entre un dispositivo móvil Samsung y el ordenador.</i>
KLM	<i>Sistema de Licencias de Samsung Knox (Knox License Management)</i>
Knox	<i>La solución de seguridad corporativa de Samsung</i>
KPE	<i>Solución de Samsung que extiende y robustece el uso empresarial de AE (Knox Platform for Enterprise)</i>
MDFPP	<i>Requisitos de Seguridad básicos para dispositivos móviles (Mobile Device Fundamentals Protection Profile)</i>
MDM	<i>Administración/Gestión de dispositivos móviles (Mobile Device Management)</i>
NFC	<i>Tecnología de intercambio de datos a muy corta distancia (Near Field Communication)</i>
NPA	<i>Proporciona información en tiempo real sobre los paquetes de red que salen de un dispositivo y el contexto que rodea el flujo de datos (Network Platform Analytics)</i>
OEM	<i>Original Equipment Manufacturer</i>
OCSP	<i>Online Certificate Status Protocol</i>
OTA	<i>Por vía inalámbrica (Over the Air)</i>

PO	<i>Profile Owner</i>
QR	<i>Quick Response code</i>
RFS	<i>Requisitos Fundamentales de Seguridad</i>
SDK	<i>Kit de desarrollo de software corporativo de Samsung (Software Development Kit)</i>
Smart Switch	<i>Samsung Smart Switch es un programa que permite transferir archivos y sincronizar datos entre un dispositivo móvil Samsung y el ordenador.</i>
STIC	<i>Seguridad Tecnologías de la Información y Comunicaciones</i>
Tarjeta SD	<i>Tarjeta de memoria Secure Digital</i>
URL	<i>Localizador de recursos uniforme (Uniform Resource Locator)</i>
USB	<i>Bus serie universal (Universal Serial Bus)</i>
WP-C	<i>Work Profile in Company owned device</i>
VPN	<i>Red privada virtual (Virtual Private Network)</i>

ANEXO A. Introducción a KNOX PLATFORM FOR ENTERPRISE (KPE)

Sobre la plataforma Knox precargada en los terminales Samsung, se implementan una serie de servicios Cloud que aportan capacidades de seguridad, gestión, control en las actualizaciones del sistema operativo e información relevante sobre el parque de terminales móviles de una empresa.

KPE COMO EXTENSIÓN DE AE

Los dispositivos móviles Samsung pueden aprovechar las características de seguridad y el hardware específicos de Samsung para mejorar la seguridad más allá de los estándares de configuración. La solución ***Knox Platform for Enterprise (KPE)*** proporciona un robusto conjunto de funcionalidades, extendiendo las ofrecidas por la plataforma Android Enterprise (AE), para cubrir los riesgos de seguridad y gestión corporativa, así como cumplir con los estrictos requisitos de sectores altamente regulados. Las políticas KPE pueden ser utilizadas con una licencia gratuita que enriquecerá la experiencia con AE.



Figura 2

ARMONIZACIÓN

Samsung ayuda a las organizaciones a incrementar la seguridad y administrar millones de dispositivos Android en todo el mundo, al ser pionera en seguridad avanzada con su plataforma empresarial Knox, creando un conjunto completo de funcionalidades que extienden las proporcionadas por Android. En los últimos años, Samsung ha trabajado con Google para simplificar la gestión de movilidad de los clientes finales y reducir la duplicidad de funcionalidades. Las características de Knox se construyen sobre el framework central de Android Enterprise (AE), para cumplir con los requisitos de seguridad obligatorios de gobiernos para despliegues de movilidad regulados. Esto permite a los proveedores de MDM ofrecer una base única para que las organizaciones

implementen Android Enterprise, al tiempo que agregan las funciones necesarias de Samsung Knox para cumplir con rigurosos requisitos de seguridad.

