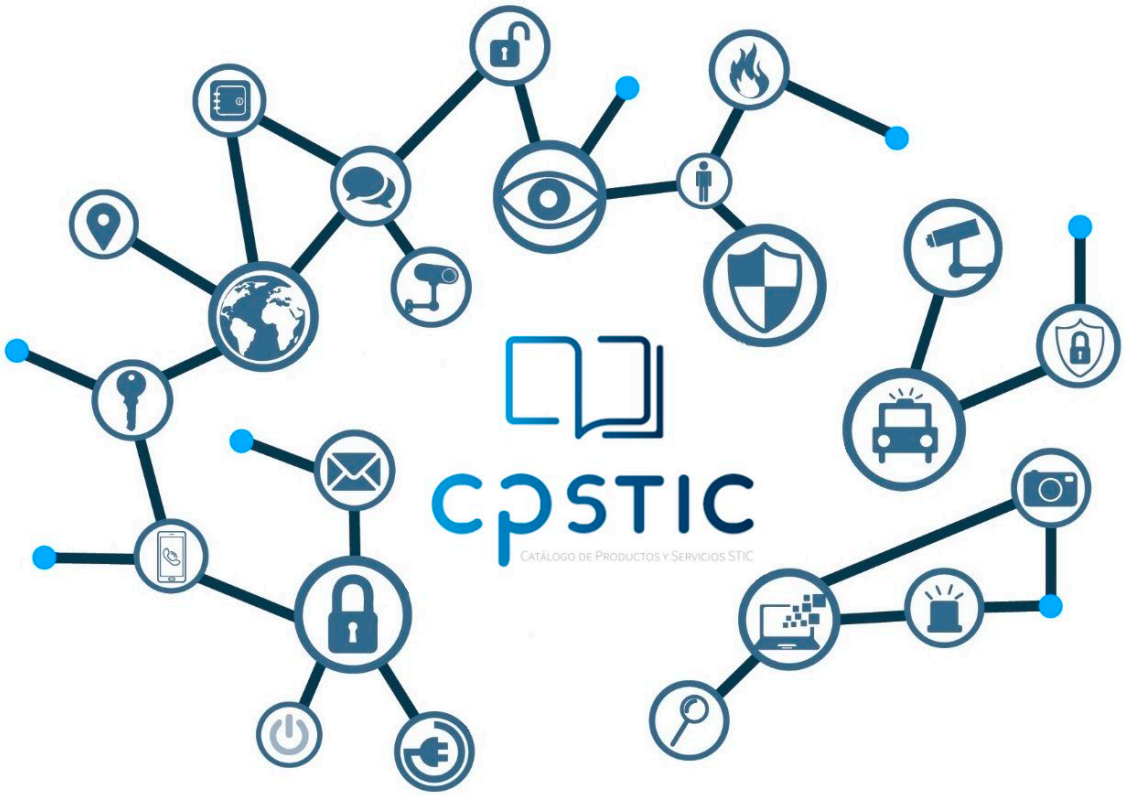
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1617

Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 12)



Septiembre de 2022

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.09.19 10:55:31 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-235-1.

Fecha de Edición: Septiembre de 2022.
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

ÍNDICE

1. INTRODUCCION

El objetivo de este documento es proporcionar una guía de configuración de los dispositivos Samsung Galaxy con Android 12 cualificados por CCN e incluidos como tales en el Catálogo de Productos CPSTIC (cpstic.ccn.es).

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 móviles[1]. La sección 1.2 detalla las novedades introducidas en la última versión de Knox, que será de interés para los Administradores IT de la organización ya familiarizados con el despliegue de la solución de movilidad y funcionalidades que proporciona Samsung.

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 esta 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
- WP-C – Work Profile in Company owned device
- 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 especial agente (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 WP-C 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 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 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, que complementará la configuración básica del área personal del usuario.

El escenario COBO, 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 DO (Device Owner), y **ningún** Workspace / Contenedor es creado.

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.

1.2 KPE 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.

Figura 1

1.2.1. 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 duplicación 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.

Este CCN-STIC está completamente armonizado con la configuración STIC de la plataforma Android de Google. Las políticas de seguridad de AE enumeradas cubren los requisitos de CCN-STIC de referencia. Las políticas de Knox incrementan las capacidades de implementación proporcionando características adicionales, y en algunos casos se pueden utilizar para minimizar las limitaciones de la herramienta de gestión. Con esta armonización, la implementación previa en modo Legacy que desplegaba terminales como Device Admin (DA), ha quedado en desuso y ya no está soportada.

