centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1606

Configuración segura de dispositivos Samsung Galaxy S10 con Android 9

Julio 2019

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.07.16 12:08:34 +02'00'

NIPO: 083-19-211-7

Fecha de Edición: julio 2019
Samsung Electronics ha participado en el desarrollo del presente documento y sus anexos.

AVISO

Esta guía de configuración segura se publica de manera provisional a la espera del proceso formal de cualificación de los dispositivos mencionados en el apartado 3.1Dispositivos Cualificados y Compatibles.
La publicación de este documento no es un indicador sobre el avance del proceso de Cualificación. En caso de que los productos mencionados finalicen con éxito el proceso de cualificación, este documento se actualizará con los cambios pertinentes.

AVISO

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

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 en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su 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, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.
Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, 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 su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El objetivo de este documento es proporcionar una guía de configuración de los dispositivos Samsung Galaxy con Android 9 cualificados por CCN y listados en el Catálogo de Productos CPSTIC.

2. Las secciones siguientes están organizadas como sigue: 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.

3. La sección 2 informa de detalles 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. Detalles 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.

4. 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 una 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. Otras configuraciones no se consideran y no se pueden realizar valoraciones generales sobre el impacto en la seguridad de los cambios que se introduzcan.

5. 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.

6. 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

7. 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*) cualificadas y que dispongan de las funcionalidades necesarias.
    - Redes de comunicaciones, de diferentes tecnologías (3G, 4G, 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.
8. 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

9. 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
10. 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 del cual exclusivamente 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.
11. En los escenarios COBO y COPE el dispositivo móvil es propiedad de la organización, y el Administrador IT tiene acceso a control total del dispositivo, implementando políticas de seguridad y restricciones.

12. 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.
13. 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.
14. Los agentes MDM, 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.
15. 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

16. 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

17. Samsung ayuda a las organizaciones a asegurar 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)

18. 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)

19. KPE proporciona seguridad de alto nivel que protege todos los aspectos de la operación del dispositivo móvil.
20. KPE resuelve los puntos críticos identificados por las organizaciones y cumple con los estrictos requisitos de sectores altamente regulados.
21. Con KPE, un dispositivo móvil Samsung Android se puede configurar para cumplir con los requerimientos ENS Alto.
22. Además de las características de AE, las siguientes funciones de KPE se deben configurar para un despliegue esté en cumplimiento con esta guía de configuración segura:
    - Modo Criterios Comunes de Knox (CC Common Criteria)
    - Restricciones de contraseña de Knox: Máximo secuencial o repetición de caracteres y números
    - Certificado de Knox: verificación de revocación y protocolo de estado de certificado en línea (OCSP)
    - Registro de auditoría de Knox
    - Cifrado Knox: cifrado de almacenamiento externo (opcional si el almacenamiento extraíble está deshabilitado)
    - Restricciones de Knox: perfiles Bluetooth permitidos
    - Restricciones de Knox: no permitir la función "Compartir vía lista"
    - Restricciones de Knox: lista de excepciones del modo host USB, habilitada para el modo DeX
    - Restricciones de Knox: rechazar puntos de acceso WiFi no protegidos
    - Restricciones de Knox: no se permite el autocompletado automático en explorador de Internet de Samsung
    - Restricciones de Knox: no permitir la sincronización automática de las cuentas de Google
    - Knox Exchange ActiveSync: Deshabilitando la recuperación de contraseña.

23. Puede encontrar información adicional en los siguientes links:

    https://www.samsungknox.com/en/solutions/it-solutions/knox-platform-for-enterprise

    https://www.samsungknox.com/en/knox-platform/knox-security

1.2.4. A DESTACAR EN KPE 3.3

Mejoras VPN

24. KPE 3.3 incluye varias novedades que mejoran la experiencia de usuario y el rendimiento de los clientes VPN en el Knox framework.
25. Las mejoras incluyen, entre otras, las siguientes:
    - Compatibilidad con túneles de múltiples aplicaciones: mejoran la experiencia del usuario cuando se utilizan túneles VPN que afectan a más de una aplicación a la vez. Como resultados, los usuarios pueden conectarse y comenzar a usar aplicaciones empresariales inmediatamente después de que se establezca el túnel VPN.
    - Sincronizar eventos de Knox con eventos de redes de Android: mejora el rendimiento de los clientes VPN al sincronizar eventos de Knox con eventos de red de Android. Este cambio significa que Knox Workspace reconoce que el cliente VPN está conectado sin demora.
        - Proporcionar información de flujo de red en curso para fines de Network Platform Analytics (NPA)[2]: esta nueva función mejora el rendimiento de las herramientas de evaluación de rendimiento de red basadas en MDM al proporcionar información sobre el flujo de datos de red mientras la conexión está en curso. Esta funcionalidad significa que los Administradores ahora tienen la posibilidad de configurar sus herramientas NPA basadas en MDM para recibir estadísticas de red mientras la conexión de red está en curso. Esta funcionalidad es especialmente útil en los casos en que las sesiones de red duran mucho tiempo.

[2] Network Platform Analytics (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.

2. PROCESO DE DESPLIEGUE

26. 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).
27. 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.
28. 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.
29. 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

30. 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

31. 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

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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

38. 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.

39. 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 fuera de la red de 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.

40. 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

41. 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

42. 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.

43. 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.

44. 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

45. En este apartado se listan los dispositivos cualificados por CCN con versión de Android 9.0 (apartado 3.1.1) así como dispositivos cualificados por CCN con una versión anterior de Android que se actualizan a la versión 9.0 (apartado 3.1.2). El listado completo y actualizado se puede encontrar en la siguiente página web:

46. https://oc.ccn.cni.es/index.php/en/cis-product-catalogue/list-of-qualified-products

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

3.1.1. DISPOSITIVOS CUALIFICADOS

NOMBRE DISPOSITIVO	MODELO	VERSION DE ANDROID	VERSIÓN DE KERNEL	COMPILACIÓN
Galaxy S10e	SM-G970F	9.0	4.14.75	PPR1.180610.011
Galaxy S10	SM-G973F	9.0	4.14.75	PPR1.180610.011
Galaxy S10+	SM-G975F	9.0	4.14.75	PPR1.180610.011
Galaxy S10 5G	SM-G977B	9.0	4.14.75	PPR1.180610.011

Tabla 1

3.1.2. DISPOSITIVOS COMPATIBLES CUALIFICADOS

NOMBRE DISPOSITIVO	MODELO	VERSIÓN DE ANDROID	VERSION DE KERNEL	COMPILACIÓN
Galaxy Tab S4	SM-T830 SM-T835	9.0	4.4.153	PPR1.180610.011
Galaxy Note9	SM-N960F	9.0	4.9.59	PPR1.180610.011
Galaxy S9	SM-G960F	9.0	4.9.59	PPR1.180610.011
Galaxy S9+	SM-G965F	9.0	4.9.59	PPR1.180610.011
Galaxy Note8	SM-N950F	9.0	4.4.111	PPR1.180610.011
Galaxy S8	SM-G950F	9.0	4.4.111	PPR1.180610.011
Galaxy S8+	SM-G955F	9.0	4.4.111	PPR1.180610.011

Tabla 2

3.1.3. DISPOSITIVOS COMPATIBLES

NOMBRE DISPOSITIVO	MODELO	VERSIÓN DE ANDROID	VERSION DE KERNEL	COMPILACIÓN
Galaxy Fold	SM-F900	9.0	4.14.78	PPR1.180610.011

Tabla 3

3.2 IDENTIFICACIÓN DE VERSIÓN DE DISPOSITIVO

48. 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.