TRUSTED EXECUTION ENVIRONMENT

Los dispositivos Samsung Galaxy incluyen un Entorno de Ejecución Confiable (Trusted Execution Environment - TEE) – un entorno secundario aislado de la plataforma Android. Este ha sido implementado usando la tecnología segura de ARM TrustZone.

La TEE es responsable de realizar operaciones sensibles tales como encriptación de archivos de sistema y:

- Protección del kernel en tiempo real (Real-time Kernel Protection - RKP)
- Knox Verified Boot – KVB
- Device Attestation
- Certificate Management

Además de la TEE, algunos terminales Samsung Galaxy incluyen un Elemento Seguro Embebido (Secure Embedded Element - eSE). En este caso, se trata de una memoria totalmente aislada disponible para almacenar credenciales o claves especialmente sensibles. Para más información contactar con el equipo de Samsung en su página web.

KNOX VERIFIED BOOT (KVB)

KVB es una implementación específica de Samsung del Android Verified Boot (AVB) v2. Las diferencias claves son:

- AVB: Chequea la integridad del kernel y los componentes de la plataforma
- KVB: Extiende la cadena de confianza a bootloader más tempranos y a otras particiones, incluyendo el Kernel, System, Vendor y Producto. Esto añade integridad, autenticidad y asegura que el dispositivo inicia usando componentes confiables que forman parte de un conjunto de binarios alineados.

KNOX PLATFORM FOR ENTERPRISE (KPE)

KPE proporciona seguridad de alto nivel que protege todos los aspectos de la operación del dispositivo móvil, resuelve los puntos críticos identificados por las organizaciones y cumple con los estrictos requisitos de sectores altamente regulados.

Con KPE, un dispositivo móvil Samsung Android se puede configurar para cumplir con los requerimientos ENS Alto.

Para más información, visite:

- <https://www.samsungknox.com/es-419/solutions/it-solutions/knox-platform-for-enterprise>
- <https://www.samsungknox.com/es-419/secured-by-knox>

ANEXO B. AUDITORIA DE CONFIGURACION SEGURA

Instrucciones para realizar una auditoría de un dispositivo configurado correctamente: Realizar el **Procedimiento** indicado en cada caso de test y comprobar que la **Validación**, evidencia que el dispositivo (y eventualmente la solución MDM) está configurado correctamente.

- La terminología “finding” en el listado de tests, se refiere a un problema de configuración detectado que debe ser subsanado.
- Para configurar el dispositivo de test en idioma Inglés así facilitar su testeo, seleccione “Ajustes” → “Administración General” → “Idioma y entrada de texto” → “Idioma” + Añadir idioma English (United Kingdom).

ID: 001	PASS []	FAIL []
Requerimiento	Samsung Android must be enrolled as a COBO device.	
Procedimiento	Enroll the Samsung Android devices in an Organization-approved use case. On the management tool, configure the default enrollment as "Fully managed". Refer to the management tool documentation to determine how to configure the device enrollment.	
Validación	Review the configuration to determine if the Samsung Android devices are enrolled in an Organization approved use case. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, verify that the default enrollment is set as "Fully managed". On the Samsung Android device: 1. Open Settings >> Biometric and Security >> Other Security Settings >> Device Admin Apps. 2. Verify that the management tool Agent is listed. If on the management tool the default enrollment is not set as "Fully managed", or the management tool Agent is not listed, this is a finding.	

ID: 002	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to not allow passwords that include more than four repeating or sequential characters.	
Procedimiento	Configure the Samsung Android devices to disallow passwords containing more than four repeating or sequential characters. On the management tool, in the device password policies, set "minimum password quality" to "Numeric(Complex)" or better. If your management tool does not support "Numeric(Complex)" but does support "Numeric", KPE can be used to achieve CCN-STIC compliance. In this case, configure this policy with value "Numeric" and use an additional KPE policy (innately by the management tool or via KSP) "Maximum Numeric Sequence Length" with value "4".	
Validación	Review the configuration to determine if the Samsung Android devices are disallowing passwords containing more than four repeating or sequential characters. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device password policies, verify "minimum password quality" is set to "Numeric(Complex)" or better. On the Samsung Android device: 1. Open Settings >> Lock screen >> Screen lock type. 2. Enter current password. 3. Tap "PIN". 4. Verify that PINs with more than four repeating or sequential numbers are not accepted. If on the management tool "minimum password quality" is not set to "Numeric(Complex)" or better, or on the Samsung Android device a password with more than four repeating or sequential numbers is accepted, this is a finding.	