Las siguientes configuraciones están disponibles para los dispositivos Samsung Galaxy con Android 12:

- Para desplegar COBO, dispositivo totalmente administrado:
    - Los privilegios para ser propietario del terminal (DO) se asignan a un MDM o a una aplicación similar para aplicar políticas y restricciones al dispositivo en su conjunto.
- Para desplegar WP-C (administración-sobre-privacidad), dispositivo totalmente administrado con separación de aplicaciones:
    - Los privilegios DO se asignan a un MDM o a una aplicación similar para aplicar política sin restricciones al dispositivo en su conjunto. Además, utilizando la funcionan de Separación de aplicaciones de Knox (Knox App Separation), se aíslan un grupo de aplicaciones del resto del sistema, implementando casos de usos como el aislamiento de aplicaciones no aprobadas para el trabajo o la separación de aplicaciones con mayor nivel de confianza.
- Para desplegar WP-C (privacidad-sobre-gestión), perfil de trabajo en un dispositivo propiedad de la empresa:
    - Se crea un perfil de trabajo en un terminal propiedad de la empresa, permitiendo el uso personal del dispositivo y el uso corporativo en un perfil separado. El perfil de trabajo es gestionado por un Profile Owner (PO) que puede aplicar ciertas configuraciones al dispositivo en su conjunto respetando la privacidad del usuario.

- Para desplegar BYOD: perfil de trabajo en un dispositivo de propiedad personal:
    - Se crea un perfil de trabajo en un dispositivo del empleado. El perfil de trabajo es gestionado por un Profile Owner (PO) que puede aplicar configuraciones solo al perfil de trabajo, con la excepción de muy pocas políticas que se pueden aplicar al terminal.

1.2.2. ANDROID 12 PRIVACIDAD DEL USUARIO

Android 12 continúa enfocado en mejorar la privacidad del usuario, como ya se vino haciendo en Android 11. Por lo tanto, AE tiene poco control sobre el perfil personal. Las aplicaciones personales en el perfil personal no pueden ser configuradas, ni monitoreadas, ni enumeradas por un MDM. Esta situación puede ser mitigada por los proveedores de servicios de la Organización interesada en un mayor control de las aplicaciones del lado personal:

- Implementando un registro zero-touch o Knox Mobile Enrollment: desde el perfil generado en KME se muestra a los terminales antiguos y a los nuevos eliminar todas las aplicaciones en el momento del registro. Desde el MDM se pueden controlar las aplicaciones descargadas creando lista de aplicaciones permitidas o aplicaciones bloqueadas.
- Como alternativa, para terminales totalmente gestionados (COBO), podríamos hacer uno de Knox Service Plugin (KSP) para permitir la instalación de aplicaciones personales.

1.2.3. ANDROID ENTERPRISE (AE)

1.2.3.1. AISLAMIENTO DE APLICACIONES

Android permite aislar una aplicación o asilar un grupo de aplicaciones.

La tecnología core para aislar una aplicación se llama SE para Android, que es una adaptación de SELinux para Android. Esta tecnología niega el acceso de las aplicaciones a los recursos a menos que lo permita una política construida por Samsung. Las aplicaciones reciben etiquetas para que no puedan acceder a los datos de otras aplicaciones o de la misma aplicación instalada bajo un usuario diferente.

Los grupos de aplicaciones pueden ser aislados mediante la creación de un perfil de trabajo. Esto da como resultado la instalación de las aplicaciones bajo un usuario de Android diferente. Si bien la comunicación está permitida entre las aplicaciones instaladas en el mismo usuario, esto está prohibido por Android para aplicaciones que no son del sistema instaladas bajo usuarios diferentes.

La creación de un perfil de trabajo no es posible en Android 12 cuando el dispositivo se ha inscrito como un dispositivo totalmente administrado (COBO). Sin embargo, Samsung proporciona un mecanismo alternativo para la separación de aplicaciones en el escenario COBO utilizando la función de Knox App Separation. Este mecanismo puede ser habilitado o deshabilitado por un administrador de IT a través de Knox Service Plugin

(KSP). Al instalar KSP en el dispositivo de destino, los administradores de IT pueden especificar qué aplicaciones desean ver aisladas en consolas UEM compatibles. Estas aplicaciones se instalarán mediante el Play Store gestionado bajo un usuario secundario de Android y se deshabilitan del usuario principal. Las aplicaciones de sistema que no tienen launcher se habilitan en el usuario secundario por defecto. Como ocurren en los perfiles de trabajo, no se permite compartir entre los usuarios, fortaleciendo el aislamiento de estas aplicaciones como grupo.

1.2.4. 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

1.2.5. A DESTACAR DE KPE EN ANDROID 12

Configuración de Criterios Comunes (Common Criteria)

Dando respuesta a la problemática de implementación del requerimiento de configurar el dispositivo en Modo Common Criteria debido principalmente a que los productos de gestión MDM no proporcionan todos los controles necesarios, se realiza la siguiente aclaración para que el Administrador IT de la organización pueda realizar la implementación de la regla de configuración lo más alineada posible al objetivo de la misma.

