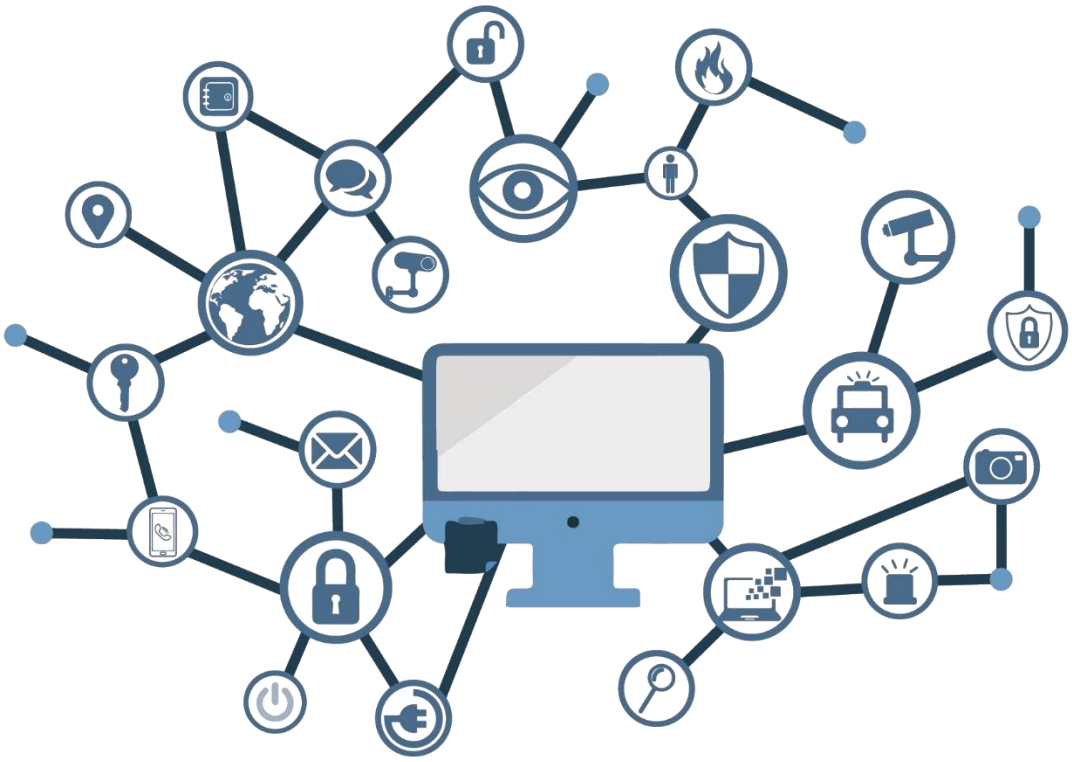
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1604

Configuración segura de dispositivos Samsung Galaxy S9 con Android 8



Julio de 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.07.12 16:24:31 +02'00'

NIPO: 083-19-054-4

Fecha de Edición: Julio de 2019.
Samsung Electronics ha participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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. Para desplegar y mantener un sistema seguro basado en dispositivos móviles será necesario disponer de bloques funcionales adicionales:
    - Dispositivos móviles, con las capacidades y la configuración apropiada
    - Soluciones de gestión de dispositivos móviles (EMM-Enterprise Mobile Management / MDM-Mobile Device Management1) aprobadas y que dispongan de las funcionalidades necesarias.
    - Redes de comunicaciones, de diferentes tecnologías.
    - 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, etc.
    - Usuarios de la organización, responsables del uso diario de los dispositivos.
2. 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.
3. Este documento se centra en las capacidades y configuraciones necesarias en el dispositivo móvil Samsung, incorporándose en algunos momentos restricciones o configuraciones recomendadas para el resto de elementos del sistema.
4. Se ha elaborado pensando en primer lugar en el equipo de administradores de dispositivos móviles de la organización que realiza el despliegue, y por tanto, contiene las directrices para la configuración y despliegue de un sistema de comunicaciones móviles con dispositivos Samsung, focalizada en la plataforma de seguridad que reside dentro del dispositivo (Samsung Knox). Se incluye como último capítulo un conjunto de directrices que pueden ser de utilidad para el usuario final.
5. 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.
6. La entidad responsable del despliegue debe garantizar que los elementos usados en conjunción con el dispositivo Samsung que contiene la plataforma

[1] Las siglas EMM, MDM, MAM, MEM que, con matices, se refieren a herramientas para la gestión de dispositivos móviles. En los documentos elaborados por el CCN, este conjunto de herramientas y productos quedan enmarcados dentro de la categoría MDM.

Knox son adecuados para su integración y permiten configurar el dispositivo según la configuración recomendada en este documento. Esto significa que la solución EMM seleccionada debe permitir configurar la plataforma Knox (el dispositivo) acorde este documento, así como los clientes VPN de terceras partes integrables con Knox dentro del dispositivo.

7. En el presente documento se hace referencia a un determinado dispositivo o terminal móvil que es considerado Plataforma Cualificada por el Centro Criptológico Nacional (CCN). Como plataforma se entiende el conjunto de hardware y software residente en dicho hardware que sirven como base para el despliegue de un sistema de comunicaciones móviles. En términos más sencillos: el dispositivo móvil que se despliega.

8. El documento tiene asimismo como hipótesis la utilización de un despliegue en el que la propiedad de los dispositivos móviles es de la organización, aunque se permita en mayor o menor medida su uso personal por parte de los usuarios finales. Se definen dos modelos básicos de despliegue autorizados, el modelo de despliegue donde al administrador TIC de organización controla políticas generales en todo el dispositivo y ejerce un control más riguroso sobre el Contenedor de Trabajo/Workpace, denominado habitualmente COPE (*Corporate Owned, Personally Enabled*), y el modelo en el que todo el dispositivo está orientado a trabajo y se limita completamente el uso personal, conocido como COBO (*Corporate Owned Business Only)* donde no se cree un contenedor, ya que el dispositivo en su conjunto está segurizado y dedicado a uso profesional.

9. En caso de que la organización quiera utilizar otros modelos de despliegue, como BYOD (Bring Your Own Device), en el que el usuario incorpora su propio terminal y es la organización la que instala un contenedor donde exclusivamente aplica políticas de seguridad, se debe analizar y asumir los condicionantes tanto técnicos como legales de manera previa a su implantación, en cualquier caso, este modelo de despliegue (BYOD) no se autoriza para el manejo de información corporativa y, por tanto, no es objeto de este documento.

10. Los dispositivos Samsung que incluyen la versión Knox 3.0 y superiores incorporan la integración con Android Enterprise, mejorándola con las APIs extendidas de Samsung Knox.

11. En la arquitectura de Android Enterprise, el modelo COBO se implementa con el modo DO (Device Owner), donde la aplicación Device Owner controla todo el dispositivo. El modelo COPE se implementa con el modo COMP (Corporate Owned Managed Profile), el cual incluye una aplicación Device Owner, y un Work Profile que contiene una aplicación PO (Profile Owner) para su gestión. Finalmente el modelo BYOD con el modo Work Profile exclusivametne, donde la aplicación PO (Profile Owner) se encuentra dentro del Work Profile y no existe gestión del área personal del dispositivo.

12. En este documento se utiliza el término contenedor para referirse al contenedor lógico en versiones de Knox menores de 3.0 o al Work Profile de Android Enterprise en versiones iguales o superiores, ya que conceptualmente para el Administrador TIC de la organización es el mismo concepto. El término utilizado por Samsung para contenedor Work Profile es Knox Workspace.
13. Los dispositivos Samsung con Android 8 son compatibles con versiones anteriores de Knox, pudiendo utilizar soluciones EMM que no soporten la arquitectura Android Enterprise.

1.1 RESUMEN GENERAL

14. El principal objeto de trabajo en este documento es el sistema operativo para dispositivos móviles basado en Android 8 con modificaciones orientadas a incrementar el nivel de seguridad que se ofrece a los usuarios finales y a las Organizaciones, dicho sistema operativo, cuando se asocia con un hardware concreto, pasa a ser considerado una plataforma. A lo largo del documento se utilizaran las denominaciones plataforma, dispositivo (teléfono/tableta) indistintamente.
15. La plataforma está diseñada y construida para utilizarse como parte de una solución de comunicación y gestión móvil que una organización pone a disposición de su personal con el fin principal de realizar tareas relacionadas con su desempeño profesional.
16. En ocasiones se hace referencia a Knox, que en este contexto debe ser entendido como el conjunto del sistema Android y las modificaciones/mejoras de seguridad integradas en el mismo por Samsung. Los términos Android 8 y Knox se referirán a la misma plataforma.
17. En un despliegue operativo, la plataforma se combinará necesariamente con una solución de gestión de dispositivos móviles (EMM) que permita a la organización supervisar, controlar y administrar los dispositivos móviles bajo su Autoridad Operativa. Por otra parte, facilita una comunicación segura a través de una red privada virtual (VPN). Esta colaboración permite ofrecer un entorno móvil seguro que puede ser administrado de manera centralizada por la organización.
18. El kit de desarrollo de software (SDK) de Samsung toma como base, el modelo de seguridad de Android existente y amplía el conjunto de configuraciones de seguridad. La capacidad para establecer estas políticas se apoya igualmente en las prestaciones de la solución de EMM. El software que se instala en el dispositivo móvil y que utiliza el SDK de Samsung se denomina Agente, el cuál es parte de la solución EMM integrada con los dispositivos a desplegar, siendo responsabilidad del administrador TIC de la organización garantizar que dicha solución EMM sea capaz de configurar el dispositivo Samsung acorde a los requerimientos de este documento, y siendo competencia de la empresa

proveedora de la solución EMM la correcta implementación de las llamadas al API del software SDK proporcionado por Samsung.

19. Se denomina EDM (Enterprise Device Management), al conjunto de funcionalidades y APIs implementadas en el dispositivo para su uso por parte del administrador TIC de la organización donde se realice el despliegue. La gestión que realiza el administrador TIC, pasa por la configuración de la consola de solución EMM que se elija, siendo responsabilidad de dicha solución EMM la de soportar las características de Samsung Knox necesarias.

20. En este documento se identifica como funcionalidad/política EDM a toda la implementada en el dispositivo mediante API, y EMM a la solución de gestión que ofrece toda o parte de la funcionalidad EDM al administrador TIC a través de su consola de configuración.

2 PRESTACIONES EVALUADAS

21. La plataforma a desplegar ofrece una amplia variedad de prestaciones de seguridad así como prestaciones básicas dentro de la evaluación. Entre estas encontramos las siguientes:

FUNCIÓN DE SEGURIDAD	DESCRIPCIÓN
PROTECCIÓN DE DATOS DEL DISPOSITIVO.	**On Device Encryption (ODE, Cifrado de datos en el dispositivo).** La plataforma permite cifrar los datos del dispositivo mediante AES 256. **Cifrado de los soportes de almacenamiento extraíbles.** La plataforma puede cifrar todos los archivos almacenados o que ya residan en soportes de almacenamiento extraíbles conectados al dispositivo. **Protección de datos confidenciales.** La plataforma permite almacenar de forma segura datos entrantes considerados confidenciales, de modo que no puedan descifrarse sin que el usuario haya iniciado sesión.
GESTIÓN DE APLICACIONES.	**Restricciones de recursos de aplicaciones.** Todas las aplicaciones se ejecutan dentro de un entorno controlado que limita las aplicaciones para que solo accedan a los datos y recursos autorizados.
CONTROL DE ACCESO.	**Bloqueo de dispositivo.** La plataforma puede configurarse para que se bloquee automáticamente después de un periodo de inactividad predefinido (de 1 a 60 minutos) y se limite el acceso a las funciones del dispositivo, salvo a aquellas para las que se ha concedido autorización expresa, como las llamadas de emergencia. **Eliminación local de datos.** La plataforma permite eliminar datos o claves de cifrado de un dispositivo después de que se agoten un número de intentos de autenticación establecido por el administrador. **Credenciales Complejas.** La plataforma puede aplicar políticas de contraseñas corporativas al exigir que los usuarios deban cumplir en las contraseñas del dispositivo el nivel de complejidad definido. **Uso de Biometría.** La plataforma puede aplicar autenticación biométrica para el acceso al dispositivo complementariamente a la política de contraseñas, restringiendo el acceso basado en intentos fallidos.

FUNCIÓN DE SEGURIDAD	DESCRIPCIÓN
	Acceso con privilegios. La plataforma puede configurarse para limitar el acceso del usuario móvil a funciones con privilegios, como las configuraciones del dispositivo. **Control de punto de acceso.** La plataforma puede configurarse para actuar como un punto de acceso con el que compartir el acceso a Internet con otros dispositivos. **Ajustes de red inalámbrica.** La configuración de red inalámbrica de la plataforma puede especificarse indicando requisitos o redes precargadas.
GESTIÓN DE DISPOSITIVOS DE LA ORGANIZACIÓN.	**Eliminación remota de datos.** Un administrador de la organización puede enviar un mensaje a la plataforma para eliminar todos los datos del almacenamiento local y de la tarjeta SD. **Política de seguridad.** La plataforma puede configurarse mediante una solución de gestión de dispositivos móviles que sea compatible con el SDK de Samsung. La organización es responsable de seleccionar la solución EMM apropiada para la implementación de las configuraciones seleccionadas. **Auditoría.** La plataforma puede supervisar y generar registros relacionados con eventos relevantes para la seguridad que se produzcan en el dispositivo.

Tabla 1: Prestaciones de seguridad evaluadas

2.1 API DE GESTIÓN DE KNOX

22. Samsung ofrece un amplio conjunto de interfaces de programación de aplicaciones (API) para mantener el control total de un dispositivo Samsung perteneciente al despliegue de una organización. Para obtener más información sobre las API y funciones específicas que ofrece Samsung, puede consultar la información completa en los siguientes enlaces:

https://seap.samsung.com/api-references/android/reference/packages.html

3 DISPOSITIVOS EVALUADOS

23. Las Plataformas Cualificadas por el Centro Criptológico Nacional (CCN) son modelos Samsung Galaxy con sistema operativo Android 8 (Oreo) de Samsung de los siguientes números de modelo y versiones:

NOMBRE	Modelo	Android	kernel	compilación
GALAXY S9+	SM-G965F	8.0	4.9.59	R16NW
GALAXY S9	SM-G960F	8.0	4.9.59	R16NW

Tabla 2: Modelos evaluados

24. Los modelos SM-G965F y SM-G960 son iguales en todas sus características, salvo en tamaño del display utilizado En la evaluación se ha utilizado el modelo SM-G965F.

25. En el siguiente listado se incluyen otros dispositivos Samsung a los que se puede aplicar las políticas y configuraciones recogidas en este documento. Estos dispositivos han superado evaluaciones Common Criteria (CC) con anterioridad, aunque no han sido evaluados por el CCN en la configuración incluida en este documento.

NOMBRE	Modelo	Android	kernel	compilación
GALAXY S8	SM-G950F	8.0	4.4.13	R16NW
GALAXY S8+	SM-G955F	8.0	4.4.13	R16NW
GALAXY Note8	SM-N950F	8.0	4.4.13	R16NW

Tabla 3: Modelos compatibles con la configuración

26. La información acerca de las Actualizaciones de Seguridad de todos los dispositivos mencionados se puede encontrar en la siguiente página web:

https://security.samsungmobile.com/

4 PROCESO DE DESPLIEGUE

27. 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 las soluciones de EMM escogidas.
    - Modelos de propiedad permitidos en la organización (COPE, COBO).

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

5 ARQUITECTURA DEL SISTEMA DE COMUNICACIONES MÓVILES

29. Uno de los primeros pasos para desplegar dispositivos Samsung es seleccionar una solución de gestión de dispositivos móviles (EMM) y una Arquitectura de Red apropiadas. Estas dos elecciones pueden hacerse en cualquier orden, en función de las preferencias de la organización, pero deben ser coherentes.
30. Existen tres arquitecturas principales para la herramienta de gestión:
    - despliegue basado en la organización (on-premise),
    - despliegue basado en la nube(cloud), y
    - enfoque híbrido.
31. El único modelo de arquitectura avalado por el CCN para su utilización requiere que tanto los dispositivos como las herramientas de gestión EMM estén bajo control real de la organización, utilizando despliegues on-premise.

5.1 DESPLIEGUE BASADO EN LA ORGANIZACIÓN

32. En este modelo de arquitectura, el entorno de la organización debe ofrecer todos los servicios necesarios para operar y gestionar los dispositivos. Entre los componentes básicos de este modelo encontramos los siguientes:

Herramienta de gestión de dispositivos móviles (EMM)

33. La herramienta de gestión de dispositivos móviles (EMM) ofrece seguridad, supervisa, gestiona y presta soporte a los dispositivos móviles en uso en las organizaciones. Al controlar y proteger los datos y los ajustes de configuración de todos los dispositivos Android pertenecientes a la red corporativa se reducen los riegos de seguridad de la organización. Los dispositivos móviles de Samsung ofrecen una amplia compatibilidad con soluciones de distintos fabricantes.

Terminación de túnel VPN

34. Con el fin de evitar el acceso no autorizado a los recursos de la organización, se debe utilizar un túnel VPN entre los dispositivos Android gestionados y el entorno de la organización. La conexión debe estar basada en certificados implementados en los dispositivos. El método ideal es implementar una autenticación mutua, que implica que tanto los dispositivos como el punto de terminación del túnel y puerta de enlace al entorno de la organización se autentican mediante un certificado.
35. La autenticación mutua permite evitar que los dispositivos inicien sesión en una red de la organización no autorizada y, al mismo tiempo, impiden que dispositivos que no sean de confianza accedan al entorno de la organización sin autorización.

36. Si se detectan certificados no válidos, el túnel finalizará, no debiendo permitirse en ningún caso el establecimiento de conexiones sin contar con certificados validados.

37. Por otra parte, una sesión de VPN inactiva debe finalizar una vez transcurrido un determinado intervalo de tiempo, seleccionado por la organización.

a) Servicios de directorio

38. Se deben configurar servicios de directorio para almacenar, organizar y ofrecer acceso a la información que contiene un directorio.

Aplicaciones Corporativas

39. Las aplicaciones profesionales permiten a los usuarios de la organización cumplir o acceder a determinadas tareas profesionales en función de los requisitos. Esto podría incluir herramientas de gestión, servicios de contabilidad y soluciones o software de gestión de contactos.

40. Dichas aplicaciones deben ser seleccionadas y positivamente autorizadas por los administradores del sistema.

Servicios de certificados

41. Debe implementarse un servicio de certificados que gestione todas las necesidades de certificados en todo el entorno de la organización. Esto incluye la emisión de los nuevos certificados de usuarios de dispositivos necesarios para facilitar unas comunicaciones seguras mediante la VPN.

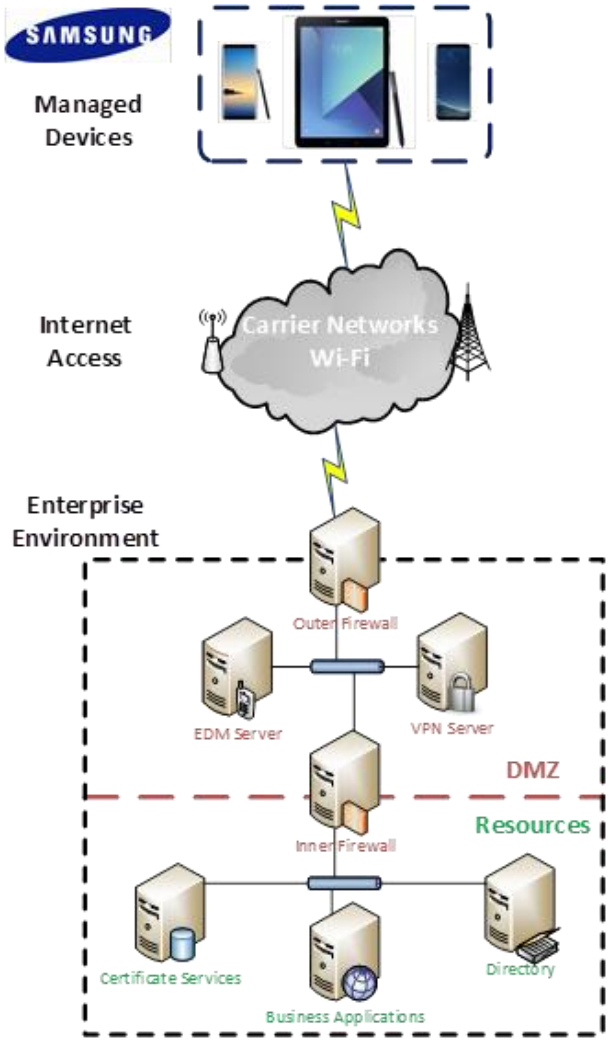


Figura 1: Visión General del Entorno de movilidad profesional

Nota: La configuración recomendada de los dispositivos gestionados (Managed Devices), es la parte tratada en esta guía, sin menoscabo de la necesaria valoración y correcta configuración de otras partes que componen el sistema y dibujan el despliegue en su totalidad. Para mayor información en la arquitectura recomendada, acudir al documento CCN-STIC dedicado a Comunicaciones Móviles Seguras.