ID: 003	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to enforce a minimum password length of six characters.	
Procedimiento	Configure the Samsung Android devices to enforce a minimum password length of six characters. On the management tool, in the device password policies, set "minimum password length" to "6".	
Validación	Review the configuration to determine if the Samsung Android devices are enforcing a minimum password length of six characters. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device password policies, verify "minimum password length" is set to "6". On the Samsung Android device: 1. Open Settings >> Lock screen >> Screen lock type. 2. Enter current password. 3. Tap "PIN". 4. Verify the text "PIN must contain at least", followed by a value of at least "6 digits", appears above the PIN entry. If on the management tool "minimum password length" is not set to "6", or on the Samsung Android device the text "PIN must contain at least" is followed by a value of less than "6 digits", this is a finding.	

ID: 004	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to not allow more than 5 consecutive failed authentication attempts.	
Procedimiento	Configure the Samsung Android devices to allow only 5 or fewer consecutive failed authentication attempts. On the management tool, in the device password policies, set "max password failures for local wipe" to "5" attempts or less. A device password must be set for "max password failures for local wipe" to become active.	
Validación	Review the configuration to determine if the Samsung Android devices are allowing only 5 or fewer consecutive failed authentication attempts. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device password policies, verify "max password failures for local wipe" is set to "5" attempts or less. On the Samsung Android device: 1. Open Settings >> Lock screen. 2. Verify "Secure lock settings" is present and tap it. 3. Enter current password. 4. Verify that "Auto factory reset" is greyed out, and cannot be configured. If on the management tool "max password failures for local wipe" is not set to "5" attempts or less, or on the Samsung Android device the "Auto factory reset" menu can be configured, this is a finding.	

ID: 005	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to lock the display after 15 minutes (or less) of inactivity	
Procedimiento	Configure the Samsung Android devices to lock the device display after 15 minutes (or less) of inactivity. On the management tool, in the device password policies, set "max time to screen lock" to "15 minutes" or less. A device password must be set for "max time to screen lock" to become active.	
Validación	Review the configuration to determine if the Samsung Android devices are locking the device display after 15 minutes (or less) of inactivity. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device password policies, verify "max time to screen lock" is set to "15 minutes" or less. On the Samsung Android device: 1. Open Settings >> Lock screen. 2. Verify "Secure lock settings" is present and tap it. 3. Enter current password. 4. Tap "Auto lock when screen turns off". 5. Verify the listed timeout values are 15 minutes or less. If on the management tool "max time to screen lock" is not set to "15 minutes" or less, or on the Samsung Android device "Secure lock settings" is not present and the listed Screen timeout values include durations of more than 15 minutes, this is a finding	

ID: 006	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to disable authentication mechanisms providing user access to protected data other than a Password Authentication Factor, including face recognition. It is possible to use biometric data if they are combined with certificates in physical devices.	
Procedimiento	Configure the Samsung Android devices to disable Face Recognition. This policy is included to allow a Samsung Android device to be deployed without an activated KPE premium license. If a license is activated, Facial Recognition will be automatically disabled. In this case, this policy does not need to be configured for CCN-STIC compliance, as Face as a biometric will be disabled. On the management tool, in the device restrictions, set "Face" to "Disable".	
Validación	Review the configuration to determine if the Samsung Android devices are disabling Face Recognition. This validation procedure is performed on both the management tool and the Samsung Android device. If a KPE premium license is activated, Facial Recognition will be automatically disabled Otherwise, On the management tool, in the device restrictions, verify that "Face" is set to "Disable". On the Samsung Android device: 1. Open Settings >> Lock screen >> Screen lock type. 2. Enter current password. 3. Verify that "Face" is disabled and cannot be enabled. If on the management tool a KPE premium license is not activated and "Face" is not set to "Disable", or on the Samsung Android device "Face" can be enabled, this is a finding.	