El requerimiento indica que solo los dispositivos móviles que hayan pasado la evaluación de Criterios Comunes (Common Criteria) se usen en la organización. Es por esto que la presente guía CCN-STIC aplica el mismo conjunto de configuraciones a los dispositivos que se requerirían en la evaluación de Criterios Comunes. El control, “Modo CC”, es una API que implementa nueva cambios funcionales separados en el dispositivo móvil.

El conjunto de opciones de configuración de Criterios Comunes en esta guía incluye controles de políticas administradas por la herramienta de gestión/MDM y un control de cumplimiento basado en directiva al usuario (UBE):

- Características impuestas por la política:
  - Habilitar el modo Knox CC (Common Criteria)
  - Habilite el cifrado de almacenamiento externo o no permita el montaje de medios físicos

- Calidad mínima de contraseña
- Deshabilitar desbloqueo biométrico "Cara"
- Verificar OCSP y/o Verificación de revocación
- Fallos máximos de contraseña para iniciar el borrado del dispositivo

➢ UBE:

- Inicio seguro/ Protección fuerte

Nota: Las políticas "Duración del historial de contraseña" y "Recuperación de contraseña" ya no son necesarias.

Para ser 100% compatible con el modo de operación CC, todas las políticas deben de configurarse correctamente. Sin embargo, las restricciones operativas o de implementación pueden requerir que no se configuren algunas políticas que causan un problema cuando se seleccionan. El Administrador IT de la organización debe determinar si el riesgo es aceptable para desviarse de cualquier configuración requerida en el despliegue.

Clarificación acerca de Inicio Seguro

Inicio seguro ofrece seguridad adicional solo cuando un dispositivo está apagado y hasta la primera autenticación. Para implementaciones con necesidades operativas que requieren que los dispositivos de los usuarios estén siempre encendidos (por ejemplo, para que los usuarios no pierdan alertas de emergencia importantes o puedan responder a las necesidades de la misión), se puede suponer que los usuarios siempre se han autenticado una vez y, por lo tanto, son seguros.

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 explican los detalles técnicos a tener en cuenta por un Administrador IT a la hora de diseñar un despliegue, teniendo en cuenta que los detalles de la solución MDM elegida, y su manejo no se recogen en esta guía.

2.1 SDK DE KNOX

Samsung Knox 3.x SDK proporciona varias API para que proveedores de soluciones MDM, configuren los componentes de seguridad de Knox que se pueden usar para implementar diferentes controles de seguridad. Estas API se pueden utilizar para configurar restricciones en el dispositivo.

2.2 LICENCIA KNOX

La solución MDM debe activar una licencia de Knox Platform for Enterprise (KPE) antes de obtener acceso a la gama completa de API y funciones de Samsung Knox. Las licencias de KPE las compra la organización a un distribuidor de Knox y se administran mediante la solución MDM. Un agente que se ejecuta en el dispositivo validará la licencia con el servidor de administración de licencias Knox de Samsung (KLM).

Nota: La licencia Knox Platform for Enterprise (KPE) ahora se proporciona sin coste.

2.3 SERVIDORES LOCALES DE KNOX

En este documento y en los despliegues que quieran obtener un nivel de seguridad demostrable acorde con esta guía (ENS Nivel Alto) se deben utilizar servidores Samsung Knox On-Premise, disponibles para organizaciones que deseen implementar y administrar los servicios de Knox en sus instalaciones.

Se espera que las organizaciones instalen, configuren y administren los servidores locales de Knox en los servidores administrados dentro de la propia organización. Samsung proporciona los paquetes de instalación del servidor local, que están disponibles para Windows y Linux.

El servidor de Knox On-Premise incluye los siguientes componentes:

• **Administración de licencias de Knox (KLM)**: el sistema de cumplimiento y administración de licencias para Samsung Knox. KLM se utiliza para activar los servicios de Knox en dispositivos compatibles.

• **Global Server Load Balancing / Servidor de Carga Balanceado (GSLB)**: un servidor de diccionario para los diversos servicios (por ejemplo, el servidor KLM). La URL del servidor GSLB está codificada en la licencia Knox proporcionada por la empresa. Durante la activación, el servidor GSLB devolverá los puntos finales (URL) para los diversos servicios a los agentes del dispositivo.

Una organización que decida implementar el servidor de Knox On-Premise deberá solicitar la licencia de Knox adecuada al proveedor de Knox. La Organización proporcionará su URL del servidor GSLB local, que se codificará en la licencia de Knox.

El agente MDM pasará la licencia de Knox a un agente KLM que se ejecuta fuera del dispositivo. Este agente se conectará al servidor GSLB, que devolverá la URL del servidor KLM. El agente después se conecta al servidor KLM para obtener la validación de la licencia de Knox.

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 el ANEXO A.

2.4 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.