6 INSTALACIÓN SEGURA DE DISPOSITIVOS DE USUARIO DE ANDROID DE SAMSUNG

42. Esta sección contiene información sobre cómo un administrador de dispositivos móviles de la organización puede instalar un dispositivo Samsung de forma segura.

43. Para lograr un despliegue de dispositivos Samsung adecuado para organizaciones, que trabajan con información que requiera protección según la legislación vigente, los administradores deberán:

    - Ejecutar el proceso de despliegue de dispositivo que se describe a continuación; y
    - Crear perfiles y configuraciones de seguridad de EMM para los dispositivos, de acuerdo con las directrices incluidas en el este documento y asociar dichos perfiles a los dispositivos.

6.1 SELECCIÓN DE LA SOLUCIÓN EMM

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

45. Para habilitar funcionalidades tales como el borrado remoto del dispositivo, la solución EMM 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 EMM pueda comunicarse con el Agente EMM instalado en el dispositivo móvil. Dicha conexión a Internet deberá realizarse siguiendo las instrucciones de despliegue de la solución EMM 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.

46. 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. La recomendación en este punto es que la organización realice todas las comunicaciones protegidas por al menos una capa de cifrado, encaminándose dentro de una VPN evaluada y apta para el nivel de seguridad aplicable siempre que sea posible.

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

6.2 PROCESO DE DESPLIEGUE DE DISPOSITIVO

48. Como se señaló anteriormente, la implementación segura de dispositivos en la organización depende de varios componentes más allá del propio dispositivo móvil. Se espera que, en el entorno de la organización, la solución EMM y otros servicios requeridos se instalen y configuren de manera segura de acuerdo con los requisitos de seguridad de la misma.

49. Una vez que el sistema EMM está instalado y disponible, es posible comenzar a aprovisionar dispositivos de usuarios. El proceso de aprovisionamiento preparará los dispositivos para la implementación de configuración y políticas de seguridad, lo que permitirá que el dispositivo se coloque en una configuración cualificada.

50. El dispositivo móvil debe estar inscrito en el servidor de EMM para permitir la gestión remota a través del EMM. **La inscripción se realiza instalando la aplicación del Agente de EMM en el dispositivo**. Existen varios métodos y configuraciones para hacer esto dependiendo del escenario de implementación. Se debe seguir la documentación de la solución EMM para la implementación.

51. Una vez que un dispositivo se ha inscrito en el EMM, se pueden establecer otras configuraciones opcionales, según la política de seguridad de la organización.

52. La siguiente lista proporciona algunas de las configuraciones adicionales más comunes que se pueden realizar en un dispositivo móvil:

    a) Aprovisionar los certificados, proporcionando los certificados de cliente por medio de un servidor de EMM inscrito a nivel local. Los certificados que normalmente se despliegan son:

        i. un certificado de autoridad de certificación (CA) de la organización (empleado para validar los certificados de servidor que presenta el terminal de VPN y el proxy inverso);

        ii. un certificado de cliente Wi-Fi (para la autenticación EAP-TLS Wi-Fi AP)

        iii. un certificado de cliente VPN (para la autenticación en el terminal de VPN de la organización);

        iv. un certificado de cliente SSL (para la autenticación en el proxy inverso para servicios de Intranet).

    b) Instalar las aplicaciones autorizadas por la organización[2].

[2] La organización debe articular un proceso de incorporación de aplicaciones software a los sistemas y dispositivos de la organización que garantice la seguridad de la información gestionada. Dicho proceso debe contar con una aprobación/denegación expresa de incorporación por parte del Autoridad en materia de Seguridad del sistema.

c) Asegurarse de que solo se instalen y habiliten aplicaciones de confianza en el dispositivo (deshabilitando las aplicaciones innecesarias, incluidas los repositorios públicos, no gestionados por la organización).

d) Configurar los ajustes de seguridad en el dispositivo según lo definido en este documento.

e) Configurar el cliente VPN para conectarse al terminal de VPN de la organización, utilizando el certificado de cliente específico del dispositivo que se haya cargado en dicho dispositivo. Habilitar la VPN como «Siempre Activa/Always On».

f) Configurar el cliente de correo electrónico para que se conecte al servidor de la organización con la autenticación del certificado de cliente.

6.3 PARÁMETROS Y CAPACIDADES RECOMENDADAS

53. En este apartado se incluyen los parámetros y capacidades sobre los que se establecerá una recomendación. Se utiliza como guía la enumeración de 12 requerimientos de seguridad de la sección 6.3.2 para que el sistema desplegado aproveche las capacidades de los dispositivos móviles y cumpla con las directrices de configuración del Centro Criptológico Nacional. Dichos requerimientos incluyen la configuración segura certificada Common Criteria más otras configuraciones, abarcando tanto ajustes específicos de Knox como generales de Android.

54. Deben seguirse las directrices incluidas en la solución de EMM seleccionada por la organización para configurar las opciones que se indican a continuación. Las clases o los métodos utilizados para configurar estos ajustes se incluyen a modo de referencia, y pueden emplearse para verificar si la solución de EMM atenderá sus necesidades.

55. El dispositivo (teléfono/tableta) Samsung con Android 8 proporciona opciones de configuración tanto para el dispositivo en su conjunto como específicamente referidas a un Contenedor. En las secciones 6.3.1 y 6.3.2.5 se proporciona detalle del concepto Contenedor aquí mencionado.

56. La organización que realiza el despliegue de terminales, especificará ajustes generales de seguridad a todo el dispositivo, creará un contenedor, donde se instalarán las aplicaciones corporativas y se configurará la seguridad. También se realizaran ajustes en relación con la interacción entre el contenedor y el resto del dispositivo.

57. Dado que el presente documento trata en todo momento sobre despliegues en los que los dispositivos son propiedad de la organización, la configuración de la parte “exterior al contenedor” debe ser también asumida y realizada de manera consciente por la misma. Esto será especialmente importante en aquellos casos en los que la información a gestionar por la organización requiera de protección, en base a la legislación vigente o a la valoración que la propia organización haya realizado durante la fase de Análisis de Riesgos.

58. Estas opciones de creación y uso de contenedores (espacio profesional del dispositivo, en contraste con el espacio "personal/no profesional"), son necesarias si se desean utilizar las funcionalidades del dispositivo en un entorno profesional.

6.3.1 CONFIGURACIONES CON Y SIN CONTENEDORES

59. En el modelo de despliegue COPE, se crea un contenedor en el dispositivo donde se aplicaran rigurosos controles, filtros y políticas, debido que será el área donde el usuario podrá acceder a aplicaciones y recursos corporativos. Los dispositivos Samsung incluyen la función integrada de crear contenedores independientes dentro del dispositivo que se habilitan por medio de las APIs incluidas en el sistema operativo Android de Samsung. Cuando se configura un contenedor Knox, este ofrece un área independiente en el dispositivo que puede tener sus propias aplicaciones y datos, a la que no puede accederse desde el área exterior al contenedor. Los contenedores Knox pueden utilizarse para separar aplicaciones distintas, como en el ya citado modelo COPE en los que una organización puede colocar sus datos en un contenedor independiente dentro de un dispositivo en el que se permite alojar información del usuario. En el caso de un despliegue COBO, no se generará ningún contenedor, siendo gestionado por el administrador TIC el dispositivo en su conjunto, bloqueando su uso personal.

60. La creación de contenedores permitiría su utilización en escenarios donde la propiedad del dispositivo sea del usuario final (BYOD). Sin embargo, dichos escenarios no se consideran en este análisis, por no estar autorizados estos escenarios para mantener una mínima garantía de seguridad y trazabilidad.

6.3.2 REQUERIMIENTOS DE SEGURIDAD

61. En este capítulo se propone una configuración basada en las 12 áreas de seguridad proporcionadas como un marco de seguridad ampliamente utilizado en despliegues de plataformas móviles para el teletrabajo en la administración y el sector público.

- Protección de los Datos en Tránsito
- Protección de los Datos en Reposo
- Política de Autenticación
- Arranque seguro del terminal
- Integridad de la plataforma y espacios de ejecución seguros para aplicaciones
- Lista Blanca de Aplicaciones
- Detección y prevención de Código Malicioso
- Cumplimiento efectivo de la Política de Seguridad
- Protección de la Interfaz Externa
- Política de Actualizaciones del Dispositivo
- Recopilación de eventos para su análisis en la organización

- Política de respuesta a incidentes

6.3.2.1 PROTECCIÓN DE LOS DATOS EN TRÁNSITO

62. Samsung Knox ofrece una amplia compatibilidad con VPN, tanto IPSec como SSL. La plataforma Knox ofrece un *framework* de VPN genérico, que permite que los proveedores software externos (terceras partes) ofrezcan sus clientes VPN como complementos a integrar en el dispositivo mediante una App (aplicación). La configuración del cliente VPN de la plataforma Knox debe realizarse mediante las políticas de EDM de Knox.

63. Un despliegue seguro requiere el uso de una VPN basada en IPSec y que utilice un método de autenticación basado en certificados.

64. En el momento de escribir este documento, la plataforma Knox admite la funcionalidad de VPN IPSec mediante la VPN de Android para Knox (*StrongSwan*) (también denominada «cliente VPN integrado») y otros clientes IPSec de diferentes fabricantes.

65. El *framework* VPN de Knox, entendido como la parte de la plataforma Knox donde se integran clientes VPN de terceros, y las API de gestión EDM permiten que las configuraciones VPN se puedan aplicar a todo el dispositivo, por contenedor o por aplicación.

66. El modo “por aplicación” permite que una solución de EMM seleccione aplicaciones (dentro y fuera del contenedor) para conectarse a la red con un perfil de VPN específico. Pueden añadirse todas las aplicaciones necesarias instaladas tanto dentro como fuera del contenedor. El uso de la VPN en el modo “por aplicación” garantiza que el tráfico procedente de todas las aplicaciones seleccionadas se transmita mediante la VPN. Las aplicaciones no tendrán acceso a la conectividad hasta que se conecte la VPN.

67. La otra opción es utilizar un cliente VPN integrado para todos los paquetes (aplicaciones) situados dentro del contenedor y otro cliente VPN, para los paquetes situados fuera del contenedor, lo que requiere dos conexiones VPN simultáneas. Esta configuración permitiría que el tráfico procedente de las aplicaciones teóricamente menos confiables se separase del de las aplicaciones del contenedor del Knox *Workspace* que trabajan con información perteneciente a la organización, que estará alojada siempre dentro del contenedor.

68. Cuando se configura la VPN en modo ”por aplicación” o ”por contenedor”, el establecimiento de túnel se realiza de forma automática, sin necesidad de que el usuario intervenga, y se establece inmediatamente después de que el *framework* se active, siempre que esté configurada en modo “*Always o*n/ Siempre encendido” o cuando las aplicaciones inicien actividad de red, siempre que esté configurada en modo ”*On demand*/ bajo demanda”, para ahorrar batería.

69. Si la VPN no está conectada, todo el tráfico saliente de la aplicación se bloqueará y no podrá abandonar el dispositivo. Cuando esté conectada, el tráfico se enviará mediante la VPN, según el modo de configuración de los dispositivos (VPN de dispositivo completo, contenedor, por aplicación, etc.). La solución de EMM aprovisiona los perfiles de VPN, que el usuario no puede deshabilitar ni modificar.

70. Estas funciones son de obligada utilización para cualquier despliegue que vaya a permitir a los usuarios finales manejar información propiedad de la organización desde sus dispositivos móviles, pues permiten que el tráfico del dispositivo se tunelice de forma automática sin interacción por parte del usuario en una configuración de tipo "*Always on*/ siempre encendido", lo que impide la filtración de datos, así como la supervisión y el filtrado del tráfico dentro de la red del cliente, si así se deseara.

71. Se recomienda el uso de la configuración de VPN "por aplicación" para todas las aplicaciones instaladas dentro del contenedor de Knox y todas las aplicaciones instaladas fuera del contenedor de Knox. De esta manera se garantiza que todo el tráfico procedente de las aplicaciones del usuario/organización se transmite mediante la VPN de la organización hasta la organización.

72. La flexibilidad de la solución de Samsung permite que los administradores configuren túneles de VPN separados para las aplicaciones situadas dentro y fuera del contenedor, de modo que se separe el tráfico de la organización y el personal (menos caracterizado y con menor priorización), pero que se siga pudiendo supervisar y controlar todo el tráfico procedente del dispositivo según sea necesario.

73. Esta es la configuración que ha sido evaluada y es la establecida para todos aquellos despliegues que vayan a manejar información propiedad de la organización o que la organización ha decidido que requiere de protección (por obligación legal o no).

6.3.2.2 PROTECCIÓN DE LOS DATOS EN REPOSO

74. La protección de datos en reposo es una parte fundamental de la solución de seguridad por capas Knox de Samsung.

75. El contenedor Knox (un entorno aislado para aplicaciones y datos de la organización, que se describirá en detalle más adelante) cuenta con su propio sistema de archivos con cifrado AES 256 y todos los datos que residen dentro del contenedor se cifran de forma predeterminada.

76. El contenedor Knox ofrece dos niveles de protección de datos en reposo:

    - **Datos protegidos**: los datos marcados como datos protegidos se encuentran cifrados cuando el dispositivo está apagado.
    - **Datos confidenciales**: los datos marcados como datos confidenciales se encuentran cifrados cuando el contenedor está en estado bloqueado.

77. Todos los dispositivos Knox de Samsung admiten, de forma predeterminada, protección DAR (*Data at Rest*) en el nivel «Datos protegidos». El cliente de correo electrónico nativo de Knox permite también utilizar la función SDP (*Sensitive Data Protection;* Protección de datos confidenciales) y cualquier aplicación puede beneficiarse del directorio "*Chamber*" que se encuentra dentro del contenedor, protegido por SDP, para proteger sus datos cuando el contenedor está en estado bloqueado y cuando el dispositivo esté apagado. Las aplicaciones de terceros también pueden utilizar el mecanismo SDP para almacenar archivos y beneficiarse del mismo nivel de protección al utilizar el SDK ISV de Knox, que ofrece un API para marcar archivos como confidenciales.

78. Fuera del contenedor Knox, protegiendo todo el dispositivo, el mecanismo ODE (*On Device Encryption*; Cifrado de datos en el dispositivo) de Samsung ofrece protección de datos en reposo para la partición de datos del usuario y, opcionalmente, en la tarjeta SD externa.

79. Los administradores pueden configurar una contraseña como la credencial desde la que derivar las claves de cifrado con la opción "*Secure Startup* (Inicio seguro)"en el menú de ajustes, o utilizar la contraseña predeterminada. Si se utiliza la contraseña predeterminada, no será necesario que el usuario introduzca ninguna contraseña. En el diseño del esquema de gestión de claves que proporciona el dispositivo, el descifrado de datos está vinculado a cada dispositivo, por el uso de la clave de hardware única del dispositivo, además de las claves derivadas de la contraseña.

80. La opción evaluada, y recomendada en esta guía para disponer de una Plataforma Cualificada (y cumplir igualmente los requisitos establecidos en la evaluación Common Criteria) es que se habiliten las opciones de "*Secure Startup* (Inicio seguro)" que vinculan la contraseña del usuario con las claves de cifrado.

81. Se ha implementado una solución completa de gestión de claves con la que atender las necesidades de los clientes de entornos en los que se gestione información sensible. Dicha solución incluye el uso de mecanismos basados en *TrustZone*[3], con claves de hardware únicas por dispositivo para proteger las claves de cifrado.

82. La plataforma Knox almacena valores criptográficos dentro de *TrustZone*, protegidos por el hardware, que la plataforma solo libera si se ha verificado la integridad de la plataforma durante el arranque. Si la integridad del dispositivo se considera comprometida (por ejemplo, tras detectar un kernel no oficial), los valores necesarios para derivar las claves de cifrado no se liberan y los datos protegidos o confidenciales del contenedor no podrán descifrarse.

83. En los dispositivos Samsung Galaxy con SO Android 8.0, la protección de ODE basada en el estado de integridad de la plataforma está habilitada de forma predeterminada.

[3] Para ampliar información sobre Trustzone: https://www.arm.com/products/silicon-ip-cpu

84. La recomendación es que las aplicaciones y los datos relativos a material propiedad de la organización, se almacenen siempre dentro del contenedor del Knox Workspace que proporciona una protección adicional sobre la ODE proporcionada por el dispositivo. Para la información que no sea propiedad de la organización, se puede utilizar el almacenamiento exterior al contenedor Knox, aunque en este caso la protección de la información será únicamente la proporcionada por Android.

85. El cliente de correo electrónico nativo de Knox se ha habilitado para utilizar la función SDP (*Sensitive Data Protection*; Protección de datos confidenciales) y las aplicaciones pueden beneficiarse del directorio «*Chamber*», protegido por SDP, para proteger sus datos cuando estén bloqueadas y cuando el dispositivo esté apagado.

6.3.2.3 POLÍTICA DE AUTENTICACIÓN

- **Usuario - Dispositivo**

86. En términos de autenticación del usuario en el dispositivo, los dispositivos compatibles con Samsung Knox ofrecen una serie de mecanismos de autenticación que el administrador puede imponer mediante la configuración realizada a través del EMM.

87. La autenticación del dispositivo se realiza desde la pantalla de bloqueo del dispositivo. Los mecanismos de autenticación de dispositivo disponibles son patrones, códigos PIN, contraseñas y métodos de autenticación biométrica, como el escaneo de huella dactilar o iris en dispositivos compatibles. El administrador puede exigir estos mecanismos mediante la política de EMM. Hay disponibles políticas con las que configurar los mecanismos de autenticación para que cumplan las políticas de la organización, como la longitud del código de acceso, la complejidad, la antigüedad, el historial, el número máximo de intentos erróneos, las políticas de contraseña permitida (políticas de secuencia de caracteres, número de caracteres que hay que cambiar al actualizar una contraseña, etc.) y muchas más.

88. El contenedor Knox *Workspace* de Samsung cuenta con un mecanismo de autenticación independiente. El contenedor debe disponer de un mecanismo de autenticación seleccionado y, al igual que ocurre con la autenticación del dispositivo, el administrador puede exigir el mecanismo que debe utilizarse. Entre los mecanismos de autenticación disponibles para el contenedor se incluyen patrones, códigos PIN, contraseñas, huellas dactilares, iris y mecanismos de autenticación de dos factores, que utilizan el escáner de huella dactilar o de iris como primer paso y el patrón, el código PIN o la contraseña como segundo paso del factor de autenticación.

89. Tal y como se describe en la sección de Protección de datos en reposo, si se ha habilitado ODE con la opción de bloqueo de pantalla y seguridad “Inicio seguro”, el usuario deberá autenticarse en el dispositivo utilizando su código

de acceso durante el arranque. El código de acceso se utiliza como parte del proceso de derivación de la clave para descifrar el dispositivo. En el caso del contenedor Knox, el código de acceso del contenedor se usa como parte del proceso de derivación de clave del sistema de archivos cifrados del contenedor. La ODE y los datos confidenciales del contenedor se protegen mediante una clave de hardware única por dispositivo basada en un mecanismo de *TrustZone*, y dicha clave nunca se revela si la plataforma se ve comprometida.

