centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1608

Procedimiento de empleo seguro de dispositivos Samsung Galaxy (Android 10)

Marzo de 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.03.30 20:07:57 +02'00'

NIPO: 083-20-124-7

Fecha de Edición: Marzo de 2021
Samsung Electronics ha participado en el desarrollo del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Marzo de 2021

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCION

El objetivo de este documento es proporcionar una guía de configuración de los dispositivos Samsung Galaxy con Android 10 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 II 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.

[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.

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*) apropiadas y que dispongan de las funcionalidades necesarias.
- Redes de comunicaciones, de diferentes tecnologías (3G, 4G, 5G, WiFi, …).
- Equipo de Administradores de dispositivos móviles de la organización donde se realiza el despliegue, así como su estructura organizativa y recursos
- Política de seguridad de las TIC, en la que se reflejen la valoración de los sistemas, los riesgos a los que se enfrentan, las contramedidas utilizadas.
- Usuarios de la organización, responsables del uso diario de los dispositivos.

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

1.1.2. ESCENARIOS EN FUNCIÓN DE LA PROPIEDAD DEL DISPOSITIVO

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

- BYOD - Bring Your Own Device
- COPE - Corporate Owned Personal 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 especial agente (Profile Owner). El presente documento no aplica a este escenario, por no considerarse un escenario valido 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, existe una aplicación agente en el área personal, denominada DO (Device Owner), que realizará la configuración de políticas en el conjunto del

dispositivo, como por ejemplo WiFi, además de restricciones en el área personal del usuario, normalmente restricciones mínimas y básicas de seguridad. Al ser un escenario COPE, existirá también un Workspace, con su agente gestor denominado (Profile Owner) dentro de él. 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, solamente existe un agente DO, 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 interface 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 (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.

1.2 KPE EXTENSIÓN DE AE

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. Con la introducción de Knox Platform for Enterprise (KPE) en Android 8.0 Oreo, las características de Knox ahora 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.

1.2.2. ANDROID ENTERPRISE (AE)

AE proporciona protecciones de seguridad básicas, políticas de administración y funciones de red. Sin embargo, AE por si solo carece de los controles necesarios para implementar un dispositivo móvil Samsung con Android que cumpla con los estándares de configuración requeridos por CCN para una clasificación ENS alto.

1.2.3. KNOX PLATFORM FOR ENTERPRISE (KPE)

KPE proporciona seguridad de alto nivel que protege todos los aspectos de la operación del dispositivo móvil.
KPE 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.

1.2.4. A DESTACAR DE KPE EN ANDROID 10

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 a la 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 nueve 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"
  - Verificación 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 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 de 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**, COPE, 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 antes de obtener acceso a la gama completa de API y funciones de Samsung Knox. Las licencias de Knox 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).

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 no requieran del nivel de seguridad al que se orienta esta guía, los servicios aquí descritos para habilitar los servicios de Knox en el dispositivo pueden ser desplegados a partir de un servicio en la nube.

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 10.0 (apartado 3.1.1) así como dispositivos cualificados por CCN con una versión anterior de Android que se actualizan a la versión 10.0 (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	VERSION DE ANDROID	VERSION DE KERNEL	COMPILACIÓN
Galaxy S20+ 5G	SM-G986B	10.0	4.19.87	QP1A.190711.020
Galaxy S20 5G	SM-G981B	10.0	4.19.87	QP1A.190711.020
Galaxy S20 Ultra 5G	SM-G988B	10.0	4.19.87	QP1A.190711.020
Galaxy S20+ 4G	SM-G985F	10.0	4.19.87	QP1A.190711.020
Galaxy S20 4G	SM-G980F	10.0	4.19.87	QP1A.190711.020

Tabla 1

3.1.2. DISPOSITIVOS COMPATIBLES CUALIFICADOS

NOMBRE DISPOSITIVO	MODELO	VERSION DE ANDROID	VERSION DE KERNEL	COMPILACIÓN
Galaxy XCoverPro	SM-G715FN	10.0	4.14.113	QP1A.190711.020
Galaxy A51	SM-A515F	10.0	4.14.113	QP1A.190711.020
Galaxy Tab S6	SM-T860 SM-T865	10.0	4.14.113	QP1A.190711.020
Galaxy Note10	SM-N970F	10.0	4.14.113	QP1A.190711.020
Galaxy Note10+	SM-N975F	10.0	4.14.113	QP1A.190711.020
Galaxy Note10+ 5G	SM-N976B	10.0	4.14.113	QP1A.190711.020
Galaxy S10+	SM-G975F	10.0	4.14.113	QP1A.190711.020
Galaxy S10	SM-G973F	10.0	4.14.113	QP1A.190711.020
Galaxy S10 5G	SM-G977B	10.0	4.14.113	QP1A.190711.020
Galaxy S10e	SM-G970F	10.0	4.14.113	QP1A.190711.020
Galaxy Note 9	SM-N960	10.0	4.9.118	QP1A.190711.020
Galaxy S9	SM-G960F	10.0	4.9.118	QP1A.190711.020
Galaxy S9+	SM-G965F	10.0	4.9.118	QP1A.190711.020

Tabla 2

3.1.3. DISPOSITIVOS COMPATIBLES

NOMBRE DISPOSITIVO	MODELO	VERSION DE ANDROID	VERSION DE KERNEL	COMPILACIÓN
Galaxy Fold	SM-F900	10.0	4.14.117	QP1A.190711.020
Galaxy Fold 5G	SM-F907	10.0	4.14.117	QP1A.190711.020

Tabla 3

3.1.4. DISPOSITIVOS ENTERPRISE EDITION

Samsung Enterprise Edition incluye el dispositivo móvil y 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, 2 y 3 se ofrecen en versión Enterprise Edition, a través de canales de venta específicos. Estos dispositivos ofrecen 1 año adicional de actualizaciones de seguridad, ampliando el soporte hasta los 4 años.

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

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.