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 Y COMPATIBLES

En este apartado se listan los dispositivos cualificados por CCN con versión de Android 12.0 (apartado 3.1.1) así como dispositivos cualificados por CCN con una versión anterior de Android que se actualizan a la versión 12.0 (apartado 3.1.2). El listado completo y actualizado se puede encontrar en la siguiente página web: cpstic.ccn.es

El listado se complementa con dispositivos que son compatibles con la presente guía, pero no han sido evaluados y cualificados por CCN (apartado 3.1.3).

3.1.1. DISPOSITIVOS CUALIFICADOS

NOMBRE DISPOSITIVO	MODELO	VERISION DE ANDROID	VERSION DE KERNEL	COMPILACIÓN
Samsung Galaxy Tab S8 5G	SM-X706B	12.0	5.10.43	SP1A.210812.016
Samsung Galaxy Tab S8+ 5G	SM-X806B	12.0	5.10.43	SP1A.210812.016
Samsung Galaxy Tab S8 Ultra 5G	SM-X906B	12.0	5.10.43	SP1A.210812.016
Samsung Galaxy S22 5G	SM-S901B	12.0	5.10.66	SP1A.210812.016
Samsung Galaxy S22+ 5G	SM-S906B	12.0	5.10.66	SP1A.210812.016
Samsung Galaxy S22 Ultra 5G	SM-S908B	12.0	5.10.66	SP1A.210812.016
Samsung Galaxy Z Fold3 5G	SM-F926B	12.0	5.4.147	SP1A.210812.016
Samsung Galaxy Z Flip3 5G	SM-F711B	12.0	5.4.147	SP1A.210812.016

Tabla 1

3.1.2. DISPOSITIVOS COMPATIBLES CUALIFICADOS

NOMBRE DISPOSITIVO	MODELO	VERSION DE ANDROID	VERSION DE KERNEL	COMPILACIÓN
Galaxy S21 Ultra+ 5G	SM-G998B	12.0	5.4.61	RP1A.200720.012
Galaxy S21 + 5G	SM-G996B	12.0	5.4.61	RP1A.200720.012
Galaxy S21 5G	SM-G991B	12.0	5.4.61	RP1A.200720.012
Galaxy Note20 4G	SM-N980F	12.0	4.19.87	RP1A.200720.012
Galaxy Note20 5G	SM-N981B	12.0	4.19.87	RP1A.200720.012
Galaxy Note20 Ultra 5G	SM-N986B	12.0	4.19.87	RP1A.200720.012
Galaxy S20 FE 4G	SM-G780F	12.0	4.19.87	RP1A.200720.012
Galaxy S20 FE 5G	SM-G781B	12.0	4.19.87	RP1A.200720.012
Galaxy Tab Active 3	SM-T570 / SM-T575	12.0	4.14.113	QP1A.190711.020
Galaxy Tab S7	SM-T870 / SM-T875	12.0	4.19.113	RP1A.200720.012
Galaxy Tab S7+	SM-T970/ SM-T976B	12.0	4.19.113	RP1A.200720.012
Galaxy Tab S6	SM-T860 / SM-T865	12.0	4.19.113	RP1A.200720.012
Galaxy Z Flip	SM-F700F/ SM-F707B	12.0	4.19.113	RP1A.200720.012
Galaxy Z Fold2 5G	SM-F916B	12.0	4.19.113	RP1A.200720.012
Galaxy A51	SM-A515F	12.0	4.14.113	RP1A.200720.012
Galaxy A52 5G	SM-A526B	12.0	4.14.113	RP1A.200720.012
Galaxy S20+ 5G	SM-G986B	12.0	4.19.87	RP1A.200720.012
Galaxy S20 5G	SM-G981B	12.0	4.19.87	RP1A.200720.012
Galaxy S20 Ultra 5G	SM-G988B	12.0	4.19.87	RP1A.200720.012
Galaxy S20+ 4G	SM-G985F	12.0	4.19.87	RP1A.200720.012
Galaxy S20 4G	SM-G980F	12.0	4.19.87	RP1A.200720.012
Galaxy S20 FE 4G / 5G	SM-G780F / SM-G781B	12.0	4.19.87	RP1A.200720.012
Galaxy Tab S6	SM-T860/ SM-T865	12.0	4.14.180	RP1A.200720.012

NOMBRE DISPOSITIVO	MODELO	VERSION DE ANDROID	VERSION DE KERNEL	COMPILACIÓN
Galaxy XCoverPro	SM-G715FN	12.0	4.14.113	RP1A.200720.012
Galaxy Note10	SM-N970F	12.0	4.14.113	RP1A.200720.012
Galaxy Note10+	SM-N975F	12.0	4.14.113	RP1A.200720.012
Galaxy Note10+ 5G	SM-N976B	12.0	4.14.113	RP1A.200720.012
Galaxy S10	SM-G973F	12.0	4.14.113	RP1A.200720.012
Galaxy S10e	SM-G970F	12.0	4.14.113	RP1A.200720.012
Galaxy S10+	SM-G975F	12.0	4.14.113	RP1A.200720.012
Galaxy S10 5G	SM-G977B	12.0	4.14.113	RP1A.200720.012