90. La organización puede decidir si configurar los dispositivos para elegir la política de autenticación de dispositivo que mejor se adapte a sus necesidades, aunque se presentan dos escenarios de uso:

91. Un código PIN numérico para acceder al dispositivo y, a continuación, una contraseña más segura para acceder al contenedor Knox.

92. Una contraseña segura para acceder al dispositivo y, a continuación, una contraseña más corta o un token para acceder al contenedor Knox.

93. El administrador deberá determinar la política basándose en el lugar donde están almacenados los datos propiedad de la organización en el dispositivo; siendo necesario recordar que los datos de la organización deberían almacenarse exclusivamente dentro del contenedor Knox.

94. Los dispositivos que utilizan Samsung Knox ofrecen a las organizaciones la flexibilidad necesaria para configurar el mecanismo de autenticación que mejor satisfaga sus necesidades operativas y que cumpla las recomendaciones de seguridad para implementaciones de la administración pública.

- **Usuario - Servicio**

95. La plataforma Samsung Knox admite funcionalidades de integración de inicio de sesión único (SSO) y Active Directory, a fin de permitir un mecanismo de autenticación centralizado a los servicios y la infraestructura de la organización desde el entorno del contenedor Knox.

96. El servicio SSO del dispositivo se configura mediante la política de EMM, y la organización debe disponer de la infraestructura y los servicios de Active Directory necesarios para beneficiarse de esta funcionalidad.

- **Dispositivo - Servicio**

97. Esta necesidad de autenticación se cubre con la capacidad de establecer conexiones VPN IPSec con autenticación mutua para acceder a la red y los servicios de la organización basados en certificados PKI protegidos en el dispositivo.

98. Samsung también dispone de otra función diferenciada en el mecanismo de autenticación de dispositivo a servicio, en forma de atestado remoto, entendiéndose como tal el proceso para garantizar que los componentes

software dentro del dispositivo no han sido manipulados, en caso contrario dicha manipulación es detectada por el servidor que realiza el atestado.

99. La función de Atestado Remoto de Knox[4] permite que el dispositivo confirme la integridad de su propio software ante un servicio remoto. La base del atestado remoto la constituye una pareja de claves pública/privada única por cada dispositivo, instalado en el entorno seguro de *TrustZone* durante la fabricación del dispositivo.

100. La clave privada de atestado solo es accesible dentro del entorno seguro de *TrustZone*, mediante la aplicación de realización de atestados. Debido a la protección de seguridad que ofrece *TrustZone* y a la pareja de claves pública/privada única, el Atestado de Knox permite que el dispositivo se autentique junto con el gestor de arranque y el estado de integridad del kernel ante un servicio remoto.

101. Varios proveedores EMM incluyen la funcionalidad de Atestado Knox entre sus servicios, lo que permite a los administradores, si lo desean, exigir que se realice el atestado del dispositivo antes de permitir la creación del contenedor Knox. El servicio de Atestado Remoto puede solicitar el veredicto de integridad, atestado, del dispositivo en cualquier momento y, así, utilizarse para determinar qué acciones emprender, de conformidad con la política de seguridad de la organización, como desconectarse del dispositivo, eliminar el contenido del contenedor de aplicaciones seguras, solicitar la ubicación del dispositivo o cualquier otro procedimiento de recuperación de seguridad posible.

102. Esta funcionalidad debe ser utilizada, y sus datos monitorizados, por aquellas organizaciones que vayan a manejar información que, o bien requiera protección en base a la legislación aplicable, o bien vayan a manejar información que la organización ha definido como sensible o digna de protección por parte del usuario final.

6.3.2.4 INICIO SEGURO

103. El proceso de arranque de Android comienza con el gestor de arranque principal, que se carga desde la memoria ROM (*Read-only Memory*; memoria de solo lectura). Este código pone en marcha el inicio básico del sistema y, a continuación, carga otro gestor de arranque, denominado gestor de arranque secundario, desde el sistema de archivos de la memoria ROM y lo ejecuta. Pueden existir varios gestores de carga secundarios, uno para cada tarea. El proceso de arranque es de naturaleza secuencial, es decir, el gestor de arranque secundario completa su tarea y ejecuta el siguiente gestor de arranque secundario de la secuencia. Finalmente, se carga el gestor de

[4] Para ampliar información sobre Atestado de Knox: https://www.samsungknox.com/en/knox-platform-for-enterprise-whitepaper

arranque de Android conocido como "*aboot*", que carga el sistema operativo Android.

104. *Secure Boot* es un mecanismo de seguridad que impide la carga de gestores de arranque (*bootloaders*) y sistemas operativos no autorizados durante el proceso de inicio. *Secure Boot* se implementa de forma criptográfica a través de los distintos gestores de arranque, verificando la firma del siguiente gestor de arranque de la secuencia mediante una cadena de certificados cuya raíz de confianza reside en el hardware. El proceso de arranque finaliza si la verificación falla en alguna de las fases.

105. *Secure Boot* es una opción eficaz para prevenir gestores de arranque no autorizados (y, en ocasiones, el kernel, cuando también se aplica al archivo binario del kernel). No obstante, *Secure Boot* no puede distinguir entre distintas versiones de archivos binarios autorizados, como un gestor de arranque con una vulnerabilidad conocida y una versión posterior parcheada, puesto que ambas versiones tienen firmas válidas. Además, cuando determinados operadores deciden permitir que se ejecuten kernels personalizados en sus dispositivos, *Secure Boot* no puede evitar que se ejecuten kernels de terceros en dichos dispositivos. Esto revela una superficie de ataque que supone una posible amenaza para las aplicaciones y los datos de la organización.

106. Para hacer frente a esta limitación, Samsung Knox implementa *Trusted B*oot (arranque de confianza), además de *Secure Boot*. Con *Trusted Boot* se registran mediciones de los gestores de arranque (*bootloaders*) en la memoria segura durante el proceso de arranque. En tiempo de ejecución, las aplicaciones de *TrustZone* utilizan estas mediciones para tomar decisiones concernientes a la seguridad, como verificar la liberación de claves criptográficas del almacén de claves de TIMA, la activación del contenedor, etc. Además, si el gestor de arranque *aboot* no puede verificar el kernel de Android, se escribe un área de memoria programable una única vez (denominada coloquialmente fusible) para indicar una sospecha de manipulación. Aunque el código de arranque se restablezca a su estado de fábrica original, esta prueba de manipulación permanece. No obstante, el proceso de arranque no se detiene y el gestor de arranque *aboot* continúa iniciando el sistema operativo Android. Los responsables TIC de la organización deben pues, tomar medidas de monitorización en tiempo de ejecución y de sensibilización del usuario final del dispositivo para mitigar los riesgos derivados de esta circunstancia.

107. Este proceso garantiza que el funcionamiento normal del dispositivo no se vea afectado.

6.3.2.5 INTEGRIDAD DE PLATAFORMA Y ESPACIOS DE EJECUCIÓN AISLADOS PARA APLICACIONES

108. Samsung Knox introduce una serie de mejoras significativas sobre la plataforma Android que garantizan la integridad del sistema, el aislamiento de los datos y una zona para pruebas de las aplicaciones.

SE Linux (Security-Enhanced Linux) para Android

109. Samsung Knox utiliza SE Linux para Android, para ejecutar políticas de Control de acceso obligatorio (Mandatory Access Control; MAC) y aislar aplicaciones y datos dentro de la plataforma. Aunque también se introdujo SE Linux para Android en la versión 4.4 de la plataforma Android, la implementación de Samsung ofrece mejoras en el nivel de protección que ofrece a las aplicaciones y los servicios de sistema.

110. La plataforma Knox introduce una función denominada SE para *Android Management Service* (SEAMS) que ofrece acceso controlado al motor de políticas SELinux. El contenedor Knox utiliza SEAMS a nivel interno y también está disponible para que proveedores externos protejan sus propias soluciones de contenedor. Por motivos de seguridad, Samsung define *a priori* los dominios de contenedores de terceros y se activan bajo demanda cuando se invoca la política de contenedor por primera vez.

TIMA (Arquitectura de medición de integridad basada en TrustZone)

111. La protección de sistema que ofrece SELinux para Android se basa en la asunción de la integridad del kernel del SO. Si el propio kernel se ve comprometido (por ejemplo, por una futura vulnerabilidad desconocida en la actualidad) los mecanismos de seguridad de SELinux para Android podrían resultar neutralizados. La arquitectura de medición de la integridad basada en *TrustZone* (*TrustZone-based Integrity Measurement Architecture*; TIMA) de Samsung se ha desarrollado para mitigar esta vulnerabilidad. TIMA aprovecha las funciones aportadas por el hardware, en concreto *TrustZone* y el hipervisor, para garantizar que no pueda deshabilitarse o ser atacada por un software malicioso.

112. La medición periódica del kernel (*Periodic Kernel Measurement*; PKM) de TIMA lleva a cabo una supervisión periódica continua del kernel para detectar si software malicioso ha modificado los datos o el código legítimo del kernel. Además, TIMA también supervisa estructuras de datos clave de SE para Android en la memoria del kernel del SO para impedir que ataques maliciosos las corrompan y puedan deshabilitar SELinux para Android.

113. La protección del kernel en tiempo real (*Real-time Kernel Protection*; RKP) lleva a cabo una supervisión constante en tiempo real, del sistema operativo desde el hipervisor para evitar la manipulación del kernel. RKP intercepta la aparición de eventos críticos dentro del kernel, que se inspeccionan en el hipervisor. Si se determina que un evento afecta a la integridad del kernel del SO, RKP detiene el evento o registra un veredicto de auditoría en el sentido de la sospecha de

que se ha producido una manipulación. Esta información de alerta se incluye en los resultados de Atestado Remoto (*Attestation*) que se envían a la solución de EMM, a fin de que los administradores TIC determinen las acciones que las políticas de seguridad de la organización deben realizar en el futuro. Este mecanismo ofrece protección contra modificaciones maliciosas e inyecciones en el código del kernel, incluidas aquellas que obligan al kernel a dañar sus propios datos. Las comprobaciones de RKP se llevan a cabo en un entorno aislado inaccesible para el kernel, de modo que no puedan extenderse posibles explotaciones del kernel para comprometer la RKP. Este entorno aislado se sitúa en las extensiones del hipervisor.

114. Desde la versión 2.8 de Knox, la protección del kernel se ha mejorado con defensa contra ataques que manipulan el flujo de control del kernel mediante técnicas de programación orientadas al retorno. Esta mejora limita la capacidad del atacante de secuestrar el flujo de control del kernel de un SO, provocando la elevación de privilegios o la obtención de privilegios de usuario *root* del dispositivo. Hay que tener en cuenta que la compatibilidad con esta función depende del hardware concreto que incluido en el dispositivo.

115. Tal y como ya se ha mencionado anteriormente en este documento, la plataforma Knox también incluye una función de atestado (verificación) remoto, que permite que un servicio remoto determine la integridad del dispositivo móvil de un modo seguro. Además del veredicto de validación (atestado), los datos de atestado incluyen todas las medidas de arranque fiable, registros de RKP y PKM que pueden indicar la presencia de software malicioso en el dispositivo y otra información que pueda usarse para vincular el resultado de la certificación al dispositivo.

Contenedor Knox

116. Samsung Knox *Workspace* es un producto de seguridad diseñado para separar, aislar, cifrar y proteger los datos de la organización de ataques. Este entorno de trabajo/ejecución garantiza la división de datos en función de su categoría, y permite que la organización aplique diferentes políticas a las diferentes zonas de ejecución /contenedores. El departamento TIC puede decidir no gestionar ni controlar la información alojada fuera del contenedor (~información personal), aunque esta práctica no se considera recomendable desde un punto de vista de seguridad, y no está permitida si se trata de dispositivos destinados al manejo de información que normativamente requiera protección o se enmarcan en sistemas que requieran de una acreditación. Una vez activado Knox *Workspace*, el producto estará estrechamente integrado en la plataforma Knox.

117. *Workspace* ofrece este entorno independiente dentro del dispositivo móvil, junto con la pantalla de inicio, el iniciador, las aplicaciones y los widgets.

118. Las aplicaciones y los datos almacenados dentro de *Workspace* (el contenedor) están aislados de las aplicaciones instaladas fuera de este; es decir, las aplicaciones instaladas fuera de *Workspace* no pueden utilizar métodos de uso compartido de datos ni de comunicación entre procesos con las aplicaciones

instaladas dentro de *Workspace*. Por ejemplo, las fotos hechas con la cámara dentro de *Workspace* no pueden visualizarse en la galería externa a *Workspace*. Esta misma restricción se aplica a las opciones de copiar y pegar. Cuando la política de seguridad de la organización lo permita, algunos datos de aplicaciones, como los datos de contactos y del calendario, podrán compartirse fuera de los límites de Workspace (del contenedor). El usuario final puede decidir compartir los contactos y las notas del calendario entre *Workspace* (interior del contendor) y el espacio personal (exterior del contenedor). No obstante, en última instancia es la política de seguridad de la organización la que controla esta opción. La organización debe gestionar *Workspace* como cualquier otro activo TIC, utilizando una solución de EMM. Este proceso de gestión del contenedor se denomina *Mobile Container Management* (MCM; Administración del contenedor móvil). Samsung Knox es compatible con muchas de las soluciones de MCM presentes en el mercado. Las herramientas MCM se ven afectadas por políticas de configuración del mismo modo que las políticas de EMM tradicionales. Samsung Knox *Workspace* incluye un amplio conjunto de políticas de autenticación, seguridad de datos, VPN, correo electrónico, listas blancas y negras de aplicaciones, etc. El administrador tiene un control estricto sobre qué aplicaciones pueden implementarse en el contenedor mediante un amplio conjunto de políticas de gestión de aplicaciones.

119. El uso compartido de archivos entre el contenedor y el entorno personal del dispositivo está deshabilitado, al igual que el uso compartido de los contactos y los eventos de calendario.

6.3.2.6 LISTA BLANCA DE APLICACIONES

120. Samsung Knox incluye amplias capacidades de gestión de aplicaciones que permiten al administrador de la organización controlar de forma estricta qué aplicaciones pueden utilizarse e instalarse en el dispositivo, incluyendo las de dentro y fuera del contenedor Knox.

121. Existe un amplio conjunto de API de política de EDM disponible para permitir la configuración de la gestión de aplicaciones a través de la solución de EMM. Esto incluye la creación de listas blancas y negras de instalación de aplicaciones por nombre y firma de paquete, listas blancas y negras de permisos de aplicaciones, la desactivación de aplicaciones instaladas y la instalación y desinstalación silenciosa de aplicaciones. Por ejemplo, el administrador puede deshabilitar algunas aplicaciones preinstaladas mediante la política de aplicaciones, bien a nivel de dispositivo o dentro del contenedor.

122. Se pueden aplicar todas las políticas de gestión de aplicaciones de forma individual tanto al dispositivo como al contenedor.

123. El contenedor Knox dispone de algunas políticas específicas adicionales para:

- Permitir o no que las aplicaciones se muevan al contenedor
- Habilitar o Deshabilitar repositorios públicos de aplicaciones.

124. La política ”Permitir que las aplicaciones se muevan al contenedor” controla si se permite al usuario instalar aplicaciones que se hayan instalado en el perfil personal del dispositivo en el contenedor Knox.

125. Si esta política estuviese habilitada, puede aplicarse la lista blanca de instalación de aplicaciones del contenedor, a fin de controlar qué elementos puede instalar el usuario. El ajuste recomendado de esta política es no permitir que el usuario mueva las aplicaciones al contenedor, lo que implica que las aplicaciones solo pueden instalarse a través de la solución de EMM o de tiendas de aplicaciones accesibles en el contenedor.

126. La política «Permitir Google Play Store» permite utilizar la tienda en el interior del contenedor. La lista blanca de aplicaciones del contenedor puede utilizarse para controlar qué elementos puede instalar el usuario. Aunque de forma predeterminada, la tienda Google Play no está habilitada en el contenedor, la organización debe definir la política de seguridad de manera consciente. Los repositorios públicos de aplicaciones como Google Play Store también pueden deshabilitarse en la zona destinada a utilización no-profesional/personal, según las necesidades de la organización.

127. Las políticas de gestión de aplicaciones permiten al administrador bloquear el dispositivo y el contenedor, de acuerdo con los requisitos de la política corporativa. La lista blanca de aplicaciones debería utilizarse para controlar qué aplicaciones puede instalar el usuario, tanto dentro como fuera del contenedor.

6.3.2.7 DETECCIÓN Y PREVENCIÓN DE CÓDIGO MALICIOSO

128. El administrador puede usar el amplio conjunto de políticas de gestión de aplicaciones que ofrece Samsung Knox para controlar qué elementos pueden instalarse en el dispositivo y mitigar la amenaza de aplicaciones maliciosas.

129. Existe un gran número de objetos de código y configuraciones dentro del área del sistema que el código malicioso puede utilizar para volverse persistente, es decir, para poder mantenerse incluso cada vez que se reinicia el dispositivo.

130. Knox previene estas modificaciones al integrar *DM-Verity*, un módulo del kernel que verifica la integridad de las aplicaciones y los datos almacenados en la partición crítica del sistema, System, así como la partición Vendor y ODM para dispositivos como Samsung Galaxy S9. En caso de que un proceso o usuario malicioso modifique algún elemento de la partición del sistema, la próxima vez que se leen esos datos, DM-Verity detecta la modificación y bloquea cualquier intento de acceso a los datos modificados.

131. Por otra parte, los mecanismos de aislamiento de datos y de integridad de la plataforma descritos en secciones anteriores de este documento están diseñados para ofrecer protección contra el daño que puede provocar una aplicación maliciosa.

132. Los administradores también pueden implementar herramientas antimalware de terceros o aprovechar las herramientas proporcionadas por los proveedores de dispositivos. Sin embargo, es necesario ser consciente en todo momento de las limitaciones intrínsecas a dichas herramientas.

6.3.2.8 APLICACIÓN DE LA POLÍTICA DE SEGURIDAD (ENFORCEMENT)

133. Samsung Knox ofrece un amplio conjunto de políticas de gestión que pueden configurarse a través de la solución de EMM. Estos mecanismos de política están integrados en el software y la configuración del dispositivo obtenidos a través de las API de gestión, a los que pueden acceder los agentes de EMM del dispositivo.

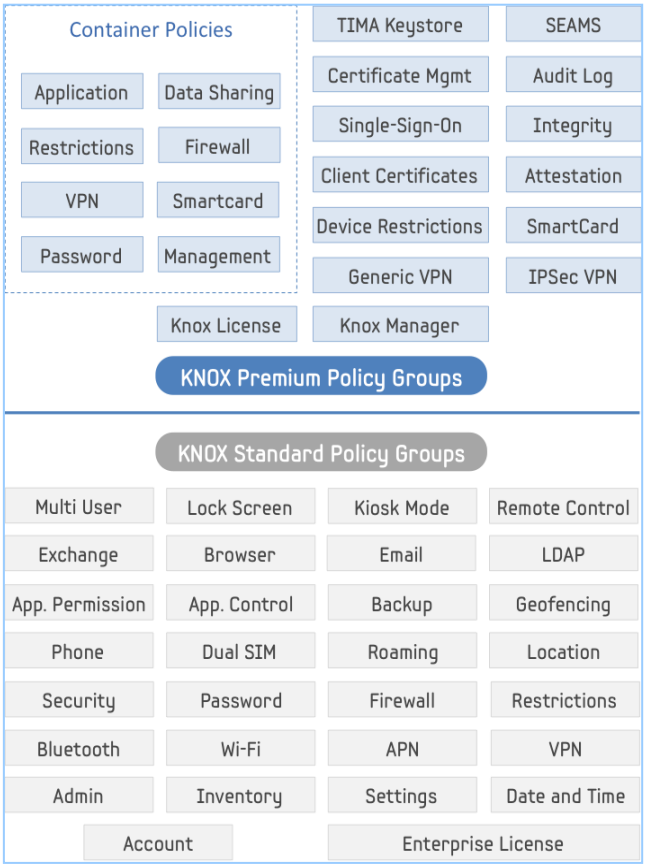


Figura 2: Resumen general de las políticas de Samsung Knox

134. Existen amplias políticas de gestión disponibles para el dispositivo en su totalidad, así como el área personal del dispositivo (fuera de contenedor) y el contenedor Knox.