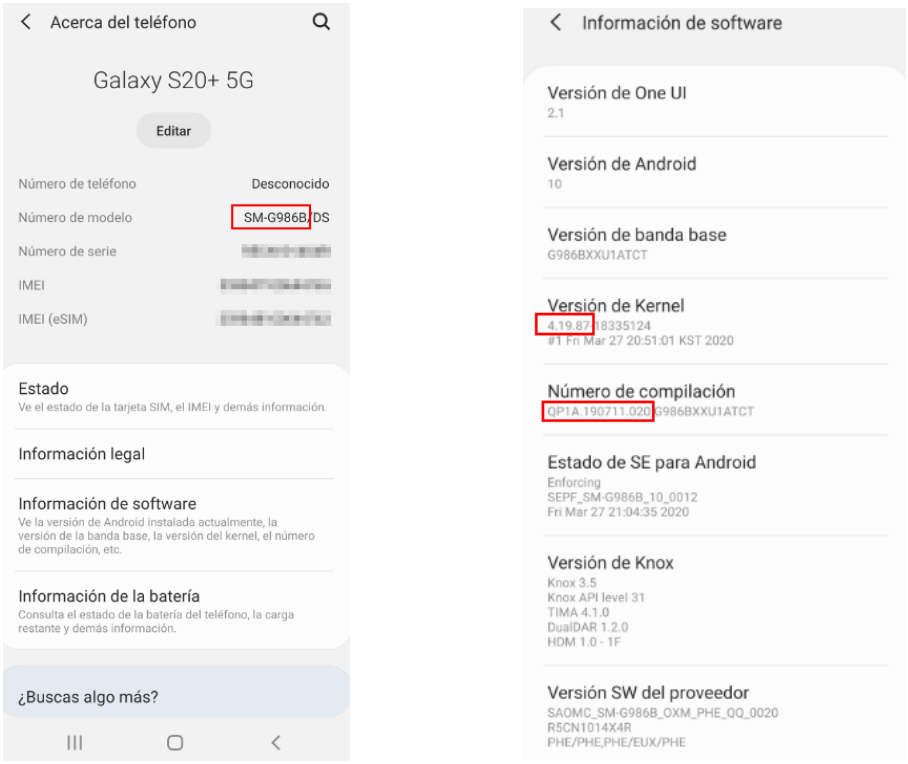

Figura 2

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 II 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 case 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 3.3.2 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
Password Requirements	Minimum password length	0+	6	
#1:Password Requirements ***#2:Password Requirements*** ***KPEPassword Requirements***	#1:Minimum password quality #2: Minimum password quality Maximum sequential numbers	#1: Unspecified, Something, Numeric, Numeric(Complex),Alphabetic, Alphanumeric, Complex #2: Password quality options as #1 0+	#1: Numeric(Complex) #2: Numeric 2	Choose Method #1 or #2. Alphabetic, Alphanumeric, and Complex are also acceptable selections but will cause the user to select a complex password, which is not required by this CCN-STIC guide.
Password Requirements	Max time to screen lock	0 minutes	15 minutes	
Password Requirements	Max password failures for local wipe	0+	10	
Restrictions	Installs from unknown sources	Allow/Disallow	Disallow	
Restrictions	Trust Agents	Enable/Disable	Disable	
Restrictions	Face	Enable/Disable	Disable	
Restrictions	Debugging features	Allow/Disallow	Disallow	
Restrictions	USB file transfer	Allow/Disallow	Disallow	For KPE(AE) deployments this configuration is the default configuration. If the management tool does not provide the capability to configure “USB file transfer”, there is NO finding because the default setting cannot be changed.
KPE Wifi	Unsecured hotspot	Allow/Disallow	Disallow	
KPE Restrictions	CC mode	Enable/Disable	Enable	
#1: ***Restrictions*** ***#2:*** ***KPE Encryption***	#1: SD Card #2: External storage encryption	#1: Enable/Disable #2: Enable/Disable	#1: Disable #2: Enable	Choose Method #1 or #2. Method #1: Disable SD card (if not using SD card). Method #2: Enable Data-at-Rest protection.

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
#1: ***KPE audit log*** ***#2:*** ***Restrictions*** ***Restrictions***	#1: Audit Log #2: Security logging Network logging	#1: Enable/Disable #2: Enable/Disable Enable/Disable	#1: Enable #2: Enable Enable	Choose Method #1 or #2. Method #1: KPE Audit Logging KPE audit log Method #2: AE Audit Logging Restrictions
#1: ***KPE Restrictions*** ***#2:*** ***KPE Restrictions***	#1: USB host mode exception list #2: USB host mode	#1: APP,AUD,CDC,COM,CON,CSC,HID,HUB,MAS,MISPER,PHY,PRI,STI,VEN,VID,WIR #2: Enable/Disable	#1: HID #2: Disable	Choose Method #1 or #2. Method #1: Use USB exception list. Method #2: Disable USB host mode (default option if exception list policy cannot be applied).

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
#1: Restrictions ***#2: Restrictions*** ***#3:*** ***KPE Bluetooth***	#1: Bluetooth #2: Bluetooth #3: Bluetooth UUID Whitelist	#1: Allow/Disallow #2: Allow/Disallow #3: A2DP_ADVAUDIODIST_UUID A2DP_AUDIOSINK_UUID A2DP_AUDIOSOURCE_UUID AVRCP_CONTROLLER_UUID AVRCP_TARGET_UUID BNEP_UUID BPP_UUID DUN_UUID FTP_UUID HFP_AG_UUID HFP_UUID HSP_AG_UUID HSP_UUID NAP_UUID OBEXOBJECTPUSH_UUID PANU_UUID PBAP_PSE_UUID PBAP_UUID SAP_UUID SPP_UUID	#1: Allow #2: Disallow #3: HFP_AG_UUID HFP_UUID HSP_AG_UUID HSP_UUID SPP_UUID A2DP_ADVAUDIODIST_UUID A2DP_AUDIOSINK_UUID A2DP_AUDIOSOURCE_UUID AVRCP_CONTROLLER_UUID AVRCP_TARGET_UUID PBAP_PSE_UUID PBAP_UUID	Choose Method #1, #2 or #3. Method #1: Organization IT Administrator decision: Allow Bluetooth and train users. Method #2: Organization IT Administrator decision: Disallow use of Bluetooth. Method #3: Use KPE Bluetooth UUID Whitelisting to allow only Organization-approved profiles.
#1:User Agreement ***#2: Restrictions*** ***#3: KPE Banner***	#1: User Agreement #2: Lock Screen Message #3: Banner text	#1: User Agreement #2: Enable/Disable #3: Configure	#1: Include Organization-mandated Warning banner text in User Agreement #2: Organization-mandated Warning banner text #3: Organization-mandated Warning banner text	Choose Method #1, #2 or #3. Method #1: Put the Organization Warning banner text in the User Agreement (preferred method). Method #2: Put the Organization Warning banner in the Lock Screen message. Method #3: Enable the KPE Reboot Banner.

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
#1: Restrictions ***#2: Restrictions*** ***#3: KPE Date Time***	#1: Config Date Time #2: Set auto (network) time required #3: Date Time Change	#1: Allow/Disallow #2: Require/Do not require #3: Enable/Disable	#1: Disallow #2: Require #3: Disable	Choose Method #1, #2 or #3. Each method uses a different API to accomplish the same result. Any of the methods are acceptable. Method #1: Restrict User from configuring time. Method #2: Require Auto Time. Method #3: Disable Date/Time change (KPE).
Restrictions	Outgoing beam	Allow/Disallow	Disallow	
KPE Restrictions	Share Via List	Allow/Disallow	Disallow	Disabling "Share Via List" will also disable functionality such as "Gallery Sharing" and "Direct Sharing".
Restrictions	Backup service	Allow/Disallow	Disallow	
Restrictions	Autofill services	Allow/Disallow	Disallow	
#1: Restrictions ***#2: KPE Account***	#1: Account Management #2: Account Addition Blacklist	#1: Account types, Enable/Disable #2: Account types, Blacklist	#1: Disable for: Work email app, Samsung accounts, Google accounts, and each IT Administrator-approved app that uses accounts for data backup/sync #2: "Blacklist all" for: Work email app, Samsung accounts, and Google accounts	Choose Method #1 or #2. Method #1: AE Account management Method #2: KPE Account Addition Blacklist
#1: ***Policy Management*** ***#2:*** ***KPE Application***	#1: Core app whitelist #2: System app disable list	#1: List of apps #2: List of apps	#1: List approved core apps #2: List non-IT Administrator-approved system app packages	Choose Method #1 or #2. Method #1: KPE(AE) enrolment Method #2: KPE system app disable list
#1: KPE Restrictions ***#2: KPE Restrictions***	#1: Revocation check #2: OCSP check (with revocation check fallback)	#1: Enable/Disable #2: Enable/Disable	#1: Enable for all apps #2: Enable for all apps	Choose Method #1 or #2. Method #1: Certificate Revocation List (CRL) checking Method #2: Online Certificate Status Protocol (OCSP), with CRL fallback
#1: ***Policy Management*** ***#2: KPE Certificate***	#1: Certificates #2: KPE Certificates	#1: Configure #2: Configure	#1: Include Organization certificates #2: Include Organization certificates	Choose Method #1 or #2. Method #1: Use AE Key management Policy Management. Method #2: Use KPE Key management KPE Certificate.

GRUPO	REGLA	OPCIONES	CONFIGURACION	COMENTARIO
#1: Restrictions ***#2: KPE Restrictions***	#1: Config credentials #2: User Remove Certificates	#1: Allow/Disallow #2: Allow/Disallow	#1: Disallow #2: Disallow	Choose Method #1 or #2. #1: Disallow User from configuring any credential. #2: Disallow User from removing certificates.
#1: Restrictions ***#2: KPE Application***	#1: List of approved apps listed in managed Google Play #2: App installation whitelist	#1: List of apps #2: List of apps	#1: List only approved work apps in managed Google Play #2: List only approved work apps	Choose Method #1 or #2. Method #1: Use managed Google Play. Method #2: 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.
Restrictions	Unredacted Notifications	Allow/Disallow	Disallow	Disable unredacted notifications on Keyguard

Tabla 4 - 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.

3.4.1. APLICACIONES DE COPIA DE SEGURIDAD EN LA NUBE PÚBLICA

El Administrador IT de la organización debe identificar cualquier servicio de este tipo que venga preinstalado y deshabilitar estas aplicaciones.

Entre las de más probable aparición se incluyen:

- Cuenta de Samsung
- Dropbox
- Drive (Google)
- OneDrive (Microsoft)

3.4.2. APLICACIONES PARA COMPARTIR CONTENIDO

Los dispositivos Samsung pueden incluir varios métodos que permiten a un dispositivo compartir contenido o enviar información a otros dispositivos cercanos. El Administrador IT de la organización debe identificar cualquier servicio preinstalado en el dispositivo y desactivar estas aplicaciones.

Entre las de más probable aparición se incluyen:

- Group Play/Juego en Grupo
- Samsung SmartThings

3.4.3. IMPRESIÓN MÓVIL

Las aplicaciones de impresión móvil ofrecen la posibilidad de impresión inalámbrica desde un dispositivo Samsung con Android. La configuración de la impresión inalámbrica desde un dispositivo móvil a una impresora de red de la organización es

problemática debido a los requisitos del servidor de impresión. Si un dispositivo móvil está conectado directamente a una red de la organización a través de una conexión VPN o WiFi, puede ser capaz de imprimir en impresoras de red si los controladores de la impresora o una aplicación de impresora están instalados. Android 10.x viene con un servicio de impresión incorporado que permite la comunicación con la mayoría de las impresoras comerciales. **Este paquete está incluido en la tabla de aplicaciones de sistema a deshabilitar.**

3.4.4. APLICACIONES CORE Y PREINSTALADAS

INTRODUCCIÓN

Es posible que la lista de aplicaciones preinstaladas mostrada a continuación no refleje el contenido exacto en los dispositivos específicos que se estén revisando en una organización. Son de esperar pequeñas modificaciones en los nombres de las aplicaciones o de los paquetes de aplicación entre las distintas compilaciones de sistemas operativos (SO) de los operadores móviles o dispositivos. La lista de aplicaciones mostrada a continuación debe compararse con la lista de aplicaciones instaladas en un dispositivo que se está revisando. Esta lista debe ser solicitada por la organización a sus proveedores y posteriormente revisada.

DESHABILITADO CORE Y APLICACIONES PREINSTALADAS

La Tabla 5 detalla las aplicaciones preinstaladas que se recomienda deshabilitar para un escenario COBO. Dependiendo de varios factores, incluida la forma en que se aprovisionó el dispositivo, la ruta de actualización de Android y las modificaciones del operador, algunas de estas aplicaciones pueden estar ya deshabilitadas o no instaladas.

NOMBRE DE LA APLICACION	NOMBRE DEL PAQUETE
Default Print Service	com.android.bips
Android Setup	com.google.android.apps.restore
OneDrive	com.microsoft.skydrive
Find My Mobile	com.samsung.android.fmm
Samsung Cloud	com.samsung.android.scloud
ShortcutBNR	com.samsung.android.shortcutbackupservice
	com.samsung.android.smartswitchassistant

NOMBRE DE LA APLICACION	NOMBRE DEL PAQUETE
Bixby Vision	com.samsung.android.visionintelligence
Samsung Members	com.samsung.android.voc
Smart Switch	com.sec.android.easyMover
Smart Switch Agent	com.sec.android.easyMover.Agent
Cameralyzer	com.sec.factory.cameralyzer

Tabla 5

La Tabla 6 muestra las aplicaciones que **NO** deben deshabilitarse para garantizar el correcto funcionamiento del dispositivo.

NOMBRE DE LA APLICACION	NOMBRE DEL PAQUETE
Android Setup	com.google.android.setupwizard
Gmail	com.google.android.gm
Google Play Services	com.google.android.gms
Google Play Store	com.android.vending
Google Services Framework	com.google.android.gsf

Tabla 6

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 "SmartThings" (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)

Ciertos accesorios pueden proporcionar conectividad de red por cable a dispositivos Samsung de Android. Por ejemplo, la Samsung DeX Station ofrece la posibilidad de conectar el dispositivo Android de Samsung a un monitor externo, teclado, mouse y cable Ethernet a través del puerto LAN. 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.

3.5.4. USO COMPARTIDO WIFI

El uso compartido de WiFi es una nueva opción incluida en la función de conexión compartida de Samsung. Permite al usuario de un dispositivo Samsung compartir su conexión WiFi con otros dispositivos habilitados WiFi, pero podría permitir que dispositivos no autorizados accedan a la red de la organización. Los usuarios deben estar formados para no utilizar y/o desactivar el uso compartido de WiFi de Samsung.

El uso compartido de WiFi se puede desactivar a través de la aplicación Configuración (Configuración >> Conexiones >> Zona activa móvil y conexión >> Zona activa móvil >> Compartir WiFi.

ANEXO I: TERMINOLOGIA

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
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)

VPN	Red privada virtual (Virtual Private Network)

ANEXO II: 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 configured to enforce a minimum password length of six characters.	
Procedimiento	Configure Samsung Android to enforce a minimum password length of six characters. On the management tool, in the device password requirements section, set the "minimum password length" to "6".	
Validación	Review Samsung Android device configuration settings to determine if the mobile device is enforcing a minimum password length of six characters. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, in the device password requirements section, verify the "minimum password length" is set to "6". On the Samsung Android device, do the following: 1. Open Settings >> Lock screen >> Screen lock type. 2. Enter current password. 3. Tap "PIN". 4. Verify the text "PIN must contain at least", followed by a value of at least "6 digits", appears above the PIN entry. If on the management tool the "minimum password length" is not set to "6", or on the Samsung Android device the text "PIN must contain at least" is followed by a value of less than "6 digits", this is a finding.	

ID: 002	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not allow passwords that include more than two repeating or sequential characters.	

ID: 002	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to prevent passwords from containing more than two repeating or sequential characters. Do one of the following: - Method #1: Require Numeric (Complex) password. - Method #2: Require Numeric password with KPE password constraints. **** Method #1: Require Numeric (Complex) password. On the management tool, in the device password requirements section, set the "minimum password quality" to "Numeric (Complex)". **** Method #2: Require Numeric password with KPE password constraints. On the management tool, do the following: 1. In the device password requirements section, set the "minimum password quality" to "Numeric". 2. In the KPE device password section, set the "maximum sequential numbers" to "2". **** Note: Alphabetic, Alphanumeric, and Complex are also acceptable selections but will cause the user to select a complex password, which is not required by this CCN-STIC guide.	

ID: 002	PASS [ ]	FAIL [ ]
Validación	Review Samsung Android configuration settings to determine if the mobile device is prohibiting passwords with more than two repeating or sequential characters. This validation procedure is performed on both the management tool and the Samsung Android device. Confirm if Method #1 or #2 is used at the Samsung device site and follow the appropriate procedure. **** Method #1: Require Numeric (Complex) password. On the management tool, in the device password requirements section, verify that "minimum password quality" is set to "Numeric (Complex)". On the Samsung Android device, do the following: 1. Open Settings >> Lock screen >> Screen lock type. 2. Enter current password. 3. Tap "PIN". 4. Enter a password with an invalid sequence and verify that text "Consecutive or repeating numbers are not allowed" is displayed above the PIN entry. If on the management tool the "minimum password quality" is not set to "Numeric (Complex)", or on the Samsung Android device the text "Consecutive or repeating numbers are not allowed" is not displayed, this is a finding. **** Method #2: Require Numeric password with KPE password constraints. On the management tool, do the following: 1. In the device password requirements section, verify the "minimum password quality" is set to "Numeric". 2. In the KPE device password section, verify that "maximum sequential characters" is "2" or less. 3. In the KPE device password section, verify that "maximum sequential numbers" is "2" or less. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap "Lock screen". 3. Tap "Screen lock type". 4. Enter current password. 5. Tap "Password". 6. Verify that passwords with two or more sequential numbers are not accepted. If on the management tool "minimum password quality" is not set to "Numeric" or "maximum sequential characters" or "maximum sequential numbers" is more than "2", or on the Samsung Android device a password with two or more sequential characters or numbers is accepted, this is a finding. **** Note: Alphabetic, Alphanumeric, and Complex are also acceptable selections but these selections will cause the user to select a complex password, which is not required by this CCN-STIC guide.

ID: 003	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to lock the display after 15 minutes (or less) of inactivity.	
Procedimiento	Configure Samsung Android to lock the device display after 15 minutes (or less) of inactivity. On the management tool, in the device password requirements section, set the "max time to screen lock" to "15 minutes" or less.	
Validación	Review Samsung Android configuration settings to determine if the mobile device has the screen lock timeout set to 15 minutes or less. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, in the device password requirements section, verify the "max time to screen lock" is set to "15 minutes" or less. On the Samsung Android device, do the following: 1. Open Settings >> Display >> Screen timeout. 2. Verify that the listed Screen timeout values are 15 minutes or less. If on the management tool the "max time to screen lock" is not set to "15 minutes" or less, or on the Samsung Android device the listed Screen timeout values include durations of more than 15 minutes, 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 Samsung Android to allow only 10 or fewer consecutive failed authentication attempts. On the management tool, in the device password requirements section, set the "max password failures for local wipe" to "10" attempts or less.	
Validación	Review Samsung Android configuration settings to determine if the mobile device has the maximum number of consecutive failed authentication attempts set at 10 or less. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, in the device password requirements section, verify the "max password failures for local wipe" is set to "10" attempts or less. On the Samsung Android device, do the following: 1. Open Settings >> Biometrics and security >> Other security settings >> Managed device info. 2. Verify "Failed password attempts before deleting all device data" is set to "10" attempts or less. If on the management tool the "max password failures for local wipe" is not set to "10" attempts or less, or on the Samsung Android device the "Failed password attempts before deleting all device data" is not set to "10" attempts or less, this is a finding.	

ID: 005	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.	

ID: 005	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to disable unauthorized application repositories. On the management tool, in the device restrictions section, set "installs from unknown sources" 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 Samsung Android configuration settings to determine if the mobile device has only approved application repositories (Organization-approved commercial app repository, management tool server, and/or mobile application store). 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 "installs from unknown sources" is set to "Disallow". On the Samsung Android device, do the following: 1. Open Settings >> Apps >> (Overflow menu) >> Special access >> Install unknown apps. 2. Tap (Overflow menu) >> Show system apps. 3. 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" 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. Note: Google Play must not be disabled. Disabling Google play will cause system instability and critical updates will not be received.	

ID: 006	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable trust agents. Note: This requirement is not applicable (NA) for specific biometric authentication factors included in the product Common Criteria evaluation.	
Procedimiento	Configure Samsung Android to disable Trust Agents. On the management tool, in the device restrictions section, set "Trust Agents" to "Disable".	
Validación	Review Samsung Android configuration settings to determine if Trust Agents are disabled. 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 "Trust Agents" are set to "Disable". On the Samsung Android device, do the following: 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: 007	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable Face Recognition. Note: This requirement is not applicable (NA) for specific biometric authentication factors included in the product Common Criteria evaluation.	

ID: 007	PASS [ ]	FAIL [ ]
Procedimiento	Configure the Samsung Android to disable Face Recognition. On the management tool, in the device restrictions section, set "Face" to "Disable".	
Validación	Review Samsung Android configuration settings to determine if Face Recognition is disabled. 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 "Face" is set to "Disable". On the Samsung Android device, do the following: 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 "Face" is not set to "Disable", or on the Samsung Android device "Face" can be enabled, this is a finding.	

ID: 008	PASS [ ]	FAIL [ ]
Requerimiento	The requirement statement specifies the Organization-mandated configuration of this MDFPP element.	
Procedimiento	Configure Samsung Android to disable developer modes. On the management tool, in the device restrictions section, set the "Debugging Features" to "Disallow".	
Validación	Review Samsung Android configuration settings to determine whether a developer mode is enabled. 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 "Debugging Features" is set to "Disallow". On the Samsung Android device, do the following: 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: 009	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable USB mass storage mode.	
Procedimiento	Configure Samsung Android to disable USB mass storage mode. For KPE (AE) deployments this configuration is the default configuration. No configuration is required. On the management tool, in the device restrictions section, set "USB file transfer" to "Disallow".	

ID: 009	PASS [ ]	FAIL [ ]
Validación	Review Samsung Android configuration settings to determine if the mobile device has a USB mass storage mode and if it has been disabled. For KPE (AE) deployments this configuration is the default configuration. If the management tool does not provide the capability to configure "USB file transfer", there is NO finding because the default setting cannot be changed. 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 "USB file transfer" has been set to "Disallow".	

ID: 010	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable authentication of personal hotspot connections to the device using a pre-shared key.	
Procedimiento	Configure Samsung Android to enable authentication of personal hotspot connections to the device using a pre-shared key. On the management tool, in the device KPE restrictions section, set "Unsecured hotspot" to "Disallow".	
Validación	Review Samsung Android configuration settings to determine if the mobile device has enabled authentication of personal hotspot connections to the device using a pre-shared key. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, in the device KPE restrictions section, verify that "Unsecured hotspot" is set to "Disallow". On the Samsung Android device, do the following: 1. Open Settings >> Connections >> Mobile Hotspot and Tethering >> Mobile Hotspot >> (overflow menu) >> Configure Mobile Hotspot. 2. Tap option "Open" in the "Security" drop-down box. 3. Verify that "Save" is disabled. If on the management tool "Unsecured hotspot" is not set to "Disallow", or on the Samsung Android device "Open" can be selected in the "Security" drop-down box and the configuration can be saved, this is a finding.	

ID: 011	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable Knox CC Mode.	
Procedimiento	Configure Samsung Android to enable KPE CC Mode. On the management tool, in the device KPE restrictions section, set "CC mode" to "Enable".	
Validación	Review Samsung Android configuration settings to determine if KPE CC Mode is enabled. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, in the device KPE restrictions section, verify that "CC 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 "CC 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: 012	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable encryption for data at rest on removable storage media or alternatively, the use of removable storage media must be disabled.	
Procedimiento	Configure Samsung Android to enable data-at-rest protection for removable media, or alternatively, disable the use of removable storage media. Do one of the following: - Method #1: Disable SD card (if not using SD card). - Method #2: Enable data-at-rest protection. **** Method #1: Disable SD card (if not using SD card). On the management tool, in the device restrictions section, set "SD Card" to "Disable". **** Method #2: Enable data-at-rest protection. On the management tool, in the device KPE encryption section, set "External storage encryption" to "Enable".	
Validación	If the mobile device does not support removable media, this requirement is not applicable. Review Samsung Android configuration settings to determine if data in the mobile device is removable storage media is encrypted, or alternatively, the use of removable storage media is disabled. 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 Administration Console and the Samsung Android device. **** Method #1: Disable SD card (if not using SD card). On the management tool, in the device restrictions section, verify that "SD Card" is set to "Disable". On the Samsung Android device, verify that a Micro SD card cannot be mounted. If on the management tool "SD Card" is not set to "Disable", or on the Samsung Android device a microSD card can be mounted, this is a finding. **** Method #2: Enable data-at-rest protection. On the management tool, in the device KPE encryption section, verify that "External storage encryption" is set to "Enable". On the Samsung Android device, do the following: 1. Insert a freshly formatted microSD card. 2. Verify that a prompt appears to encrypt the microSD card. 3. Perform the encryption. 4. Remove and reinsert the microSD card and verify that a notification appears stating that the mounted microSD card is encrypted. If on the management tool "External storage encryption" is not set to "Enable", or on the Samsung Android device a microSD card can be used without first being encrypted, this is a finding.	

ID: 013	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable audit logging.	
Procedimiento	Configure Samsung Android to enable audit logging. Do one of the following: - Method #1: KPE Audit logging - Method #2: AE Audit logging **** Method #1: KPE Audit logging On the management tool, in the device KPE audit log section, set "Audit log" to "Enable". **** Method #2: AE Audit logging On the management tool, do the following: 1. In the device restrictions section, set "Security logging" to "Enable". 2. In the device restrictions section, set "Network logging" to "Enable".	
Validación	Review Samsung Android device configuration settings to confirm that Audit logging is enabled. Confirm if Method #1 or #2 is used at the Samsung device site and follow the appropriate procedure. This validation procedure is performed on the management tool Administration Console only. **** Method #1: KPE Audit logging On the management tool, for the device KPE audit log section, verify that "Audit log" is set to "Enable". If on the management tool the "Audit log" is not set to "Enable", this is a finding. **** Method #2: AE Audit logging On the management tool, do the following: 1. In the device restrictions section, verify that "Security logging" is set to "Enable". 2. In the device restrictions section, verify that "Network logging" is set to "Enable". If on the management tool both "Security logging" and "Network logging are not set to "Enable", this is a finding.	

ID: 014	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enforce a USB host mode exception list.	

ID: 014	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android with a USB host mode exception list, or alternatively, disable the use of USB host mode. Do one of the following: - Method #1: Use USB exception list. - Method #2: Disable USB host mode. **** Method #1: Use USB exception list. On the management tool, in the device KPE restrictions section, add the "HID" USB class to the "USB host mode exception list". **** Method #2: Disable USB host mode. On the management tool, in the device KPE restrictions section, set "USB host mode" to "Disable".	
Validación	Review Samsung Android device configuration settings to determine if USB host mode exception list is configured, or alternatively, if USB host mode is disabled. 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 Administration Console and the Samsung Android device. **** Method #1: Use USB exception list. On the management tool, in the device KPE restrictions section, verify that "HID" is the only USB class included in the "USB host mode exception list". On the Samsung Android device, do the following: 1. Connect a micro USB-to-USB "On the Go" (OTG) adapter to the device. 2. Connect a USB thumb drive to the adapter. 3. Verify that the device cannot access the USB thumb drive. If on the management tool the "USB host mode exception list" includes a USB class other than "HID", or on the Samsung Android device the USB thumb drive can be mounted, this is a finding. **** Method #2: Disable USB host mode. On the management tool, in the device KPE restrictions section, set "USB host mode" to "Disable". On the Samsung Android device, do the following: 1. Connect a micro USB-to-USB "On the Go" (OTG) adapter to the device. 2. Connect a USB thumb drive to the adapter. 3. Verify that the device cannot access the USB thumb drive. If on the management tool the "USB host mode" is not set to "Disable", or on the Samsung Android device the USB thumb drive can be mounted, this is a finding.	

ID: 015	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable all Bluetooth profiles except for HSP (Headset Profile), HFP (HandsFree Profile), SPP (Serial Port Profile), A2DP (Advanced Audio Distribution Profile), AVRCP (Audio/Video Remote Control Profile), and PBAP (Phone Book Access Profile).	

ID: 015	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to disable all Bluetooth profiles except for HSP, HFP, SPP, A2DP, AVRCP, and PBAP. Do one of the following (Method #2 or #3 must be used if the management tool supports management of Bluetooth profiles): - Method #1: Organization IT Administrator decision: Allow Bluetooth and train users to connect only authorized Bluetooth devices. - Method #2: Organization IT Administrator decision: Disallow use of Bluetooth. - Method #3: Use KPE Bluetooth UUID Whitelisting to allow only Organization-approved profiles. **** Method #1: Organization IT Administrator decision: Allow Bluetooth and train users to connect only authorized Bluetooth devices. On the management tool, in the device restrictions section, set "Bluetooth" to "Allow". **** Method #2: Organization IT Administrator decision: Disallow use of Bluetooth. On the management tool, in the device restrictions section, set "Bluetooth" to "Disallow". **** Method #3: Use KPE Bluetooth UUID Whitelisting to allow only Organization-approved profiles. On the management tool, in the device KPE Bluetooth section, add each Organization-approved profile UUID to the "Bluetooth UUID whitelist": - HFP (HFP_AG_UUID, HFP_UUID) - HSP (HSP_AG_UUID, HSP_UUID) - SPP (SPP_UUID) - A2DP (A2DP_ADVAUDIODIST_UUID, A2DP_AUDIOSINK_UUID, A2DP_AUDIOSOURCE_UUID) - AVRCP (AVRCP_CONTROLLER_UUID, AVRCP_TARGET_UUID) - PBAP (PBAP_PSE_UUID, PBAP_UUID)	

ID: 015	PASS [ ]	FAIL [ ]
Validación	Review Samsung Android configuration settings to determine if all Bluetooth profiles are disabled except for HSP, HFP, SPP, A2DP, AVRCP, and PBAP. Confirm if Method #1, #2, or #3 is used at the Samsung device site and follow the appropriate procedure. Method #2 or #3 must be used if the management tool supports management of Bluetooth profiles. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. **** Method #1: Organization IT Administrator decision: Allow Bluetooth and train users to connect only authorized Bluetooth devices. On the management tool, in the device restrictions section, verify "Bluetooth" is set to "Allow". On the Samsung Android device, do the following: 1. Open Settings >> Connections >> Bluetooth. 2. Verify only Bluetooth devices that use Organization-approved profiles are listed. If on the management tool "Bluetooth" is not set to "Allow", or on the Samsung Android device Bluetooth devices that use non-Organization-approved profiles are listed, this is a finding. **** Method #2: Organization IT Administrator decision: Disallow use of Bluetooth. On the management tool, in the device restrictions section, verify that "Bluetooth" is set to "Disallow". On the Samsung Android device, do the following: 1. Open Settings >> Connections >> Bluetooth. 2. Verify that Bluetooth is "Off" and cannot be toggled to "On". If on the management tool "Bluetooth" is not set to "Disallow", or on the Samsung Android device Bluetooth is not "Off" or can be toggled "On", this is a finding. **** Method #3: Use KPE Bluetooth UUID Whitelisting to allow only Organization-approved profiles. On the management tool, in the device KPE Bluetooth section, verify that only Organization-approved profile UUIDs are listed in the "Bluetooth UUID whitelist": - HFP (HFP_AG_UUID, HFP_UUID) - HSP (HSP_AG_UUID, HSP_UUID) - SPP (SPP_UUID) - A2DP (A2DP_ADVAUDIODIST_UUID,A2DP_AUDIOSINK_UUID, A2DP_AUDIOSOURCE_UUID) - AVRCP (AVRCP_CONTROLLER_UUID, AVRCP_TARGET_UUID) - PBAP (PBAP_PSE_UUID, PBAP_UUID) On the Samsung Android device, do the following: 1. Open Settings >> Connections >> Bluetooth. 2. Verify only Bluetooth devices that use Organization-approved profiles are listed. If on the management tool the "Bluetooth UUID whitelist" contains non-Organization-approved profile UUIDs, or on the Samsung Android device Bluetooth devices that use non-Organization-approved profiles are listed, this is a finding.	

ID: 016	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to display the Organization advisory warning message at start-up 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 Discussion): Do one of the following: - 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. - Method #3: Configure the warning banner text in the KPE Reboot Banner on each managed mobile device. **** 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. **** Method #3: Configure the warning banner text in the KPE Reboot Banner on each managed mobile device. On the management tool, in the device KPE Banner section, set "Banner Text" to the Organization-managed warning banner text.	
Validación		

ID: 017	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disallow configuration of Date Time.	

ID: 017	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to disallow configuration of the date and time. Do one of the following: - Method #1: Restrict user from configuring time. - Method #2: Require Auto Time. - Method #3: Disable Date/Time change (KPE). **** Method #1: Restrict user from configuring time. On the management tool, in the device restrictions section, set "Config Date Time" to "Disallow". **** Method #2: Require Auto Time. On the management tool, in the device restrictions section, set "Set auto (network) time required" to "Required". **** Method #3: Disable Date/Time change (KPE). On the management tool, in the device KPE Date Time section, set "Date Time Change" to "Disable". Note: Each method uses a different API to accomplish the same result. Any of the methods are acceptable.	
Validación		

ID: 018	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disallow outgoing beam.	
Procedimiento	Configure Samsung Android to disallow outgoing beam. On the MDM console, in the Work Environment restrictions section, set "outgoing beam" to "disallow".	
Validación	Review Samsung Android Work Environment configuration settings to verify that outgoing beam is disallowed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, in the Work Environment restrictions section, verify that "disallow outgoing beam" is selected. On the Samsung Android device, open a picture, contact, or web page and put it back to back with an unlocked outgoing beam-enabled device. Verify that outgoing beam cannot be started. If on the MDM console "outgoing beam" is not set to "disallow", or on the Samsung Android device the user is able to successfully start outgoing beam, this is a finding.	

ID: 019	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enforce that Share Via List is disabled.	
Procedimiento	Configure Samsung Android to disallow Share Via List. On the management tool, set "Share Via List" to "Disallow". Note: Disabling Share Via List will also disable functionality such as Gallery Sharing and Direct Sharing.	

ID: 019	PASS [ ]	FAIL [ ]
Validación	Review Samsung Android configuration settings to determine if Share Via List is disallowed. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, verify that "Share Via List" is set to "Disallow". On the Samsung Android device, attempt to share by long pressing a file and tapping "Share". If on the management tool "Share Via List" is not set to "Disallow", or on the Samsung Android device the user is able to share, this is a finding.	

ID: 020	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not allow backup of all applications, configuration data to remote systems (device management backup). - Disable Backup Services	
Procedimiento	Configure Samsung Android to disable backup to remote systems (including commercial clouds) (device management backup). On the management tool, set "Backup service" to "Disallow".	
Validación	Review Samsung Android configuration settings to determine if the capability to back up to a remote system has been disabled. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, verify that "Backup service" is set to "Disallow". On the Samsung Android device, do the following: 1. Open Settings >> Accounts and backup >> Backup and restore. 2. Verify that "Backup service not available" is listed. If on the management tool "Backup service" is not set to "Disallow", or on the Samsung Android device "Backup service not available" is not listed, this is a finding.	

ID: 021	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable the Auto Fill services.	
Procedimiento	Configure the Samsung Android to disable autofill services. On the management tool, in the Work Environment restrictions section, set "Autofill services" to "Disallow".	
Validación	Review Samsung Android configuration settings to determine if autofill services are disabled. This validation procedure is performed on both the management tool Administration Console and the Samsung Android device. On the management tool, verify that "Autofill services" is set to "Disallow". On the Samsung Android device, do the following: 1. Open Settings >> General management >> Language and input. 2. Verify that "Autofill service" is not present. If on the management tool "Autofill services" is not set to "Disallow", or on the Samsung Android device "Autofill service" is present, this is a finding.	

ID: 022	PASS [ ]	FAIL [ ]
Requerimiento	The Samsung Android must be configured to prevent users from adding personal email accounts to the work email app.	
Procedimiento	Configure the Samsung Android to prevent users from adding personal email accounts to the work email app. Refer to the management tool documentation to determine how to provision users' work email accounts for the work email app. Do one of the following: - Method #1: AE Account management - Method #2: KPE Account Addition Blacklist **** Method #1: AE Account management On the management tool, do the following: 1. In the restrictions section, set "Account Management" to "Disable" for: Work email app. 2. Provision the user's email account on their behalf. **** Method #2: KPE Account Addition Blacklist On the management tool, do the following: 1. In the Work Environment KPE Account section, set "Account Addition Blacklist" to "Blacklist all" for: Work email app. 2. Provision the user's email account on their behalf.	

ID: 022	PASS [ ]	FAIL [ ]
Validación	Review Samsung Android configuration settings to determine if users are prevented from adding personal email accounts to the work email app. 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 Administration Console and the Samsung Android device. **** Method #1: AE Account management On the management tool, do the following: 1. In the restrictions section, set "Account Management" to "Disable" for: Work email app. 2. Provision the user's email account on their behalf. On the Samsung Android device, do the following: 1. Open Settings >> Accounts and backup >> Accounts. 2. Verify that no account can be added. 3. Verify that the user's Work email app has been provisioned with the work email account. If on the management tool "Account Management" is not set to "Disable" for the Work email app, or on the Samsung Android device an account can be added, this is a finding. **** Method #2: KPE Account Addition Blacklist. On the management tool, do the following: 1. In the Work Environment KPE Account section, set "Account Addition Blacklist" to "Blacklist all" for: Work email app. 2. Provision the user's email account on their behalf. On the Samsung Android device, do the following: 1. Open Settings >> Accounts and backup >> Accounts. 2. Verify that no account can be added. 3. Verify that the user's work email app has been provisioned with the work email account. If on the management tool "Account Addition Blacklist" is not set to "Blacklist all" for the Work email app, or on the Samsung Android device an account can be added, this is a finding.

ID: 023	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enforce the system application disable list.	

ID: 023	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android Work Environment to enforce the system application disable list. Do one of the following: - Method #1: KPE(AE) enrolment - Method #2: KPE system app disable list **** Method #1: KPE(AE) enrolment The required configuration is the default configuration when the device is enrolled as a KPE (AE) deployment. If the device configuration is changed, use the following procedure to bring the device back into compliance: On the management tool, configure a list of approved Google core and preinstalled apps in the core app white list. **** Method #2: KPE system app disable list On the management tool, in the Work Environment KPE application section, add all non-approved system app packages to the "system app disable list".	
Validación	Review Samsung Android configuration settings to determine if the system application disable list is enforced. 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 Administration Console and the Samsung Android device. **** Method #1: KPE(AE) enrolment The required configuration is the default configuration when the device is enrolled as a KPE (AE) deployment. On the management tool, verify that "core app white list" contains only approved core and preinstalled apps. On the Samsung Android device, review the apps and confirm that apps listed in the in this Configuration Guide are not present. If on the management tool the "core app white list" contains non-approved core and preinstalled apps, or on the Samsung Android device non-approved apps are listed, this is a finding. **** Method #2: KPE system app disable list On the management tool, verify that the "system app disable list" contains all apps that have not been approved for use in the Organization. On the Samsung Android device, review the apps and confirm that none of the apps listed in the “system app disable list” are present. If on the management tool the "system app disable list" contains non-approved core and preinstalled apps, or on the Samsung Android device non-approved apps are listed, this is a finding.	

ID: 024	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable Certificate Revocation checking.	

ID: 024	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to enable Certificate Revocation checking. Do one of the following: - Method #1: CRL checking - Method #2: OCSP with CRL fallback **** Method #1: CRL checking On the management tool, set "Revocation check" to "enable for all apps". Refer to the management tool documentation to determine how to configure Revocation checking to "enable for all apps". Some may, for example, allow a wildcard string: "*". **** Method #2: OCSP with CRL fallback On the management tool, do the following: 1. In the certificate section, set "Revocation check" to "enable for all apps". 2. In the restrictions section, set "OCSP check" to "enable for all apps". Refer to the management tool documentation to determine how to configure Revocation and OCSP checking to "enable for all apps". Some may, for example, allow a wildcard string: "*".	
Validación		

ID: 025	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must have the Organization root and intermediate PKI certificates installed.	
Procedimiento	Configure the Samsung Android to install Organization root and intermediate PKI certificates. Do one of the following: - Method #1: Use AE Key management. - Method #2: Use KPE Key management. **** Method #1: Use AE Key management. On the management tool, in the certificate section, install the Organization root and intermediate PKI certificates. **** Method #2: Use KPE Key management. On the management tool, in the KPE certificate section, install the Organization root and intermediate PKI certificates.	

ID: 025	PASS [ ]	FAIL [ ]
Validación	Review Samsung Android configuration settings to determine if the Organization root and intermediate PKI certificates are installed. 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 Administration Console and the Samsung Android device. **** Method #1: Use AE Key management. On the management tool, verify that the Organization root and intermediate PKI certificates are installed. On the Samsung Android device, do the following: 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. If on the management tool the Organization root and intermediate PKI certificates are not listed or on the Samsung Android device the Organization root and intermediate PKI certificates are not listed, this is a finding. **** Method #2: Use KPE Key management. On the management tool, in the KPE certificate section, verify that the Organization root and intermediate PKI certificates are installed. On the Samsung Android device, do the following: 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. If on the management tool the Organization root and intermediate PKI certificates are not listed or on the Samsung Android device the Organization root and intermediate PKI certificates are not listed, this is a finding.	