Tabla 2

3.1.3. DISPOSITIVOS ENTERPRISE EDITION

Samsung Galaxy Enterprise Edition añade al dispositivo móvil una serie de características exclusivas pensadas para ofrecer una seguridad mejorada, mayor personalización y soporte técnico. Una gran selección de dispositivos incluidos en las tablas 1 y 2 se ofrecen en versión Enterprise Edition, a través de canales de venta específicos. Estos dispositivos ofrecen hasta 5 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, la versión de Kernel y número de Compilación de un dispositivo, 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 el prefijo de la versión de Kernel así como el prefijo del número de compilación.

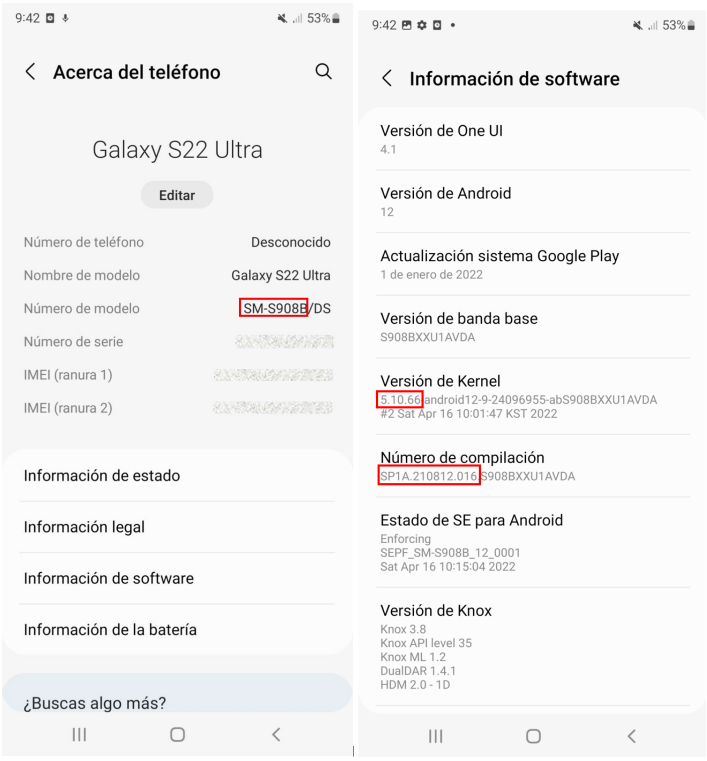


Figura 2

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 obligatoria, la cual se puede auditar ejecutando los casos de test indicados en el ANEXO B de esta guía.

Las reglas de configuración del dispositivo están detalladas desde un punto de vista de la plataforma del dispositivo, siendo 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 correspondiente.

3.3.1. TABLA DE CONFIGURACIÓN

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 * 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 / Mlid: 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+	5 attempts	API: setMaximumFailedPasswordsForWipe *
Device Password Policies	Max time to screen lock	0+ minutes	10 minutes	API: setMaximumTimeToLock *
Device Restrictions	Face	Enable/Disable	Disable	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE This policy is included to allow a Samsung Android device to be deployed as an AE device 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.
Device Restrictions	Trust agents	Enable/Disable	Disable	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
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 *
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	Include Organitation certificates in Work Profile	Device Policy Management	API: installCaCert *

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
Device Restrictions	App installation whitelist	List of apps	List only approved work apps	Use KPE app installation whitelist. Refer to the management tool documentation to determine the following: - If an application installation blacklist is also required to be configured when enforcing an "app installation whitelist"; and - If the management tool supports adding apps to the "app installation whitelist" by package name and/or digital signature or supports a combination of the two.
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 *
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 3 - Reglas Configuración para un despliegue COBO

3.4 DESACTIVACIÓN DE APLICACIONES

Samsung Knox para Android soporta políticas de deshabilitación de aplicaciones que permiten al Administrador IT de la organización desactivar aplicaciones principales y preinstaladas especificando el nombre de paquete. Como en cada dispositivo y variante de operador se preinstalarán diferentes conjuntos de aplicaciones, el Administrador debe coordinar previamente con su proveedor de dispositivos y tener identificadas a priori que aplicaciones vienen preinstaladas en los dispositivos que le proporcionan, de manera que pueda decidir que aplicaciones representan una amenaza para la información confidencial en el dispositivo y configurar la deshabilitación de dichas aplicaciones mediante la configuración de políticas de desactivación de aplicaciones.

Esta tarea debe ser realizada antes de la recepción del dispositivo por parte de la Organización o del Usuario final del dispositivo.

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 aprobada por CCN con FIPS 140-2 WiFi validado. Miracast solo debe utilizarse con televisores, monitores y dongles Miracast con clientes WiFi validados FIPS 140-2.