135. El acceso a las API de SDK Premium y Standard de Knox está controlado a través de un mecanismo de licencia. Los proveedores de EMM reciben un SDK para permitirles desarrollar agentes de gestión del dispositivo.

136. Mediante una política, el administrador puede impedir que el usuario elimine al administrador del dispositivo, así como la instalación y habilitación de otros administradores de dispositivo.

137. Las políticas de gestión están compuestas por políticas"usuario" o "global". Las políticas globales (por ejemplo, habilitar/deshabilitar el Bluetooth) se aplican a todo el dispositivo. Las políticas basadas en un usuario pueden aplicarse de forma individual al contenedor y los perfiles personales (por ejemplo, políticas de gestión de aplicaciones).

6.3.2.9 PROTECCIÓN DE LA INTERFAZ EXTERNA DEL DISPOSITIVO

138. Los dispositivos Samsung Knox incluyen políticas de restricción de EDM que permiten al administrador controlar y proteger interfaces externas del dispositivo. Todas las interfaces externas se pueden configurar, habilitar o deshabilitar a través de una política EDM, que no puede ser anulada por el usuario.

139. Los *firewalls* del dispositivo y el contenedor también pueden configurarse a través de una política EDM. La configuración incluye las normas "permitir", "denegar" y "redirigir" para direcciones IP y puertos (incluidos rangos), la configuración de proxy y el filtrado de URL.

140. En este sentido, es importante recordar las buenas prácticas y recomendaciones de configuración en cuanto a reglas para firewalls y otros dispositivos de interconexión que pueden ser consultadas en otros documentos CCN-STIC.

141. En el contenedor Knox, se deshabilita el acceso al soporte de almacenamiento externo (tarjeta SD y USB) para garantizar el aislamiento de los datos de la organización. Tal y como se ha descrito anteriormente, el administrador puede controlar de forma estricta el uso compartido de datos dentro y fuera del contenedor.

142. Otros interfaces, como Wi-Fi, NFC, Bluetooth o los interfaces USB pueden deshabilitarse mediante políticas de restricción de EDM. Las configuraciones recomendadas para cada uno de estos interfaces se incluyen más adelante.

6.3.2.10 POLÍTICA DE ACTUALIZACIONES DEL DISPOSITIVO

143. Samsung actualiza periódicamente los dispositivos con nuevas funciones y soluciona problemas que son detectados por diferentes fuentes, tanto funcionales como relativas a la seguridad.

144. La periodicidad y garantía de estas actualizaciones es uno de los parámetros más importantes que una organización debe considerar a la hora de adquirir/desplegar dispositivos, debiendo contar con garantía por parte del distribuidor de que el dispositivo recibirá actualizaciones de seguridad durante todo el ciclo de vida útil que la organización haya definido.

145. Las actualizaciones del firmware del dispositivo deben aplicarse a los dispositivos por vía inalámbrica (OTA).

146. Los dispositivos Samsung Knox cuentan con un amplio conjunto de políticas de auditoría que permiten que el administrador supervise el software y el estado del dispositivo, incluidas las aplicaciones instaladas, y que tome las medidas apropiadas, como bloquear el contenedor Knox hasta que finalice la actualización del firmware del dispositivo.

147. No existen políticas de EDM específicas que permitan enviar actualizaciones de firmware del dispositivo; no obstante, un administrador puede gestionar el modo en el que se aplican las actualizaciones a un dispositivo, por ejemplo, deshabilitando las actualizaciones inalámbricas.

148. A partir de dispositivos Samsung con Android 7, Samsung ha introducido un servicio mejorado de actualizaciones de firmware inalámbricas denominado Enterprise-FOTA (E-FOTA). E-FOTA concede a los administradores TIC la posibilidad de especificar el despliegue de una versión de firmware de SO concreta en los dispositivos de sus usuarios, lo que permite un detallado nivel de control para evitar cualquier posible interrupción del servicio. Además, puede programarse una fecha de actualización configurada por el administrador que tiene en cuenta el horario laboral y puede forzar las actualizaciones. Esta opción es aconsejable para aquellos sectores en los que la exigencia de seguridad y trazabilidad sea mayor, como el de la administración y los servicios financieros o la asistencia sanitaria. En la actualidad, Samsung ofrece el servicio de E-FOTA a los usuarios a través de los proveedores de EMM. Samsung también puede actualizar el SE (Android Security Enhancement) del dispositivo para políticas de Android de forma independiente a las actualizaciones de firmware, de forma segura y a través de los servidores de distribución de políticas de Samsung. Samsung actualiza constantemente las políticas de SE para Android del dispositivo para garantizar la seguridad general y el aislamiento de los datos de la organización.

149. La política EDM de aplicaciones incluye una API que permite actualizar las aplicaciones de forma silenciosa, sin necesidad de la intervención del usuario.

6.3.2.11 RECOPILACIÓN DE EVENTOS PARA SU ANÁLISIS POR LA ORGANIZACIÓN

150. Samsung Knox ofrece una función de registro de datos de auditoría independiente de la funcionalidad de registro normal del dispositivo. A través de la solución de EMM es posible habilitar y gestionar la funcionalidad de registro de auditoría, así como la recuperación de los registros.

151. El registro de datos de auditoría abarca un amplio conjunto de eventos relativos a la seguridad, entre los que se incluyen eventos fallidos de desbloqueo, instalación o desinstalación de aplicaciones y eventos de interfaz.

6.3.2.12 RESPUESTA A INCIDENTES

152. Los dispositivos Samsung Knox ofrecen diversas opciones de respuesta a incidentes.

153. El dispositivo y el contenedor Knox pueden bloquearse, deshabilitarse y borrarse de forma remota a través de la solución de EMM, ya sea manualmente o a través del administrador o, en ciertos casos, como respuesta a un evento específico, como una serie de introducciones incorrectas del código de acceso.

154. Samsung Knox ofrece la posibilidad de eliminar el contenedor, del dispositivo completo y de cualquier tarjeta SD que se esté utilizando (si así lo permite la política de la organización). Las soluciones de EMM suelen ofrecer opciones para accionar políticas pre-definidas en el caso de que se detecte que el dispositivo no está configurado según la política de la organización o comprometido. Estos servicios se denominan “Servicios de Cumplimiento” o Compliance. El administrador TIC de la organización podrá tomar las medidas necesarias basándose en eventos o estados del dispositivo.

155. Además de esto, Samsung Knox ofrece un mecanismo de certificación del dispositivo que permite a los dispositivos certificar su integridad ante la solución de EMM o incluir registros de incidentes de manipulación a los que, a continuación, se puede responder.

156. Samsung Knox ofrece la funcionalidad de eliminar certificados aprovisionados por la organización.

7 CONFIGURACIÓN RECOMENDADA

157. Samsung, en colaboración con el Centro Criptológico Nacional, ha elaborado una configuración recomendada que permite que la solución cumpla los requisitos del marco de seguridad detallados en este documento, permitiendo a los administradores gestionar y paliar los riesgos de forma óptima.

158. Las políticas deben ser aplicadas y gestionadas a través de una solución de EMM compatible que no pueda ser anulada por el usuario, lo que garantiza que la organización tenga el nivel de control sobre el dispositivo que requiere la política de seguridad de la organización.

7.1 POLÍTICAS PARA DISPOSITIVOS COMPATIBLES CON SAMSUNG KNOX

159. Estas políticas abarcan la configuración del dispositivo en su totalidad, dentro y fuera del contenedor Knox. En la siguiente sección se detalla la configuración específica para el contenedor Knox.

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Tiendas de aplicaciones	Deshabilitar o eliminar las tiendas de aplicaciones Google Play y Samsung Galaxy Apps e impedir la instalación de aplicaciones desde orígenes desconocidos.	Las tiendas de aplicaciones pueden deshabilitarse a través de la política de EDM para evitar la instalación arbitraria de aplicaciones. Esta opción también se puede gestionar con las funcionalidades de lista blanca de aplicaciones que ofrece Samsung. El administrador puede deshabilitar la instalación desde orígenes desconocidos, impidiendo que el usuario instale aplicaciones de origen desconocido.

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Lista blanca	Deshabilitar o eliminar aplicaciones innecesarias. Si se habilita Google Play Store, permitir tan solo la instalación de las aplicaciones incluidas en la lista blanca.	Las políticas de gestión de aplicaciones de Samsung permiten al administrador deshabilitar aplicaciones ya instaladas en el dispositivo, en función de las necesidades, así como crear una lista blanca de instalación de aplicaciones aprobadas que el usuario puede instalar desde tiendas de aplicaciones situadas fuera del contenedor.
Modo desarrollador	Impedir todos los ajustes de modo desarrollador, incluyendo la depuración de USB y el modo de almacenamiento USB.	Esto impide que el usuario acceda a las opciones de desarrollador de Android y evita que utilice ADB, lo que debería ser innecesario para un usuario corporativo. Samsung ofrece opciones de gestión USB adicionales para impedir que el dispositivo se utilice en modo de almacenamiento masivo o que utilice cualquier tipo de conectividad USB.
Almacenamiento cifrado	Exigir el cifrado interno.	El administrador puede ejecutar la funcionalidad de Cifrado de datos en el dispositivo, que protege todos los datos del usuario del dispositivo.
Tarjeta SD	Deshabilitar el acceso a la tarjeta SD.	El uso de la ranura de la tarjeta SD en el dispositivo puede deshabilitarse para impedir que los datos del dispositivo se copien a soportes de almacenamiento externos.

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Contraseña	Exigir contraseña: Verdadero Longitud mínima: 8 caracteres Número máximo de intentos erróneos: 5 Requerir contraseña compleja: Verdadero La contraseña debe incluir una letra mayúscula, una minúscula y símbolos. Historial de códigos de acceso: 8 Antigüedad máxima del código de acceso: 90 días Eliminar los datos del soporte de almacenamiento externo durante la eliminación de los datos del dispositivo: Verdadero	
Tiempo de inactividad para bloqueo	10 minutos	Tiempo de inactividad para que la pantalla se bloquee automáticamente cuando no se está utilizando.
VPN	Aplicar el modo de VPN ”por aplicación” a todas las aplicaciones instaladas fuera del contenedor Knox.	Esta opción permite que todo el tráfico del dispositivo se tunelice y se beneficie de las propiedades de VPN por aplicación de Samsung Knox, como el modo de funcionamiento siempre activo, que evita posibles filtraciones de datos si se desconecta la VPN.

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Certificados	Habilitar la validación de certificado en la instalación. Instalar certificados de la organización.	Samsung ofrece API de EDM de gestión de certificados del dispositivo que permiten proporcionar y gestionar certificados CA y de cliente, incluyendo la opción de habilitar el certificado en el momento de la instalación.
Interfaces	Deshabilitar las interfaces innecesarias (USB, Bluetooth, NFC), a menos que exista una necesidad explícitamente justificada por la organización.	Los administradores pueden gestionar y deshabilitar todas las interfaces del dispositivo mediante la solución de EMM, de acuerdo con la política de la organización. Diferentes grupos de usuarios pueden requerir diferentes configuraciones dentro de la organización, debiendo estar justificados cada uno de ellos en caso de habilitarse el interfaz.
Atestado	Habilitar la funcionalidad de verificación remota.	Los dispositivos compatibles con Samsung Knox disponen de una función de validación remota segura (Atestado) que permite determinar la integridad de los dispositivos. Esta opción se puede habilitar. Las soluciones de EMM pueden permitir que determinadas funcionalidades, como el contenedor Knox, solo se aprovisionar a dispositivos que puedan certificar un buen estado conocido.

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Almacén de claves de TIMA	Habilitar	Habilitar esta función permite que las aplicaciones almacenen claves en el almacén de claves protegido de TrustZone de Samsung Knox mediante las API de almacenamiento de claves estándares de Android, realizando pocas modificaciones o ninguna.
Verificación de arranque de confianza de ODE	Habilitar	Tal y como se ha abordado anteriormente en el presente informe, habilitar esta función implicará que las claves criptográficas de ODE solo se liberen desde TrustZone en el momento de arranque del dispositivo si la integridad de este es válida y si el usuario introduce un código de acceso válido. Ambos deben ser correctos para permitir el descifrado de los datos del dispositivo. La protección de TrustZone mejora la defensa contra ataques sin conexión. En dispositivos Samsung con Android N y superiores, la verificación de arranque de confianza ODE está habilitada de forma predeterminada y, por tanto, no es preciso activarla a través de la política de EDM.

7.2 POLÍTICAS PARA EL CONTENEDOR SAMSUNG KNOX

160. Estas políticas abarcan la configuración del contenedor Knox y son independientes de las que se aplican fuera del contenedor.

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Tiendas de aplicaciones	Deshabilitar las tiendas de aplicaciones de Samsung Knox y Google Play. Las aplicaciones necesarias de estas tiendas podrán instalarse utilizando la aplicación de tienda instalada fuera del contenedor para, a continuación, instalarlas dentro del contenedor mediante la herramienta de ajustes de Knox.	En el modelo COPE y dispositivos soportando Knox 3.0 o superiores, Google Play es un servicio gestionado (managed Google Play).

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Permitir que las aplicaciones se muevan al contenedor	Habilitar únicamente tras articular un proceso de aprobación de aplicaciones a los dispositivos de la organización. Las aplicaciones que pueden moverse al contenedor estarán restringidas por la lista blanca.	Samsung Knox ofrece la función de mover las aplicaciones instaladas fuera del contenedor al contenedor Knox. Esta opción está deshabilitada de forma predeterminada, pero puede habilitarse a través de la solución de EMM. En ese caso, la aplicación puede ejecutarse en el contenedor, con todos los datos de aplicación de dicha instancia aislados de las aplicaciones instaladas fuera del contenedor y protegidos por el mecanismo DAR del contenedor Knox. Mover aplicaciones al contenedor está sujeto a cualquier política de gestión de aplicaciones que se aplique al contenedor, como una lista blanca. Esto implica que un administrador puede permitir la instalación de una aplicación en el dispositivo fuera del contenedor, pero que el usuario solo instale un subconjunto dentro del contenedor.
Lista blanca	Lista blanca de aplicaciones esenciales solo para acceder y manipular datos corporativos, p. ej., cliente de correo, navegador y paquete Office. Si se habilitan la tienda Knox Store o Google Play, permitir tan solo la instalación de las aplicaciones incluidas en la lista blanca.	Tal y como se ha expuesto anteriormente, al contenedor Samsung Knox se le pueden aplicar políticas de gestión de aplicaciones exhaustivas que solo permitan el uso de determinadas aplicaciones esenciales en el contenedor.

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Navegador	Habilitar La organización debe dotarse de la infraestructura de interconexión necesaria para el nivel de seguridad donde se posicione.	Permite al administrador controlar si el usuario puede utilizar o no aplicaciones de navegador web en el contenedor Knox.
VPN	Aplicar el modo de VPN por aplicación a todas las aplicaciones del contenedor Knox, incluidos los servicios en segundo plano y los widgets.	Esta opción permite que todo el tráfico del dispositivo se tunelice y se beneficie de las propiedades de VPN por aplicación de Samsung Knox, como el modo de funcionamiento siempre activo, que evita posibles filtraciones de datos si se desconecta la VPN.
Correo electrónico	Configurar el cliente de correo electrónico para que se conecte al servidor de la organización con la autenticación del certificado de cliente.	La configuración del cliente de correo del contenedor puede establecerse a través de la solución de EMM.
Añadir cuenta de correo electrónico	Deshabilitar	Esta opción impide que el usuario pueda añadir cuentas adicionales dentro del contenedor Knox. En función de la política de contenedor, el usuario podrá usar cuentas de correo electrónico personales o no confidenciales fuera del contenedor Knox.

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Contraseña	Habilitar la política de contraseñas de Knox: Verdadero Tiempo de inactividad de Knox: 30 minutos Número máximo de intentos erróneos: 5 Longitud mínima: 8 caracteres Calidad: alfanumérica Historial de contraseñas: 8 Antigüedad máxima del código de acceso: 90 días Número mínimo de caracteres que deben cambiarse: establecerlo en más de 1, para evitar el cambio de contraseña escalonado.	
Credenciales	Los certificados de cliente requeridos deberán instalarse a través de la política.	Samsung ofrece API de EDM de gestión de certificados del contenedor que permiten proporcionar y gestionar certificados CA y de cliente, incluyendo la opción de habilitar el certificado en el momento de la instalación.
Permitir que los archivos se muevan al contenedor	No permitir /Falso	El uso en despliegues del contenedor Samsung Knox permite que el administrador controle el movimiento de datos dentro y fuera del contenedor. Esta acción está deshabilitada de forma predeterminada.

REGLA DE CONFIGURACIÓN	AJUSTE RECOMENDADO	NOTAS
Permitir que los archivos se muevan desde el contenedor	No permitir /Falso	El uso en despliegues del contenedor Samsung Knox permite que el administrador controle el movimiento de datos dentro y fuera del contenedor. Esta acción está deshabilitada de forma predeterminada. El contenedor Knox dispone de un sistema de archivos aislado independiente al que no se puede acceder desde el exterior del contenedor.
Sincronización de datos del contenedor Knox	Deberían establecerse los siguientes ajustes para no permitir el movimiento de datos entre el contenedor Knox y el dispositivo. Pre-visualización de las notificaciones de Knox. Exportación de contactos al modo personal. Exportación de elementos del calendario al modo personal.	Además de los archivos, Samsung Knox permite al administrador controlar si se pueden compartir los contactos y los eventos del calendario de Knox con el área personal del dispositivo. Esta opción está deshabilitada de forma predeterminada. Además, de forma predeterminada, las notificaciones de las aplicaciones del contenedor Knox no se pre visualizan en el panel de notificaciones. De forma opcional, el administrador puede habilitar la pre-visualización de notificaciones de Knox.

7.3 CONFIGURACIÓN DE VPN

161. Las organizaciones deben utilizar un cliente VPN IPSec, que cumpla con los requisitos de seguridad exigidos al sistema. En este sentido, el cliente VPN IPSec de Samsung Knox puede ser una opción a considerar, respetando siempre las configuraciones recomendadas.

162. Debe usarse la configuración “por aplicación” de Samsung Knox. Cabe señalar que la función de VPN ”por aplicación” de Samsung dota a los administradores

de un control detallado de las aplicaciones que tienen acceso a una conexión VPN concreta (con la posibilidad de hasta 5 conexiones VPN distintas a la vez). El administrador puede configurar que se redirija a través de la VPN el tráfico de una sola aplicación, de un grupo de aplicaciones o, de hecho, de todas las aplicaciones.

163. Todos los paquetes de aplicaciones deberían añadirse a cada una de las configuraciones de VPN, a fin de garantizar que todo el tráfico del contenedor y del dispositivo se envíe a través de los túneles de VPN. La configuración recomendada establece al menos dos túneles de VPN, uno para las aplicaciones instaladas dentro del contenedor y otro para las aplicaciones que se instalen y ejecuten fuera del contenedor. En esta configuración se automatiza el establecimiento de VPN y se impide que el tráfico salga del dispositivo hasta que se haya establecido la conexión VPN.

REGLA DE CONFIGURACIÓN	FUNCIÓN DE PLATAFORMA
Knox IPSec VPN	*int* createVpnProfile (String profileInfo) int addAllPackagesToVpn (String profileName) int addAllContainerPackagesToVpn (int mContainerId, String profileName) int activateVpnProfile (String profileName, boolean enable)

8 MODO COMMON CRITERIA

164. Samsung ofrece una forma rápida de realizar los ajustes para habilitar servicios y configurar el dispositivo tal y como se ha evaluado en la certificación Common Criteria. Esta configuración se denomina Modo CC.