ID: 007	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to disable authentication mechanisms providing user access to protected data other than a Password Authentication Factor, including trust agents.	
Procedimiento	Configure the Samsung Android devices to disable Trust Agents. On the management tool, in the device restrictions, set "Trust Agents" to "Disable".	
Validación	Review the configuration to determine if the Samsung Android devices are disabling Trust Agents. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions, verify that "Trust Agents" are set to "Disable". On the Samsung Android device: 1. Open Settings >> Biometrics and security >> Other security settings >> Trust agents. 2. Verify that all listed Trust Agents are disabled and cannot be enabled. If on the management tool "Trust Agents" are not set to "Disable", or on the Samsung Android device a "Trust Agent" can be enabled, this is a finding.	

ID: 008	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to not allow backup of all applications and configuration data to remote systems.	
Procedimiento	Configure the Samsung Android devices to disable backup to remote systems (including commercial clouds). On the management tool, in the device restrictions, set "Backup service" to "Disable".	
Validación	Review the configuration to determine if the Samsung Android devices are disabling backup to remote systems (including commercial clouds). This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions section, verify that "Backup service" is set to "Disable". On the Samsung Android device: 1. Open Settings >> Accounts and backup. 2. Verify that any backup service listed cannot be configured to back up data. If on the management tool "Backup service" is not set to "Disable", or on the Samsung Android device a listed backup service can be configured to back up data, this is a finding.	

ID: 009	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to disable developer modes.	
Procedimiento	Configure the Samsung Android devices to disable developer modes. On the management tool, in the device restrictions, set "Debugging Features" to "Disallow".	
Validación	Review the configure to determine if the Samsung Android devices are disabling developer modes. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions, verify that "Debugging Features" is set to "Disallow". On the Samsung Android device: 1. Open "Settings". 2. Verify "Developer options" is not listed. If on the management tool "Debugging Features" is not set to "Disallow" or on the Samsung Android device "Developer options" is listed, this is a finding.	

ID: 010	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to disable all Bluetooth profiles except for HSP (Headset Profile), HFP (Hands-Free Profile), SPP (Serial Port Profile), A2DP (Advanced Audio Distribution Profile), AVRCP (Audio/Video Remote Control Profile), and PBAP (Phone Book Access Profile).	
Procedimiento	Configure the Samsung Android devices to disable Bluetooth, or if the IT admin has approved the use of Bluetooth (for example, for hands-free use), train users to only pair devices which support HSP, HFP, SPP, A2DP, AVRCP, PBAP profiles. On the management tool, in the device restrictions section, set "Bluetooth" to the IT admin-approved selection; "Allow" - if the IT admin has approved the use of Bluetooth - or "Disallow", if not.	
Validación	Review the Samsung documentation and inspect the configuration to verify the Samsung Android devices are paired only with devices which support HSP, HFP, SPP, A2DP, AVRCP, and PBAP Bluetooth profiles. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions section, verify "Bluetooth" is set to the IT admin-approved selection; "Allow" - if the IT admin has approved the use of Bluetooth - or "Disallow", if not. On the Samsung Android device: 1. Open Settings >> Connections >> Bluetooth 2. Verify that all listed paired Bluetooth devices use only authorized Bluetooth profiles. If on the management tool "Bluetooth" is not set to the IT admin-approved value, or the Samsung Android device is paired with a device which uses unauthorized Bluetooth profiles, this is a finding.	