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 prohíbe 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	*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)*

ANEXO A. Knox Cloud Services

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.

A continuación, se lista cada producto, así como una descripción general de su funcionamiento.

Cabe resaltar que los servicios de Knox Mobile Enrollment (KME), Knox Configure (KC) y Knox E-FOTA (KE1) han pasado satisfactoriamente los test funcionales de un laboratorio acreditado en el ENECSTI, por el Organismo de Certificación del Centro Criptológico Nacional, siendo dichos servicios recomendados para su uso en un entorno empresarial.

- Knox Mobile Enrollment: Servicio Cloud que permite automatizar la inscripción de dispositivos, ya sea de forma individual o masiva. Es la forma más rápida y eficaz de inscribir una gran cantidad de dispositivos en un MDM para uso corporativo. Una vez que un administrador de TI configura un dispositivo con el servicio, el usuario del dispositivo simplemente tiene que encenderlo y conectarse a Wi-Fi o 3G/4G/5G durante el proceso de configuración inicial del dispositivo.

  El IMEI o el número de serie de los dispositivos comprados se carga y registra en la cuenta KME del Cliente por parte de un revendedor participante en KDP (Knox Deployment Program). Luego, el administrador puede configurar este conjunto de dispositivos para la inscripción.

  Algunas de las opciones de uso de KME son:

  - Inscripción automatizada de MDM/EMM: inicie sesión automáticamente en los agentes de MDM/EMM con las credenciales de usuario proporcionadas por el administrador de TI.
  - Proceso de configuración del dispositivo simplificado: omita los pasos de configuración no deseados, como el registro de la cuenta de Google.
  - Ampliamente compatible con casi todas las soluciones MDM/EMM.
  - Soporta inscripción para gestión Android Enterprise.
  - Permite eludir la protección de restablecimiento de fábrica de Google (FRP).
  - Permite especificar certificados raíz o intermedios que se instalarán durante la inscripción de KME (por ejemplo, la instalación del paquete de certificados intermedios y raíz).

  Para más información, consultar el enlace del producto: https://www.samsungknox.com/es-419/solutions/it-solutions/knox-mobile-enrollment

  Así como la Admin guide: https://docs.samsungknox.com/admin/knox-mobile-enrollment/welcome.htm

- Knox Configure: 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

- Knox E-FOTA: Knox Enterprise Firmware-Over-The-Air es una solución Cloud que permite aplicar campañas de actualización del Sistema Operativo a los terminales Samsung. En estas campañas, el administrador de la consola, puede controlar qué versión del Sistema Operativo se va a instalar en los terminales y bajo qué condiciones se llevará a cabo tanto la descarga como posteriormente la instalación. Además, puede configurar que los terminales permanezcan en una versión concreta del Sistema Operativo. Este servicio es indispensable para aquellos organismos que trabajen con aplicaciones internas o configuraciones que pueden ser impactadas por los cambios de versiones del Sistema Operativo.

  Algunas de las opciones de uso de E-FOTA permiten:

  - Actualización selectiva de versiones del sistema operativo
  - No se necesita interacción del usuario
  - Programar actualizaciones según calendario, condiciones de red y batería.
  - Actualización forzada de los dispositivos de destino

  Para más información del servicio, consultar el enlace: https://www.samsungknox.com/es-419/solutions/it-solutions/samsung_e-fota

  Además, la información más técnica está disponible en la Admin Guide: https://docs.samsungknox.com/admin/efota-one/welcome.htm

- 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, consultar el enlace: https://www.samsungknox.com/es-419/solutions/it-solutions/knox-asset-intelligence

- 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

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 display the Organization advisory warning message at startup or each time the user unlocks the device.	
Procedimiento	Configure the Organization warning banner by either of the following methods (required text is found in the Vulnerability Discussion): Method #1: Place the Organization warning banner in the user agreement signed by each Samsung Android device user (preferred method). Method #2: Configure the warning banner text in the Lock screen message on each managed mobile device. On the management tool, in the device restrictions section, set "Lock Screen Message" to the Organization -mandated warning banner text.	

ID: 002	PASS [ ]	FAIL [ ]
Validación	Confirm if Method #1 or #2 is used at the Samsung device site and follow the appropriate procedure. This validation procedure is performed on both the management tool and the Samsung Android device. Validation Procedure for Method #1: Place the Organization warning banner in the user agreement signed by each Samsung Android device user (preferred method). Review the signed user agreements for several Samsung Android device users and verify that the agreement includes the required Organization warning banner text. Validation Procedure for Method #2: Configure the warning banner text in the Lock screen message on each managed mobile device. On the management tool, in the device restrictions section, verify that "Lock Screen Message" is set to the Organization -mandated warning banner text. On the Samsung Android device, verify that the required Organization warning banner text is displayed on the Lock screen. If the warning text has not been placed in the signed user agreement, or if on the management tool "Lock Screen Message" is not set to the Organization -mandated warning banner text, or on the Samsung Android device the required Organization warning banner text is not displayed on the Lock screen, this is a finding.	