165. Si la organización utiliza una solución de EMM compatible, el administrador de la organización podrá utilizar este atajo de configuración, siendo responsable de revisar con posterioridad los ajustes que incluye y realizar las configuraciones adicionales en el resto de componentes de la solución.

166. En el caso de que la solución EMM no soporte todavía la llamada remota a alguna de las APIs necesarias para habilitar el modo Common Criteria, el administrador de la organización puede realizar el proceso utilizando la configuración detallada a continuación.

167. Adicionalmente, Samsung pone a disposición el archivo CCMode.apk, que puede descargarse desde la siguiente página web

https://support.samsungknox.com/hc/en-us/articles/115015195728

168. En dicha página web podrá consultar asimismo la lista de aplicaciones facilitadas con cada dispositivo Samsung, así como descargar la aplicación Modo CC, que aparecerá en primer lugar.

- **Instalación de la aplicación Modo CC**

169. Antes de instalar la aplicación Modo CC deberá habilitar las fuentes de aplicaciones desconocidas, ya que la aplicación no se instalará desde Google Play Store. Existen dos modos de hacerlo:

Accediendo a Settings/Lock screen and security/Unknown sources (Ajustes/Pantalla de bloqueo y seguridad/Fuentes desconocidas) y modificando el ajuste a “permitido”.

170. Permitiendo que el proceso de instalación de la aplicación le pida que habilite las fuentes desconocidas. Este le pedirá que permita la instalación de esta aplicación desde un Origen desconocido como autorización única (también puede optar por habilitarlo por completo cuando se le solicite). Seleccionar la opción predeterminada no habilitará las fuentes desconocidas para todas las aplicaciones, sino solo para la aplicación Modo CC que se instalará en ese momento.

171. Seleccionar la habilitación de fuentes desconocidas implica un riesgo, debido a la vulnerabilidad que presenta poder instalar aplicaciones desde elementos externos a Play Store. De forma predeterminada, Play Store seguirá analizando las aplicaciones instaladas en busca de vulnerabilidades conocidas, pero no se recomienda mantener esta opción habilitada.

172. **Nota:** Después de instalar la aplicación Modo CC deben deshabilitarse la capacidad de instalar desde fuentes desconocidas, en caso de haberlos habilitado.

- **Requisitos previos para el Modo CC**

173. Antes de completar la activación del Modo CC es necesario establecer una contraseña en el dispositivo; hasta que no se configure la contraseña, no será posible completar la activación. La contraseña podrá establecerse antes de iniciar la activación del Modo CC o podrá hacerse durante el proceso (saliendo de la aplicación y estableciendo la contraseña), pero es más sencillo hacerlo antes.

174. La contraseña debe contener, al menos, 4 caracteres, siendo uno de ellos 1 letra.

- **Activación del Modo CC**

175. **Nota:** Para completar la activación el dispositivo debe tener una conexión a Internet, a través de red móvil o Wi-Fi.

176. Los dispositivos pueden agruparse según las similitudes de sus funciones y procesos. Debido a las diferencias entre los grupos, los pasos para establecer un dispositivo en el Modo CC variarán ligeramente y, por tanto, se expondrán en este documento de forma independiente.

177. **Nota:** Cuando un dispositivo se ha establecido en Modo CC, la única manera de deshabilitarlo es ejecutar un restablecimiento de los valores de fábrica o conectarlo a una solución de EMM que pueda deshabilitarlo.

- **Activación en el Galaxy S9/8 y Galaxy S9/8 +**

178. **Nota:** Si su entorno requiere que la generación de la clave de ODE se realice durante el proceso de configuración (o después de la carga de fábrica), el restablecimiento de los valores de fábrica del dispositivo antes de empezar el proceso de inscripción forzará la generación de una nueva clave de ODE cuando el restablecimiento de los valores de fábrica haya finalizado.

    - Establecer la contraseña del dispositivo
    - Abra *Settings/Lock screen and security* (Ajustes/Pantalla de bloqueo y seguridad) y seleccione *Secure startup* (Inicio seguro).
    - Seleccione *Require password when device turns on* (Solicitar contraseña al encender el dispositivo) y haga clic en OK.
    - Introduzca su contraseña.
    - Inicie la aplicación Modo CC.
    - Acepte la licencia de Modo CC y seleccione *Confirm* (Confirmar).
    - Seleccione *Activate* (Activar).
    - Seleccione *Activate License* (Activar licencia).
    - Escoja Samsung Knox.

179. **Nota:** Aquellos clientes que utilicen un servidor de licencias local pueden seleccionar ***onprem*** e introducir la información de la licencia de su servidor. Consulte al administrador de su servidor para obtener más información sobre esta opción.

    - Acepte la licencia de KLMS y seleccione *Confirm* (Confirmar).
    - Seleccione *Turn On CCMODE* (Activar MODO CC).
    - En la ventana emergente de activación del Modo CC, seleccione *Agree* (Aceptar).
    - Seleccione OK para reiniciar el dispositivo.

180. En este momento se reiniciará el dispositivo. A continuación, tendrá que introducir la contraseña y el Modo CC estará activado. Una vez activo el Modo CC, el dispositivo estará configurado de modo que tras 5 intentos de inicio fallidos se forzará un restablecimiento de los valores de fábrica, lo que eliminará todos los datos. Esta opción puede modificarse mediante la solución de EMM.

- **Modo CC y tarjetas SD en el Galaxy S9/8 y Galaxy S9/8 +**

181. En los dispositivos con ranuras para tarjetas SD también debe habilitarse el cifrado de la tarjeta SD. Este ajuste se habilitó como parte de la activación del Modo CC.

182. Al insertar una tarjeta SD (en caso de que no hubiera una desde el principio) se le pedirá que cifre dicha tarjeta. Si no sigue los mensajes y no introduce la contraseña del dispositivo para cifrar la tarjeta SD, esta no se montará y no podrá acceder a ella.

183. **Nota:** Si no introduce la contraseña de encriptación de la tarjeta SD cuando se le solicite, el único modo de que vuelva a aparecer el mensaje emergente es extraer la tarjeta SD y volver a introducirla.

- **Eliminación de la aplicación Modo CC**

184. Una vez se ha activado el Modo CC, la aplicación puede eliminarse del dispositivo. Para eliminar la aplicación del dispositivo, primero debe deshabilitarla como administrador del dispositivo. Para ello, diríjase a *Settings/Lock screen and security/Other security settings/Device Administrators (Ajustes/Bloqueo de pantalla y seguridad/Otros ajustes de seguridad/Administradores del dispositivo)*. Desactive la selección de la aplicación Modo CC y seleccione *Deactivate* (Desactivar). Ahora puede eliminar la aplicación desde el *Application Manager* (Gestor de aplicaciones).

- **Estado de Modo CC**

185. El Modo CC cuenta con los siguientes estados:

ESTADO	DESCRIPCIÓN
***Ready* (Listo) (blanco)**	No se ha activado el Modo CC.
***Enforced* (Exigido)**	Se ha activado el Modo CC, pero no se han seleccionado parte de los ajustes o configuraciones necesarios.
***Enabled* (Habilitado)**	Se ha activado el Modo CC y se han seleccionado todos los ajustes o configuraciones necesarios.
***Disabled* (Deshabilitado)**	Se ha activado el Modo CC, pero se ha producido un error en alguna comprobación de integridad o prueba de autodiagnóstico (como una prueba de autodiagnóstico FIPS 140-2).

Tabla 4: Estados de aplicación del modo CC

186. Puede consultar el estado del Modo CC desde Settings/About device (Ajustes/Acerca del dispositivo) o Settings/About device/Software information (Ajustes/Acerca del dispositivo/Información de software**)** y, a continuación, accediendo a Software Security Version (Versión de seguridad del software). Aquí se muestra el estado actual.

187. **Nota:** El estado Ready (Listo) no tiene ningún indicador asociado. Tan solo los estados Enforced (Ejecutado), Enabled (Habilitado) y Disabled (Deshabilitado) muestran un estado específico.

9 REDES INALÁMBRICAS

188. Es posible utilizar varios métodos para acceder a las redes Wi-Fi, incluyendo puntos de acceso abiertos, WEP cifrado, WPA2 PSK cifrado y redes protegidas por 802.1x EAP-TLS. Los ajustes de cada punto de acceso se almacenan de forma independiente, de modo que las credenciales de una red no se usan para ninguna otra. En el caso de las redes no abiertas, el administrador del punto de acceso en concreto deberá facilitar la configuración necesaria para acceder a ellas.

189. Encontrará una selección de redes *Wi-Fi* en el menú *Settings/Connections (Ajustes/Conexiones)*. Aquí puede utilizarse una selección para habilitar/deshabilitar toda la conectividad Wi-Fi. Para otras configuraciones, seleccione el elemento *Wi-Fi*, en lugar del botón *on/off* (encendido/apagado). Cuando está activado es posible conectarse a cualquier red visible desde el listado de puntos de acceso que se muestra debajo de la configuración. Esto incluye tanto las redes visibles, pero no configuradas (p. ej., redes a las que no se ha conectado con anterioridad), las redes visibles a las que se ha conectado y configuraciones de red guardadas que no se encuentran al alcance en ese momento. Si estuviera conectado a alguna red, esta se mostraría al principio de la lista como *Connected* (Conectada).

190. Al final de la lista de puntos de acceso (suponiendo que la conectividad Wi-Fi está activada) se muestra la opción *Add network* (Añadir red**)**. Desde esta selección podrá configurar una red que puede estar oculta (p. ej., porque no se está transmitiendo su SSID) o fuera del alcance.

191. Utilice la información facilitada por el administrador del punto de acceso para rellenar la información del menú emergente *Add network (Añadir red)*.

192. **Nota:** En el Modo CC, algunos modos de 802.1x EAP (como LEAP y PEAP) están deshabilitados.

- **Configuración de las conexiones EAP-TLS**

193. Para configurar una conexión mediante EAP-TLS, seleccione la opción *Add network (Añadir red)* e introduzca la información siguiente:

    - *Network name* (Nombre de la red):– el SSID de la red inalámbrica.
    - *Security* (Seguridad): seleccione 802.1x EAP en la lista.
    - *EAP method* (Método EAP): – seleccione TLS en la lista.
    - *CA certificate* (Certificado de CA):– seleccione el certificado de CA empleado para validar el certificado de punto de acceso de la lista desplegable.
    - *User certificate* (Certificado de usuario):– seleccione en la lista desplegable el certificado de usuario que se utilizará para autenticar el dispositivo en el punto de acceso.
    - *Identity* (Identidad):– el identificador del dispositivo/usuario (facilitado por el administrador del punto de acceso).

194. También pueden configurarse las opciones avanzadas siguientes:

- Proxy: – puede especificar un servidor proxy (ninguno, manual o configuración automática).
- IP settings (Ajustes de IP):– especifique si la conexión utilizará un servidor DHCP o una dirección IP estática.
- *Key Management* (Gestión de claves):– si está disponible en su punto de acceso, esta opción se corresponde con la gestión de claves de movilidad rápida.
- FT – 802.11r Fast Roaming.
- CCKM – Cisco Centralized Key Management.

195. **Nota:** Las funciones de gestión de claves se incluyen en la configuración con el fin de que esta sea lo más completa posible; no se incluyen como parte de la configuración probada y deberían dejarse en blanco.

10 EMPAREJAMIENTO BLUETOOTH

196. En el caso de que un usuario tenga necesidad de conectar su dispositivo móvil a uno o varios dispositivos Bluetooth distintos es importante asegurarse de que se emparejan correctamente. Algunos periféricos no cuentan con interfaces de emparejamiento (como los auriculares o el ratón), mientras que otros sí (como otros dispositivos inteligentes, por ejemplo un coche).

197. La diferencia fundamental entre estos tipos de dispositivos es la capacidad de transferir información a ellos. Por ejemplo, mientras habla o escucha a través de unos auriculares Bluetooth con micrófono no puede transferir archivos ni datos almacenados en ellos. Las conexiones a dispositivos que permiten estas funciones deben emparejarse siempre de forma expresa antes de usar ninguna funcionalidad entre ellos.

Inicio de un emparejamiento desde su dispositivo

198. Para configurar un emparejamiento seguro desde su dispositivo, siga estos pasos:

    a) Habilite la conexión Bluetooth (bien mediante *Settings/Connections* (Ajustes/Conexiones) o los ajustes rápidos).

    b) Abra *Settings/Connections/Bluetooth* (Ajustes/Conexiones/Bluetooth). Configure el otro dispositivo para que esté visible.

    c) Cuando abra los ajustes de Bluetooth, su dispositivo realizará una búsqueda automática de otros dispositivos. Si no se encontrase el dispositivo, pulse *SCAN* (Buscar) y se iniciará otra búsqueda de dispositivos.

    d) Pulse el nombre del dispositivo.

    e) En el diálogo *Bluetooth pairing request* (Solicitud de emparejamiento Bluetooth), asegúrese que el PIN mostrado coincide en ambos dispositivos. Se trata de un número de 6 dígitos y cambiará cada vez que intente emparejar dos dispositivos (aunque sean los mismos).

    f) Si el PIN de ambos dispositivos coincide, pulse OK para aceptar el emparejamiento.

199. Ahora, los dispositivos están emparejados.

Aceptar un emparejamiento desde su dispositivo

200. Para establecer un emparejamiento seguro iniciado desde otro dispositivo que se conecta al suyo, siga los pasos indicados a continuación:

    a) Habilite la conexión Bluetooth (bien mediante Settings/Connections (Ajustes/Conexiones) o los ajustes rápidos).

b) Abra Settings/Connections/Bluetooth (Ajustes/Conexiones/Bluetooth). Esto hará que su dispositivo sea visible hasta que se cierre esta pantalla.

c) Desde el otro dispositivo, busque y encuentre su dispositivo, y seleccione la opción de emparejamiento.

d) En la opción de menú Bluetooth pairing request (Solicitud de emparejamiento Bluetooth), asegúrese que el PIN mostrado coincide en ambos dispositivos. Se trata de un número de 6 dígitos y cambiará cada vez que intente emparejar dos dispositivos (aunque sean los mismos).

e) Si el PIN de ambos dispositivos coincide, pulse OK para aceptar el emparejamiento.

201. Ahora, los dispositivos están emparejados.

11 REGISTROS DE AUDITORÍA

202. En un despliegue que cumpla las recomendaciones establecidas en este documento, la función de auditoría debe habilitarse y los eventos ser recuperados mediante la solución de EMM. Para habilitar la recopilación de registros de auditoría, el cliente EMM instalado en el dispositivo debe tener la licencia Knox Premium SDK "KLM" o Knox Platform for Enterprise (KPE) Premium activada.

203. Los registros de auditoría se almacenan en formato comprimido para minimizar el espacio y maximizar el número de registros que pueden guardarse. Cuando el espacio asignado está lleno se sobrescriben los eventos más antiguos, de modo que se conserven siempre los más recientes (almacenamiento de registros circular o en búfer). Las notificaciones se envían a la solución de EMM en función del espacio de registros que se está llenando, para enviar una advertencia antes de que tenga lugar el borrado.

204. La cantidad mínima de espacio asignado al almacenamiento de datos de auditoría es de 10 MB, con un máximo de 50 MB, en función del espacio libre disponible cuando se activa. Cuando se activa la función de auditoría debe haber, al menos, 200 MB de espacio disponible (en caso contrario se notificará un error a la solución de EMM), y no se utilizará más del 5 % del espacio libre disponible, hasta un máximo de 50 MB. El espacio asignado no se ajusta después de su configuración inicial.

205. Dentro del registro también se pueden filtrar de forma explícita los eventos que se deben almacenar en el registro.

206. Para la selección de valores relacionados con las capacidades de auditoría en el sistema, los administradores TIC de la organización pueden acudir a los documentos CCN-STIC en los que se tratan en profundidad las capacidades y exigencias relacionadas en función del nivel de seguridad exigible al sistema.

11.1 TIPOS DE EVENTOS DE AUDITORÍA

207. Existen tres clases de eventos de auditoría que pueden registrarse: Sistemas y Aplicaciones, Kernel y Tablas IP. Cada uno de ellos puede controlarse de forma individual, a fin de registrar solo clases de eventos seleccionadas. El registro del kernel y de la tabla de IP genera una gran cantidad de eventos, por lo que se aconseja prestar atención, ya que la solución de EMM recopila los registros con mucha frecuencia si están activados, o la función de almacenamiento de registros circular podría provocar que los eventos se sobrescriban y pierdan.

11.2 AJUSTES DE RECOPILACIÓN DE DATOS DE AUDITORÍA

AJUSTE	VALOR	DESCRIPCIÓN	CLASE O MÉTODO
Habilitar auditoría	-	Habilita la recopilación de datos de auditoría.	enableAuditLog()
Deshabilitar auditoría	-	Deshabilita la recopilación de datos de auditoría.	disableAuditLog()
Configurar filtros de registro	Ver tabla de ajustes de filtros	Configura qué eventos deben registrarse (ver tabla de filtros).	setAuditLogRules( )
Habilitar la auditoría de tablas de IP	-	Habilita la recopilación de tablas de IP.	enableIPTablesLogging()
Deshabilitar la auditoría de tablas de IP	-	Deshabilita la recopilación de tablas de IP.	disableIPTablesLogging()

208. Ajustes de filtros de recopilación de datos de auditoría:

Miembro	Valores	Valores y descripción
setSeverityRule(int severityRule)	1 = Alerta 2 = Crítica 3 = Error 4 = Advertencia 5 = Aviso	Especifica el nivel mínimo de gravedad que se debe registrar. Se registrarán todos los eventos con el número especificado o inferior.
setOutcomeRule(int outcomeRule)	0 = Fallo 1 = Correcto 2 = Todo	Especifica el filtro basándose en los resultados de cada evento.
setGroupsRule(List<Integer> groupsRule)	1 = Seguridad 2 = Sistema 3 = Red 4 = Eventos 5 = Aplicación CERO = Todos	Especifica los grupos de eventos que deben registrarse. El valor CERO registrará eventos de todos los grupos.

Miembro	Valores	Valores y descripción
setKernelLogsEnabled(boolean enableKernel)	Verdadero = Habilitado Falso = Deshabilitado	Habilita o deshabilita el registro de datos del kernel.

11.3 CAMPOS DE REGISTRO DE AUDITORÍA

209. Los registros de auditoría constan de 8 campos que se describen en la tabla siguiente.

CAMPO	DESCRIPCIÓN
Marca temporal	Valor largo que representa la marca temporal de UTC.
Severidad	Número entero que representa la gravedad: 1 (alerta), 2 (crítica), 3 (error), 4 (advertencia), 5 (aviso)
Grupo	Número entero que representa el código de grupo: 1 (seguridad), 2 (sistema), 3 (red), 4 (eventos), 5 (aplicación)
Resultado	Número entero que representa el resultado del evento: 1 (correcto), 0 (fallo)
PID	Número entero que representa el ID del proceso
USERID	Número entero que representa el ID del usuario para el cual se generó el registro. El ID 0 se corresponde con un usuario normal. El ID 1 se corresponde con eventos del sistema. El ID 100-102 se corresponde con usuarios del contenedor (pueden definirse varios contenedores).
Componente	Cadena que representa el nombre del componente de software/instalación.
Mensaje	Descripción del evento en forma de mensaje libre (por lo general, mensaje inteligible para personas).

11.4 EVENTOS Y GESTIÓN DE AUDITORÍAS

210. Una nota importante acerca de las capacidades de auditoría, es que están vinculadas a la inscripción en un servidor de administración (EMM). Si el dispositivo no está inscrito, no es posible habilitar la función de auditoría y, cuando se anula la inscripción de un dispositivo, los registros de auditoría se

eliminan como parte del proceso de anulación de registro, de modo que se perderán los posibles eventos creados entre el último análisis o carga y el momento en el que se produce la anulación del registro.

