centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1005

Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 16)



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

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.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 3
3 ORGANIZACIÓN DEL DOCUMENTO 3
4 FASE PREVIA A LA INSTALACIÓN 5
4.1 ENTREGA SEGURA DEL PRODUCTO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 6
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 7
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
4.5.1 KNOX MOBILE ENROLLMENT (KME) 9
4.5.2 KNOX CONFIGURE 9
4.5.3 KNOX ASSET INTELLIGENCE 10
4.5.4 KNOX MANAGE 10
4.5.5 ENTERPRISE FIRMWARE OVER-THE-AIR (E-FOTA) 10
4.5.6 KNOX SERVICE PLUGIN (KSP) 10
4.5.7 SEPARATED APPS 11
4.5.8 SAMSUNG DEX 12
4.5.9 GALAXY AI 13
5 FASE DE INSTALACIÓN 14
6 FASE DE CONFIGURACIÓN 15
6.1 MODO DE OPERACIÓN SEGURO 15
6.2 ACTUALIZACIONES 21
6.3 AUDITORÍA 21
7 REFERENCIAS 56
8 ABREVIATURAS 57

ÍNDICE DE TABLAS

Tabla 1: Configuración Recomendada 21
Tabla 2: Controles de Auditoría 53

ÍNDICE DE FIGURAS

Figura 1: Etiquetas de Sellado 5
Figura 2: Identificación de Modelo y Versión de Android 6
Figura 3: Separated Apps 11
Figura 4: DPC QR 54
Figura 5: Aplicación DPC 55

1 INTRODUCCIÓN

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).

2 OBJETO Y ALCANCE

El siguiente procedimiento de empleo seguro es válido para dispositivos móviles Samsung, teléfonos y tabletas, incluidos en CCN-STIC-105 Catálogo de Productos de Seguridad TIC (CPSTIC) con una versión de sistema operativo Android 16 o superior mientras no exista una publicación más reciente que substituya este procedimiento

Los dispositivos Samsung cualificados pueden consultarse en el CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte [REF1], así como en su versión online [REF2].

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 consultar [REF3] y [REF4].

3 ORGANIZACIÓN DEL DOCUMENTO

El Apartado 4.4 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.

El Apartado 4.5 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 móviles.

El Apartado 6.1 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 Apartado 6.3 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 uso profesional. Otros escenarios no están considerados en el proceso y no se realiza ninguna declaración sobre los mismos.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Si bien los dispositivos Samsung requieren una configuración inicial antes de poder integrarse al entorno de la organización, es fundamental garantizar que se reciba de forma segura, sin manipulaciones ni modificaciones.

Es crucial que los dispositivos que se desplegarán en la organización provengan de proveedores de confianza para minimizar la posibilidad de manipulación.

Se deben comprobar que las etiquetas de sellado de la caja no hayan sido manipuladas, y en el caso de existir una etiqueta de seguimiento comprobar su autenticidad.



Figura 1: Etiquetas de Sellado

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.