ID: 003	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".	

ID: 003	PASS [ ]	FAIL [ ]
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: 004	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable a screen-lock policy that will lock the display after a period of inactivity	
Procedimiento	Implement a "minimum password quality"	
Validación	Verify minimum password quality has been implemented. If a "minimum password quality" has not been implemented, this is a finding.	

ID: 005	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".	

ID: 005	PASS [ ]	FAIL [ ]
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: 006	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.	

ID: 006	PASS [ ]	FAIL [ ]
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: 007	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to lock the display after 10 minutes (or less) of inactivity	
Procedimiento	Configure the Samsung Android devices to lock the device display after 10 minutes (or less) of inactivity. On the management tool, in the device password policies, set "max time to screen lock" to "10 minutes" or less. A device password must be set for "max time to screen lock" to become active.	

ID: 007	PASS [ ]	FAIL [ ]
Validación	Review the configuration to determine if the Samsung Android devices are locking the device display after 10 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 "10 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 10 minutes or less. If on the management tool "max time to screen lock" is not set to "10 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 10 minutes, this is a finding	

ID: 008	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.	
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".	

ID: 008	PASS [ ]	FAIL [ ]
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: 009	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: 010	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: 011	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".	

ID: 011	PASS [ ]	FAIL [ ]
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: 012	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.	

ID: 012	PASS [ ]	FAIL [ ]
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: 013	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: 013	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: 014	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.	

ID: 014	PASS [ ]	FAIL [ ]
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: 015	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 KNOX-12-110140 (Disallow USB file transfer) has been implemented. If "Disallow USB file transfer" has not been implemented, this is a finding.	

ID: 016	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: 016	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: 017	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 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: 018	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: 019	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 Authorizing Official (IT admin). In addition to any local policy, the IT admin must not approve applications which have certain prohibited characteristics, these are covered in KNOX-12-110200. 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.	

ID: 019	PASS [ ]	FAIL [ ]
Validación	Review the configuration to determine if the Samsung Android devices are allowing users to install only applications that have been approved by the Authorizing Official (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: 020	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not allow installation of applications with the following characteristics: - back up MD data to non-Organization cloud servers (including user and application access to cloud backup services);- transmit MD diagnostic data to non- Organization servers; - voice assistant application if available when MD is locked; - voice dialing application if available when MD is locked; - allows synchronization of data or applications between devices associated with user; and - allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs or printers.	
Procedimiento	The Authorizing Official (IT admin) must not approve applications with the following characteristics for installation by users in the Device: - back up MD data to non- Organization cloud servers (including user and application access to cloud backup services); - transmit MD diagnostic data to non- Organization servers; - voice assistant application if available when MD is locked; - voice dialing application if available when MD is locked; - allows synchronization of data or applications between devices associated with user; - payment processing; and - allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs, display screens (screen mirroring), or printers.	
Validación	Verify requirement KNOX-12-110190 (managed Google Play) has been implemented. If "managed Google Play" has not been implemented, this is a finding.	

ID: 021	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not display the following (Work Environment) notifications when the device is locked: all notifications	

ID: 021	PASS [ ]	FAIL [ ]
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: 022	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: 023	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: 024	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: 025	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".	

ID: 025	PASS [ ]	FAIL [ ]
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: 026	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.	

ID: 026	PASS [ ]	FAIL [ ]
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: 027	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: 028	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must not accept the certificate when it cannot establish a connection to determine the validity of a certificate.	
Procedimiento	Implement CC Mode	
Validación	Verify requirement KNOX-12-110270 (CC Mode) has been implemented. If "CC Mode" has not been implemented, this is a finding.	

ID: 029	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android device users must complete required training.	
Procedimiento	Have all Samsung device users' complete training on the following topics. Users should acknowledge they have reviewed training via a signed User Agreement or similar written record. Training topics: - Operational security concerns introduced by unmanaged applications/unmanaged personal space including applications using global positioning system (GPS) tracking. - Need to ensure no Organization data is saved to the personal space or transmitted from a personal app (for example, from personal email). - If the Purebred key management app is used, users are responsible for maintaining positive control of their credentialed device at all times. The Organization PKI certificate policy requires subscribers to maintain positive control of the devices that contain private keys and to report any loss of control so the credentials can be revoked. Upon device retirement, turn-in, or reassignment, ensure a factory data reset is performed prior to device hand-off. Follow Mobility service provider decommissioning procedures as applicable. - How to configure the following UBE controls (users must configure the control) on the Samsung device: 1. Secure use of Calendar Alarm. 2. Local screen mirroring and MirrorLink procedures (authorized/not authorized for use). 3. Do not connect Samsung devices (via either DeX Station or dongle) to any Organization network via Ethernet connection. 4. Do not upload Organization contacts via smart call and caller ID services. 5. Disable Wi-Fi Sharing. 6. Do not configure the Organization network (work) VPN profile on any third-party VPN client installed in the personal space. - IT admin guidance on acceptable use and restrictions, if any, on downloading and installing personal apps and data (music, photos, etc.) in the Samsung device personal space.	