11.5 EVENTOS DE AUDITORÍA

211. La siguiente lista de registros de auditoría se generan en relación con la funcionalidad requerida en el MDFPP, Perfil de protección Common Criteria.

Eventos del servicio de auditoría y del sistema:

Mensaje	Descripción
El estado de AuditLog ha cambiado a <enable>	Muestra el estado del registro de auditoría. Tenga en cuenta que, al deshabilitarlo, los registros de auditoría se eliminan.
AuditLog ha alcanzado su tamaño crítico. El porcentaje es <value>	Muestra que el espacio de almacenamiento de datos de auditoría ha alcanzado el porcentaje de llenado establecido en <value>.
Arranque de Android completado	Se ha completado el inicio del sistema operativo.
Android se apagará	Se ha enviado una orden de apagado al dispositivo (desde alguna fuente).
Las normas de filtro de AuditLog han cambiado	Las normas de filtro del registro de datos de auditoría han cambiado.

Eventos del Modo Common Criteria:

Mensaje	Descripción
El administrador <admin pkg name> ha solicitado <enable, disable> el Modo CC	Muestra si la política habilita o deshabilita el Modo CC.

Eventos estado de arranque Common Criteria

212. La siguiente tabla muestra los eventos que se generan cuando el Modo CC se habilita por primera vez y en cada arranque siguiente.

Mensaje	Descripción
Integrity verification <status>	Muestra si los test de integridad fueron satisfactorios.

Mensaje	Descripción
FIPS self-test <status>	Muestra si BoringSSL FIPS self-tests se han completado satisfactoriamente.
Direction lock <status>	Desbloqueo asistido status
Password attempts <status>	Contraseña (intento) ha sido configurada.
Screen lock <status>	Complejidad de la Contraseña. Se mostrará OK cuando la complejidad de la contraseña es al menos alfanumérica.
Recovery password <status>	Exchange ActiveSync recuperación de contraseña status
Password history length <status>	Contraseña historia y status
Certificate revocation <status>	Revocación de Certificado status
Device encryption <status>	Secure Startup/Inicio Seguro status
Face lock <status>	Bloqueo facial status

Eventos relacionados con el cifrado:

213. Estos eventos incluyen el Cifrado de datos en el dispositivo, el Cifrado de soportes externos y las funciones FDP_DAR_EXT.2 Common Criteria.

Mensaje	Descripción
El administrador <admin pkg name> ha solicitado el cifrado del soporte de almacenamiento	Estos mensajes muestran que la solución de EMM habilita el Cifrado de datos en el dispositivo. Se solicita el ajuste, a continuación se solicita el proceso de cifrado y, por último, se muestra que este está activo una vez finalizado el proceso de cifrado.
El administrador <admin pkg name> ha solicitado el cifrado de la tarjeta SD.	Estos mensajes muestran que la solución de EMM está habilitando el cifrado de la tarjeta SD.

Mensaje	Descripción
El administrador <admin pkg name> ha solicitado el cifrado del soporte de almacenamiento externo	Estos mensajes muestran que la solución de EMM está habilitando el cifrado del soporte de almacenamiento externo (del mismo modo que cuando se conecta un soporte al puerto USB).
Cifrado de la tarjeta de almacenamiento <succeeded/failed>	Muestra que el cifrado del soporte de almacenamiento de la tarjeta SD se ha completado con éxito o que ha fallado.
id_usuario[<uid>]/pid[<pid>] no pudo acceder al archivo [<archivo>]	Muestra un error de los servicios de almacenamiento relacionado con FDP_DAR_EXT.2.

Eventos de administración:

Mensaje	Descripción
El administrador <pkg name> ha cambiado el número máximo de errores de contraseña tras el cual se borrarán los datos del dispositivo a <value>	Muestra que se ha determinado el número máximo de errores de contraseña tras el cual se borrarán los datos del dispositivo en <value>.
El administrador <admin pkg name> ha cambiado la longitud mínima de la contraseña a <value>.	La longitud mínima de la contraseña se ha establecido en <value>.
El administrador <admin pkg name> ha cambiado la longitud mínima de la contraseña a <value>.	La calidad (complejidad) de la contraseña se ha establecido en <value>.
El administrador <admin_pkg> ha cambiado el tiempo de bloqueo de pantalla a <value msec>	El tiempo de espera de la sesión para bloquear la pantalla se ha establecido en <value msec>
El administrador <admin_pkg> ha cambiado el número máximo de errores de contraseña para deshabilitar el inicio de sesión a <value>	El número máximo de errores de contraseña se ha establecido en <value>

Mensaje	Descripción
El administrador <admin_pkg> ha cambiado el número máximo de caracteres repetidos en <value>	El número máximo de veces que puede repetirse el mismo carácter en una contraseña se ha establecido en <value>
El administrador <admin_pkg> ha cambiado el plazo de caducidad de la contraseña a <value msec>	El plazo de caducidad de la contraseña se ha establecido en <value msec>
El administrador <uid> ha <allowed|disallowed> <biometric type>.	El administrador ha permitido o bloqueado el acceso al método de biométrica concreto indicado: BIOMETRIC_AUTHENTICATION_FINGERPRINT (HUELLA DACTILAR) BIOMETRIC_AUTHENTICATION_IRIS (IRIS)
Admin <admin_pkg> tiene <allowed/disabled> agentes de confianza. *Admin <admin_pkg> tiene <enabled/disabled> agente de confianza <agent_ComponentInfo>.*	Configuración Smart Lock ha sido habilitado/deshabilitado
El administrador <admin_pkg> ha <enabled, disabled> el texto de reinicio [con texto <text>] *Se ha habilitado la secuencia de bloqueo de pantalla.* *Se ha modificado la secuencia de bloqueo de pantalla a <value>* *El administrador <admin> ha borrado la secuencia de bloqueo de pantalla*	Ajuste del mensaje de inicio de sesión

Mensaje	Descripción
Admin <admin_pkg> tiene <allowed|enabled, disallowed|disabled> <feature>	Administrador ha habilitado o deshabilitado las siguientes funcionalidades: Camera Microphone Developer mode Airplane mode USB Tethering setting Wi-Fi Tethering setting Bluetooth tethering NFC Cellular data USB debugging USB Media Player (MTP) VPN S-Beam Android Beam S-Voice USB Host Storage Bluetooth discoverable state Set VPN Always On mode
Admin <admin_pkg> ha cambiado WiFi permitido a <true, false>	Admin ha habilitado o deshabilitado Wi-Fi
Admin <admin_pkg> ha cambiado permitir bluetooth a <true, false>	Admin ha habilitado o deshabilitado Bluetooth
Admin <admin_pkg> ha <permitido/bloqueado> <A2DP/AVRCP/HFP/HSP/PBAP/SPP> perfil bluetooth.	Admin ha habilitado o deshabilitado perfiles específicos de Bluetooth.
Admin <admin_pkg> ha <enabled, disabled> hora automatica. *Admin <admin_pkg> ha <enabled, disabled> cambios de fecha y hora.* *Admin <admin_pkg> ha <enabled, disabled> hora automática requerida.*	Admin ha habilitado o deshabilitado configuración de fecha y hora.

Mensaje	Descripción
Admin <admin_pkg> ha configurado su aplicacion como removable/not emovable *Admin <admin_pkg> ha configurado un <target_pkgName> como removable/not removable.*	El agente EMM o alguna aplicación específica se han configurado como desinstalable. En caso contrario el usuario no podrá eliminarlo dichas aplicaciones.

Gestión del contenedor de Knox:

214. La mayoría de las funciones de gestión del contenedor (como la gestión de contraseñas o el acceso a cámara) generan los mismos mensajes que afuera del contenedor. Los mensajes generados dentro del contenedor se marcarán con el ID del contenedor (por lo general, 100).

Mensaje	Descripción
El administrador <admin pkg name> ha solicitado correctamente la creación del contenedor.	Se ha solicitado la creación de un contenedor Knox.

Eventos Uso compartido del contenedor Knox:

Mensaje	Descripción
El administrador <uid> ha <allowed|disallowed> el movimiento de aplicaciones al contenedor.	El administrador ha permitido o deshabilitado el movimiento de aplicaciones al contenedor.
El administrador <uid> ha <allowed|disallowed> el movimiento de archivos al contenedor.	El administrador ha permitido o deshabilitado el movimiento de archivos al contenedor.
El administrador <uid> ha <allowed|disallowed> el movimiento de archivos al propietario.	El administrador ha permitido o deshabilitado el movimiento de archivos desde el contenedor.

Eventos de Acceso a soportes externos:

Mensaje	Descripción
El administrador <admin pkg name> ha <enabled/disabled> el acceso a la tarjeta SD externa	Muestra que se ha permitido o bloqueado el montaje de la tarjeta SD.
[SDFAT](mmcblk0p1[<ID>]): trying to unmount... *[SDFAT](mmcblk0p1[<ID>]): unmounted successfully!*	Muestra eventos de desmontado para SD card.
[SDFAT](mmcblk0p1[<ID>]): trying to mount... *[SDFAT](mmcblk0p1[<ID>]): mounted successfully!*	Muestra eventos de montado para SD card.

Eventos de restablecimiento de valores de fábrica:

215. Estos eventos solo se corresponden con errores de restablecimiento, puesto que, por definición, un restablecimiento con éxito borraría los registros de auditoría.

Mensaje	Descripción
Iniciando la eliminación de los datos del usuario	Este evento aparece cuando se produce un fallo en la eliminación de datos y los registros no se borran.

Eventos de comandos de administración:

Mensaje	Descripción
El administrador <admin pkg name> ha bloqueado el dispositivo	El administrador ha forzado el bloqueo del dispositivo.
El administrador <admin pkg name> ha solicitado la eliminación total de los datos del dispositivo	El administrador ha enviado un comando para forzar el restablecimiento de los valores de fábrica.

Eventos de gestión de claves:

Mensaje	Descripción
Generación de claves fallida, con error <number>	Se ha producido un error en la generación de una pareja de claves.
Actividad de importación de claves (almacén de claves=<keystore>, nombre de clave=<keyname>, ID de usuario=<target uid>, solicitada por <pkg name>: UID=<uid> función=<SystemApp, UserApp> | <Administrator, NonAdministrator>) finalizada correctamente *Se ha producido el error <error msg> en la actividad de importación de claves (almacén de claves=<keystore>, nombre de clave=<keyname>, ID de usuario=<target uid>, solicitada por <pkg name>: UID=<uid> función=<SystemApp, UserApp> | <Administrator, NonAdministrator>)*	Muestra que la importación de claves al almacén de claves ha finalizado correctamente o ha fallado.
Actividad de destrucción de claves (almacén de claves=<keystore>, nombre de clave=<keyname>, ID de usuario=<target uid>, solicitada por <pkg name>: UID=<uid> función=<SystemApp, UserApp> | <Administrator, NonAdministrator>) finalizada correctamente *Se ha producido el error <error msg> en la actividad de desrucción de claves (almacén de claves=<keystore>, nombre de clave=<keyname>, ID de usuario=<target uid>, solicitada por <pkg name>: UID=<uid> función=<SystemApp, UserApp> | <Administrator, NonAdministrator>)*	Muestra que el borrado de claves al almacén de claves ha finalizado correctamente o ha fallado.
Chequeo de Integridad de Clave Fallido: nombre clave = <filename>, uid=<uid>	Muestra que el chequeo de integridad de una clave en el almacén de claves ha fallado.

Eventos de revocación de certificación:

Mensaje	Descripción
El ID de administrador <admin pkg name> ha <enabled, disabled> la comprobación de la revocación de certificado para <pkg name>	Muestra la habilitación o deshabilitación de la comprobación de la revocación de certificado. <pkg name> muestra si se ha modificado para paquetes específicos. Si se aplica a todos los paquetes, se muestra «*».
El ID de administrador <admin pkg name> ha <enabled, disabled> el OCSP para <pkg name>	Muestra la habilitación o deshabilitación de la comprobación de OCSP. <pkg name> muestra si se ha modificado para paquetes específicos. Si se aplica a todos los paquetes, se muestra «*».
La instalación del certificado finalizó correctamente. Almacén de claves <keystore>, <certificate information> *La eliminación del certificado finalizó correctamente. Almacén de claves <keystore>, <certificate information>*	Muestra el estado de añadir y eliminar certificados de usuario de la Trust Anchor Database (Base de datos de ancla de confianza).
El borrado de credenciales finalizó correctamente. Almacén de claves: <Wi-Fi, VPN and Apps> *El borrado de credenciales finalizó correctamente. Almacén de claves: predeterminado*	Muestra el borrado de credenciales en la Trust Anchor Database asociado a aplicaciones específicas (o todas).
Se produjo un error al verificar la cadena. Certificado [<num>]: <cert subject> Emisor: <cert issuer> Motivo: <error msg>	Se muestra cuando se produce un error de validación de certificado X.509v3.
Se produjo un error en CertPathValidator: <error>	Muestra mensajes de error de fallos en el chequeo de certificados, CRL u OCSP.
Se produjo un error en CertPathValidator: no ha sido posible determinar el estado de revocación debido a un error de red.	Muestra mensajes de error de fallos de CRL u OCSP.

Mensaje	Descripción
Se produjo un error en CertPathValidator: CTRL-EVENT-EAP-TLS-CERT-ERROR reason=<Certificate info> err=<error>.	Errores en la Verificación de Certificado EAP-TLS

Eventos de gestión de Wi-Fi:

Mensaje	Descripción
El ID de administrador <admin pkg name> ha cambiado la restricción de SSID de Wi-Fi a <true/false>	Habilita o deshabilita la lista blanca/negra de SSID.
El ID de administrador <admin pkg name> ha <added/removed> el SSID <SSID name> a/de la restricción de <blacklist/whitelist>	El administrador ha añadido o eliminado SSID específicas a la lista blanca o negra. Se puede usar «*» en la lista negra para indicar que todas las redes han sido bloqueadas, salvo las permitidas de forma expresa.
El ID de administrador <admin pkg name> ha eliminado todos los SSID de la <blacklist/whitelist> de restricción	El administrador ha eliminado todos los SSID de la lista especificada.
El ID de administrador <admin pkg name> ha <allowed/blocked> el acceso al SSID de Wi-Fi <SSID name>	Control de SSID individual sin habilitar la lista blanca/negra.
El ID de administrador <admin pkg name> ha configurado un nuevo perfil de Wi-Fi: SSID: <SSID name> Tipo de seguridad <security> Certificado de CA: <cert>	El administrador ha enviado un nuevo perfil de Wi-Fi al dispositivo.

Eventos de status de Conexión Wi-Fi:

Mensaje	Descripción
Wi-Fi is <connected to, disconnected from> <SSID> network using EAP-TLS channel	Wi-Fi está conectada/desconectada de SSID usando EAP-TLS
Realizando intent de conectar a un AP. SSID: <SSID>	Wi-Fi está intentando conectar a un AP

Mensaje	Descripción
Connecting to Wi-Fi network whose ID is <number> <succeeded, failed>	Conexión a la red Wi-Fi Establecida/Fallida
AP está bloqueado por el Administrador. SSID: <SSID>	El SSID está bloqueado por el administrador

Eventos de sesión remota:

Mensaje	Descripción
La aplicación (<pkg name>, <uid>) ha iniciado un protocolo de enlace SSL/TLS con un terminal de conexión remoto (<dst name>:<dst port>) *La aplicación (<pkg name>, <uid>) ha finalizado un protocolo de enlace SSL/TLS con un terminal de conexión remoto (<dst name>:<dst port>)* *La aplicación (<pkg name>, <uid>) ha finalizado una sesión SSL/TLS con un terminal de conexión remoto (<dst name>:<dst port>)* *La aplicación (<pkg name>, <uid>) ha iniciado un protocolo de enlace HTTPS con un terminal de conexión remoto (<dst name>:<dst port>)* *La aplicación (<pkg name>, <uid>) ha finalizado un protocolo de enlace HTTPS con un terminal de conexión remoto (<dst name>:<dst port>)* *La aplicación (<pkg name>, <uid>) ha finalizado una sesión HTTPS con un terminal de conexión remoto (<dst name>:<dst port>)*	Muestra que las aplicaciones han iniciado conexiones SSL, TLS o HTTPS con terminales remotos.
La aplicación (<pkg name>, < uid>) recibió una excepción de protocolo SSL: Protocolo de conexión (fallido, abortado) Motivo: <error msg>	Muestra que las aplicaciones han intentado iniciar conexiones SSL, TLS o HTTPS con terminales remotos, pero que se produjo el error que se especifica en el <error msg>

Mensaje	Descripción
Se produjo un error al verificar el identificador. Identificador presentado: <identifier> Lista de identificadores de referencia: <reference identifiers>	Muestra el identificador presentado que debe comprobarse y rechazarse.
El Wi-Fi no ha podido conectarse a la red <access point>. Motivo: <msg reason>. *El Wi-Fi está conectado a la red <SSID> utilizando el canal <Type of Channel>* *El Wi-Fi se ha desconectado de la red <SSID> usando el canal EAP-TLS*	Mensajes de estado de EAP-TLS Errores: Error de autenticación – Certificado de cliente no válido
Se produjo un error en el protocolo de enlace SSL: Error de SSL_connect <error #>: rutinas de SSL:<routine>:<error msg>	Los errores de certificado se muestran en el procesamiento de EAP-TLS
EAP-TLS handshake failed: CTRL-EVENT-EAP-TLS-ALERT <error> *EAP-TLS handshake failed: CTRL-EVENT-EAP-TLS-HANDSHAKE-FAIL <error>*	EAP-TLS errores de negociación de conexión.
Wi-Fi ha fallado en contectarse a la red <SSID> usando canal EAP-TLS. Reason: Authentication failure	EAP-TLS Fallo en la autenticación de la conexión.

Eventos de instalación/actualización de aplicaciones:

Mensaje	Descripción
El administrador <admin pkg name> ha <allowed/blocked> el acceso a Google Play Store (com.android.vending)	Muestra si Google Play Store está permitida o no.
El administrador <admin pkg name> ha <allowed/disallowed> la instalación de una aplicación ajena a Google Play	El administrador ha permitido o bloqueado «Orígenes desconocidos» para la instalación de aplicaciones.
Iniciando la instalación de la aplicación <pkg name> *La instalación de la aplicación <pkg name> <succeeded/failed>*	La instalación o actualización de una aplicación ha comenzado y ha finalizado correctamente o ha fallado.

Mensaje	Descripción
La desinstalación de la aplicación <pkg name> <succeeded/failed>	La eliminación de la aplicación ha finalizado correctamente o ha fallado.
El administrador <admin pkg name> ha <installed/removed> la aplicación <pkg name>	El administrador ha instalado o eliminado la aplicación mediante la política
Aplicación instalada desde ruta de archivo insegura <path>	La aplicación instalada contiene una ruta de archivo insegura (como una extensión de archivo incorrecta, aunque el archivo fuese un paquete adecuado).
El administrador <admin pkg name> ha instalado una aplicación desde <path>	El administrador ha instalado una aplicación desde la ruta especificada.
El administrador <admin pkg name> ha impedido la instalación de <pkg names>	La política se ha configurado para evitar la instalación de las aplicaciones indicadas. Se utiliza «*» para señalar todas las aplicaciones que deben evitarse.
El administrador <uid> ha <added/removed> <signature> a la <whitelist/blacklist> de firmas de aplicaciones	El administrador ha añadido o eliminado una firma de desarrollador a una lista blanca o negra de aplicaciones. Esto permitirá o bloqueará todas las aplicaciones que lleven esta firma.
El administrador <uid> ha <added/removed> <signature> a la <whitelist/blacklist> de nombres de paquetes	El administrador ha añadido o eliminado un nombre de paquete a una lista blanca o negra de aplicaciones. Pueden usarse «*» y «?» como caracteres comodín a la hora de designar los nombres de paquetes.