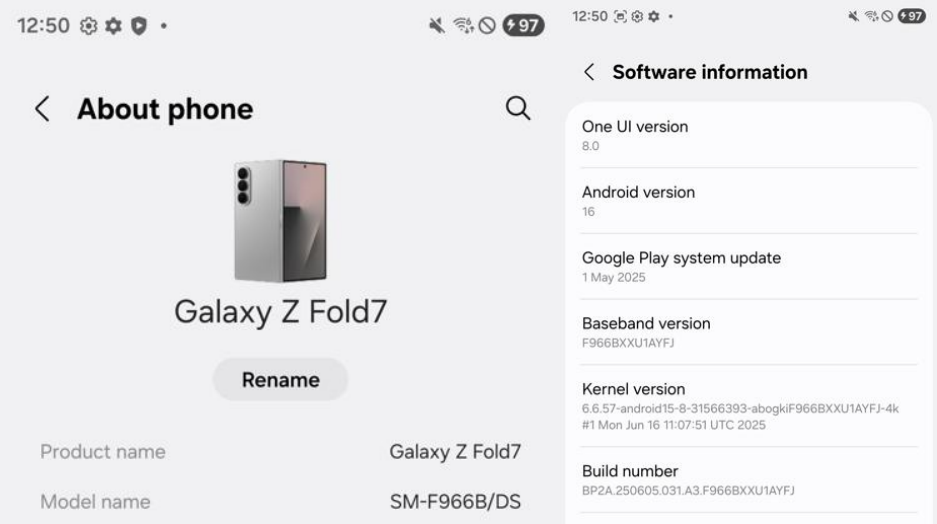


Figura 2: Identificación de Modelo y Versión de Android

4.2 ENTORNO DE INSTALACIÓN SEGURO

En la sección 6.1 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 interfaz 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 enrolan 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.

4.3 REGISTRO Y LICENCIAS

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/re-seller 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.

4.4 CONSIDERACIONES PREVIAS

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

a) Dispositivos móviles, con las capacidades y la configuración apropiada.

b) 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.

c) Redes de comunicaciones, de diferentes tecnologías (3G, 4G, 5G, WiFi, …).

d) Equipo de Administradores de dispositivos móviles de la organización donde se realiza el despliegue, así como su estructura organizativa y recursos

e) 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.

f) 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.

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 de 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.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

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 para las APIs de Samsung Knox, mayores serán las 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 y 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.

4.5.1 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)

4.5.2 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 [REF5], así como la Admin guide [REF6].

4.5.3 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 [REF7] y [REF8].

4.5.4 KNOX MANAGE

Es 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 [REF9], así como la guía de administración, con información más técnica [REF10].

4.5.5 ENTERPRISE FIRMWARE OVER-THE-AIR (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 [REF11].

4.5.6 KNOX SERVICE PLUGIN (KSP)

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.

Por esa 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.

4.5.7 SEPARATED APPS

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 aplicaciones 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 están 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, o en dispositivos con Android 14 Knox 3.10 o superiores alternativamente se puede realizar asignando y configurando, al igual se hace con KSP, la aplicación Separated Apps [REF12].

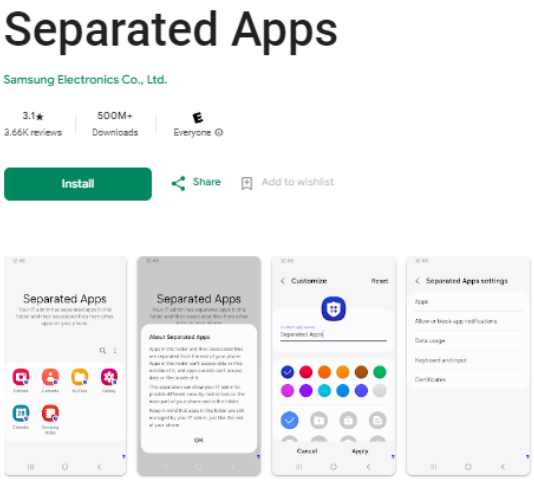


Figura 3: Separated Apps

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 [REF13].

4.5.8 SAMSUNG 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:

- Adaptador multipuerto
- Adaptador USB tipo C a HDMI

Desde Android 16, Samsung está migrando DeX para usar la solución Desktop Windowing introducida por Google en Android 16. Esta nueva solución se conoce como nextDeX por Samsung, y el nombre DeX se mantiene en el dispositivo Samsung y en la documentación. Como parte de esta migración, algunas de las API anteriores de DeX KPE han quedado obsoletas y eliminadas de Android 16.

4.5.9 GALAXY AI

Disponible en un número limitado de dispositivos Samsung Galaxy, ofrece un conjunto de funciones que mejoran la productividad.

Si bien muchas de estas funciones requieren iniciar sesión en una cuenta Samsung y procesamiento en la nube, varias pueden ejecutarse directamente en el dispositivo.

Estas funciones incluyen:

- Grabadora de voz, conversión de texto a voz y traducción.
- Traducción de Samsung Notes.
- Intérprete de Samsung para traducción de voz en vivo.

Samsung proporciona las API de KPE para garantizar que solo se pueda usar el procesamiento de IA en el dispositivo, y esta configuración se puede implementar a través de KSP.

Más información disponible en el siguiente enlace [REF14].

Desde Android 15, KSP proporciona controles MDM avanzados de la política de IA. Estos controles son para las mismas opciones de Galaxy AI que se muestran en la aplicación Ajustes (Ajustes >> Galaxy AI), donde las funciones específicas de IA se pueden desactivar por completo. En KSP estas opciones se pueden configurar desde el menú "Política de restricciones avanzadas (Premium)".

5 FASE DE INSTALACIÓN

Como se ha explicado en la sección 4.5 el componente MDM juega un papel principal en los despliegues de movilidad. El Administrador IT de la Organización debe informarse de las soluciones MDM cualificadas en CPSTIC y utilizar sus guías de procedimiento seguro en conjunción con las de los dispositivos móviles utilizados.

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.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

La configuración recomendada para un despliegue COBO se detalla en la siguiente tabla.

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Password Policies	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex	Numeric(Complex)	Esto permite el código PIN. API: setPasswordQuality * o setRequiredPasswordComplexity Si la herramienta de administración no admite "Numeric(Complex)" pero sí admite "Numeric", se puede usar KPE para lograr el cumplimiento con CCN-STIC. En este caso, configure esta directiva con el valor "Numeric" y use una directiva KPE adicional (de forma nativa por la herramienta de administración o mediante KSP) "Maximum Numeric Sequence Length" con el valor "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 : Un patrón o PIN que repite (4444) o sigue una secuencia ordenada (1234, 4321, 2468). Media: 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: 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.			

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
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	Disable	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 *

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Restrictions	Bluetooth	Allow/Disallow	IT Admin decision	Se proporciona orientación para que el administrador de TI apruebe Bluetooth. API: `addUserRestriction`, `DISALLOW_BLUETOOTH` *
Device Restrictions	Wi-Fi Direct	Allow/Disallow	Disallow	API: addUserRestriction, DISALLOW_WIFI_DIRECT
Device Restrictions	Mount physical media	Allow/Disallow	Disallow	No aplicable a dispositivos que no admiten medios de almacenamiento extraíbles. Deshabilita el uso de todo el almacenamiento extraíble, por ejemplo, tarjetas SD y memorias USB. API: `addUserRestriction`, `DISALLOW_MOUNT_PHYSICAL_MEDIA`
Device Restrictions	USB file transfer	Allow/Disallow	Disallow	Se prohibirán las capacidades de transferencia de archivos mediante arrastrar y soltar en DeX, pero todas las demás funciones de DeX seguirán estando disponibles. API: `addUserRestriction`, `DISALLOW_USB_FILE_TRANSFER` *

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Restrictions	Config tethering	Allow/Disallow	Disallow	API: `addUserRestriction`, `DISALLOW_CONFIG_TETHERING` * Si la implementación requiere el uso de Mobile Hotspot y Tethering, se puede usar KPE para permitir su uso en una configuración aprobada por CCN-STIC. En este caso, no configure esta política y, en su lugar, sustitúyala por la directiva KPE (de forma nativa por la herramienta de administración o mediante KSP) "Allow open Wi-Fi connection" con el valor "disable" y añada el tema de formación "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 *

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Policy Restrictions	Galaxy AI	Enable/Disable Cloud Processing	Disable	KPE proporciona la API `allowIntelligenceOnlineProcessing` para deshabilitar el procesamiento en la nube de Galaxy AI.
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	La herramienta de administración debe proporcionar medios para leer el registro en la consola. 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 *
Device Restrictions	Install from unknown sources globally	Allow/Disallow	Disallow	API: addUserRestriction, DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY *

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Restrictions	CC mode	Enable/Disable	Enable	API: setCommonCriteriaModeEnabled *
Device Restrictions	Wi-Fi Sharing	Enable/Disable	Disable	API: DISALLOW_SHARING_ADMIN_CONFIGURED_WIFI
Device Restrictions	Wi-Fi Sharing	Enable/Disable	Disable	KPE proporciona la API `allowWiFiSharing`, que puede utilizarse mediante KSP para deshabilitar la función de compartir Wi-Fi.
Device Restrictions	Bluetooth	List of Bluetooth Profiles to Allow Default Blacklist	HSP_UUID HFP_UUID SPP_UUID A2DP_ADVAUDIODIST_UUID AVRCP_CONTROLLER_UUID AVRCP_TARGET_UUID Enable	KPE proporciona la API `addBluetoothUUIDsToWhiteList`, que puede utilizarse para permitir una lista de perfiles Bluetooth específicos. La aplicación de la lista negra predeterminada garantiza que no se puedan usar perfiles distintos de los especificados. Esta política también puede configurarse con KSP.
Device Restrictions	Factory Reset	Enable, Disable	Disable	API: addUserRestriction, DISALLOW_FACTORY_RESET
Device Restrictions	Admin unlock Factory Reset Protection (FRP)	Enable, Disable	Enable	API: setFactoryResetProtectionPolicy

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Restrictions	Assistant	Enable, Disable	Disable	API: `addUserRestriction`, `DISALLOW_ASSIST_CONTENT` Nota: este control también deshabilita la invocación de Gemini, si ya estaba instalado previamente.
Device Restrictions	Wireless Printing	Enable, Disable	Disable	API: addUserRestriction, DISALLOW_PRINTING
Device Restrictions	Screen Capture	Enable, Disable	Disable	API: setScreenCaptureDisabled

Tabla 1: Configuración Recomendada

6.2 ACTUALIZACIONES

Samsung publica mensualmente el Boletín de Seguridad [REF15] donde el Administrador IT de la Organización puede conocer las vulnerabilidades y mejoras que incorporar cada actualización de Software de los dispositivos móviles de Samsung.

El historial de versiones, así como el nivel de Parche de Seguridad que incorpora cada versión, para cada modelo se puede consultar en el siguiente link:

Ajustes > Acerca del Teléfono

Nombre del Modelo (sin incluir ningún prefijo como "/DS")

https://doc.samsungmobile.com/**SM-XXXX**/EUX/doc.html

Como ejemplo:

Galaxy S25 [SM-S931B]

[REF16]

6.3 AUDITORÍA

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 eight characters.	
Procedimiento	Configure the Samsung Android devices to enforce a minimum password length of eight characters. On the management tool, in the device password policies, set "minimum password length" to "8".	
Validación	Review the configuration to determine if the Samsung Android devices are enforcing a minimum password length of eight 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 “8”. 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 "8 digits", appears above the PIN entry. If on the management tool "minimum password length" is not set to "8", or on the Samsung Android device the text "PIN must contain at least" is followed by a value of less than "8 digits", this is a finding.	

ID: 004	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not allow more than 10 consecutive failed authentication attempts.	
Procedimiento	Configure the Samsung Android devices to allow only 10 or fewer consecutive failed authentication attempts. On the management tool, in the device password policies, set "max password failures for local wipe" to "10" 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 10 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 "10" 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 "10" 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 adming-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".	

ID: 011	PASS [ ]	FAIL [ ]
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)	

ID: 014	PASS [ ]	FAIL [ ]
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".	

ID: 015	PASS [ ]	FAIL [ ]
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 data 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".	

ID: 020	PASS [ ]	FAIL [ ]
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 ID 020 (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.	

ID: 022	PASS [ ]	FAIL [ ]
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.	

ID: 025	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android allowlist must be configured to not include artificial intelligence (AI) applications that process device data in the cloud, including Google Gemini.	

ID: 025	PASS [ ]	FAIL [ ]
Procedimiento	This validation procedure is performed only on the EMM Administration Console. On the EMM console: 1. Review the list of selected Managed Google Play apps. 2. Verify no AI applications that processes device data in the cloud, including Google Gemini, are included. Note: This restriction does not include Galaxy on device AI. Galaxy on device AI is a ""built-in"" capability of Android 16 and processes device data on the device." If the EMM console device policy includes AI applications that processes device data in the cloud, including Google Gemini, this is a finding. Disallow modify accounts If "disallow modify accounts" has not been implemented, this is a finding. Apply the "Disallow Intelligence Online Processing" using the KPE API or KSP. The KPE API is allowIntelligenceOnlineProcessing(false) and the KSP restriction is "Allow process data only on device", which should be set to true.	
Validación	Review managed Samsung Android 16 device configuration settings to determine if the mobile device has an AI application that processes device data in the cloud, including Google Gemini. Verify ID 20 requirement (disallow modify accounts) has been implemented. Verify that the KPE API "isIntelligenceOnlineProcessingAllowed()" returns false or that the KSP configuration has the restriction "Allow process data only on device" set to true.	

ID: 026	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable ad hoc wireless client-to-client connection capability.	

ID: 026	PASS [ ]	FAIL [ ]
Procedimiento	Configure the Samsung Android devices to disallow Wi-Fi Direct. On the management tool, in the user restrictions, set "Wi-Fi Direct" to "Disallow". Wi-Fi direct connections and pairing between devices will become unavailable.	
Validación	Review the configuration to determine if the Samsung Android devices are disallowing Wi-Fi Direct. This validation procedure is performed on both the management tool and the Samsung Android device. On the management tool, in the user restrictions, verify "Wi-Fi Direct" has been set to "Disallow". On the Samsung Android device: 1. Open Settings >> Connections >> Wi-Fi. 2. From the hamburger menu, select Wi-Fi Direct. 3. Verify that Wi-Fi Direct cannot be selected. If on the management tool "Wi-Fi Direct" is not set to "Disallow", or on the Samsung Android device a Wi-Fi direct device is listed that can be connected to, this is a finding.	

ID: 027	PASS [ ]	FAIL [ ]
Requerimiento	The Samsung Android device must be configured to enforce that Wi-Fi Sharing is disabled.	

ID: 027	PASS [ ]	FAIL [ ]
Procedimiento	Configure the Samsung Android 16 device to disable Wi-Fi Sharing. Mobile Hotspot must be enabled to enable Wi-Fi Sharing. If the AO has not approved Mobile Hotspot, and it has been disabled on the EMM console, no further action is needed. If Mobile Hotspot is being used, then use the following procedure and “User-Based Enforcement (UBE)” control: Train users to disable/not enable Samsung Wi-Fi Sharing. -Settings / Connections / Mobile Hotspot and Tethering / Mobile Hotspot -Tap "Network name" -Tap "Advanced" -Verify that "Wi-Fi sharing" is toggled off or the option is disabled On the EMM console: 1. Open "Set user restrictions". 2. Toggle "Disallow sharing admin configured Wi-Fi" to "ON". KPE policy can be used to configure this setting without “User-Based Enforcement (UBE)” control, by setting the "Allow Wi-Fi Sharing" option in KSP to disable.	

ID: 027	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm Wi-Fi Sharing is disabled. Mobile Hotspot must be enabled to enable Wi-Fi Sharing. If the IT Admin of the Organization has not approved Mobile Hotspot, and it has been verified as disabled on the EMM console, no further action is needed. If Mobile Hotspot is being used, use the following procedure to verify Wi-Fi Sharing is disabled: This is a “User-Based Enforcement (UBE)” control. Check a sample of Samsung phones at the site and verify that the mobile hotspot Wi-Fi sharing option is toggled to off. -Settings / Connections / Mobile Hotspot and Tethering / Mobile Hotspot -Tap "Network name" -Tap "Advanced" -Verify that "Wi-Fi sharing" is toggled off or the option is disabled If the Wi-Fi sharing is not set to disabled, this is a finding. On the EMM console: 1. Open "Set user restrictions". 2. Verify "Disallow sharing admin configured Wi-Fi" is toggled to "ON". If on the EMM console, "Disallow sharing admin configured Wi-Fi" is not enabled, this is a finding.	

ID: 028	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).	

ID: 028	PASS [ ]	FAIL [ ]
Procedimiento	Configure the Samsung Android devices to disable Bluetooth, or if the IT Admin of the Organization has approved the use of Bluetooth (for example, for hands-free use), train users to only pair devices that support HSP, HFP, SPP, A2DP, AVRCP, and PBAP profiles. On the management tool, in the device restrictions section, set "Bluetooth" to the IT Admin of the Organization-approved selection: "Allow" if the IT Admin of the Organization has approved the use of Bluetooth or "Disallow" if the IT Admin of the Organization has not approved its use. If a COBO deployment requires the use of specific Bluetooth profiles, Knox Platform for Enterprise (KPE) can be used to allow them in an approved configuration. In this case, do not configure this policy, and instead replace with KPE policy (innately by the management tool or via Knox Service Plugin [KSP]) "Add Bluetooth UUIDs To WhiteList " with values "HSP_UUID, HFP_UUID, SPP_UUID, A2DP_ADVAUDIODIST_UUID, AVRCP_CONTROLLER_UUID, AVRCP_TARGET_UUID" and default blacklist as "enable".	
Validación	Review the Samsung documentation and inspect the configuration to verify the Samsung Android devices are paired only with devices that 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 of the Organization-approved selection: "Allow" if the IT Admin of the Organization has approved the use of Bluetooth or "Disallow" if the IT Admin of the Organization has not approved its use. On the Samsung Android device: 1. Open Settings >> Connections >> Bluetooth. 2. Verify all listed paired Bluetooth devices use only authorized Bluetooth profiles. If on the management tool "Bluetooth" is not set to the IT Admin of the Organization-approved value, or the Samsung Android device is paired with a device that uses unauthorized Bluetooth profiles, this is a finding.	

ID: 029	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must disable the use of assistants (including Samsung Assistant)	
Procedimiento	Configure Samsung Android device to disable the use of all assistants. On the MDM console, do the following: 1. Open user restrictions 2. Enable "Disallow assist content" 3. Do not allowlist the Gemini App in the Managed Samsung Play Store. Note: This control also disables Gemini from being invoked, if it was previously installed.	
Validación	Review configuration settings to confirm the use of assistants has been disabled. This check procedure is performed on the device management tool and the Samsung Android device. On the MDM console: 1. Open user restrictions 2. Verify that "Disallow assist content" is enabled. 3. Verify that the Gemini App in the Managed Samsung Play Store has not been added to the allowlist. On the managed Samsung Android device: 1. Try to invoke the Google Assistant and note that it will not execute. 2. Verify that the Gemini app is not installed and that it is not listed in the Managed Samsung Play Store. If the use of assistants has been disabled, this is a finding. Note: This control also disables Gemini from being invoked, if it was previously installed.	

ID: 030	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android device must disable wireless printing.	

ID: 030	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android device to disable wireless printing. On the MDM console, do the following: 1. Open user restrictions 2. Enable "Disallow printing"	
Validación	Review configuration settings to confirm wireless printing has been disabled. This check procedure is performed on the device management tool and the Samsung Android device. On the MDM console: 1. Open user restrictions 2. Verify that "Disallow printing" is enabled. On the managed Samsung Android device: 1. Open a document or image from the file app and try to print. 2. Verify that you cannot print If wireless printing has not been disabled, this is a finding.	

ID: 031	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android device must disable screen capture.	
Procedimiento	Install a configuration profile to disable screen capture. On the MDM console, do the following: 1. Open Camera, screen capture, and audio section 2. Enable the "Disable Screen Capture" setting	

ID: 031	PASS [ ]	FAIL [ ]
Validación	Review configuration settings to confirm screen capture has been disabled. This check procedure is performed on the device management tool and the Samsung Android 16 device. On the MDM console: 1. Open Camera, screen capture, and audio section 2. Verify that "Disable Screen Capture" setting is enabled On the managed Samsung Android device: 1. Press the Power button and the volume down button at the same time. Verify that the message "Taking screenshots is blocked by your admin". If screen capture has not been disabled, this is a finding.	

Tabla 2: Controles de Auditoría

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 enlace REF17.

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



Figura 4: DPC QR

Una vez instalada la aplicación de test, se pueden ejecutar las políticas de la tabla de configuración en la sección 6.1, para una familiarización con las mismas y su consiguiente mapeo a la solución MDM específica elegida.

Como ejemplo, 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.

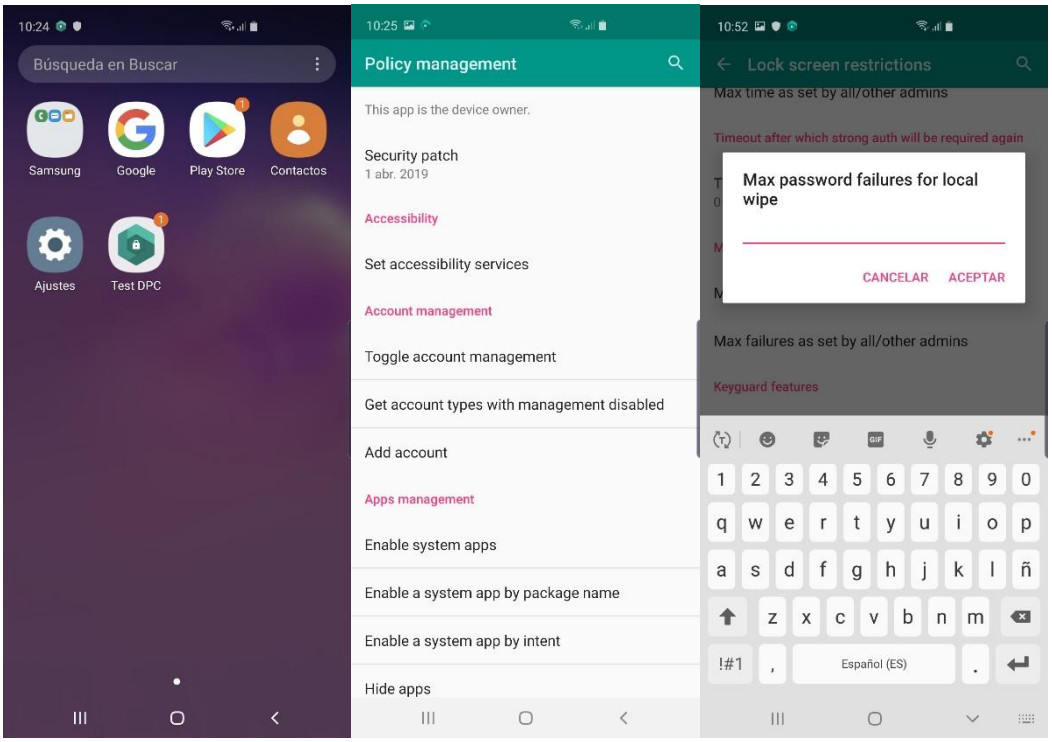


Figura 5: Aplicación DPC

7 REFERENCIAS

REF1 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

REF2 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

REF3 www.samsung.com/es/business/mobile/enterprise-edition/

REF4 www.samsungknox.com

REF5 https://www.samsungknox.com/es-419/solutions/it-solutions/knox-configure

REF6 https://docs.samsungknox.com/admin/knox-configure/welcome.htm

REF7 https://www.samsungknox.com/es-419/solutions/it-solutions/knox-asset-intelligence

REF8 https://www.samsungknox.com/en/knox-platform/supported-devices

REF9 https://www.samsungknox.com/es-419/solutions/it-solutions/knox-manage

REF10 https://docs.samsungknox.com/admin/knox-manage/welcome.htm

REF11 https://www.samsungknox.com/es-419/solutions/it-solutions/samsung_e-fota

REF12 https://play.google.com/store/apps/details?id=com.samsung.android.appseparation&hl=en_GB&gl=US

REF13 https://docs.samsungknox.com/admin/knox-platform-for-enterprise/migrate-to-android-14/separated-apps-for-android-14/

REF14 https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/data-processing-for-galaxy-ai

REF15 https://security.samsungmobile.com/securityUpdate.smsb

REF16 https://doc.samsungmobile.com/SM-S931B/EUX/doc.html

REF17 https://github.com/googlesamples/android-testdpc

8 ABREVIATURAS

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

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