ID: 011	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to enable encryption for data at rest on removable storage media or, alternately, the use of removable storage media must be disabled.	
Procedimiento	Configure the Samsung Android devices to enable data-at-rest protection for removable media, or alternatively, disable their use. This requirement is not applicable for devices that do not support removable storage media. On the management tool, in the device restrictions, set "Mount physical media" to "Disallow". This disables the use of all removable storage, e.g., micro SD cards, USB thumb drives, etc. If your deployment requires the use of micro SD cards, KPE can be used to allow its usage in a CCN-STIC approved configuration. In this case, do not configure this policy, and instead replace with KPE policy (innately by management tool or via KSP) "Enforce external storage encryption" with value "enable".	
Validación	Review the configuration to determine if the Samsung Android devices are either enabling data-at-rest protection for removable media, or are disabling their use. This requirement is not applicable for devices that do not support removable storage media. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions, verify that "Mount physical media" is set to "Disallow". On the Samsung Android device, verify that a microSD card cannot be mounted. The device should ignore the inserted SD card and no notifications for the transfer of media files should appear, nor should any files be listed using a file browser, such as Samsung My Files. If on the management tool "Mount physical media" is not set to "Disallow", or on the Samsung Android device a microSD card can be mounted, this is a finding.	

ID: 012	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to disable USB mass storage mode.	
Procedimiento	Configure the Samsung Android devices to disable USB mass storage mode. On the management tool, in the device restrictions, set "USB file transfer" to "Disallow". DeX drag & drop file transfer capabilities will be prohibited, but all other DeX capabilities remain useable.	
Validación	Review the configuration to determine if the Samsung Android devices are disabling USB mass storage mode. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions, verify that "USB file transfer" has been set to "Disallow". On the PC, browse the mounted Samsung Android device and verify that it does not display any folders or files. If on the management tool "USB file transfer" is not set to "Disallow", or the PC can mount and browse folders and files on the Samsung Android device, this is a finding.	

ID: 013	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to not allow backup of all applications, configuration data to locally connected systems.	
Procedimiento	Verify "USB file transfer" has been "Disallowed"	
Validación	Verify requirement ID014 "Disallow USB file transfer" has been implemented. If "Disallow USB file transfer" has not been implemented, this is a finding.	

ID: 014	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to enable authentication of personal hotspot connections to the device using a preshared key.	
Procedimiento	Configure the Samsung Android devices to enable authentication of personal hotspot connections to the device using a pre-shared key. On the management tool, in the device restrictions, set "Config tethering" to "Disallow". If your deployment requires the use of Mobile Hotspot & Tethering, KPE policy can be used to allow its usage in a CCN-STIC approved configuration. In this case, do not configure this policy, and instead replace with KPE policy (innately by the management tool or via KSP) "Allow open Wi-Fi connection" with value "Disable" and add Training Topic "Don't use Wi-Fi Sharing" (see supplemental document for additional information)	
Validación	Review the configuration to determine if the Samsung Android devices are enabling authentication of personal hotspot connections to the device using a preshared key. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions, verify "Config tethering" is set to "Disallow". On the Samsung Android device: 1. Open Settings >> Connections. 2. Verify that "Mobile Hotspot and Tethering" is greyed out. If on the management tool "Config tethering" is not set to "Disallow", or on the Samsung Android device "Mobile Hotspot and Tethering" is not greyed out, this is a finding.	

ID: 015	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to disallow configuration of the device's date and time.	
Procedimiento	Configure the Samsung Android devices to disallow users from changing the date and time. On the management tool, in the device restrictions, set "Config Date/Time" to "Disallow".	
Validación	Review the configuration to determine if the Samsung Android devices are disallowing the users from changing the date and time. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions, verify that "Config Date/Time" is set to "Disallow". On the Samsung Android device: 1. Open Settings >> General management >> Date and time. 2. Verify that "Automatic date and time" is on and the user cannot disable it. If on the management tool "Config Date/Time" is not set to "Disallow", or on the Samsung Android device "Automatic date and time" is not set or the user can disable it, this is a finding.	

ID: 016	PASS []	FAIL []
Requerimiento	Samsung Android must have the Organization root and intermediate PKI certificates installed	
Procedimiento	Install the Organization root and intermediate PKI certificates into the Samsung Android devices. The current Organization root and intermediate PKI certificates may be obtained in self-extracting zip files at https://cyber.mil/pki-pke (for NIPRNet). On the management tool, in the device policy management, install the Organization root and intermediate PKI certificates.	
Validación	Review the configuration to determine if the Samsung Android devices have the Organization root and intermediate PKI certificates installed. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device policy management, verify that the Organization root and intermediate PKI certificates are installed. On the Samsung Android device: 1. Open Settings >> Biometrics and security >> Other security settings >> View security certificates. 2. In the User tab, verify that the Organization root and intermediate PKI certificates are listed in the Device. If on the management tool the Organization root and intermediate PKI certificates are not listed in the Device, or on the Samsung Android device the Organization root and intermediate PKI certificates are not listed in the Device, this is a finding.	

ID: 017	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to enforce an application installation policy by specifying an application allowlist that restricts applications by the following characteristics: names.	
Procedimiento	Configure the Samsung Android devices to allow users to install only applications that have been approved by the IT Admin. In addition to any local policy, the IT admin must not approve applications which have certain prohibited characteristics. On the management tool, in the app catalog for managed Google Play, add each IT admin-approved app to be available. NOTE: Managed Google Play is an allowed App Store.	
Validación	Review the configuration to determine if the Samsung Android devices are allowing users to install only applications that have been approved by the IT Admin. This validation procedure is performed only on the management tool. On the management tool, in the app catalog for managed Google Play, verify that only IT admin-approved apps are available. If on the management tool the app catalog for managed Google Play includes non-IT admin-approved apps, this is a finding.	

ID: 018	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to not display the following (Work Environment) notifications when the device is locked: all notifications	
Procedimiento	Configure the Samsung Android devices to not display (Work Environment) notifications when the device is locked. On the management tool, in the device restrictions section, set "Unredacted Notifications" to "Disallow".	
Validación	Review the configuration to determine if the Samsung Android devices are not displaying (Work Environment) notifications when the device is locked. Notifications of incoming phone calls are acceptable even when the device is locked. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, in the device restrictions section, verify that "Unredacted Notifications" is set to "Disallow". On the Samsung Android device: 1. Open Settings >> Lock screen. 2. Verify that "Notifications" menu is disabled. If on the management tool "Unredacted Notifications" is not set to "Disallow", or on the Samsung Android device "Notifications" menu is not disabled, this is a finding.	

ID: 019	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to enable audit logging.	
Procedimiento	Configure the Samsung Android devices to enable audit logging. On the management tool, in the device restrictions section, set "Security logging" to "Enable".	
Validación	Review the configuration to determine if the Samsung Android devices are enabling audit logging. This validation procedure is performed on the management tool only. On the management tool, in the device restrictions, verify that "Security logging" is set to "Enable". If on the management tool "Security logging" is not set to "Enable", this is a finding.	

ID: 020	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to prevent users from adding personal email accounts to the work email app	
Procedimiento	Configure the Samsung Android devices to prevent users from adding personal email accounts to the work email app. On the management tool, in the device restrictions, set "Modify accounts" to "Disallow".	
Validación	Review the configuration to determine if the Samsung Android devices are preventing users from adding personal email accounts to the work email app. On the management tool, in the device restrictions section, verify "Modify accounts" is set to "Disallow". On the Samsung Android device: 1. Open Settings >> Accounts and backup >> Manage accounts. 2. Verify that no account can be added. If on the management tool "Modify accounts" is not set to "Disallow", or on the Samsung Android device an account can be added, this is a finding.	

ID: 021	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to not allow backup of all applications, configuration data to remote systems. - Disable Data Sync Framework	
Procedimiento	Implement "Disallow modify accounts"	
Validación	Verify requirement KNOX-12-110230 (Disallow modify accounts) has been implemented. If "Disallow modify accounts" has not been implemented, this is a finding.	

ID: 022	PASS []	FAIL []
Requerimiento	Samsung Android must allow only the Administrator (management tool) to perform the following management function: install/remove Organization root and intermediate PKI certificates.	
Procedimiento	Configure the Samsung Android devices to prevent users from removing Organization root and intermediate PKI certificates. On the management tool, in the device restrictions, set "Config credentials" to "Disallow".	
Validación	Review the configuration to determine if the Samsung Android devices are preventing users from removing Organization root and intermediate PKI certificates. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions, verify that "Config credentials" is set to "Disallow". On the Samsung Android device: 1. Open Settings >> Biometrics and security >> Other security settings >> View security certificates. 2. In the System tab, verify that no listed certificate in the Device can be untrusted. 3. In the User tab, verify that no listed certificate in the Device can be removed. If on the management tool the device "Config credentials" is not set to "Disallow", or on the Samsung Android device a certificate can be untrusted or removed, this is a finding.	

ID: 023	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to enforce an application installation policy by specifying one or more authorized application repositories, including Organization-approved commercial app repository, management tool server, or mobile application store	
Procedimiento	Configure the Samsung Android devices to disable unauthorized application repositories. On the management tool, in the device restrictions, set "installs from unknown sources globally" to "Disallow". NOTE: Google Play must not be disabled. Disabling Google Play will cause system instability and critical updates will not be received.	
Validación	Review the configuration to determine if the Samsung Android devices are disabling unauthorized application repositories. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions, verify that "installs from unknown sources globally" is set to "Disallow". On the Samsung Android device: 1. Open Settings >> Biometric and security >> Install unknown apps. 2. In the "Personal" tab, ensure that each app listed has the status "Disabled" under the app name or that no apps are listed. 3. In the "Work" tab, ensure that each app listed has the status "Disabled" under the app name or that no apps are listed. If on the management tool "installs from unknown sources globally" is not set to "Disallow", or on the Samsung Android device an app is listed with a status other than "Disabled", this is a finding.	

ID: 024	PASS []	FAIL []
Requerimiento	Samsung Android must be configured to enable Common Criteria (CC) Mode.	
Procedimiento	Configure the Samsung Android devices to enable Common Criteria (CC) mode. On the management tool, in the device restrictions, set "Common Criteria mode" to "Enable".	
Validación	Review the configuration to determine if the Samsung Android devices are enabling Common Criteria (CC) mode. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the device restrictions, verify that "Common Criteria mode" is set to "Enable". On the Samsung Android device, put the device into "Download mode" and verify that the text "Blocked by CC Mode" is displayed on the screen. If on the management tool "Common Criteria mode" is not set to "Enable", or on the Samsung Android device the text "Blocked by CC Mode" is not displayed in "Download mode", this is a finding.	

ANEXO C. Test Device Policy Control (Test DPC)

Test DPC es una aplicación diseñada para ayudar a los MDM, ISV (Independent Software Vendor) y OEM (Original Equipment Manufacturer) a **probar** sus aplicaciones y plataformas en un perfil administrado por la empresa de Android (es decir, el perfil de trabajo / Workspace / Contenedor). Sirve como un controlador de políticas de dispositivo y una aplicación de prueba para ejecutar las API disponibles Android Enterprise.

El Administrador IT de la organización solamente debe utilizar esta aplicación en un dispositivo destinado a test y nunca en un despliegue real.

Se puede encontrar información adicional en el siguiente enlace:

<https://github.com/googlesamples/android-testdpc>

Para realizar el Aprovisionamiento por Código QR:

- Ajustes-> Administración General->Restablecer Valores de fábrica
- Tocar la pantalla de bienvenida en el asistente de configuración 6 veces.
- Escanee este código QR
- Siga las instrucciones en pantalla



Tag content:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.afwsamples.testdpc/com.afwsamples.testdpc.DeviceAdminReceiver",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "gJD2YwtOiwJHkSMkkfLRlj-quNqG1fb6v100QmzM9w=",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://testdpc-latest-apk.appspot.com"
}
```

Una vez instalada la aplicación de test, se pueden ejecutar las políticas de la tabla de configuración del punto 3.3.1, para una familiarización con las mismas y su consiguiente mapeo a la solución MDM específica elegida.

Como ejemplo, en la Figura 3 se muestra cómo se establece la política de restablecimiento de valores de fábrica después de un número fallido de entrada de contraseña.

Android lock screen restrictions	max password failures for local wipe	0+	10	Unsuccessful logon attempts before device wipe
---	--------------------------------------	----	----	--

Android lock screen restrictions / max password failures for local wipe

Indica:

Android (política de Android Enterprise, en contraste con política específica de Samsung Knox)

Lock screen restrictions: la opción de menú de la aplicación Test DPC

max password failures for local wipe: Texto de la política.

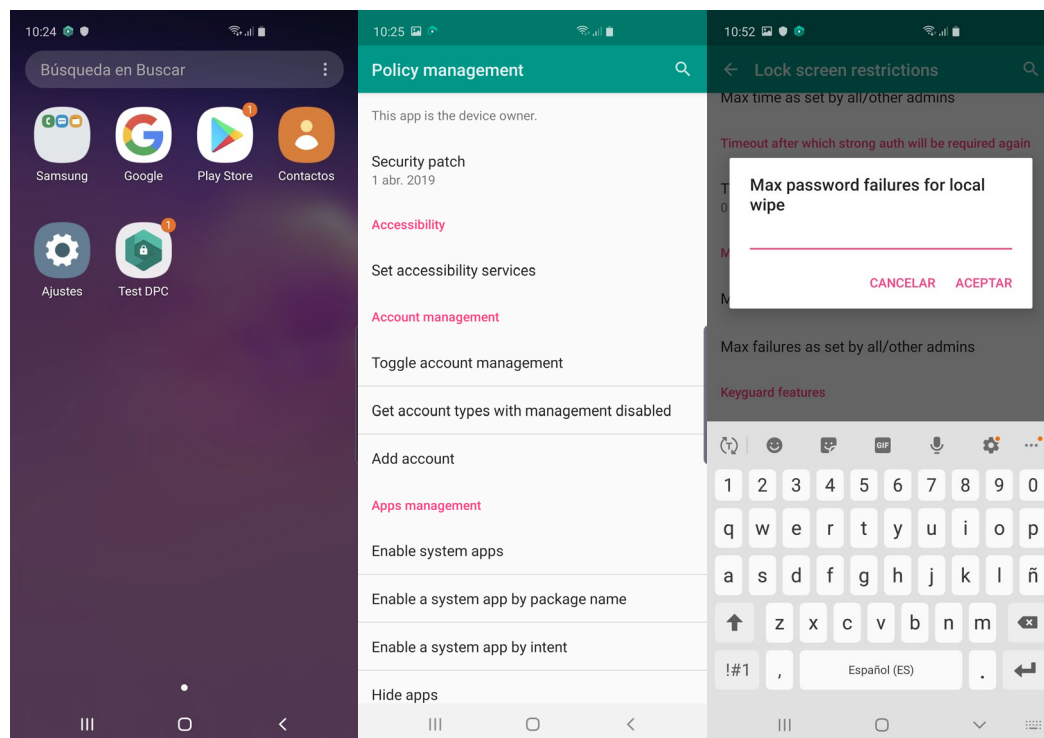


Figura 1