Eventos de Gestión de Aplicación:

Mensaje	Descripción
Admin <admin_pkg> has <enabled/disabled> application <pkg name> *Admin <admin_pkg> has <enabled/disabled> system app <pkg name>*	El paquete of aplicación de Sistema ha sido habilitado/deshabilitado.
Admin <admin_pkg> has <enabled/disabled> Auto Fill Setting.	Autocompletar para el Explorador de Internet ha sido habilitado/deshabilitado. Nota: Solo Aplica al explorador de internet de serie en el dispositivo, no Chrome o ningún otro.
Admin <admin_pkg> has <added/removed> account <value> to the <addition/removal> <blacklist/whitelist>.	El Administrador ha configurado una cuenta/dominio de correo electrónico como habilitada o deshabilitada para ser configurada en el dispositivo.

Eventos de Gestión de correo electrónico:

Mensaje	Descripción
Admin id has added account <email addresses> to the addition blacklist	Direcciones de correo electrónico se han añadido a la lista negra.
Admin id has added account <email address> to the addition whitelist	Direcciones de correo electrónico se han añadido a la lista blanca.

Eventos de sincronización:

Mensaje	Descripción
La sincronización de cuenta <account name> finalizó correctamente	La cuenta ha finalizado correctamente una sincronización con el servidor asociado.

Eventos del usuario:

Mensaje	Descripción
Bloqueo de pantalla habilitado: contraseña	Esta opción muestra que el usuario ha establecido o restablecido su contraseña.

Eventos de ubicación:

Mensaje	Descripción
El administrador <admin pkg name> ha <started/stopped> el GPS	El administrador ha iniciado o detenido la radio GPS.
El administrador <admin pkg name> ha <enabled/disabled> el proveedor de servicios de ubicación <GPS/network/passive>	El administrador ha habilitado o deshabilitado el servicio de proveedor de ubicación especificado.

Eventos de actualización inalámbrica de firmware:

Mensaje	Descripción
Actualización de software: Actualización de software <version> finalizada correctamente *Actualización de software: Se produjo un error en la actualización de software <version>*	Muestra el estado del proceso de actualización inalámbrica de firmware para todos los operadores. El primer mensaje aparecerá antes del reinicio en el que se aplicará la actualización. El éxito o el error de la actualización se registrará en el reinicio posterior a la ejecución del proceso de actualización.
Actualización de software: Se inició la actualización de software <packageName> *Actualización de software: Actualización de software <version> finalizada correctamente* *Actualización de software: Se produjo un error en la actualización de software <version>*	Muestra el estado del proceso de actualización inalámbrica de firmware de Verizon Wireless. El primer mensaje aparecerá antes del reinicio en el que se aplicará la actualización. El éxito o el error de la actualización se registrará en el reinicio posterior a la ejecución del proceso de actualización.

Eventos de integridad:

Mensaje	Descripción
Se produjo un error en la verificación. No ha sido posible reiniciar el dispositivo. Se produjo un error en la verificación de integridad. Debe restablecer su dispositivo a los valores predeterminados de fábrica. Esta acción eliminará sus datos.	NOTA: Este texto se muestra en pantalla y fuerza un borrado de datos (sin archivo de registro).

12 ENVÍO SEGURO

216. Aunque un dispositivo Samsung requiere una configuración inicial para poder añadirse al entorno de la organización, es de vital importancia asegurarse de que el dispositivo se transporte y reciba de forma segura antes de su configuración, sin ninguna manipulación o modificación.

217. Es muy importante que los dispositivos que vayan a desplegarse en la organización se adquieran a través de proveedores de confianza y que, en la medida de lo posible, se implementen medidas de mitigación de los riesgos relacionados con la cadena de suministro.

218. En el momento de su recepción, las cajas que contengan el dispositivo, deberán constar tanto de una etiqueta de seguimiento como de dos etiquetas colocadas en ambos extremos de la caja, que indican si esta se ha abierto antes de su entrega. Si estos precintos estuviesen rotos, no se deben aceptar los dispositivos y deben devolverse al proveedor.

219. La etiqueta de seguimiento debería ser similar a la Figura 3. Etiqueta de seguimiento, mientras que las dos etiquetas de precinto deberían parecerse a la Figura 4. Precinto de seguridad (negro) o Figura 5. Precinto de seguridad (blanco).

Figura 3. Etiqueta de seguimiento

Figura 4. Precinto de seguridad (negro)

Figura 5. Precinto de seguridad (blanco)

- **Versiones de software pre-instaladas**

220. Los dispositivos Android de Samsung incluyen un gran número de aplicaciones software de diversos orígenes, diseñadas para ofrecer la máxima funcionalidad posible que espera el usuario. Se puede consultar una lista de las aplicaciones y sus versiones incluidas en cada dispositivo en la siguiente página web: https://support.samsungknox.com/hc/en-us/articles/115015195728

- **Versiones de software del dispositivo**

221. Para verificar las versiones de cualquier software incluido en el dispositivo (en comparación con la lista incluida en el sitio web), abra *Settings/Application manager* (Ajustes/Gestor de aplicaciones). En el apartado *All* (Todos) podrá ver las distintas aplicaciones instaladas en el dispositivo (tanto las instaladas de forma predeterminada como las que instaló usted mismo). Al seleccionar una aplicación se mostrarán sus propiedades. El número de versión se muestra al principio, bajo el nombre.

13 ACTUALIZACIONES SEGURAS

222. Una vez que se ha desplegado un dispositivo móvil en la organización, sería recomendable aceptar las actualizaciones del software instalado en el dispositivo para beneficiarse de las últimas funciones mejoradas del SO, así como disponer de las últimas actualizaciones de seguridad disponibles. Los dispositivos reciben las actualizaciones según un ciclo de producción en el que pueden intervenir tanto Google, como Samsung o proveedores de servicios de comunicaciones, basándose en distintos factores.

223. La periodicidad y el marco temporal durante el que se recibirán estas actualizaciones son factores clave en la selección del dispositivo, y es una de las principales variables que debe utilizar la organización a la hora de seleccionar uno u otro dispositivo para su despliegue.

224. Cuando haya actualizaciones disponibles, estas estarán firmadas por Samsung con una clave privada única para la combinación de dispositivo/operador (p. ej., Galaxy S9 con el Operador A no tendrá una actualización firmada con la misma clave que un Galaxy S9 con el Operador B). La clave pública está incrustada en la imagen del gestor de arranque (*bootloader*) y se utiliza para verificar la integridad y la validez del paquete de actualización.

225. Cuando haya actualizaciones disponibles para un dispositivo concreto (por lo general, se despliegan por fases en la red del operador), se pedirá al usuario que descargue e instale dicha actualización (consulte la Guía de usuario para obtener más información sobre la comprobación, descarga e instalación de la actualización). El software del dispositivo comprueba automáticamente la integridad y validez del paquete de actualización. Si la comprobación falla, se informa al usuario de que se produjo un error en la actualización y de que esta no se pudo instalar.

13.1 MÉTODOS DE ACTUALIZACIÓN PERMITIDOS

226. Cuando se habilita el Modo CC solo se permite la instalación de actualizaciones de firmware inalámbricas (FOTA) en el dispositivo. El resto de métodos de instalación de actualizaciones (como ODIN) permanecerán bloqueados y no podrán usarse para actualizar el firmware. Este planteamiento ofrece seguridad contra ataques locales y físicos que podrían modificar el software sin que el usuario lo percibiera.

13.2 BLOQUEO DE ACTUALIZACIONES

227. Es posible bloquear las actualizaciones de firmware inalámbricas en un dispositivo configurando *allowOTAUpgrade()* como falso mediante la solución de EMM. Esta opción puede emplearse bien para congelar el software instalado o para conceder a una organización tiempo para comprobar la actualización antes de permitir su despliegue en la comunidad de usuarios.

228. Esta opción no está recomendada, pero puede ser aceptable en casos particulares, donde el equipo de administradores TIC lo considere necesario en base al análisis de riesgos realizado en su organización.

14 ESTADOS EN EL CICLO DE VIDA

229. Se puede considerar que un dispositivo móvil pasa por cuatro estados en su ciclo de vida en el uso corporativo, según la función con la que el usuario accede al dispositivo:

    - modo de administrador;
    - modo de usuario;
    - modo de error; y
    - modo de recuperación.

230. Se considera que un dispositivo está en modo de administrador cuando el dispositivo está siendo gestionado y configurado por la organización (administradores TIC) y antes de su entrega al usuario.

231. El dispositivo se prepara y configura para su despliegue en el entorno de la organización mediante las llamadas a funciones API que realiza el agente EMM residente en el dispositivo. Los administradores del dispositivo móvil deben seguir y aplicar todas las directrices del administrador de forma fiable. Un usuario sin privilegios no tendrá acceso a este modo de funcionamiento.

232. Si se produce algún error o fallo de funcionamiento durante la transición del modo de administrador al modo de usuario, que provoque que el dispositivo entre temporalmente en modo de error de funcionamiento, el administrador deberá seguir las directrices de la solución de administración de dispositivos móviles para reparar el error y restaurar las capacidades operativas normales del dispositivo. Si no fuese posible eliminar el error o el fallo operativo correctamente, el dispositivo no deberá entregarse al usuario final y deberá devolverse al proveedor.

233. Después de configurar el dispositivo de acuerdo con los ajustes decididos como apropiadas por el administrador TIC de la organización, el dispositivo estará listo para su uso por parte de un usuario final. Cuando el usuario reciba el dispositivo, solo podrá ver la interfaz de usuario *TouchWiz* y no será posible hacer otros cambios en la configuración de seguridad. Una vez entregado al usuario, el dispositivo se dirá que está en modo de usuario. Dentro del modo de usuario, las únicas funciones relevantes para la seguridad a las que este podrá acceder son ”protección por contraseña de bloqueo de pantalla”, ”cambio de contraseña” y ”eliminación local de datos del dispositivo”. Por lo general, un administrador no accederá al dispositivo en este modo de funcionamiento.

234. El dispositivo también podrá encontrarse en un estado “modo de recuperación”, omitiendo el proceso de arranque estándar y permitiendo hacer cambios en la configuración de instalación de Android. No obstante, esto requiere que el gestor de arranque (*bootloader*) del dispositivo esté desbloqueado y, por lo tanto, no está dentro del ámbito de consideración de este documento.

15 ELIMINACIÓN DE DATOS

235. La configuración de seguridad evaluada ofrece la capacidad de eliminar los datos del dispositivo tanto localmente, como de forma remota. Según la configuración del dispositivo, es posible eliminar los datos externos al contenedor, del contenedor Knox solamente o ambos.

236. Una organización puede dar la orden de eliminación remota de datos (bien del dispositivo o solo del contenedor Knox, en función de la configuración), en los siguientes supuestos:

- La organización envía una orden de eliminación remota de datos al dispositivo:

a) cuando se ha perdido o han robado el dispositivo;

b) como respuesta a la notificación de un incidente;

c) en un esfuerzo por resolver problemas móviles actuales; y

d) por otros motivos de procedimiento, como cuando un dispositivo o usuario abandonan la organización.

15.1 ELIMINACIÓN DE LOS DATOS DEL DISPOSITIVO

237. La configuración de seguridad evaluada ofrece un proceso de eliminación local y remota de los datos de dispositivos de usuarios de Android. Este tipo de eliminación de datos funciona en el nivel del almacenamiento, y elimina todos los datos del dispositivo. En una configuración de contenedor Knox, esta opción elimina todos los datos, incluido el contenedor Knox (así como todo lo que no esté dentro del contenedor). Este tipo de eliminación de datos está disponible en todas las configuraciones.

238. La eliminación local de datos la inicia de forma manual el usuario del dispositivo Android o cuando se supera el número máximo de intentos de inicio de sesión incorrectos. Por lo general, el proceso de eliminación remota de datos se inicia de forma remota por el administrador TIC de la organización mediante un comando de eliminación remota de datos.

15.2 ELIMINACIÓN DE LOS DATOS DEL CONTENEDOR KNOX

239. Cuando se ha habilitado un contenedor Knox, también se pueden eliminar solamente los datos almacenados en el contenedor. Al eliminar los datos del contenedor Knox se eliminará el contenedor, incluyendo las aplicaciones y los datos, pero no eliminará ningún elemento externo al contenedor Knox. Este proceso de eliminación remota de datos debe iniciarlo de forma remota el administrador del dispositivo móvil y de la organización mediante un comando de eliminación remota de datos.

240. El único modo de que un usuario pueda eliminar los datos del contenedor Knox de forma local es cancelar la inscripción del dispositivo en la solución de EMM. Una vez hecho esto, el contenedor Knox, todos los datos y las aplicaciones, así como el agente de EMM, se eliminarán del dispositivo.

15.3 ELIMINACIÓN DE LOS DATOS DEL USUARIO

241. A fin de proteger la confidencialidad e integridad de la información de su dispositivo, el dispositivo está configurado para que los datos que contiene puedan eliminarse. En el caso de eliminarse, la clave de cifrado del dispositivo se borrará y se producirá una eliminación parcial de todos los datos del usuario. Esto implica que no podrá accederse a los datos del usuario, sin posibilidad de recuperación. A continuación, el dispositivo se reiniciará y se restablecerán los ajustes predeterminados de fábrica.

242. El dispositivo podrá borrarse en los siguientes supuestos:

- cuando inicie una eliminación de datos manual (*Settings/General management* [Ajustes/Administración general] y *Reset/Factory data reset* [Restablecer/Restablecer valores de fábrica]);
- cuando el usuario o un tercero superen el número máximo de intentos incorrectos de inicio de sesión permitidos por el límite del dispositivo local para la eliminación de los datos que contiene (establecido por el administrador de su organización);
- la organización puede decidir enviar una orden de eliminación remota de datos al dispositivo en función de diferentes eventos, por ejemplo:
    - cuando se ha perdido o han robado el dispositivo;
    - como respuesta a la notificación de un incidente;
    - en un esfuerzo por resolver problemas móviles actuales;
    - por otros motivos de procedimiento, como cuando abandona la organización.

16 USO DEL CLIENTE VPN

243. A pesar de que los dispositivos Samsung incluyen un cliente VPN certificado conforme según a Common Criteria, algunas organizaciones pueden necesitar un cliente VPN de un proveedor externo. Android ofrece la clase pública *android.net.VpnService* para proveedores externos, a fin de crear clientes VPN que puedan instalarse y usarse para funcionalidades adicionales a las que ofrecen los clientes VPN integrados de Android o Samsung. El cliente de software VPN creado mediante esta interfaz podría ofrecer su propia interfaz de gestión externa a la proporcionada por Samsung.

244. Puede encontrarse más información al respecto aquí:

    https://seap.samsung.com/api-references/android-premium/reference/com/sec/enterprise/knox/profile_creation.pdf

245. Se puede descargar el cliente VPN de https://seap.samsung.com/

246. Después de iniciar sesión, siga la ruta siguiente:

    Home > SDKs Overview > Knox VPN SDK > Tools >

    Knox VPN Client - Android VPN Management for Knox

247. A continuación, haga clic en ”*Download*” (Descargar) para obtener el archivo APK.

17 GUÍA PARA EL USUARIO FINAL

248. El usuario final de un dispositivo móvil, que debido a la información que maneja, quede bajo la autoridad operativa de la organización, tiene la responsabilidad de colaborar con la organización a mantener la seguridad del dispositivo Samsung y seguir la normativa tanto interna como externa que le sea de aplicación.

249. Algunos aspectos importantes de la seguridad del dispositivo se basan en las acciones del usuario, de modo que el mismo deberá ser consciente de sus responsabilidades y tomar las medidas apropiadas para ayudar a garantizar la seguridad del dispositivo. En concreto, el usuario del dispositivo es responsable de:

- Establecer y garantizar la protección con una contraseña lo suficientemente compleja.
- Ser consciente de su entorno circundante cuando utilice el dispositivo.
- Informar de cualquier actividad sospechosa o incidente de seguridad.
- Ser cauto a la hora de instalar aplicaciones.
- Usar el dispositivo de acuerdo con la política de la organización.
- Ayudar a la organización a inscribir el dispositivo en la configuración evaluada (aplicar seguridad al dispositivo) y proteger el dispositivo móvil cuando no lo esté usando.

17.1 GESTIÓN DE CONTRASEÑAS

250. Los usuarios deberán establecer una contraseña la primera vez que se configure el dispositivo, a fin de proteger la clave que cifrará los datos del dispositivo y de protegerlo contra el acceso no autorizado a sus funciones. Es de vital importancia que seleccione una contraseña apropiada y que no la comunique nunca a nadie.

Establecimiento de contraseñas

251. La complejidad aceptable de una contraseña la determinará el administrador y consistirá en lo siguiente:

- Número mínimo de letras requerido en la contraseña (a-z, A-Z).
- Número mínimo de letras minúsculas requerido en la contraseña (a-z).
- Número mínimo de dígitos y caracteres especiales requerido en la contraseña (0-9 y caracteres especiales +=%_@#$/^&*()‘-”:!;?,`.~\|<>{}[]).
- Número mínimo de dígitos requerido en la contraseña (0-9).
- Número mínimo de símbolos requerido en la contraseña (+=%_@#$/^&*()‘-”:!;?,`.~\|<>{}[]).
- Número mínimo de letras mayúsculas requerido en la contraseña (A-Z).

252. Es importante que el usuario final entienda y asuma los requisitos establecidos en la Política de seguridad de la información o la Política de dispositivos móviles de su organización.

253. A la hora de establecer una contraseña, debería procurar **no**:

- Utilizar información conocida sobre su persona (p. ej., dirección, cumpleaños, nombres de mascotas, su nombre o cualquier información disponible públicamente).
- Incluir su nombre de usuario o el nombre de su organización en la contraseña.
- Establecer una contraseña similar a una contraseña anterior (no basta con añadir un «1» o «!» al final de la contraseña).
- Usar palabras del diccionario (Bienvenido1!).

254. Un buen método para crear contraseñas es pensar en una frase y utilizar los primeros caracteres de cada palabra. Por ejemplo:

¡Sí que quiero establecer una contraseña muy segura y que tenga 16 caracteres!

¡Sqqeucmsyqt16c!

Nota: No utilice esta contraseña.

17.2 USO DE LA CONTRASEÑA

255. El administrador establecerá una fecha de caducidad de la contraseña, que le exigirá que la cambie una vez transcurrido este tiempo (p. ej., 90 días). Es importante que elija una contraseña única cada vez y que no reutilice contraseñas anteriores, ni siquiera derivadas.

256. También tiene la responsabilidad de no revelar su contraseña a nadie. Esto incluye:

- Anotar su contraseña y colocarla en un lugar accesible para otras personas (como su ordenador o recursos en línea).
- Reutilizar la misma contraseña de otras cuentas (p. ej., correo electrónico, Twitter o Facebook).
- Facilitar la contraseña a terceros, incluidos familiares, de modo que puedan utilizar el dispositivo. Es importante destacar que su organización nunca le pedirá su contraseña, puesto que no la necesita.

17.3 SEGURIDAD FÍSICA DEL DISPOSITIVO

257. Es importante que el usuario mantenga el control del dispositivo en todo momento, a fin de reducir el riesgo de manipulación por parte de terceros no autorizados. Cuando no lo esté usando, deberá guardar el dispositivo en un lugar lo suficientemente seguro. En caso de duda, consulte la Política de

dispositivos móviles o póngase en contacto con el Equipo de seguridad o Administrador TIC de su organización.

258. El usuario final no debe conectar su dispositivo Samsung en ningún ordenador ni dispositivo que no esté gestionado por la organización o que no haya sido autorizado explícitamente por el Administrador TIC de su organización. En este sentido, se debe especialmente cuidadoso en las conexiones para la carga del dispositivo, utilizándose solo accesorios autorizados por la organización.

17.4 CONTROL DE APLICACIONES

259. Como parte de la configuración del dispositivo, el administrador TIC/Seguridad de la organización podrá decidir restringir o aplicar niveles de restricción a las aplicaciones del dispositivo. El usuario del dispositivo debe conocer la Política de uso aceptable del móvil de su organización, incluidas las posibles directrices o limitaciones relativas a las aplicaciones que puede descargar e instalar.