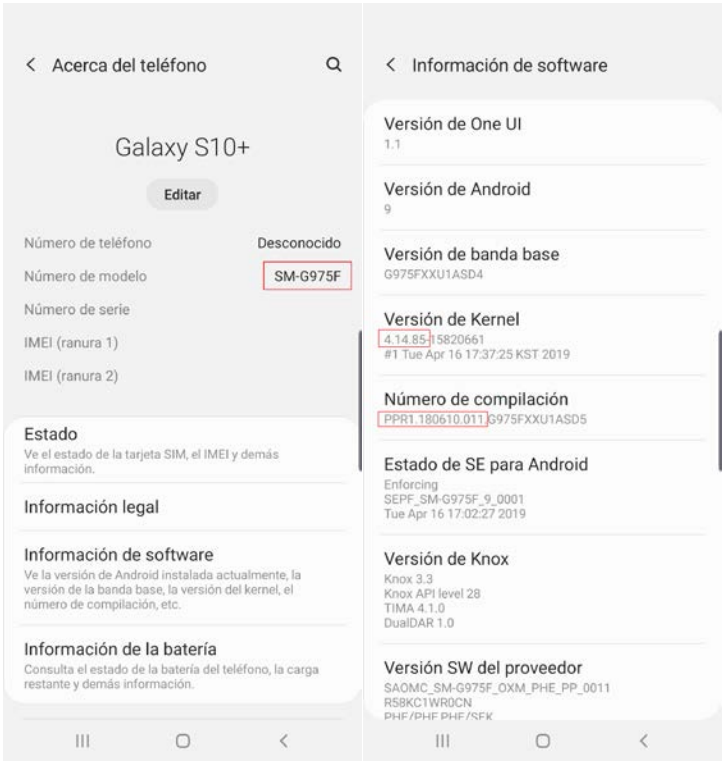

Figura 2

3.3 REGLAS DE CONFIGURACIÓN GENERAL DEL DISPOSITIVO

49. 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.

50. 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.

51. 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.

52. 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	CONFIGURACIÓN	COMENTARIO
Android account	account management	Configure	Disable for the work email app	Refer to MDM documentation to determine how to provision user's work email accounts for the work email app.
Android certificate	install a CA certificate	Configure	Install the Organization root and intermediate certificates	Select PEM encoded representations of the Organization root and intermediate certificates.
Android device owner management	enable backup service	Select/Unselect	Unselect	
Android lock screen restrictions	disable face	Select/Unselect	Select	
Android lock screen restrictions	disable trust agents	Select/Unselect	Select	
Android lock screen restrictions	disable unredacted notifications	Select/Unselect	Select	
Android lock screen restrictions	max password failures for local wipe	0+	10	Unsuccessful logon attempts before device wipe
Android lock screen restrictions	max time to screen lock	0+	15	
Android password constraints	minimum password length	0+	6	Minimum device password length
Android password constraints	minimum password quality	None, Pattern, PIN, Alphabetic, Alphanumeric, Complex, Biometric	Alphanumeric	
Android password constraints	password history length	0+	0	
Android user restrictions	disallow autofill	Select/Unselect	Select	
Android user restrictions	disallow config date time	Select/Unselect	Select	

GRUPO	REGLA	OPCIONES	CONFIGURACIÓN	COMENTARIO
Android user restrictions	disallow debugging features	Select/Unselect	Select	
Android user restrictions	disallow install unknown sources	Select/Unselect	Select	Disallow unknown app installation sources.
Android user restrictions	disallow mount physical media	Select/Unselect	Select	
Android user restrictions	disallow outgoing beam	Select/Unselect	Select	
Android user restrictions	disallow USB file transfer	Select/Unselect	Select	Disabling USB Media Player will also disable USB MTP, USB mass storage, and USB vendor protocol (KIES/Smart Switch).
Knox Bluetooth	allowed profiles	HSP, HFP, PBAP, A2DP, AVRCP, SPP, NAP, BNEP, HID, BPP, DUN, SAP	HFP, HSP, SPP	Disables all Bluetooth profiles except for those specified in the settings.
Knox Wifi	allow unsecured hotspot	Select/Unselect	Unselect	Disallow unsecured hotspots.
Knox application	application installation whitelist	Configure	Add each IT Administrator-approved package	
Knox application	system application disable list	Configure	Add all non-IT Administrator-approved system app packages, add all system app packages that have been identified as having non-Organization-approved characteristics, add all preinstalled public cloud backup system apps.	
Knox audit log	enable audit log	Select/Unselect	Select	This simultaneously enables audit logging for Workspace events.
Knox banner	banner text	Configure	Organization-mandated warning banner text	
Knox certificate	OCSP check	Configure	Enable for all apps	Refer to the MDM documentation to determine how to configure OCSP checking to “enable for all apps”. Some may, for example, allow a wildcard string: “*” (asterisk).
Knox certificate	revocation check	Configure	Enable for all apps	Refer to the MDM documentation to determine how to configure revocation checking to “enable for all apps”. Some may, for example, allow a wildcard string: “*” (asterisk).

GRUPO	REGLA	OPCIONES	CONFIGURACIÓN	COMENTARIO
Knox encryption	enable external storage encryption	Select/Unselect	Select	
Knox password constraints	maximum sequential characters	0+	2	
Knox restrictions	Disallow share via list	Select/Unselect	Select	Note: Disabling "Share Via List" will also disable functionality such as "Gallery Sharing" and "Direct Sharing".
Knox restrictions	USB host mode exception list	APP, AUD, CDC, COM, CON, CSC, HID, HUB, MAS, MIS, PER, PHY, PRI, STI, VEN, VID, WIR	HID	
Knox restrictions	allow auto-fill	Select/Unselect	Unselect	
Knox restrictions	allow google accounts auto sync	Select/Unselect	Unselect	
Knox restrictions	enable CC mode	Select/Unselect	Select	Common Criteria (CC) Mode is fundamental to MDFPP compliance and is a top-level requirement. Puts the devices in CC Mode as defined by the Samsung Galaxy Device MDFPP Security Target. The following configuration must also be implemented for the Samsung Android device to be operating in the NIAP-certified complaint CC mode of operation: minimum password quality, disable face, max password failures for local wipe, password recovery, password history length, revocation check, OCSP check, Secure Startup, enable external storage encryption, or disallow mount physical media.
Microsoft Exchange ActiveSync	password recovery	Enable/Disable	Disable	The Organization mobile service provider should verify the Exchange server is configured to disable Microsoft Exchange ActiveSync (EAS) password recovery.
managed Google Play	application installation whitelist	Configure	Add each IT Administrator-approved package	

GRUPO	REGLA	OPCIONES	CONFIGURACIÓN	COMENTARIO
managed Google Play	system application disable list	Configure	Add all non-IT Administrator-approved system app packages, add all system app packages that have been identified as having non-Organization-approved characteristics, add all preinstalled public cloud backup system apps	

Tabla 4 - Reglas Configuración para un despliegue COBO

3.4 DESACTIVACIÓN DE APLICACIONES

53. Samsung Knox para Android soporta políticas de desactivación 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 en el dispositivo y configurar la desactivación de dichas aplicaciones mediante la configuración de políticas de desactivación de aplicaciones.
54. Esta tarea debe ser realizada antes de la recepción del terminal por parte de la Organización o del Usuario final del dispositivo.

3.4.1. APLICACIONES DE COPIA DE SEGURIDAD EN LA NUBE PÚBLICA

55. El Administrador IT de la organización debe identificar cualquier servicio de este tipo que venga preinstalado y deshabilitar estas aplicaciones.
56. Entre las de más probable aparición se incluyen:
    - Cuenta de Samsung (incluyendo Samsung Cloud)
    - Dropbox
    - Drive (Google)
    - OneDrive (Microsoft)

3.4.2. APLICACIONES PARA COMPARTIR CONTENIDO

57. 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.
58. Entre las de más probable aparición se incluyen:

- Group Play/Juego en Grupo
- Samsung Connect (Conexión rápida)

3.4.3. IMPRESIÓN MÓVIL

59. 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 9.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

60. 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

61. 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

NOMBRE DE LA APLICACION	NOMBRE DEL PAQUETE
Find My Mobile	com.samsung.android.fmm
Samsung Cloud	com.samsung.android.scloud
ShortcutBNR	com.samsung.android.shortcutbackupservice
	com.samsung.android.smartswitchassistant
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

62. 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)

63. 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 el MDM no puede desactivar, la mitigación debe incluir la **formación adecuada de los usuarios finales**.

64. La organización que quiera hacer uso de estos dispositivos y alcanzar el nivel de seguridad al que se orienta este documento debe articular una política de seguridad interna para trasladar al usuario final estos conocimientos y responsabilidades.

65. 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

66. 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

67. 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.

68. Se accede a las funciones "Conexión rápida" y "Conexión de Samsung" (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.

69. 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.

70. 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.

71. 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.

72. 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.

73. 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. BORRADO DE CERTIFICADOS

74. El Administrador IT de la organización puede instalar certificados PKI de la organización en el dispositivo directamente y a través de MDM. El usuario puede eliminar manualmente los certificados instalados a través de la aplicación Configuración (Pantalla de bloqueo y Seguridad >> Otras configuraciones de seguridad >> Certificados de usuario). Los usuarios deben estar formados para no eliminar el certificado raíz de la organización y los certificados PKI intermedios.

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

75. 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.

76. **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.**

3.5.5. USO COMPARTIDO WIFI

77. 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.

78. 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 CONFIGURACIÓN SEGURA

79. Instrucciones para realizar una auditoría de un dispositivo configurado correctamente:

80. 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 dispostivo de test en idioma Inglés así faciliar su testeo, seleccione "Ajustes" → "Administración General" → "Idioma y enrada de texto" → "Idioma" + Añadir idioma English (United Kingdom).*

ID: 001	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to prevent users from adding personal email accounts to the work email app.	
Procedimiento	Configure Samsung Android to prevent users from adding personal email accounts to the work email app. On the MDM console, for the device, do the following: 1. In the 'Android account' group, configure 'account management' to 'disable for the work email app'. 2. Provision the user's email account for the work email app. Refer to the MDM documentation to determine how to provision users' work email accounts for the work email app.	

ID: 001	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that users are prevented from adding personal email accounts to the work email app. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, do the following: 1. In the 'Android account' group, verify that 'account management' is configured to 'disable for the work email app'. 2. Provision the user's email account for the work email app. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Accounts and backup'. 3. Tap 'Accounts'. 4. Tap 'Add account'. 5. Verify that an account for the work email app cannot be added. If on the MDM console 'account management' is not disabled for the work email app, or on the Samsung Android device the user can add an account for the work email app, this is a finding.	

ID: 002	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enforce the system application disable list.	
Procedimiento	Configure Samsung Android to enforce the system application disable list. Do one of the following: - Method # 1 (preferred): Use managed Google Play for the device (managed device). - Method #2: Use the Knox system application disable list. **** Method #1: On the MDM console, for the device, in the 'managed Google Play' group, add all non-IT Administrator of the Organization-approved system app packages to the system application disable list. **** Method #2: On the MDM console, for the device, in the 'Knox application' group, add all non-IT Administrator of the Organization -approved system app packages to the system application disable list. **** Note: Refer to the 'System Apps for disablement (other characteristics)' and 'System Apps That Must Not Be Disabled' tables in section 3.4 of this CCN-STIC guide.	

ID: 002	PASS [ ]	FAIL [ ]
Validación	Review device configurations settings to confirm that the system application disable list has been configured. This procedure is performed on both the MDM Administration console and the Samsung Android device. Confirm if Method #1 or Method #2 is used at the Samsung device site and follow the appropriate procedure. **** Method #1: On the MDM console, for the device, in the 'managed Google Play' group, verify that the system application disable list contains all apps that have not been approved for the Organization use by the IT Administrator of the Organization. On the Samsung Android device, review the apps on the 'Personal' App screen and confirm that none of the apps listed in the system application disable list are present. If the system application disable list does not contain all the apps that have not been approved by the IT Administrator of the Organization, or if an app listed can be found on the 'Personal' App screen of the Samsung Android device, this is a finding. **** Method #2: On the MDM console, for the device, in the 'Knox application' group, verify that the system application disable list contains all apps that have not been approved for the Organization use by the IT Administrator of the Organization. On the Samsung Android device, review the apps on the 'Personal' App screen and confirm that none of the apps listed in the system application disable list are present. If the system application disable list does not contain all the apps that have not been approved by the IT Administrator of the Organization, or if an app listed can be found on 'Personal' App screen of the Samsung Android device, this is a finding.	

ID: 003	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: list of digital signatures, list of package names.	

ID: 003	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to enforce an application installation whitelist. The application installation 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 for the Device (managed device). - Method #2: Use Knox application installation whitelist. **** Method #1: On the MDM console, for the device, in the 'managed Google Play' group, add each IT Administrator of the Organization -approved package to the managed Google Play application installation whitelist. **** Method #2: On the MDM console, for the device, in the 'Knox application' group, add each IT Administrator of the Organization -approved package to the application installation whitelist. Refer to the MDM documentation to determine the following: - If an application installation blacklist is also required to be configured when enforcing an application installation whitelist. - If the MDM supports adding packages to the application installation whitelist by package name and/or digital signature or supports a combination of the two. **** Note: Refer to the 'System Apps That Must Not Be Disabled' table in the section 3.4 of this CCN-STIC guide. These apps must be included in the application installation whitelist to allow updates.
Validación	Review device configuration settings to confirm that an application installation whitelist has been configured. This procedure is performed only on the MDM Administration console. Confirm if Method #1 or Method #2 is used at the Samsung device site and follow the appropriate procedure. **** Method #1: On the MDM console, for the device, in the 'managed Google Play' group, verify that each package listed on the application installation whitelist has been approved for the Organization use by the IT Administrator of the Organization. If the application installation whitelist contains non-IT Administrator of the Organization -approved packages, this is a finding. **** Method #2: On the MDM console, for the device, in the 'Knox application' group, verify that each package listed on the application installation whitelist has been approved for the Organization use by the IT Administrator of the Organization. If the application installation whitelist contains non-IT Administrator of the Organization -approved packages, this is a finding.

ID: 004	PASS [ ]	FAIL [ ]
Requerimiento	The Samsung Android whitelist must be configured to not include applications with the following characteristics: - back up mobile device data to non-the Organization cloud servers (including user and application access to cloud backup services); - transmit mobile device diagnostic data to non-the Organization servers; - voice assistant application if available when the mobile device is locked; - voice dialing application if available when the mobile device is locked; - allows synchronization of data or applications between devices associated with the user; and - allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other mobile devices or printers.	
Procedimiento	Configure Samsung Android to include all system apps in the system app disable list that have been identified as having non-the Organization -approved characteristics. Do one of the following: - Method # 1 (preferred): Use managed Google Play for the device (managed device). - Method #2: Use the Knox system application disable list. **** Method #1: On the MDM console, for the device, in the 'managed Google Play' group, add all system app packages that have been identified as having non-Organization -approved characteristics to the system application disable list. **** Method #2: On the MDM console, for the device, in the 'Knox application' group, add all system app packages that have been identified as having non- Organization -approved characteristics to the system application disable list. **** Note: Refer to the 'System Apps for Disablement (Non- Organization -Approved Characteristics)' and 'System Apps That Must Not Be Disabled' tables in the section 3.4 of this CCN-STIC guide.	
Validación	Review device configuration settings to confirm that the system application disable list has been configured to include all system apps that have been identified as having non- Organization -approved characteristics. This procedure is performed on both the MDM Administration console and the Samsung Android device. Confirm if Method #1 or Method #2 is used at the Samsung device site and follow the appropriate procedure.	

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 [the Organization -approved commercial app repository, MDM server, mobile application store]: - disallow unknown app installation sources.	

ID: 005	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to disallow installation from unauthorized application repositories. On the MDM console, for the device, in the 'Android user restrictions' group, select 'disallow install unknown sources'.	
Validación	Review device configuration settings to confirm that installation from unauthorized application repositories is disallowed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android user restrictions' group, verify that 'disallow install unknown sources' is selected. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Apps'. 3. Tap the Overflow menu (three vertical dots). 4. Tap 'Special Access'. 5. Tap 'Install unknown apps'. 6. Tap a listed app. 7. Verify that 'Allow from this source' cannot be enabled. If on the MDM console 'disallow install unknown sources' is not selected, or on the Samsung Android device the user can enable 'allow from this source' for an app, this is a finding.	

ID: 006	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable the Knox audit log.	
Procedimiento	Configure Samsung Android to enable the Knox audit log. On the MDM console, for the device, in the 'Knox audit log' group, select 'enable audit log'.	
Validación	Review device configuration settings to confirm that the Knox audit log is enabled. This procedure is performed on the MDM Administration console only. On the MDM console, for the device, in the 'Knox audit log' group, verify that 'enable audit log' is selected. If on the MDM console the 'enable audit log' is not selected, this is a finding.	

ID: 007	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 redact notifications when the device is locked. On the MDM console, for the device, in the 'Android lock screen restrictions' group, select 'disable unredacted notifications'.	

ID: 007	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that the content of notifications is redacted when the device is locked. This procedure is performed on both the MDM console and the Samsung Android device. On the MDM console, for the device, in the 'Android lock screen restrictions' group, verify that 'disable unredacted notifications' is selected. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Lock screen'. 3. Verify that 'Notifications' is disabled. If on the MDM console 'disable unredacted notifications' is not selected, or on the Samsung Android device 'Notifications' is not disabled, this is a finding.	

ID: 008	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android device users must complete required training.	
Procedimiento	Have all Samsung device users complete training on the following topics. Users should acknowledge that they have reviewed training via a signed User Agreement or similar written record. Training topics: - Operational security concerns introduced by unmanaged applications/unmanaged personal space, including applications using global positioning system (GPS) tracking. - Need to ensure no Organization data is saved to the personal space or transmitted from a personal app (for example, from personal email). - How to configure the following UBE controls (users must configure the control) on the Samsung device: **Secure use of Calendar Alarm **Local screen mirroring and MirrorLink procedures (authorized/not authorized for use) **Do not connect Samsung devices (either via DeX Station or dongle) to any the Organization network via Ethernet connection **Do not upload the Organization contacts via smart call and caller ID services **Do not remove the Organization intermediate and root PKI digital certificates **Disable WiFi Sharing **Do not configure a the Organization network (work) VPN profile on any third-party VPN client installed in the personal space **Enable Secure Startup, and must not disable at any time **Must not disable Strong Protection at any time - IT Administrator of the Organization guidance on acceptable use and restrictions, if any, on downloading and installing personal apps and data (music, photos, etc.) in the Samsung device personal space.	

ID: 008	PASS [ ]	FAIL [ ]
Validación	Review a sample of site User Agreements for Samsung device users or similar training records and training course content. Verify that Samsung device users have completed the required training. The intent is that required training is renewed on a periodic basis in a time period determined by the IT Administrator of the Organization. If any Samsung device user has not completed the required training, this is a finding.	

ID: 009	PASS [ ]	FAIL [ ]
Requerimiento	Any accessory that provides wired networking capabilities to a Samsung Android device must not be connected to the Organization network (for example: DeX Station [LAN port], USB to Ethernet adapter, etc.).	
Procedimiento	When using an accessory that provides wired networking capabilities to a Samsung Android device, do not connect the accessory to the Organization network. Note: This setting cannot be managed by the MDM administrator and is a UBE requirement.	
Validación	Review accessories that provide wired networking capabilities to Samsung Android devices at the site and verify that the accessories are not connected to a the Organization network. If accessories that provide wired networking capabilities to Samsung Android devices are connected to the Organization networks, this is a finding. Note: Connections to a site's guest network that provides Internet-only access can be used. Note: This setting cannot be managed by the MDM administrator and is a User-Based Enforcement (UBE) requirement.	

ID: 010	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 MDM console, in the Android password constraints, set the 'minimum password length' to '6' or greater.	

ID: 010	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that the minimum password length is six or more characters. This procedure is performed on both the MDM administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android password constraints' group, verify that the 'minimum password length' is '6' or greater. 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 entered with fewer than six characters are not accepted. If on the MDM console 'minimum password length' is less than '6', or on the Samsung Android device a password of less than '6' characters is accepted, this is a finding.	

ID: 011	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not allow passwords that include more than two repeating or sequential characters.	
Procedimiento	Configure Samsung Android to prevent passwords from containing more than two repeating or sequential characters. On the MDM console, for the device, in the 'Knox password constraints' group: 1. Set 'maximum sequential characters' to '2'. 2. Set 'maximum sequential numbers' to '2'.	

ID: 011	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that passwords with two repeating or sequential characters are prevented. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, do the following: 1. For the device, in the 'Knox password constraint' group, verify that 'maximum sequential characters' is '2' or less. 2. For the device, in the 'Knox password constraint' group, 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 characters or numbers are not accepted. If on the MDM console '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.	

ID: 012	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 MDM console, for the device, in the 'Android lock screen restrictions' group, set the 'max time to screen lock' to '15' minutes.	
Validación	Review device configuration settings to confirm that the device locks the screen after 15 minutes (or less) of inactivity. This procedure is performed on both the MDM Administration Console and the Samsung Android device. On the MDM console, in the Android lock screen restrictions, verify that the 'max time to screen lock' is '15' minutes or less. On the Samsung Android device, do the following: 1. Unlock the device. 2. Refrain from performing any activity on the device for 15 minutes. 3. Verify that the device requires the user to enter the device unlock password to access the device. If on the MDM console 'max time to lock' is not set to '15' minutes or less, or the Samsung Android device does not require the user to authenticate to unlock after 15 minutes of inactivity, this is a finding.	

ID: 013	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 consecutive failed authentication attempts before device wipe. On the MDM console, for the device, in the 'Android lock screen restrictions' group, set the 'max password failures for local wipe' to '10'.	
Validación	Review device configuration settings to confirm that the maximum number of consecutive failed authentication attempts is set to '10' or fewer. This procedure is performed on the MDM Administration console only. On the MDM console, for the device, in the 'Android lock screen restrictions' group, verify that the 'max password failures for local wipe' is '10' or fewer. If on the MDM console, 'max password failures for local wipe' is more than '10', this is a finding.	

ID: 014	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's Common Criteria evaluation.	
Procedimiento	Configure Samsung Android to disable trust agents. On the MDM console, for the device, in the 'Android lock screen restriction' group, select 'disable trust agents'.	
Validación	Review device configuration settings to confirm that trust agents are disabled. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android lock screen restrictions' group, verify that 'disable trust agents' is selected. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Biometrics and security'. 3. Tap 'Other security settings'. 4. Tap 'Trust agents'. 5. Verify that all listed trust agents are disabled and cannot be enabled. If on the MDM console 'disable trust agents' is not selected, or on the Samsung Android device a trust agent can be enabled, this is a finding.	

ID: 015	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's Common Criteria evaluation.	
Procedimiento	Configure Samsung Android to disable Face Recognition. On the MDM console, for the device, in the 'Android lock screen restriction' group, select 'disable face'.	

ID: 015	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that Face Recognition is disabled. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android lock restrictions' group, verify that 'disable face' is selected. 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. Verify that 'Face' is disabled and cannot be enabled. If on the MDM console 'disable face' is not selected, or on the Samsung Android device 'Face' can be enabled, this is a finding.	

ID: 016	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable automatic completion of Samsung Internet browser text input.	
Procedimiento	Configure Samsung Android to disable automatic completion of Samsung Internet app text input. On the MDM console, for the device, in the 'Knox restrictions' group, unselect 'allow autofill'.	
Validación	Review device configuration settings to confirm that automatic completion of Samsung Internet app text input is disabled. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Knox restrictions' group, verify that 'allow autofill' is not selected. On the Samsung Android device, do the following: 1. From the 'Personal' App screen, launch the 'Samsung Internet' app. 2. From the collapsed menu icon (three horizontal bars) on the toolbar, tap 'Settings'. 3. Tap 'Privacy and security'. 4. Verify that 'Autofill forms' is disabled and cannot be enabled. If on the MDM console 'allow autofill' is selected, or on the Samsung Android device 'Autofill forms' can be enabled by the user, this is a finding.	

ID: 017	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable the autofill services.	
Procedimiento	Configure Samsung Android to disable the autofill services. On the MDM console, for the device, in the 'Android user restrictions' group, select 'disallow autofill'.	

ID: 017	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that autofill services are disabled. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android user restrictions' group, verify that 'disallow autofill' is selected. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'General management'. 3. Tap 'Language and input'. 4. Verify that 'Autofill service' is not present. If on the MDM console 'disallow autofill' is selected, or on the Samsung Android device 'Autofill service' is present, this is a finding.	

ID: 018	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable all Bluetooth profiles except HSP (Headset Profile), HFP (HandsFree Profile), and SPP (Serial Port Profile).	
Procedimiento	Configure Samsung Android to disable all Bluetooth profiles except HSP, HFP, and SPP. On the MDM console, for the device, in the 'Knox Bluetooth' group, select 'HFP, HSP, and SPP' in the 'allowed profiles'.	
Validación	Review device configuration settings to confirm that all Bluetooth profiles are disabled except HSP, HFP, and SPP. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Knox Bluetooth' group, verify that only 'HFP, HSP, and SPP' are selected in the 'allowed profiles'. On the Samsung Android device, verify that a Bluetooth peripheral that uses a profile other than HSP, HFP, or SPP (e.g., a Bluetooth keyboard) cannot be paired. If on the MDM console 'allowed profiles' has any selection other than 'HSP, HFP, and SPP', or the Samsung Android device is able to pair with a Bluetooth keyboard, this is a finding. Note: Disabling the Bluetooth radio will satisfy this requirement.	

ID: 019	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable USB mass storage mode.	
Procedimiento	Configure Samsung Android to disallow USB file transfer. On the MDM console, for the device, in the 'Android user restrictions' group, select 'disallow USB file transfer'.	

ID: 019	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that USB file transfer has been disallowed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android user restrictions' group, verify that 'disallow USB file transfer' is selected. Connect the Samsung Android device to a non-Organization network-managed PC with a USB cable. On the PC, browse the mounted Samsung Android device and verify that it does not display any folders or files. If on the MDM console 'disallow USB file transfer' is not selected or the PC can mount and browse folders and files on the Samsung Android device, this is a finding.	

ID: 020	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable Knox Common Criteria (CC) Mode.	
Procedimiento	Configure Samsung Android to enable Knox CC Mode. On the MDM console, for the device, in the 'Knox restrictions' group, select 'enable CC mode'. The following configuration must also be implemented for the Samsung Android device to be operating in the NIAP-certified compliant CC mode of operation: - Minimum password quality - Disable face - Max password failures for local wipe - Password recovery - Password history length - Revocation check - OCSP check - Secure Startup (for devices prior to Galaxy S10) - Strong Protection (for Galaxy S10 [or newer] devices) - Enable external storage encryption or disallow mount physical media	

ID: 020	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that Knox CC Mode is enabled. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Knox restrictions' group, verify that 'enable CC mode' is selected. On the Samsung Android device, to verify that CC mode has not failed, do the following: 1. Open Settings. 2. Tap 'About phone'. 3. Tap 'Software information'. 4. Verify that the Security software version for MDF does not display 'Disabled'. For Samsung Android devices prior to Galaxy S10, to verify that CC Mode is enabled, do the following: 1. Open Settings. 2. Tap 'Biometric and security'. 3. Tap 'Secure startup'. 4. Verify that 'Do not require' is disabled. For Galaxy S10 (or newer devices), to verify that CC Mode is enabled, do the following: 1. Open Settings. 2. Tap 'Biometric and security'. 3. Verify that 'Strong Protection' is enabled and cannot be disabled. If on the MDM console 'enable CC mode' is not selected, or on the Samsung Android device the software version for 'MDF' displays 'Disabled', or on a Galaxy S10 (or newer device) 'Strong Protection' can be disabled, or on a device older than a Galaxy S10 'Do not require' is not disabled, this is a finding.	

ID: 021	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disallow configuration of date and time.	
Procedimiento	Configure Samsung Android to disallow configuration of the date and time. On the MDM console, for the device, in the 'Android user restrictions' group, select 'disallow config date time'.	

ID: 021	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that configuration of the date and time is disallowed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android user restrictions' group, verify that 'disallow config date time' is selected. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'General management'. 3. Tap 'Date and time'. 4. Verify that 'Automatic date and time' is on and the user cannot disable it. If on the MDM console 'disallow config date time' is not selected, or on the Samsung Android device 'Automatic date and time' is not set or the user can disable it, this is a finding.	

ID: 022	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enforce a USB host mode exception list. Note: This configuration allows DeX mode (with input devices).	
Procedimiento	Configure Samsung Android with a USB host mode exception list. On the MDM console, for the device, in the 'Knox restrictions' group, select 'HID' in the 'USB host mode exception list'.	
Validación	Review device configuration settings to confirm that the USB host mode exception list is configured. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Knox restrictions' group, verify that 'HID' is selected 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 MDM console 'USB host mode exception list' has any selection other than 'HID', or on the Samsung Android device the USB thumb drive can be mounted, this is a finding.	

ID: 023	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disallow the Share Via List feature.	
Procedimiento	Configure Samsung Android to disallow Share Via List. On the MDM console, for the device, in the 'Knox restrictions' group, select 'disallow share via list'. Note: Disabling 'share via list' will also disable functionality such as 'Gallery Sharing' and 'Direct Sharing'.	

ID: 023	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that Share Via List is disallowed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Knox restrictions' group, verify that 'disallow share via list' is selected. On the Samsung Android device, in the device, attempt to share by long pressing a file and tapping 'Share'. If on the MDM console 'disallow share via list' is not selected, or on the Samsung Android device the user is able to share, this is a finding.	

ID: 024	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disallow outgoing beam.	
Procedimiento	Configure Samsung Android to disallow outgoing beam. On the MDM console, for the device, in the 'Android user restrictions' group, select 'disallow outgoing beam'.	
Validación	Review device configuration settings to confirm that outgoing beam is disallowed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android user restrictions' group, verify that 'disallow outgoing beam' is selected. On the Samsung Android device, open a picture, contact, or webpage 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 'disallow outgoing beam' is not selected, or on the Samsung Android device the user is able to successfully start outgoing beam, this is a finding.	

ID: 025	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enforce that Wi-Fi Sharing is disabled.	
Procedimiento	Configure Samsung Android to disable Wi-Fi Sharing. Mobile Hotspot must be enabled in order to enable Wi-Fi Sharing. If the IT Administrator has not approved Mobile Hotspot, and it has been disabled on the MDM console, the following guidance is not applicable. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Connections'. 3. Tap 'Mobile Hotspot and Tethering'. 4. Tap 'Mobile hotspot'. 5. Disable 'Wi-Fi sharing' if it is enabled.	

ID: 025	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm Wi-Fi Sharing is disabled. Mobile Hotspot must be enabled in order to enable Wi-Fi Sharing. If the IT Administrator of the Organization has not approved Mobile Hotspot, and it has been verified as disabled on the MDM console, the following guidance is not applicable. This setting cannot be managed by the MDM administrator and is a User-Based Enforcement (UBE) requirement. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Connections'. 3. Tap 'Mobile Hotspot and Tethering'. 4. Tap 'Mobile hotspot'. 5. Verify that 'Wi-Fi sharing' is disabled. If on the Samsung Android device 'Wi-Fi sharing' is enabled, this is a finding.	

ID: 026	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not allow backup of [all applications, configuration data] to locally connected systems.	
Procedimiento	Configure Samsung Android to disable backup to locally connected systems. Disabling backup to locally connected systems is implemented by the configuration policy rule 'Disable USB mass storage'. On the MDM console, for the device, in the 'Android user restrictions' group, select 'disallow USB file transfer'.	
Validación	Review device configuration settings to confirm that backup to locally connected systems has been disabled. Disabling backup to locally connected systems is validated by the validation procedure in 'Disable USB mass storage'. Review device configuration settings to confirm that USB file transfer has been disallowed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android user restrictions' group, verify that 'disallow USB file transfer' is selected. Connect the Samsung Android device to a non-Organization network-managed PC with a USB cable. On the PC, browse the mounted Samsung Android device and verify that it does not display any folders or files. If on the MDM console 'disallow USB file transfer' is not selected, or the PC can mount and browse folders and files on the Samsung Android device, this is a finding.	

ID: 027	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not allow backup of [all applications, configuration data] to remote systems.	

ID: 027	PASS [ ]	FAIL [ ]
Procedimiento	Configure the Samsung Android to disable backup to remote systems (including commercial clouds). On the MDM console, for the device, do the following: 1. In the 'Android device owner' group, unselect 'enable backup service'. 2. In the 'Knox restrictions' group, unselect 'allow google accounts auto sync'. 3. Add all preinstalled public cloud backup system apps to the system application disable list if not already configured.	
Validación	Review device configuration settings to confirm that backup to a remote system has been disabled. This procedure is performed on the MDM Administration console and the Samsung device. On the MDM console, for the device, do the following: 1. In the 'Android device owner', verify that 'enable backup service' is not selected. 2. In the 'Knox restrictions' group, verify that 'allow google accounts auto sync' is not selected. 3. Verify that the system application disable list contains all preinstalled cloud backup system apps. On the Samsung Android device: 1. Open Settings. 2. Tap 'Accounts and backup'. 3. Tap 'Backup and restore'. 4. Verify that 'Backup service not available' is listed. 5. Tap back and tap 'Accounts'. 6. Tap a listed Google account. 7. Tap 'Sync account' and verify that all sync options are disabled and cannot be enabled. 8. Review the apps on the 'Personal' App screen and confirm that none of the cloud backup system apps are present. If on the MDM console 'enable backup service' is selected or 'allow google accounts auto sync' is selected, or on the Samsung Android device 'Backup service not available' is not listed, 'sync options' are enabled for a Google Account, or a 'cloud backup' system app is present on the 'Personal' App screen, this is a finding.	

ID: 028	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to disable developer modes.	
Procedimiento	Configure Samsung Android to disallow debugging features. On the MDM console, for the device, in the 'Android user restrictions' group, select 'disallow debugging features'.	

ID: 028	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that debugging features are disallowed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android user restrictions' group, verify that 'disallow debugging features' is selected. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'About phone'. 3. Tap 'Software information'. 4. Tap 'Build number'. 5. Verify that the message 'Unable to perform action' is displayed. If on the MDM console 'disallow debugging features' is not selected, or on the Samsung Android device the 'Unable to perform action' message is not displayed, this is a finding.	

ID: 029	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable authentication of personal hotspot connections to the device using a preshared key.	
Procedimiento	Configure Samsung Android to disallow unsecured hotspots. On the MDM console, in the Knox Wifi restrictions, unselect 'allow unsecured hotspot'.	
Validación	Review device configuration to confirm that unsecured hotspots are disallowed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Knox Wifi' group, verify that 'allow unsecured hotspot' is not selected. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Connections'. 3. Tap 'Mobile Hotspot and Tethering'. 4. Tap 'Mobile Hotspot'. 5. Tap Overflow menu (three vertical dots). 6. Tap 'Configure Mobile Hotspot'. 7. Tap 'Open in Security drop down'. 8. Verify that 'Save' is disabled. If on the MDM console 'allow unsecured hotspot' is selected, or on the Samsung Android device an Open Mobile Hotspot configuration can be saved, this is a finding.	

ID: 030	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable encryption for data at rest on removable storage media or alternately, the use of removable storage media must be disabled.	
Procedimiento	Configure Samsung Android to disallow mount of physical storage media or enable Knox external storage encryption. If the mobile device does not support removable media, this guidance is not applicable. Do one of the following: - Method #1: Disallow mounting of physical storage media. - Method #2: Enable external storage encryption. **** Method #1: On the MDM console, for the device, in the 'Android user restrictions' group, select 'disallow mount physical media'. **** Method #2: On the MDM console, for the device, in the 'Knox encryption' group, select 'enable external storage encryption'.	
Validación	Review device configuration settings to confirm that mounting of physical storage media is disallowed or Knox external storage encryption is enabled. If the mobile device does not support removable media, this procedure is not applicable and is not a finding. This procedure is performed on both the MDM Administration console and the Samsung Android device. Confirm if Method #1 or Method #2 is used at the Samsung device site and follow the appropriate procedure. **** Method #1: On the MDM console, for the device, in the 'Android user restrictions' group, verify that 'disallow mount physical media' is selected. On the Samsung Android device, verify that a MicroSD card cannot be mounted. If on the MDM console 'disallow mount physical media' is not selected or a MicroSD card can be mounted by the Samsung Android device, this is a finding. **** Method #2: On the MDM console, for the device, in the 'Knox encryption' group, verify that 'enable external storage encryption' is selected. On the Samsung Android device, verify that a MicroSD card must be encrypted before use. If on the MDM console 'enable external storage encryption' is not selected, or a MicroSD card can be used on the Samsung Android device without first being encrypted, this is a finding.	

ID: 031	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable Certificate Revocation List (CRL) status checking.	

ID: 031	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to enable CRL checking for all apps. On the MDM console, for the device, in the 'Knox certificate' group, configure 'revocation check' to 'enable for all apps'. Refer to the MDM documentation to determine how to configure revocation checking to 'enable for all apps'. Some may, for example, allow a wildcard string: '*' (asterisk).	
Validación	Review device configuration settings to confirm that CRL checking is enabled for all apps. This procedure is performed on the MDM Administration console only. On the MDM console, for the device, in the 'Knox certificate' group, verify that 'revocation check' is configured to 'enable for all apps'. If on the MDM console 'revocation check' is not configured to 'enable for all apps', this is a finding.	

ID: 032	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must have the Organization root and intermediate PKI certificates installed.	
Procedimiento	Configure Samsung Android to install Organization root and intermediate certificates. On the MDM console, for the device, in the 'Android certificate' group, use 'install a CA certificate' to install the Organization root and intermediate certificates.	
Validación	Review device configuration settings to confirm that the Organization root and intermediate PKI certificates are installed. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android certificate' group, verify that the Organization root and intermediate PKI certificates are listed. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Biometrics and security'. 3. Tap 'Other security settings'. 4. Tap 'View security certificates'. 5. Verify the Organization root and intermediate certificates are listed under the 'Personal' list in both the 'System' and 'User' tabs. If on the MDM console the Organization root and intermediate certificates are not listed in the 'Android certificate' group, or on the Samsung Android device 'View security certificates' does not list the Organization root and intermediate certificates, this is a finding.	

ID: 033	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to display the Organization advisory warning message at startup or each time the user unlocks the device.	

ID: 033	PASS [ ]	FAIL [ ]
Procedimiento	Configure the Organization warning banner by either of the following methods: - Method #1: Place the Organization warning banner text in the user agreement signed by each Samsung device user. - Method #2: Configure Samsung Android to display the Organization-mandated warning banner text. Use either Method #1 (preferred) or Method #2. **** Method #1: Include the Organization warning banner text in the user agreement that will be signed by each Samsung device user. **** Method #2: On the MDM console, for the device, in the 'Knox banner' group, configure the 'banner text' with the Organization-mandated warning banner text. Note: On some MDM consoles, the Knox banner is automatically enabled while the Samsung Android device is enrolled. In this case, the above guidance is not applicable.	
Validación	Confirm if Method #1 or Method #2 is used at the Samsung device site and follow the appropriate procedure. **** Method #1: Review the signed user agreements for several Samsung device users and verify that the agreement includes the required Organization warning banner text. If the required Organization warning text is not included in all reviewed signed user agreements, this is a finding. **** Method #2: This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Knox banner' group, verify that the 'banner text' is configured with the required Organization warning banner text On the Samsung Android device, verify that after a reboot the required Organization warning banner text is displayed. If on the MDM console the 'banner text' is not configured with the required Organization warning banner text, or after a reboot the required Organization warning banner text is not displayed on the Samsung Android device, this is a finding.	

ID: 034	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android devices must have the latest available Samsung Android operating system installed.	
Procedimiento	Install the latest released version of the Samsung Android operating system on all managed Samsung devices.	

ID: 034	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that the most recently released version of Samsung Android is installed. This procedure is performed on both the MDM console and the Samsung Android device. In the MDM management console, review the version of Samsung Android installed on a sample of managed devices. This procedure will vary depending on the MDM product. On the Samsung Android device, to see the installed operating system version: 1. Open Settings. 2. Tap 'About phone'. 3. Tap 'Software information'. On the Samsung Android device, to confirm that the installed operating system is the latest released version: 1. Open Settings. 2. Tap 'Software updates'. 3. Tap 'Check for system updates'. 4. Verify that 'No update is necessary at this time' is displayed. If the installed version of the Android operating system on any reviewed Samsung devices is not the latest released by the wireless carrier, this is a finding.	

ID: 035	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable the Online Certificate Status Protocol (OCSP).	
Procedimiento	Configure Samsung Android to enable OCSP checking for all apps. On the MDM, for the device, in the 'Knox certificate' group, configure 'OCSP check' to 'enable for all apps'. Refer to the MDM documentation to determine how to configure OCSP checking to 'enable for all apps'. Some may, for example, allow a wildcard string: '*' (asterisk).	
Validación	Review device configuration settings to confirm that OCSP checking is enabled for all apps. This procedure is performed on the MDM Administration console only. On the MDM console, for the device, in the 'Knox certificate' group, verify that 'OCSP check' is configured to 'enable for all apps'. If on the MDM console 'OCSP check' is not configured to 'enable for all apps', this is a finding.	

ID: 036	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to not enable Microsoft Exchange ActiveSync (EAS) password recovery. This requirement is not applicable if not using Microsoft EAS.	
Procedimiento	Configure Samsung Android to not enable Microsoft EAS password recovery. The Organization mobile service provider should verify that the Exchange server is configured to disable Microsoft EAS password recovery.	

ID: 036	PASS [ ]	FAIL [ ]
Validación	Verify that the Microsoft EAS password recovery has been disabled on the Exchange server. If on the Microsoft EAS server 'password recovery' is not disabled, this is a finding.	

ID: 037	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to set the password history with a length of 0.	
Procedimiento	Configure Samsung Android to set the password history with a length of '0'. On the MDM console, for the device, in the 'Android password constraints' group, set 'password history length' to '0'.	
Validación	Review device configuration settings to confirm that the password history is set to a length of '0'. This procedure is performed on the MDM console only. On the MDM console, for the device, in the 'Android password constraints' group, verify that 'password history length' is set to '0'. If on the MDM console 'password history length' is not set to '0', this is a finding.	

ID: 038	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enforce that Secure Startup is enabled. This requirement is Not Applicable (NA) to Galaxy S10 (or newer) devices.	
Procedimiento	Configure Samsung Android to enable Secure Startup. This guidance is only applicable to devices prior to Galaxy S10. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Biometrics and security'. 3. Tap 'Other security settings'. 4. Tap 'Secure startup'. 5. Tap option 'Require password when device powers on'. 6. Tap 'Apply'. 7. Enter the current password.	

ID: 038	PASS [ ]	FAIL [ ]
Validación	Review device configuration settings to confirm that Secure Startup is enabled. This procedure is performed on the Samsung Android device prior to Galaxy S10 only. This setting cannot be managed by the MDM administrator and is a User-Based Enforcement (UBE) requirement. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Biometric and security'. 3. Tap 'Other security settings'. 4. Tap 'Secure startup'. 5. Verify that 'Require password when device powers on' is already selected and 'Do not require' is not selected. If on the Samsung Android device 'Do not require' is selected, this is a finding.	

ID: 039	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enable a screen-lock policy that will lock the display after a period of inactivity.	
Procedimiento	Configure Samsung Android to enforce a screen-lock policy that will lock the display after a period of inactivity, with a lock type that is configured with a minimum password quality. On the MDM console, for the device, in the 'Android password constraints' group, set 'minimum password quality' (or password type) to 'alphanumeric'.	
Validación	Review device configuration settings to confirm that the device uses a screen-lock policy that will lock the display after a period of inactivity and that the lock type is configured with a minimum password quality. This procedure is performed on both the MDM Administration console and the Samsung Android device. On the MDM console, for the device, in the 'Android password constraints' group, verify that the 'minimum password quality' is 'alphanumeric'. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap 'Lock screen'. 3. Tap 'Screen lock type'. 4. Verify that 'Swipe, Pattern, PIN, and None' cannot be enabled. If on the MDM console 'minimum password quality' is not set to 'alphanumeric', or on the Samsung Android device the user can select a screen lock type other than 'password', this is a finding.	

ID: 040	PASS [ ]	FAIL [ ]
Requerimiento	Samsung Android must be configured to enforce that Strong Protection is enabled. This requirement is Not Applicable (NA) for devices older than Galaxy S10.	

ID: 040	PASS [ ]	FAIL [ ]
Procedimiento	Configure Samsung Android to enable Strong Protection. This guidance is only applicable to Galaxy S10 (or newer) devices. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap "Biometrics and security". 3. Tap "Other security settings". 4. Tap "Strong Protection". 5. Tap to enable. 6. Enter the current password.	
Validación	Review device configuration settings to confirm that Strong Protection is enabled. This procedure is performed on the Samsung Android Galaxy S10 (or newer) devices only. This setting cannot be managed by the MDM administrator and is a User-Based Enforcement (UBE) requirement. On the Samsung Android device, do the following: 1. Open Settings. 2. Tap "Biometric and security". 3. Tap "Other security settings". 4. Verify "Strong Protection" is enabled. If on the Samsung Android device "Strong Protection" is disabled, this is a finding.	

ANEXO III: TEST DEVICE POLICY CONTROL (TEST DPC)

81. 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.

82. **El Administrador IT de la organización solamente debe utilizar esta aplicación en un dispositivo destinado a test y nunca en un despliegue real.**[3]

83. 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

84. 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.

85. 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

[3] Se puede encontrar información adicional en el siguiente enlace: https://github.com/googlesamples/android-testdpc

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.

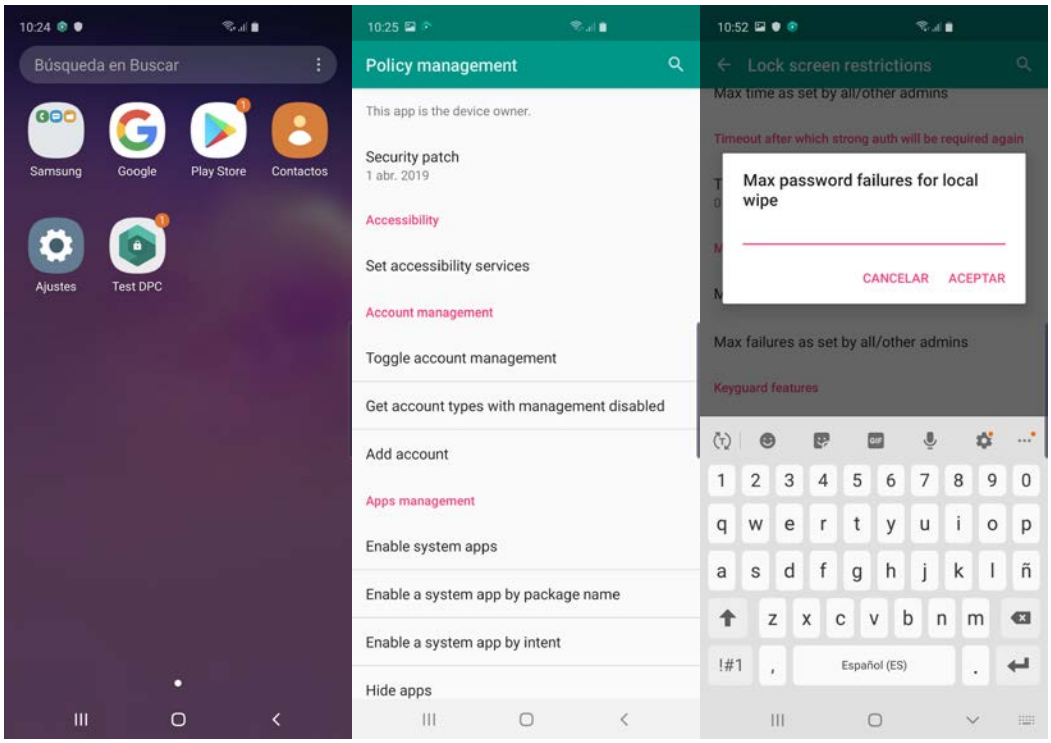

Figura 3