ID: 026	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 Samsung Android to prevent a user from removing Organization root and intermediate PKI certificates. Do one of the following: - Method #1: Disallow user from configuring any credential. - Method #2: Disallow user from removing certificates. **** Method #1: Disallow user from configuring any credential. On the management tool, set "Config credentials" to "Disallow". **** Method #2: Disallow user from removing certificates. On the management tool, in the KPE restrictions section, set "User Remove Certificates" to "Disallow".	

ID: 026	PASS [ ]	FAIL [ ]
Validación	Review Samsung Android configuration settings to determine if the user is unable to remove Organization root and intermediate PKI certificates. 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 Administration Console and the Samsung Android device. **** Method #1: Disallow user from configuring any credential. On the management tool, verify that "Config credentials" is set to "Disallow". On the Samsung Android device, do the following: 1. Open Settings >> Biometrics and security >> Other security settings >> View security certificates. 2. In the System tab, verify that no listed certificate can be untrusted. 3. In the User tab, verify that no listed certificate 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. **** Method #2: Disallow user from removing certificates. On the management tool, in the device KPE restrictions section, verify "User Remove Certificates" is set to "Disallow". On the Samsung Android device, do the following: 1. Open Settings >> Biometrics and security >> Other security settings >> View security certificates. 2. In the System tab, verify that no listed certificate can be untrusted. 3. In the User tab, verify that no listed certificate can be removed. If on the management tool the device "User Remove Certificates" is not set to "Disallow", or on the Samsung Android device a certificate can be untrusted or removed, this is a finding.	

ID: 027	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enforce an application installation policy by specifying an application whitelist that restricts applications by the following characteristics: names.	

ID: 027	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to use an application whitelist. The application whitelist does not control user access to/execution of all core and preinstalled applications. Do one of the following: - Method #1: Use managed Google Play. - Method #2: Use KPE app installation whitelisting. **** Method #1: Use managed Google Play. On the management tool, in the Work Environment app catalogue for managed Google Play, add each Organization-approved app to be available. **** Method #2: Use KPE app installation whitelisting. On the management tool, in the KPE restrictions section, add each Organization-approved app to the "app installation whitelist". Note: 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.	
Validación	Review the Samsung Android configuration setting to determine if the mobile device has an application whitelist configured. Verify that all applications listed on the whitelist have been approved by the Organization. This validation procedure is performed only on the management tool Administration Console. Confirm if Method #1 or #2 is used at the Samsung device site and follow the appropriate procedure. **** Method #1: Use managed Google Play. On the management tool, verify that only Organization-approved apps are available. If on the management tool the app catalogue for managed Google Play includes non-Organization-approved apps, this is a finding. **** Method #2: Use KPE app installation whitelisting. On the management tool, in the KPE restrictions section, verify that only Organization-approved apps are listed in the "app installation whitelist". If on the management tool "app installation whitelist" contains non-Organization-approved apps, this is a finding.	

ID: 028	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not display the following notifications when the device is locked: all notifications.	
Procedimiento	Configure Samsung Android to not display notifications when the device is locked. Disable unredacted notifications on the Keyguard. On the management tool, set "Unredacted Notifications" to "Disallow".	

ID: 028	PASS [ ]	FAIL [ ]
Validación	Review Samsung Android configuration settings to determine if Samsung Android displays notifications on the lock screen. 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. Disable unredacted notifications on the Keyguard. On the management tool, verify that "Unredacted Notifications" is set to "Disallow". On the Samsung Android device, do the following: 1. Open Settings >> Lock screen. 2. Verify that "Notifications" are disabled. If on the management tool "Unredacted Notifications" is not set to "Disallow", or on the Samsung Android device "Show notification content" is not disabled, this is a finding.	

ANEXO III: TEST DEVICE POLICY CONTROL (TEST DPC)

Test DPC es una aplicación diseñada para ayudar a los MDM, ISV y OEM 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 3.3.2, para una familiarización con las mismas y su consiguiente mapeo a la solución MDM específica elegida.

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

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

Android lock screen restrictions / max password failures for local wipe

Indica:

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

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

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

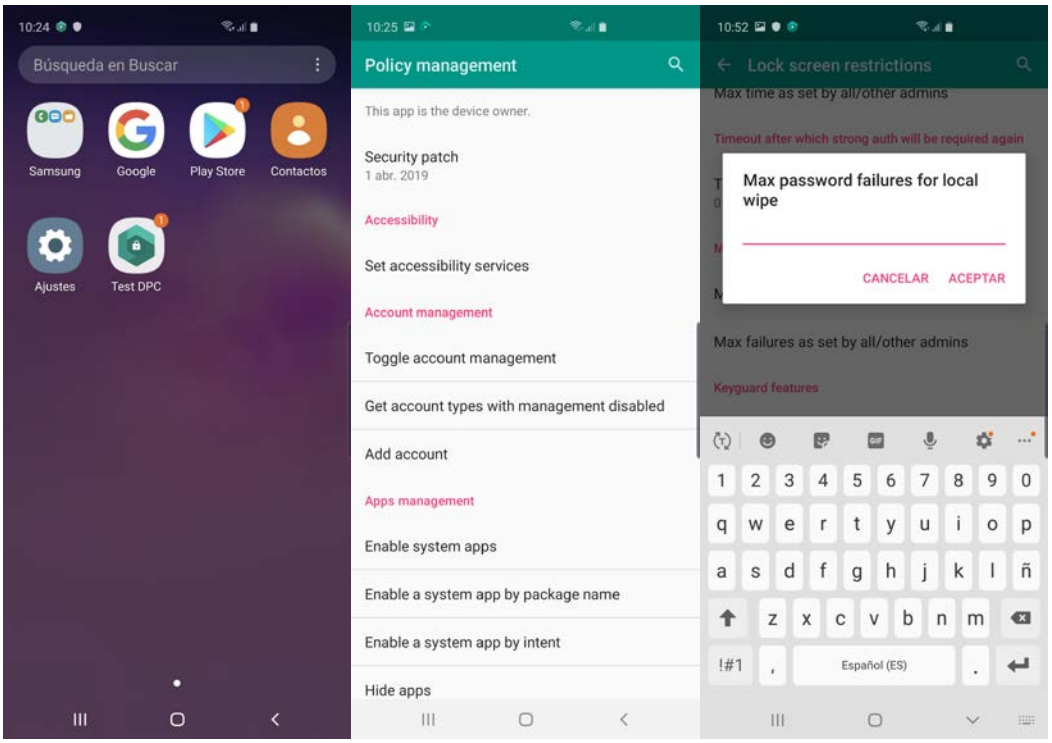

Figura 3