17.5 INFORME DE CUALQUIER ACTIVIDAD SOSPECHOSA Y DE LOS INCIDENTES DE SEGURIDAD

260. Es muy importante que el usuario del dispositivo informe de cualquier actividad sospechosa o incidente de seguridad, puesto que podrían tener consecuencias negativas para la organización. La actividad sospechosa podría incluir situaciones en las que:

- El dispositivo funcione de forma anómala (p. ej., problemas de rendimiento, aplicaciones o mensajes inusuales); y
- Terceros externos muestren un interés inusual en el dispositivo.
- Los incidentes de seguridad podrían incluir situaciones en las que:
- El dispositivo se haya dejado sin supervisión durante períodos de tiempo significativos.
- Se halla confiscado el dispositivo o se encuentre fuera de su control durante períodos de tiempo significativos (p. ej., control fronterizo en un país extranjero).
- El usuario del dispositivo perciba una manipulación patente del dispositivo.

Nota: Es muy importante, y más aún cuando viaje al extranjero, que el usuario conozca los métodos para informar de actividades sospechosas o incidentes de seguridad. Si no estuviera seguro de sí una situación constituye una actividad sospechosa o un incidente de seguridad, informe de ella igualmente.

17.6 COMPROBACIÓN DE LA VERSIÓN DEL DISPOSITIVO

261. Existe una serie de componentes para determinar qué dispositivo se está usando y los componentes del mismo (como la versión de sistema operativo, la versión de compilación, etc.). Estos datos están disponibles en *Settings/About device (Ajustes/Acerca del teléfono/tableta)* o *Settings/About phone/Software information (Ajustes/Acerca del dispositivo/Información de software)*. Encontrará la siguiente información sobre la versión:

    - Model number (Número de modelo): – se trata del modelo de hardware, específico del fabricante.
    - Android version (Versión de Android): – se trata de la versión del SO Android.
    - Build number (Número de compilación): – se trata de la versión de imagen binaria específica del dispositivo.
    - Security software version (Versión de software de seguridad): – aquí se muestran las evaluaciones de Criterios comunes y la versión de los componentes de software relativos a las evaluaciones del dispositivo.

262. En relación con la evaluación de Common Criteria del dispositivo móvil, se mostrará:

263. «MDF vABC Release XYZ». Donde ABC es la versión del MDFPP (perfil de protección de los aspectos básicos del dispositivo móvil) y XYZ es el número de versión del software que se ha validado.

17.7 INSCRIPCIÓN DE UN DISPOSITIVO EN LA SOLUCIÓN DE EMM

264. Si el dispositivo va a administrarlo una organización mediante un servicio de EMM (Enterprise *Mobile Management*; gestión de dispositivos móviles), se tendrá que inscribir el dispositivo en este servicio.

265. Este proceso se realiza durante la instalación de la aplicación Agente de EMM que facilitará el administrador TIC/Seguridad de su organización. En el caso de instalar el agente manualmente, antes de instalar el agente de EMM se deberán habilitar los orígenes de aplicaciones desconocidos, ya que el agente no se instalará desde Google Play Store. Puede hacerlo desde *Settings/Lock screen and security/Unknown sources (Ajustes/Pantalla bloqueo y seguridad/Fuentes desconocidas)*. Al marcar esta casilla se pedirá que se confirme la habilitación de orígenes desconocidos, debido al riesgo de vulnerabilidad que presenta poder instalar aplicaciones desde elementos externos a Play Store.

266. Los dispositivos Samsung que incluyen la versión Knox 3.0 y superiores incorporan la integración con Android Enterprise, mejorándola con las APIs extendidas de Samsung Knox, esto permite despliegue de modo DO (Device Owner), donde la aplicación Device Owner controla todo el dispositivo, modo

COMP (Corporate Owned Managed Profile), el cual incluye una aplicación Device Owner, y un Work Profile que contiene una aplicación PO (Profile Owner) para su gestión o el modo Work Profile exclusivametne, donde la aplicación PO (Profile Owner) se encuentra dentro del Work Profile y no existe gestión del área personal del dispositivo. El fabricante de la solución EMM seleccionada por el administrador de la organización proporcionará los detalles de enrolamiento.

267. El usuario final puede consultar con el administrador de su organización cómo obtener e instalar el agente de EMM.

ANEXO I: TERMINOLOGIA

ADB	Herramienta de depuración para Android (*Android Debug Tool*)
ADT	Herramientas de desarrollo para Android (*Android Development Tools*)
API	Interfaz de programación de aplicación (*Application Programming Interface*)
APN	Nombre de punto de acceso (*Access Point Name*)
BYOD	Política «Traiga su propio dispositivo» (*Bring-Your-Own-Device*)
CA	Autoridad de certificación (*Certification Authority*)
COBO	De propiedad corporativa uso exclusivo trabajo (*Corporately Owned Business Only*)
COMP	De propiedad corporativa Perfil de Tabajo Gestionado (Corporate Owned Managed Profile)
COPE	De propiedad corporativa con habilitación personal (*Corporately Owned Personally Enabled*)
CPA	Protección de producto comercial (*Commercial Product Assurance*)
DEK	Clave de cifrado de datos (*Data Encryption Key*)
DH	Protocolo dictográfico Diffie-Hellman
DO	Propietario del Dispositivo (Device Owner)
FIPS	Estándar de procesamiento de información federal (*Federal Information Processing Standards*)
GCM	Modo de contador de Galois (*Galois Counter Mode*)
IKE	Intercambio de claves de Internet (*Internet Key Exchange*)
IPSec	Seguridad de protocolo de Internet (*Internet Protocol Security*)
Knox	La solución de seguridad corporativa de Samsung
LDAP	Protocolo ligero de acceso a directorios (*Lightweight Directory Access Protocol*)
MAC	Control de acceso obligatorio (*Mandatory Access Control*)
EDM	Administración/Gestión de dispositivos móviles (Enterprise Device Management)
EMM	Administración/Gestión de corporativa de parque móvil (Enterprise *Mobile Management*)
NAT	Traducción de direcciones de red (*Network Address Translation*)
NFC	Tecnología de intercambio de datos a muy corta distancia (*Near Field Communication*)
ODE	Cifrado de datos en el dispositivo (*On Device Encryption*)
OTA	Por vía inalámbrica (*Over the Air*)
PKM	Medición periódica del kernel (*Periodic Kernel Measurement*)
PO	Perfil de Trabajo Gestionado (Profile Owner)

RAM	Memoria de acceso aleatorio (*Random Access Memory*)
RKP	Protección del kernel en tiempo real
ROM	Memoria de solo lectura (*Read Only Memory*)
Tarjeta SD	Tarjeta de memoria *Secure Digital*
SDK	Kit de desarrollo de software corporativo de Samsung (*Software Development Kit*)
SEAMS	Control de acceso al motor de políticas SE Linux, SE for Android Management Service
SSL	Capa de sockets seguros (*Secure Sockets Layer*)
SSO	Inicio de sesión único (*Single Sign On*)
TIMA	Arquitectura de medición de integridad basada en *TrustZone*
URL	Localizador de recursos uniforme (*Uniform Resource Locator*)
USB	Bus serie universal (*Universal Serial Bus*)
VPN	Red privada virtual (*Virtual Private Network*)

ANEXO II: API UTILIZADAS EN LA CONFIGURACIÓN CC

268. Los ajustes incluidos a continuación muestran las API que se utilizan para ajustar un dispositivo de acuerdo con una configuración evaluada Common Criteria.

Ajustes de Modo CC:

269. Para ajustar un dispositivo de acuerdo con la configuración evaluada, debe habilitarse el Modo CC.

Ajuste	Valor	Descripción	Clase o método
Modo CC	Habilitar/ Deshabilitar	Este ajuste habilita el cifrado validado por el FIPS, deshabilita la conectividad USB en modo de recuperación y solo permite instalar actualizaciones FOTA (actualizaciones de firmware inalámbricas) en el sistema.	setCCMode()

270. Para garantizar el control general de la configuración, una vez habilitado, el usuario final no puede deshabilitar el Modo CC salvo que restablezcan los valores de fábrica. Es posible modificar el estado del Modo CC desde la solución de EMM; un usuario solo puede desactivar el Modo CC al restablecer los valores de fábrica.

Modo CC sin compatibilidad con EMM

271. Los proveedores de soluciones EMM aún no admiten el Modo CC de forma generalizada. Para facilitar a los clientes la habilitación del Modo CC, Samsung ofrece una aplicación independiente que permite habilitar este ajuste de forma local en el dispositivo. Samsung pone a disposición el archivo CCMode.apk, que puede descargarse desde la siguiente página web

https://support.samsungknox.com/hc/en-us/articles/115015195728

Modo CC y criptografía aprobada

272. Parte de la configuración evaluada de Criterios comunes consiste en la disponibilidad de motores criptográficos cuyo uso por parte del sistema y las

aplicaciones está aprobado. Para la configuración de Criterios comunes, Samsung ha decidido utilizar en sus dispositivos módulos criptográficos con la validación FIPS 140-2.

273. Samsung ofrece los siguientes módulos criptográficos en todos los dispositivos evaluados:

- Módulo criptográfico del kernel de Samsung
- Módulo de objeto BoringSSL FIPS
- Módulo SCrypto
- Samsung Flash Memory Protector (FMP)

274. Todos los módulos se ejecutan siempre en un modo validado por el FIPS. Por motivos de compatibilidad, BoringSSL ofrece acceso a algoritmos no validados por el FIPS que los desarrolladores no deberían utilizar dentro de una configuración validada (pero que son necesarios para garantizar la funcionalidad con numerosos servicios comerciales).

Nota: Solo se han evaluado estos módulos. También es posible que algunas aplicaciones implementen su propia criptografía. Solo se han validado los módulos criptográficos facilitados junto con el dispositivo; cualquier otra criptografía deberá evaluarse de forma específica. Samsung recomienda que los desarrolladores utilicen las funciones criptográficas facilitadas junto con el dispositivo.

Estado de Modo CC

275. El Modo CC cuenta con los siguientes estados:

Estado	Descripción
Ready (Listo) (blanco)	No se ha activado el Modo CC.
Enforced (Exigido)	Se ha activado el Modo CC, pero no se han seleccionado parte de los ajustes o configuraciones necesarios.
Enabled (Habilitado)	Se ha activado el Modo CC y se han seleccionado todos los ajustes o configuraciones necesarios.
Disabled (Deshabilitado)	Se ha activado el Modo CC, pero se ha producido un error en alguna comprobación de integridad o prueba de autodiagnóstico (como una prueba de autodiagnóstico FIPS 140-2).

276. El estado de Modo CC puede consultarse accediendo a Settings/About phone/Software Security Version (Configuración/Acerca del teléfono/tableta /Versión de seguridad de software). Al hacer clic en el elemento se mostrará el estado actual.

Nota: El estado *Ready* (Listo) no tiene ningún indicador asociado. Tan solo los estados *Enforced* (Ejecutado), *Enabled* (Habilitado) y *Disabled* (Deshabilitado) muestran un estado específico.

277. **Requisitos/Configuraciones del Modo CC**

278. Cuando se activa el Modo CC por primera vez, el estado cambia de *Ready* (Listo) a *Enforced* (Ejecutado). Para cambiar el estado a *Enabled* (Habilitado) deben configurarse los siguientes ajustes:

a) Habilitar la Política de número máximo de errores de contraseña.

b) Habilitar Inicio Seguro

c) Habilitar *SD Card Encryption* (Cifrado de la tarjeta SD).

d) Habilitar la comprobación de CRL (Lista de revocación de certificado).

e) Establecer la Calidad de la Contraseña.

f) Deshabilitar Bloqueo Facial

g) Deshabilitar Historial de Contraseñas

h) Deshabilitar Recuperar Contraseña (política Exchange Active Sync, si aplica)

Nota: Para poder cambiar a *Enabled* (Habilitado) no solo deben configurarse los ajustes de cifrado, sino que el usuario debe haber cifrado el soporte de almacenamiento.

Ajustes de cifrado (Ajustes del Dispositivo):

279. Existen dos conjuntos de ajustes de cifrado, uno para el almacenamiento interno y otro para el almacenamiento externo (tarjeta SD). Deben habilitarse ambos, aunque no se utilice ninguna tarjeta SD en el dispositivo.

Ajuste	Valor	Descripción	Clase o método
On Device Encryption (ODE; con Inicio Seguro)	Activar	Este ajuste permite cifrar todos los soportes de almacenamiento internos.	setInternalStorageEncryption()
SD Card Encryption (Cifrado de la tarjeta SD)	Habilitar	Este ajuste permite cifrar todos los medios de almacenamiento externos (tarjeta SD).	setRequireStorageCardEncryption()

Ajustes de autenticación (Ajustes del Dispositivo):

Ajuste	Valor	Descripción	Clase o método
Número máximo de errores de contraseña (borrar)	50 o menos	El número máximo de veces que puede introducirse una contraseña antes de que los datos del dispositivo se borren.	setMaximumFailedPasswordsForWipe()
Complejidad de la Contraseña	Recomendado: PASSWORD_QUALITY_ALPHANUMERIC	Especifica la complejidad de la contraseña.	setPasswordQuality()
Historia de la Contraseña	Deshabilitar	Restringe la posibilidad de reusar contraseñas.	setPasswordHistoryLength()
Bloqueo Facial	Deshabilitar (Facial)	Deshabilita la posibilidad de utilizar reconocimiento facial para desbloquear la pantalla.	setBiometricAuthenticationEnabled()BIOMETRIC_AUTHENTICATION_FACE = FALSE

Ajustes de Microsoft® Exchange ActiveSync (Ajustes del Dispositivo)

280. Muchos entornos utilizan Microsoft® Exchange Server junto con ActiveSync para la gestión de políticas relacionadas con el acceso a Servidor Exchange. Para entornos que usen políticas ActiveSync (EAS) para realizar algún tipo de gestión en los dispositivos móviles, la configuración Recuperar Contraseña debe estar deshabilitada (configurada a Falso).

Ajustes de revocación de certificado (Dispositivo y Contenedor):

Ajuste	Valor	Descripción	Clase o método
Comprobación de revocación de certificado	Habilitar para todas las aplicaciones	Especifica que la comprobación de CRL está habilitada para todas las aplicaciones del dispositivo.	enableRevocationCheck()

ANEXO III: MAPEADO DE POLÍTICAS GENERALES PARA TODO EL DISPOSITIVO A API

Regla de configuración	Función de Plataforma
Habilitar Common Criteria	boolean setMaximumFailedPasswordsForDeviceDisable (int num) boolean enableRevocationCheck (String pkgName, boolean enable) void setRequireDeviceEncryption (ComponentName admin, boolean value) void setInternalStorageEncryption (boolean isEncrypt) boolean setCCMode (boolean enable)
Tiendas de aplicaciones	void disableAndroidMarket (); boolean setAllowNonMarketApps (boolean allow)
Lista blanca	boolean setDisableApplication (String packageName) boolean uninstallApplication (String packageName, boolean keepDataAndCache) List<String> uninstallApplications (List<String> packageList) boolean addAppPackageNameToWhiteList (String packageName, boolean defaultBlackList)
Modo de desarrollador	boolean allowDeveloperMode (boolean allow) boolean setUsbDebuggingEnabled (boolean enable) boolean setUsbKiesAvailability (boolean enable) boolean setUsbMediaPlayerAvailability (boolean enable) boolean setUsbMassStorage (boolean enable) boolean allowUsbHostStorage (boolean allow) boolean setScreenCapture (boolean enable) boolean setTethering (boolean enable) boolean setUsbTethering (boolean enable)
Almacenamiento cifrado con Inicio Seguro	void setRequireDeviceEncryption (ComponentName admin, boolean value) void setInternalStorageEncryption (boolean isEncrypt)

Regla de configuración	Función de Plataforma
Tarjeta SD	boolean setSdCardState (boolean enable)
Contraseña	void setPasswordQuality (ComponentName admin, int quality) void setPasswordMinimumLength (ComponentName admin, int length) boolean setMaximumFailedPasswordsForDeviceDisable (int num) void setPasswordHistoryLength (ComponentName admin, int length) void setPasswordExpires (ComponentName admin, int value)
Tiempo de inactividad para bloqueo	void setMaximumTimeToLock (ComponentName admin, long timeMs)
VPN	int createVpnProfile (String profileInfo) int addAllPackagesToVpn (String profileName) int addAllContainerPackagesToVpn (int mContainerId, String profileName) int activateVpnProfile (String profileName, boolean enable)
Certificados	boolean installCertificateToKeystore (String type, byte[] value, String name, String password, int keystore) boolean installCertificateToKeystore (String type, byte[] value, String name, String password, int keystore) boolean enableCertificateValidationAtInstall (boolean enable)

Regla de configuración	Función de Plataforma
Interfaces	boolean allowDeveloperMode (boolean allow) boolean allowBluetooth (boolean enable) boolean setEnableNFC (boolean enable) boolean allowSBeam (boolean allow) boolean allowAndroidBeam (boolean allow) boolean setCameraState (boolean enable) boolean allowSVoice (boolean allow) boolean setBackup (boolean enable) boolean allowGoogleAccountsAutoSync (boolean allow) boolean setAutoFillSetting (boolean enable) boolean setPopupsSetting (boolean enable) boolean setCookiesSetting (boolean enable) boolean setJavaScriptSetting (boolean enable) boolean setLocationProviderState (String provider, boolean enable)
Atestado	void startAttestation_nonce (String nonce)
Almacén de claves de TIMA	boolean enableTimaKeystore (boolean enable)
Verificación de arranque de confianza de ODE	boolean enableODETrustedBootVerification (boolean enable)

ANEXO IV: MAPEADO POLÍTICAS ESPECIFICAS PARA EL CONTENEDOR A API

Regla de configuración	Función de Plataforma
Tiendas de aplicaciones	void disableAndroidMarket ()
Permitir que las aplicaciones se muevan al contenedor	boolean allowMoveAppsToContainer (boolean allow) boolean addAppPackageNameToWhiteList (String packageName, boolean defaultBlackList)
Lista blanca	boolean setDisableApplication (String packageName) boolean uninstallApplication (String packageName, boolean keepDataAndCache) List<String> uninstallApplications (List<String> packageList) boolean addAppPackageNameToWhiteList (String packageName, boolean defaultBlackList)
Navegador	void enableAndroidBrowser ()
VPN	int createVpnProfile (String profileInfo) int addAllPackagesToVpn (String profileName) int addAllContainerPackagesToVpn (int mContainerId, String profileName) int activateVpnProfile (String profileName, boolean enable)
Añadir cuenta de correo electrónico	boolean allowAccountAddition (boolean allowed)
HTTP Proxy	int setGlobalProxy (ProxyProperties properties)
Contraseña	void setPasswordQuality (ComponentName admin, int quality) void setMaximumTimeToLock (ComponentName admin, long timeMs) void setPasswordMinimumLength (ComponentName admin, int length) boolean setMaximumFailedPasswordsForDeviceDisable (int num) void setPasswordHistoryLength (ComponentName admin, int length) void setPasswordExpires (ComponentName admin, int value) boolean setMinimumCharacterChangeLength (int

Regla de configuración	Función de Plataforma
	length)
Credenciales	boolean installCertificateToKeystore (String type, byte[] value, String name, String password, int keystore) boolean installCertificateToKeystore (String type, byte[] value, String name, String password, int keystore) boolean enableCertificateValidationAtInstall (boolean enable)
Permitir que los archivos se muevan al contenedor	boolean allowMoveFilesToContainer (boolean allow)
Permitir que los archivos se muevan desde el contenedor	boolean allowMoveFilesToOwner (boolean allow) boolean allowShareClipboardDataToOwner (boolean allow)
Sincronización de datos del contenedor Knox	void setAllowChangeDataSyncPolicy (List<String> applications, String property, boolean value) boolean allowClipboardShare (boolean allow) boolean setCameraState (boolean enable) boolean setMicrophoneState (boolean enable) boolean setScreenCapture (boolean enable) boolean allowVideoRecord (boolean allow) boolean installApplication (String packageName) boolean updateApplication (String apkFilePath)