ID: 029	PASS [ ]	FAIL [ ]
Validación	Review a sample of site User Agreements of Samsung device users or similar training records and training course content. Verify that Samsung device users have completed required training. The intent is that required training is renewed on a periodic basis in a time period determined by the IT admin. If any Samsung device user has not completed required training, this is a finding.	

ID: 030	PASS [ ]	FAIL [ ]
Requerimiento	The Samsung Android device must have the latest available Samsung Android operating system (OS) installed.	
Procedimiento	Install the latest released version of Samsung Android OS on all managed Samsung devices. Note: In most cases, OS updates are released by the wireless carrier (for example, Sprint, T-Mobile, Verizon Wireless, and ATT).	

ID: 030	PASS [ ]	FAIL [ ]
Validación	Review the configuration to confirm if the Samsung Android devices have the most recently released version of Samsung Android installed. This procedure is performed on both the management tool and the Samsung Android device. In the management tool management console, review the version of Samsung Android installed on a sample of managed devices. This procedure will vary depending on the management tool product. See the notes below to determine the latest available OS version. On the Samsung Android device, to see the installed OS version: 1. Open Settings. 2. Tap "About phone". 3. Tap "Software information". If the installed version of Android OS on any reviewed Samsung devices is not the latest released by the wireless carrier, this is a finding. NOTE: Some wireless carriers list the version of the latest Android OS release by mobile device model online: ATT: https://www.att.com/devicehowto/dsm.html#!/popular/make/Samsung T-Mobile: https://support.t-mobile.com/docs/DOC-34510 Verizon Wireless: https://www.verizonwireless.com/support/software-updates/ Google Android OS patch website: https://source.android.com/security/bulletin/ Samsung Android OS patch website: https://security.samsungmobile.com/securityUpdate.smsb	

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

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+	5	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.

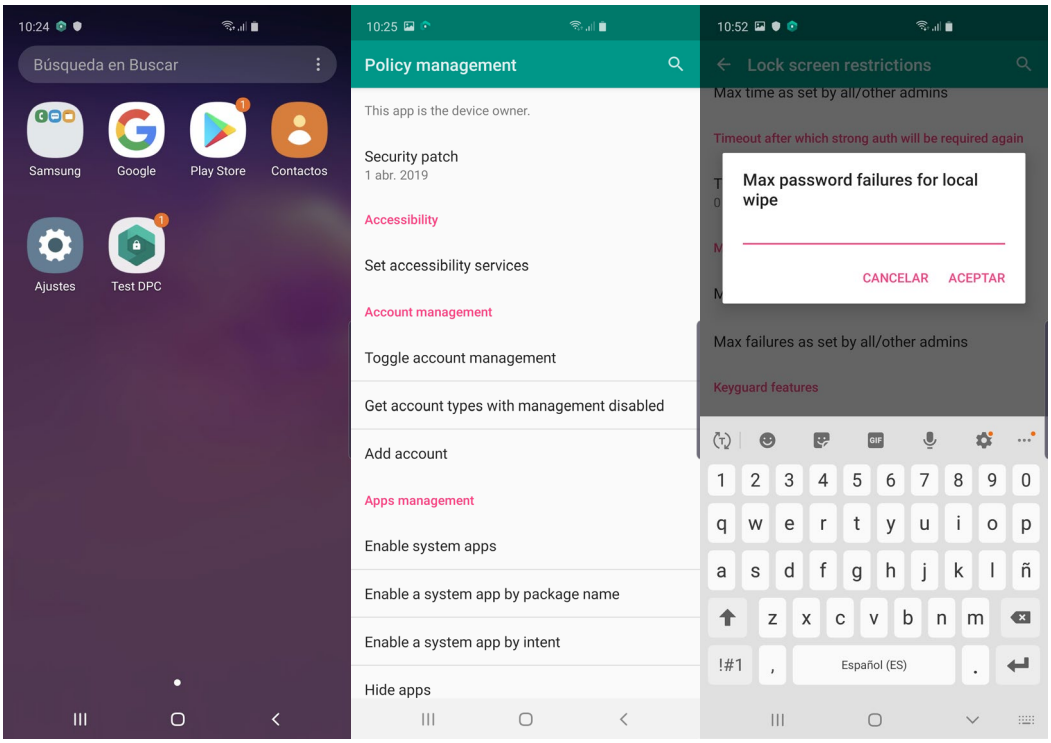


Figura 3

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL