GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-457)

Gestión de dispositivos móviles: MDM (Mobile Device Management)

NOVIEMBRE 2013

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

NIPO: 002-13-040-7

Fecha de Edición: noviembre de 2013

Raúl Siles, fundador y analista de seguridad de Taddong S.L., ha participado en la elaboración y modificación del presente documento y sus anexos.

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, 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 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.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad 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 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.

Noviembre de 2013

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN

1. El desarrollo de los dispositivos y comunicaciones móviles y de las tecnologías inalámbricas en los últimos años ha revolucionado la forma de trabajar y comunicarse. El uso creciente de estas tecnologías sitúa a los dispositivos móviles como uno de los objetivos principales de las ciberamenazas.
2. La proliferación de dispositivos móviles en los últimos años, junto al aumento de las capacidades, prestaciones y posibilidades de utilización de los mismos, hace necesario evaluar en profundidad la seguridad ofrecida por este tipo de dispositivos, así como de los mecanismos de protección de la información que gestionan, dentro de los entornos de Tecnologías de la Información y las Comunicaciones (TIC).
3. Se considera dispositivo móvil aquél dispositivo de uso personal o profesional de reducido tamaño que permite la gestión de información y el acceso a redes de comunicaciones y servicios, y que habitualmente dispone de capacidades de telefonía, , tanto de voz como de datos, como por ejemplo teléfonos móviles, *smartphones* (teléfonos móviles avanzados o inteligentes), tabletas (o *tablets*) y agendas electrónicas (PDA), independientemente de sí disponen de teclado o pantalla táctil.
4. Pese a que los dispositivos móviles se utilizan para comunicaciones personales y profesionales, privadas y relevantes, y para el almacenamiento de información sensible, el nivel de percepción de la amenaza de seguridad real existente no ha tenido trascendencia en los usuarios finales y las organizaciones.
5. La utilización y amplia adopción, sin precedentes, de los dispositivos móviles como herramientas básicas de productividad en el ámbito profesional, junto a su utilización simultánea en el ámbito personal, hacen necesario que las organizaciones realicen una gestión minuciosa, exhaustiva y continua de los mismos, acorde con las políticas de seguridad de la organización.
6. Esta estrategia, conocida como movilidad empresarial, permite a los usuarios y empleados de las organizaciones llevar a cabo sus actividades diarias de negocio a través de dispositivos móviles que aprovechan las tecnologías que facilitan el acceso remoto a los datos corporativos, incrementando su eficiencia y productividad con independencia de la ubicación física en la que se encuentran y con mayor flexibilidad para viajar.
7. Las soluciones tecnológicas que permiten la gestión de los dispositivos móviles a nivel empresarial se conocen como MDM, de sus siglas en inglés, *Mobile Device Management*. Estas soluciones permite gestionar de forma eficiente la diversidad y el despliegue masivo, dinámico y a gran escala de dispositivos móviles en una organización, con un enfoque principalmente orientado a incrementar su seguridad, y mejorando colateralmente la productividad del usuario final.
8. El presente documento realiza un análisis detallado de las características, funcionalidades y mecanismos de seguridad existentes en las diferentes soluciones MDM (compuestas de productos y servicios) disponibles en la industria actualmente.

2 OBJETO

9. El propósito del presente documento es proporcionar una lista de características, capacidades y recomendaciones de seguridad que permitan la adecuada gestión de los dispositivos móviles en entornos empresariales a través de las soluciones MDM.

10. Los contenidos han sido estructurados para que sirvan de referencia antes de la adquisición de una solución MDM, permitiendo evaluar qué funcionalidades son necesarias para la organización en base a su política y requerimientos de gestión y seguridad.

11. Adicionalmente, los contenidos pueden ser consultados durante la implantación de la solución MDM con el objetivo de revisar y habilitar las funcionalidades requeridas en el entorno de aplicación, e incluso posteriormente, con el objetivo de personalizar o incrementar las capacidades de gestión y seguridad ya existentes.

12. El objetivo es poder aplicar los contenidos de la presente guía durante todo el ciclo de vida de la solución MDM. Debe tenerse en cuenta que existen definidos modelos de ciclo de vida para la incorporación de soluciones MDM en las organizaciones, con cinco fases claramente diferenciadas como: inicio, desarrollo, implementación, operación y mantenimiento, y renovación de los dispositivos móviles [Ref.- 58].

13. Adicionalmente, se han clasificado a modo de resumen y como referencia las funcionalidades de seguridad mínimas recomendadas, así como las funcionalidades más avanzadas, disponibles en las soluciones MDM para dos tipos de entornos diferentes.

14. Los dos tipos de entornos se han clasificado, en función de su nivel de seguridad y de la sensibilidad y criticidad de la información que gestionan, en dos categorías de características: básicas y avanzadas (ver apartado “7. LISTADO RESUMEN DE CARACTERÍSTICAS DE LAS SOLUCIONES MDM”).

15. La presente guía proporciona los detalles genéricos de la funcionalidad, capacidades, y aspectos a considerar en la aplicación e implementación de las principales recomendaciones de seguridad a través de la soluciones MDM, y presenta la información necesaria para la evaluación y análisis de los mecanismos de gestión frente a los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles en la actualidad.

16. Se recomienda iniciar una estrategia de movilidad empresarial en la organización y de gestión de los dispositivos móviles con un despliegue piloto que únicamente involucre a un número reducido de usuarios, suficientemente representativo de los diferentes perfiles existentes en la organización, con un nivel de riesgo reducido respecto al tipo de información manejada, y con alta probabilidad de éxito desde el punto de vista del negocio y propósito principal de la organización.

17. En ningún caso, la presente guía profundiza en los detalles específicos de implantación y configuración de ninguna de las soluciones MDM disponibles en la industria, siendo necesaria la consulta de los manuales de instalación, administración y usuario de cada fabricante para una correcta implantación.

18. Es importante destacar que la implantación de una solución MDM debe ser complementada con un programa de formación y concienciación de seguridad para los usuarios de la organización, con el objetivo de educarles en los comportamientos adecuados que les permiten proteger el dispositivo móvil y los datos que éste gestiona, así como destacar comportamientos no recomendados que ponen en riesgo la seguridad de la organización, como por ejemplo la conexión a cargadores de electricidad públicos aparentemente

inofensivos pero que pueden extraer información del dispositivo móvil a través de la conexión de datos USB.

19. Debido a que la industria móvil (o de los dispositivos y plataformas móviles) se encuentra en una continua y desenfrenada evolución, con nuevas características y funcionalidades disponibles cada pocos meses tanto en los propios dispositivos móviles como en las soluciones de gestión MDM, el presente documento pretende sentar las bases para una adecuada gestión de estos dispositivos desde el punto de vista de seguridad, profundizando a modo de ejemplo en algunas funcionalidades disponibles actualmente en las principales plataformas móviles y soluciones MDM.

20. Los fabricantes de soluciones MDM están continuamente innovando en nuevos mecanismos de seguridad, gestión de apps y segregación de datos personales y corporativos, por lo que publicarán en breve nuevas características y funcionalidades que no están cubiertas en este documento y que, por tanto, deberán ser evaluadas de forma individual siguiendo los mismos principios de análisis aquí expuestos.

21. Esta evolución en las soluciones MDM está también directamente condicionada por la evolución general de la industria respecto a las capacidades y mecanismos de seguridad disponibles en las propias plataformas móviles más usadas en la actualidad [Ref.- 59].

22. La serie CCN-STIC-45X, "Seguridad de dispositivos móviles", se ha estructurado en tres niveles: una guía genérica centrada en al análisis de seguridad de dispositivos móviles (CCN-STIC-450), complementada por guías específicas para los principales sistemas operativos empleados por los dispositivos móviles hoy en día, y por la presente guía que cubre los aspectos relacionados con su gestión y seguridad empresarial. Por este motivo, la lectura y aplicación de la presente guía complementa a las otras guías individuales asociadas a un sistema operativo (y versión concreta del mismo), recomendándose en primer lugar la lectura de la guía general de seguridad:

    - CCN-STIC-450 - Seguridad de dispositivos móviles [Ref.- 1]

    Adicionalmente, se recomienda la lectura de las guías de esta misma serie asociadas a sistemas operativos y versiones concretas, en caso de ser necesaria su aplicación en terminales existentes en la organización:

    - CCN-STIC-451 - Seguridad de dispositivos móviles: Windows Mobile 6.1
    - CCN-STIC-452 - Seguridad de dispositivos móviles: Windows Mobile 6.5
    - CCN-STIC-453 - Seguridad de dispositivos móviles: Android 2.x
    - CCN-STIC-454 - Seguridad de dispositivos móviles: iPad
    - CCN-STIC-455 - Seguridad de dispositivos móviles: iPhone

NOTA: Esta serie de guías están diseñadas considerando como requisito la necesidad de encontrar un equilibrio entre seguridad y funcionalidad en relación a las capacidades disponibles en los dispositivos móviles a proteger, con el objetivo de poder hacer uso de la mayoría de características disponibles en los mismos de forma segura.

3 ALCANCE

23. Las Autoridades responsables de la aplicación de la Política de Seguridad de las TIC (STIC) determinarán su análisis y aplicación a los entornos de gestión de dispositivos móviles ya existentes o futuros bajo su responsabilidad.

4 ENTORNO DE APLICACIÓN DE ESTA GUÍA

24. Las soluciones MDM (*Mobile Device Management*) aplican a los principales sistemas operativos de dispositivos móviles o plataformas móviles utilizadas en la actualidad: Android de Google y AOSP [Ref.- 2], BlackBerry de BlackBerry (previamente Research In Motion Limited o RIM) [Ref.- 3], iOS de Apple (dispositivos iPhone, iPad, y iPod Touch) [Ref.- 4], y Windows Phone de Microsoft [Ref.- 5].

NOTA: Las diferentes referencias a lo largo del presente documento a las principales plataformas móviles más utilizadas en la actualidad emplean siempre el orden alfabético: Android, BlackBerry, iOS y Windows Phone.

25. Opcionalmente, la solución MDM puede incluir soporte para plataformas móviles que tuvieron gran aceptación en la industria en el pasado y que, aunque no estén disponibles en la actualidad, los dispositivos móviles basados en éstas pueden seguir siendo utilizados a nivel empresarial, como Symbian y Windows Mobile.

26. En el caso específico de Android, se recomienda verificar si la solución MDM proporciona soporte para las APIs de seguridad empresariales proporcionadas por fabricantes específicos, como Samsung KNOX [Ref.- 67] o SAFE (*Samsung Approved For Enterprise*).

27. Algunas soluciones MDM están más orientadas a, o focalizadas única y exclusivamente en, una plataforma móvil concreta, mientras que otras soluciones son multiplataforma, y permiten la gestión de diferentes tipos, modelos y versiones de dispositivos móviles existentes en la organización.

28. Actualmente algunas organizaciones están cada vez más interesadas en una solución de gestión única, no sólo que permita administrar los dispositivos móviles, sino también los dispositivos tradicionales (ordenadores portátiles, de escritorio, etc, basados típicamente en los sistemas operativos Windows, Linux y Mac OS X), o incluso dispositivos adicionales como impresoras, dispositivos embebidos o módulos M2M, por lo que es interesante evaluar también el soporte que ofrece la solución MDM para este otro tipo de dispositivos.

29. Las plataformas de gestión de dispositivos móviles están extendiendo por tanto sus capacidades a la gestión de todos los dispositivos informáticos empleados por los usuarios dentro de la organización, permitiendo también aplicar controles y gestionar los ordenadores portátiles y de escritorio. Esta característica debe ser tenida en cuenta a la hora de definir el alcance y seleccionar una solución MDM específica.

30. El principal objetivo de las soluciones MDM es permitir la correcta gestión de los dispositivos móviles asociados a la organización y reducir su superficie de exposición frente a ataques de seguridad, incluyendo la protección del propio dispositivo móvil, de sus comunicaciones y de la información y datos que gestiona y almacena.

31. Otra de las principales áreas de gestión asociada a los dispositivos móviles es la de la gestión de las aplicaciones móviles que pueden ser instaladas en estos. El término empleado para la gestión de aplicaciones móviles es MAM (*Mobile Application Management*) o MEAM (*Mobile Enterprise Application Management*), y las soluciones asociadas pueden estar integradas o no en las soluciones MDM. En el presente documento se considera que las características MAM están disponibles dentro de la propia solución MDM, como una funcionalidad más.

32. Adicionalmente a la gestión empresarial de los dispositivos móviles y de las aplicaciones móviles, la industria ha identificado la necesidad de proteger los datos y contenidos

corporativos distribuidos hacia o accedidos desde los dispositivos móviles, con arquitecturas y soluciones denominadas MCM (*Mobile Content Management*). De nuevo, en el presente documento se considera que las características MCM están disponibles dentro de la propia solución MDM, como una funcionalidad más.

33. En resumen, las soluciones MDM deben focalizar sus capacidades de gestión empresarial en tres ámbitos principales: dispositivos móviles, aplicaciones móviles y contenidos corporativos (accedidos desde los dispositivos y aplicaciones móviles).

NOTA: Las aplicaciones móviles son referenciadas en la industria de manera abreviada, y a lo largo del presente documento (en adelante), como app(s).

34. Existe numerosa terminología en la industria para referenciar las diferentes necesidades y funcionalidades asociadas a la gestión de los dispositivos móviles y sus capacidades, adoptándose diferentes acrónimos, como:

    - MEM (*Mobile Enterprise Management*), para referirse a las soluciones que engloban tanto MDM[1] como MAM[2]. En ocasiones también se emplea el término EMM (*Enterprise Mobility Management*).
    - En ocasiones, el término MEM se emplea para referirse a *Mobile Expense Management*, una variación de la gestión empresarial de los costes móviles y de telecomunicaciones, referida tradicionalmente como *Telecom Expense Management* (TEM).
    - MOM (*Mobile Operations Management*), término que engloba todas las facetas de la gestión de las plataformas móviles en la organización: Mobile Device Management, Mobile Application Management, Mobile Policy Management, Mobile Support Management, y Mobile Expense Management.
    - El término MEAP (*Mobile Enterprise Application Platforms*) se emplea en ocasiones para referenciar soluciones MDM basadas en una aplicación contenedora (ver apartado "4.6.6. SOLUCIONES DE GESTIÓN BASADAS EN UN CONTENEDOR"), aunque el término puede incluir otras infraestructuras y servicios asociados.
    - Los mecanismos de protección de los datos y contenidos corporativos, además de reverenciarse con el término MCM, también se referencian como MDP (*Mobile Data Protection*).
    - Otro término empleado para la gestión de contenidos corporativos, adicionalmente a MCM, es ECM (*Enterprise Content Management*).

35. Existen en la industria soluciones de gestión y acceso a contenidos, así como entornos empresariales colaborativos, para el acceso a la información y datos corporativos de forma segura desde cualquier cliente, incluyendo dispositivos móviles. Sin embargo, este tipo de soluciones no se han considerado parte de la solución MDM y no son analizadas específicamente en la presente guía.

[1] El término MDM no debe ser confundido con el acrónimo *Master Data Management* (MDM).
[2] La presente guía considera que las soluciones MDM engloban tanto las capacidades de MDM como de MAM, por lo que serían equivalentes a MEM.

36. Con el objetivo de determinar la solución MDM más idónea para una organización, uno de las primeros aspectos a considerar es si el entorno empresarial hará uso de una plataforma móvil única o, si por el contrario, si será un entorno multiplataforma, con dispositivos de diferentes fabricantes y sistemas operativos móviles.

37. En el primer caso es posible emplear soluciones MDM exclusivas de la plataforma móvil seleccionada, que aprovechan todas y cada una de las capacidades y funcionalidades de gestión asociadas a esa plataforma, debido a la existencia de un entorno móvil homogéneo. Adicionalmente en este caso también existe la opción de emplear soluciones multiplataforma, menos específicas y, habitualmente, con capacidades más reducidas para una plataforma móvil concreta.

38. En el segundo caso es posible emplear soluciones MDM multiplataforma, que proporcionan capacidades de gestión para entornos heterogéneos con diferentes tipos de dispositivos móviles, o hacer uso de múltiples soluciones MDM, lo que dificulta su gestión y la aplicación de una política de seguridad única a todas las plataformas móviles, pero que permite aprovechar las capacidades de gestión más avanzadas de cada una de las plataformas móviles individualmente.

39. En este segundo caso (entornos multiplataforma), la opción ideal sería disponer de una solución MDM única y multiplataforma (lo que simplifica su administración y mantenimiento) que permita trasladar la política de seguridad genérica de la organización a las particularidades de cada una de las plataformas móviles.

40. Las arquitecturas de las soluciones MDM emplean un modelo cliente-servidor, encargándose el servidor (o servidores) MDM de la gestión de los dispositivos móviles, que disponen de un cliente o agente de gestión que mantiene un canal de comunicación permanente con el servidor de gestión.

41. Habitualmente este canal de comunicación es utilizado para gestionar remotamente la disponibilidad y estado del dispositivo móvil, empleándose mensajes breves o notificaciones *push* (potencialmente a través de servidores *push* intermedios) con el objetivo de reducir el consumo de recursos en el terminal, y que desencadenan la posterior realización de acciones más complejas.

42. Una vez se recibe una notificación *push*, el cliente o agente residente en el dispositivo móvil puede establecer canales de comunicación adicionales con los servidores de gestión MDM para llevar a cabo las tareas indicadas.

43. Este cliente o agente de gestión puede ser instalado por la organización en el dispositivo móvil o puede estar disponible por defecto como parte de los mecanismos de gestión de la plataforma móvil a través de las APIs o librerías de gestión proporcionadas por el fabricante.

44. La adopción masiva de dispositivos móviles por parte de las organizaciones y su diversidad está suponiendo numerosos quebraderos de cabeza y nuevos retos para los responsables TIC de las organizaciones, al intentar llevar a cabo su integración en la organización de forma segura y fluida.

45. Sin embargo, este cambio en el acceso a los sistemas de información, comunicaciones y datos corporativos por parte de los usuarios puede ser orientado como una nueva oportunidad para redefinir la política de uso (AUP, *Acceptable Use Policy*) existente actualmente y mejorar tanto la arquitectura de seguridad TIC como los mecanismos de seguridad disponibles.

46. Por ejemplo, debido a que el método de conexión principal de los dispositivos móviles a las redes corporativas se basa en las tecnologías Wi-Fi, es fundamental revisar y mejorar la

infraestructura Wi-Fi de la organización para proporcionar comunicaciones seguras, disponer de mecanismos avanzados de control de acceso a la red (NAC, *Network Access Control*), de sistemas de detección/protección de intrusos inalámbricos (WIPS, *Wireless Intrussion Protection System*) y soluciones de filtrado de contenidos web (*proxies*) [Ref.- 66].

47. Los mecanismos de control de la organización deben comenzar por el control de acceso a la red (mediante una combinación de soluciones NAC y MDM), definiendo quién tiene acceso a la misma (pudiendo hacer uso de mecanismos de gestión de identidad), monitorizando quién hace uso de ella, y bloqueando o permitiendo el acceso según la política de seguridad, en base a las credenciales del usuario y/o del dispositivo móvil, y del nivel de seguridad actual de este último.

48. Las soluciones MDM deben disponer de capacidades generales para la gestión de los dispositivos móviles, incluyendo por ejemplo, la actualización del sistema operativo de la plataforma móvil, actualización de la política de seguridad, actualización de apps, modificación de la configuración del dispositivo, eliminación de elementos de la configuración o de datos corporativos o de la totalidad de los contenidos del dispositivo, localización de la ubicación física y seguimiento del dispositivo, distribución de certificados digitales personales y de autoridades de certificación (CA, *Certification Authority*) de confianza, capacidades de inventario para validar el cumplimiento de las políticas de la organización, comprobación de la versión de sistema operativo y apps para el análisis de vulnerabilidades, etc.

49. Las características y funcionalidad requeridas por una organización depende mucho de sus necesidades y requisitos a la hora de integrar los dispositivos móviles como un elemento fundamental del negocio.

50. Por este motivo, algunas organizaciones darán mayor prioridad al hardware de los dispositivos móviles y a su coste, otras se centrarán en la facilidad de uso y la solución remota de problemas de conectividad, mientras que otras priorizarán la confidencialidad de la información empleada por ciertas apps críticas para el negocio. En resumen, los objetivos de cada organización respecto a la solución MDM pueden ser muy diversos.

51. Por tanto, el presente documento refleja de manera independiente las diferentes características y funcionalidades disponibles en las soluciones MDM actualmente, pero su valoración final y orden de importancia para una organización concreta deben ser priorizados tras llevar a cabo un estudio de las necesidades específicas de la organización.

52. Antes del despliegue inicial de una estrategia de movilidad empresarial y su solución MDM asociada, es necesario realizar un análisis detallado del nivel actual de penetración de los dispositivos móviles en la organización, obteniendo detalles de las diferentes unidades de negocio o departamentos, revisando los inventarios de dispositivos móviles ya asignados o registrados, e identificando a través de los controles de seguridad existentes la existencia de estos dispositivos en la red Wi-Fi corporativa, y de los accesos desde este tipo de dispositivos a los recursos corporativos o a Internet [Ref.- 53].

4.1 NORMA DE SEGURIDAD PARA LOS DISPOSITIVOS MÓVILES

53. Antes de la implantación de una solución MDM es requisito indispensable disponer de o definir una política de seguridad corporativa centrada en la utilización de los dispositivos móviles en la organización.

NOTA: La definición, detalles y contenido de la política de seguridad de la organización o política de seguridad corporativa asociada a los dispositivos móviles queda fuera del alcance de la

presente guía y se considera un requisito previo indispensable para la implantación de una solución de gestión MDM. Esta política deberá estar alineada con la política de seguridad general de la organización.

54. La política de seguridad de la organización debe contemplar tanto aspectos técnicos como no técnicos asociados a la protección del usuario y su privacidad, los dispositivos móviles, las comunicaciones asociadas, las apps y los datos corporativos y personales.

55. La política de seguridad debe asimismo reflejar el uso permitido y aceptado de los dispositivos móviles en la organización, el comportamiento esperado por parte de los usuarios, y proporcionar las pautas y controles de seguridad a implantar.

56. El objetivo principal de la política de seguridad es mitigar los riesgos identificados por la organización y asociados a la utilización de dispositivos móviles y a la posible exposición de datos confidenciales y sensibles.

57. El objetivo de la solución MDM es aplicar la política de seguridad definida por la organización en los dispositivos móviles gestionados y detectar violaciones en la misma.

58. Esta política de seguridad debe cubrir múltiples aspectos asociados a la integración y uso de dispositivos móviles a nivel corporativo, identificar el motivo fundamental para permitir su utilización a nivel profesional y las ventajas competitivas desde el punto de vista del negocio para promover su uso (casos o escenarios de uso), establecer el conjunto de plataformas móviles soportadas, qué recursos de la organización serán accedidos desde los dispositivos móviles, qué tipo de apps están permitidas (o prohibidas) en estos dispositivos, el uso y acceso a redes de comunicaciones (tanto corporativas como externas), los requisitos de protección de datos, los mecanismos de control y gestión de los dispositivos móviles, etc.

59. La política de seguridad de la organización estará condicionada por el cumplimiento y conformidad con los requisitos impuestos por las leyes y regulaciones que apliquen al sector y negocio de la organización, así como otros aspectos propios del país de aplicación. Por ejemplo, en el caso de la Administración Pública Española, es necesario que la política de seguridad esté (al menos) alineada con la LOPD y la LSSI.

60. Dos de los aspectos fundamentales qué deben estar contemplados en la política de seguridad, y qué deben ser aplicados y monitorizados posteriormente a través de la solución MDM, son el tipo de redes de comunicaciones a las que podrán conectarse los dispositivos móviles, y el tipo de datos e información que podrán almacenar y manejar.

61. Es necesario definir el tipo de redes de comunicaciones a las que podrán tener acceso los dispositivos móviles, tanto desde el punto de vista de la tecnología empleada (redes Wi-Fi, redes móviles 2/3/4G, etc), como del propietario de la red (la red de la propia organización, red Wi-Fi del usuario en casa, redes de terceros en entornos Wi-Fi privados o públicos…), así como del nivel de seguridad de la red, especialmente para redes Wi-Fi. Además, debe definirse el tipo genérico de comunicaciones permitidas, incluyendo comunicaciones de datos (privadas o públicas, como Internet), voz, SMS, etc.

62. Complementando el requisito de comunicaciones previo, la organización debería definir a qué redes de datos móviles podrán conectarse los dispositivos móviles (2/3/4G), qué tipo de plan de datos emplearán, y quién asumirá los costes (el usuario o la organización).

63. Asimismo, es necesario definir el tipo de información que podrán almacenar, gestionar y transferir los dispositivos móviles gestionados, tanto dentro como fuera de la organización,

teniendo en cuenta la posibilidad de establecer mecanismos de control y prevención de fuga de datos sensibles, DLP (*Data Loss Prevention*).

64. Para ello, es necesario clasificar previamente la información gestionada por la organización en diferentes niveles en función de su confidencialidad y criticidad (por ejemplo: pública, difusión limitada, confidencial, reservado, secreto, etc) o según lo establecido en el ENS.

65. Adicionalmente, la política de seguridad debe contemplar otros aspectos como el modelo de gestión de dispositivos móviles a implantar, los requisitos globales de seguridad de los mismos, el proceso de adquisición, renovación y eliminación de dispositivos, el modelo de adquisición de apps, los requisitos de cifrado de datos, la política del código de acceso, la utilización de los servicios de localización, la definición de los servicios que serán accedidos desde los dispositivos móviles (por ejemplo, e-mail, VPN, CRM…), etc [Ref.- 41].

4.2 AMENAZAS DE SEGURIDAD SOBRE LOS DISPOSITIVOS MÓVILES

66. A la hora de definir una política de seguridad para los dispositivos móviles de la organización, es necesario evaluar los escenarios y las amenazas principales de seguridad que afectan a estos dispositivos hoy en día, y en particular, a la organización bajo estudio.

67. Debe tenerse en cuenta que la movilidad y uso permanente de los dispositivos móviles implica una mayor exposición a amenazas sobre estos frente a otros dispositivos de la organización (como ordenadores portátiles o de escritorio que sólo se utilizan dentro de la organización), por lo que es necesario disponer de mecanismos de protección adicionales.

68. Los dispositivos móviles son utilizados frecuentemente fuera del control de la organización, especialmente en lo que se refiere a la ausencia de controles de seguridad físicos, salvo los proporcionados por el usuario.

69. Por este motivo, los mecanismos de protección a implantar (como por ejemplo autentificación y cifrado robustos) deben considerar que el dispositivo móvil puede acabar en manos ajenas no autorizadas y deben proteger los datos que almacena y los accesos a servicios remotos de los que dispone.

70. Dentro de estos escenarios y amenazas más comunes sobre los dispositivos móviles, encontramos frecuentemente, entre otras:

- Acceso físico no autorizado al dispositivo móvil:
  - Temporalmente (por un periodo breve).
  - Pérdida o robo del dispositivo móvil (durante un periodo extendido).
- Acceso no autorizado a la información almacenada:
  - Datos y documentos corporativos.
  - Credenciales de acceso a servicios corporativos.
- Acceso no autorizado y manipulación de la información transmitida:
  - Ataques de hombre en medio (MitM, *Man-in-the-Middle*).
- Código móvil malicioso (*malware*) en apps (aplicaciones móviles):
  - Fraude (servicios *SMS Premium*), anuncios, privacidad, etc.
  - Uso no autorizado de las capacidades de comunicaciones del dispositivo: NFC, Bluetooth, Wi-Fi, 2/3/4G (SMS, voz y datos), etc.

- Dispositivos móviles sobre los que se ha realizado el proceso de *jailbreak* o *root* (ver apartado "5.5.7. DETECCIÓN DE JAILBREAK O ROOT").
- Utilización de apps y servicios "en la nube" no aprobados por la organización para manejar o almacenar datos corporativos sensibles.
- Separación inadecuada en la utilización del dispositivo móvil para tareas profesionales y personales.
- Etc.

71. Adicionalmente a las amenazas de seguridad previamente mencionadas, es necesario evaluar como gestionar otras situaciones que tienen implicaciones directas en la seguridad del entorno móvil, como por ejemplo:

    - ¿Qué ocurre cuando un empleado (o usuario) deja la organización sin devolver el dispositivo móvil corporativo?
    - ¿Cómo se lleva a cabo la renovación frecuente de los dispositivos móviles: proceso de reciclado?
    - ¿Cómo integrar dispositivos personales en la organización (BYOD)?
    - Etc.

72. Las soluciones MDM permiten establecer restricciones muy granulares en el uso de los dispositivos móviles, pero siempre debe tenerse en cuenta que el beneficio real de estas limitaciones respecto a la seguridad y la reducción real de riesgo que proporcionan debe ser evaluado detalladamente por la organización antes de su aplicación.

73. Por ejemplo, existen soluciones MDM que permiten desactivar la cámara del dispositivo móvil, haciendo que incluso desaparezca del terminal el icono asociado, al encontrarse el dispositivo en una ubicación determinada, como por ejemplo las oficinas principales de la organización.

74. El objetivo principal de esta medida es evitar que puedan tomarse fotografías de información confidencial dentro de la organización a través del dispositivo móvil. Sin embargo, debe tenerse en cuenta que es posible hacer uso de otras cámaras de fotos, de pequeño tamaño o incluso embebidas en un bolígrafo, por lo que este control en los dispositivos móviles puede ser inútil si no se complementa con controles adicionales que apliquen a otros dispositivos y al acceso físico a los edificios de la organización.

4.3 INVENTARIO Y MONITORIZACIÓN DE LOS DISPOSITIVOS MÓVILES

75. La solución MDM debe disponer de capacidades de inventario y monitorización de los dispositivos móviles gestionados por la organización y permitir responder a una serie de preguntas en todo momento, en tiempo real, así como de manera histórica.

76. Las capacidades de inventario de la solución MDM deben permanecer constantemente actualizadas, con el objetivo de ofrecer una visión lo más precisa posible de la situación real de la organización.

77. El siguiente conjunto de preguntas constituye un ejemplo concreto del tipo de información que debería estar disponible a través de la solución MDM (y otros mecanismos de monitorización complementarios):

    - ¿Qué dispositivos móviles hay conectados en mi red actualmente?

- ¿Con qué frecuencia se conectan (individualmente y por tipo)?

- ¿Cuántos dispositivos móviles son utilizados por cada usuario para acceder a los datos y servicios corporativos?
- ¿Cuál es el estado o nivel de seguridad de cada dispositivo móvil?
  - ¿Tienen instalada la última versión de sistema operativo?
  - ¿Cumplen con la política de seguridad de la organización?
  - ¿Qué vulnerabilidades públicamente conocidas afectan a cada dispositivo? (adicionalmente debería conocerse a través de fuentes externas si existe solución para mitigar esas vulnerabilidades)
- ¿Qué hace cada dispositivo móvil en mi red concretamente?
  - ¿A qué servicios y datos están accediendo (acceso a Internet, acceso a datos corporativos, acceso a servicios y aplicaciones internas…)?
- ¿Qué controles de seguridad se están aplicando en los propios dispositivos? (adicionalmente debería correlarse esa información con los controles de seguridad disponibles en la red de la organización)
  - ¿Cuál es el estado actual de cada uno de esos controles?
  - Por ejemplo, ¿cuántos dispositivos móviles BYOD tienen un código de acceso habilitado? o ¿cuántos dispositivos móviles propiedad de la organización tienen el cifrado completo del dispositivo habilitado?
- Etc.[3]

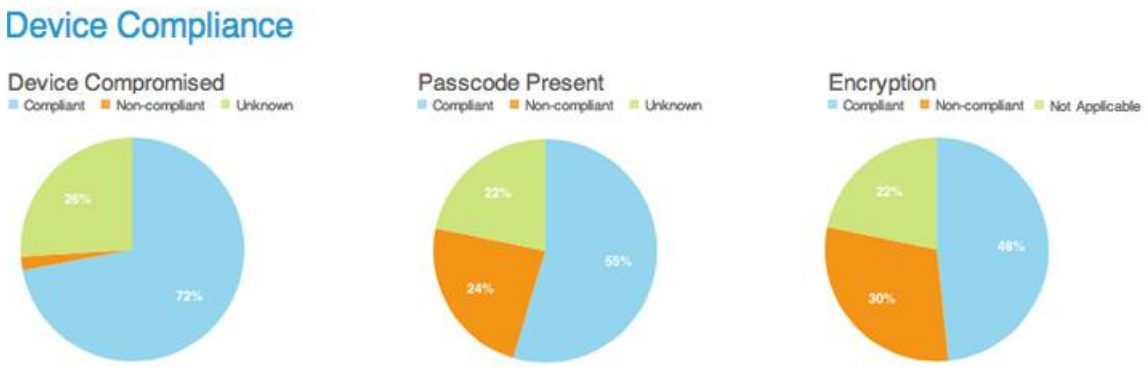

FIGURA 1.- Ejemplo de información disponible a través de la solución MDM.

78. El objetivo principal de las capacidades de inventario y monitorización es disponer de una visión precisa, actualizada y realista del estado y de la utilización de los recursos de la organización por parte de los dispositivos móviles, y en particular, de su nivel de seguridad para poder evaluar el riesgo asociado a su utilización real.

79. El objetivo final es permitir únicamente el acceso a los recursos de la organización a aquellos dispositivos móviles que cumplen con la política de seguridad y que, por tanto, no suponen un riesgo según los requisitos de seguridad establecidos.

80. Las capacidades de inventario y monitorización (ver apartado "5.3. INVENTARIO Y MONITORIZACIÓN") deben permitir, a través del análisis de los *logs* o registros de la

[3] Imagen obtenida de http://www.air-watch.com/solutions/mobile-security.

solución MDM, la red Wi-Fi corporativa, los servidores de autentificación y las herramientas de seguridad empresariales, obtener detalles sobre las violaciones de la política de seguridad de la organización, su nivel de cumplimiento, los consumos de ancho de banda y almacenamiento, etc.

81. Específicamente, es fundamental que las capacidades de monitorización permitan la detección y notificación automática e inmediata de violaciones en la política de seguridad de la organización.

82. Una vez se detectan violaciones en la política de seguridad, la solución MDM puede notificar al usuario y/o al administrador TIC, restringir el acceso del dispositivo móvil a los servicios y datos corporativos, o incluso realizar un borrado remoto completo del mismo.

83. Algunos motivos vinculados a la violación o incumplimiento de la política de seguridad incluyen, por ejemplo, disponer de una versión desactualizada del sistema operativo o del agente de la solución de gestión MDM, haber realizado el proceso de *jailbreak* o *root*, o emplear un terminal de un fabricante o modelo de dispositivo móvil no soportados.

84. La solución MDM debe proporcionar capacidades de monitorización y búsqueda en base a diferentes criterios, como por grupos de usuarios (Ej. altos ejecutivos y responsables de departamento), por tipo de dispositivo o plataforma móvil (Ej. Android) o incluso por el operador de telecomunicaciones empleado.

4.4 BYOD (BRING YOUR OWN DEVICE) Y BYOA (BRING YOUR OWN APP)

85. Una de las principales tendencias de la industria móvil durante los últimos años es BYOD (*Bring Your Own Device*), es decir, un escenario en el que se permite a los usuarios y empleados de la organización hacer uso de sus dispositivos móviles personales para el acceso al entorno, servicios y datos corporativos.

86. Esta tendencia tuvo una adopción inicial muy alta, principalmente en los departamentos financieros de las organizaciones, debido al ahorro de costes asociado a la adquisición inicial de los dispositivos móviles, frente a la opción de que los dispositivos móviles sean subvencionados por la organización y proporcionados a los usuarios como una herramienta de trabajo más.

87. Debido a que los dispositivos móviles actuales son sistemas complejos, avanzados y están de moda, su precio es bastante elevado, hecho que tiene influencia especialmente en las decisiones de la organización cuando es necesario adquirir un número elevado de éstos (decenas, cientos o miles de dispositivos móviles).

88. El hecho de que la organización no tenga que hacer ese desembolso inicial, y el coste del dispositivo móvil sea financiado por el usuario, al ser este su propietario en lugar de la organización, conllevó una reducción de costes inmediata para muchas organizaciones.

89. Sin embargo, es necesario tener en cuenta que un entorno BYOD más heterogéneo conlleva una serie de gastos e inversiones adicionales de gestión, mantenimiento e integración de los dispositivos móviles en los entornos TIC de las organizaciones, que normalmente no es tenido en cuenta.

90. La ventaja principal de BYOD para el usuario es que éste puede hacer uso libremente del dispositivo móvil que mejor se adapta a él, qué más le gusta o con el que está más familiarizado.

91. La desventaja principal de BYOD para la organización es que tiene que acomodar las dos facetas del dispositivo móvil, personal y profesional, en el entorno TIC y de manera segura, así como definir y conjugar los requisitos y necesidades de ambos mundos.

92. La tendencia BYOD debe asumir que los dispositivos móviles personales no son de confianza desde el punto de vista de seguridad, salvo que hayan sido configurados con unos requisitos mínimos de seguridad y pasen a ser gestionados y monitorizados por la organización.

93. Una aproximación intermedia adoptada por algunas organizaciones conocida como CYOD (*Choose Your Own Device*), con el objetivo principal de intentar obtener lo mejor de ambos mundos, es que el usuario pueda elegir el dispositivo móvil que utilizará, pero en lugar de hacerlo de todos los disponibles en el mercado, únicamente lo seleccionará de una reducida lista preaprobada de dispositivos móviles que cumplen con los requisitos de seguridad y tecnológicos de la organización.

94. Estas aproximaciones complementan el escenario dónde el dispositivo móvil es propiedad de la organización y sólo puede ser empleado para tareas profesionales, o un escenario intermedio, conocido como COPE (*Corporataly-Owned, Personally-Enabled*), donde el dispositivo móvil es propiedad de la organización pero se permite su utilización para ciertas tareas personales (normalmente, una variante de CYOD) [Ref.- 54].

95. Finalmente, debe considerarse también otro modelo de uso reciente en la industria basado en la posibilidad de compartir un dispositivo móvil entre diferentes empleados de la organización, debiendo la solución MDM proporcionar capacidades multiusuario para permitir y segmentar el acceso a los datos y servicios a cada uno de los usuarios, o en su defecto, permitir una rápida y segura transición del dispositivo móvil al ser transferido de un usuario a otro.

96. La definición de una política de seguridad para los dispositivos móviles, mencionada previamente como requisito básico antes de la adopción de una solución MDM, se hace aún más patente en entornos BYOD, siendo necesario que la política diferencie entre los requisitos asociados a los dispositivos de la organización y los dispositivos móviles personales empleados en el entorno corporativo.

97. Existen numerosas implicaciones legales asociadas al uso de dispositivos móviles, y los datos que éstos gestionan, en entornos BYOD, debido al carácter personal de los mismos, que quedan fuera del alcance del presente documento.

98. A modo de referencia, algunos de los aspectos legales a considerar (especialmente si no se dispone de consentimiento del usuario por escrito) son la monitorización de los dispositivos móviles y su tráfico de red para detectar violaciones en la política de seguridad de la organización, el borrado de datos o apps personales, el acceso a datos personales almacenados en el dispositivo móvil o en servicios “en la nube” durante las auditorías o la investigación de un incidente de seguridad, la monitorización de los dispositivos móviles fuera de las dependencias de la organización, como por ejemplo mediante la utilización de mecanismos de localización del dispositivo móvil para conocer su ubicación física, o la responsabilidad a la hora de compensar, reparar o sustituir el dispositivo móvil del usuario por haber sido robado, perdido o dañado, así como las implicaciones legales de la distribución o uso de software pirata o sin licencia y malware [Ref.- 53].

99. Los aspectos legales son condición suficiente en muchas organizaciones para mantener la propiedad de los dispositivos móviles que son entregados a los usuarios y facilitar así las tareas de monitorización, el borrado remoto de datos o la realización de auditorías de

seguridad sobre los mismos, manteniendo en todo momento el control sobre la propiedad intelectual y los derechos de autor de los contenidos por parte de la organización.

100. Se recomienda por tanto consultar al departamento legal de la organización para analizar y profundizar en estos aspectos, que habitualmente tienen implicaciones directas sobre la privacidad del usuario.

101. Por otro lado, una de las características deseadas de las soluciones MDM para entornos BYOD, y potencialmente también para entornos únicamente corporativos, es la posibilidad de definir el número de dispositivos móviles gestionados permitidos por usuario.

102. En el caso de implantar un entorno BYOD, se recomienda disponer (a través de un servidor web interno) de tutoriales, vídeos y documentación qué permitan a los empleados de la organización llevar a cabo el registro de sus dispositivos móviles personales en la solución MDM de manera sencilla y con la menor implicación posible por parte de los administradores TIC (ver apartado "5.2. REGISTRO DE LOS DISPOSITIVOS MÓVILES EN LA SOLUCIÓN MDM").

103. Las guías para el usuario final deben proporcionar toda la información necesaria para suscribir de forma segura los dispositivos móviles personales en la solución MDM, incluyendo todas las plataformas móviles soportadas, y que éstos pasen a ser dispositivos móviles gestionados por la organización.

104. Aunque la industria ha adoptado de forma general el término BYOD (*Bring Your Own Device*) para referenciar este escenario de uso, el término correcto y que refleja el riesgo para las organizaciones debería ser CYOD (*Connect Your Own Device*), ya que no existe riesgo de seguridad asociado hasta que el usuario **conecta** su dispositivo móvil personal a la red (por ejemplo, vía Wi-Fi) o sistemas (por ejemplo, vía USB) de la organización para acceder a los servicios y datos corporativos.

105. Debido al dinamismo y continua evolución de la industria móvil, recientemente ha surgido otra tendencia que está siendo adoptada ampliamente por numerosas organizaciones, denominada BYOA (*Bring Your Own App(lication)*).

106. En escenarios BYOA los usuarios instalan apps de los mercados de aplicaciones públicos en sus dispositivos móviles personales o corporativos para incrementar su productividad, empleándolas para realizar sus tareas profesionales y manejar, por tanto, datos corporativos.

107. Para acomodar todos estos escenarios de uso, una tendencia más reciente y práctica, desde el punto de vista empresarial, es clasificar los dispositivos móviles en dos grandes grupos, dispositivos gestionados y no gestionados, independientemente de quién es el propietario del propio dispositivo móvil (o *hardware*).

108. Los dispositivos gestionados son aquellos que han seguido el proceso de registro o *enrollment*, y por tanto, sobre los que se ha aplicado la política de seguridad de la organización y la configuración adecuada a los requisitos de seguridad del dispositivo y de la información que maneja. Estos dispositivos están englobados y gestionados por la solución MDM.

109. Por el contrario, los dispositivos no gestionados son aquellos sobre los que la organización no ha llevado las tareas de configuración previamente definidas, y por tanto, no dispone de control sobre su configuración o el nivel de seguridad de los mismos.

110. Esta clasificación puede ser extendida igualmente a las aplicaciones móviles, disponiendo entonces de dos tipos de apps, apps gestionadas frente a no gestionadas.

4.5 GESTIÓN LOCAL DE DISPOSITIVOS MÓVILES

111. Los diferentes fabricantes de las principales plataformas móviles proporcionan herramientas y software para la gestión local de los dispositivos por parte del usuario.

112. Estas soluciones locales están centradas únicamente en una plataforma móvil concreta y permiten la gestión de un número muy reducido de dispositivos, de manera manual, a través del puerto USB del ordenador donde están instaladas.

113. En algunos casos, a través de las soluciones de gestión local es posible establecer parámetros de configuración avanzados y de seguridad, actualizar el sistema operativo y las apps del dispositivo móvil, transferir y sincronizar datos (correo electrónico, contactos, calendario, etc) y contenido multimedia (imágenes y fotos, vídeos, música, documentos, etc), así como realizar copias de seguridad de los contenidos y la configuración.

114. Android es una plataforma móvil con limitaciones significativas en la gestión local de los dispositivos móviles, ya que el modelo empleado por Google se basa principalmente en la gestión y sincronización de los mismos a través de los servicios disponibles "en la nube", como Google Apps.

115. En el caso de dispositivos móviles Android se dispone del kit de desarrollo de software (SDK, *Software Development Kit*) [Ref.- 32], que permite llevar a cabo una gestión limitada del dispositivo y la realización de otras tareas avanzadas a través del puerto USB, más orientadas a desarrolladores que al usuario final.

116. Los dispositivos móviles BlackBerry ≤7.x disponen del BlackBerry Desktop Software tanto para PC (Windows) como para Mac OS X [Ref.- 33].

117. Para los dispositivos móviles basados en BlackBerry 10.x debe hacerse uso de BlackBerry Link [Ref.- 34], también disponible para PC (Windows) y Mac OS X.

118. Apple proporciona diferentes herramientas para la gestión local de los dispositivos móviles iOS, desde iTunes [Ref.- 35] (para Mac y PC) hasta iPhone Configuration Utility (iPCU) [Ref.- 20] o Apple Configurator [Ref.- 21] (ver apartado "6.3.3. SOLUCIONES MDM A PEQUEÑA ESCALA PARA iOS").

119. Microsoft empleó durante muchos años la herramienta Microsoft ActiveSync para la gestión local de dispositivos móviles Windows Mobile desde ordenadores Windows, complementada posteriormente con otras soluciones, como Security Configuration Manager PowerToy for Windows Mobile (SCMPT).

120. Posteriormente, la gestión de Windows Phone 7.x se realizó a través de Zune para Windows [Ref.- 29] y de Windows Phone 7 Connector para Mac OS X [Ref.- 30] (sustituida por [Ref.- 31]).

121. Finalmente, para la gestión local de Windows Phone 8 se dispone de la aplicación Windows Phone tanto para ordenadores de escritorio como para Mac OS X [Ref.- 31].

122. Pese a las capacidades existentes en las soluciones de gestión locales para las diferentes plataformas móviles, no es posible su aplicación a nivel empresarial, ya que su utilización se hace impracticable cuando es necesario gestionar un número significativo de dispositivos móviles.

123. Por este motivo, entre otros, es necesario disponer de soluciones MDM empresariales para gestionar los dispositivos móviles existentes en la organización de manera centralizada, sencilla, remota y homogénea.

4.6 SOLUCIONES MDM EN LA INDUSTRIA

124. Cada uno de los fabricantes de las principales plataformas móviles proporciona sus propias soluciones de gestión empresarial de los dispositivos, centradas principalmente o únicamente en su plataforma móvil.

125. Las soluciones MDM pueden, en primera instancia, ser clasificadas en dos grandes grupos: aquellas que proporcionan sus servicios de forma remota a través de arquitecturas "en la nube" (*cloud computing*) y aquellas más tradicionales que requieren disponer de una arquitectura de gestión dentro de la propia organización (*on-premises*), compuestas habitualmente por uno o varios servidores MDM.

126. En el caso de soluciones MDM que se despliegan en la propia organización, es fundamental analizar la arquitectura o arquitecturas soportadas por el fabricante de la solución MDM y entender en detalle las comunicaciones desde y hacia los servidores MDM.

127. Este conocimiento permitirá identificar el modelo de arquitectura a emplear para la integración de la solución MDM en la organización, diseñando y definiendo cuál será la ubicación de los servidores MDM (por ejemplo, en la DMZ o en una red interna de la organización) y las reglas de filtrado necesarias en los cortafuegos perimetrales o internos de la organización.

128. A continuación se describen brevemente las soluciones MDM proporcionadas por los fabricantes de las principales plataformas móviles.

4.6.1 GOOGLE (ANDROID)

129. Google promueve una solución de gestión de dispositivos móviles basada entorno a su modelo de negocio con servicios "en la nube", y concretamente a través de la plataforma Google Apps [Ref.- 36] y Google Apps For Business and Government[Ref.- 72].

130. Google App for Business es un marco de trabajo empresarial, tanto para el uso de aplicaciones comunes entre los empleados, creación de dominios y políticas con estos dominios y subdominios, como gestión de terminales y aplicaciones de los mismos.

131. Las organizaciones con cuenta en Google Apps de tipo *Business*, *Government* o *Education*, disponen de la aplicación móvil "Google Apps Device Policy" [Ref.- 37] en Google Play que permite al administrador TIC realizar una gestión limitada de los dispositivos móviles de los usuarios, incluyendo la aplicación de políticas de seguridad, por ejemplo relativas a los requisitos del código de acceso o al cifrado del dispositivo (Android 3.x & 4.x o iOS 3.1+), eliminación y localización del mismo.

132. A través de esta app, o agente de gestión, es posible hacer sonar el dispositivo móvil o localizarlo, bloquear el dispositivo o cambiar el código de acceso remotamente, llevar a cabo el borrado remoto de datos (*wipe*; excluyendo la tarjeta de almacenamiento externa), o auditar las apps de los dispositivos Android que acceden a datos corporativos en Google Apps.

FIGURA 2.- Panel de Administración avanzada de dispositivos de Googel Apps Business[Ref.- 72]

133. Si un dispositivo móvil está configurado para utilizar "Google Apps Device Policy" con varias cuentas de Google Apps, cada una de ellas con políticas de seguridad distintas, se aplicará la política más restrictiva.

134. Las tareas de gestión pueden ser realizadas por el administrador TIC mediante la consola del administrador de Google o, en algunos casos, por el propio usuario a través del panel de control "Mis dispositivos" (o "My Devices") de Google Apps[4].

135. La solución de Google aplica a dispositivos Android desde la versión 2.2 y otros dispositivos móviles soportados por Google Sync, como iPhone y iPad, Windows Phone y dispositivos con soporte para Microsoft Exchange ActiveSync (EAS) [Ref.- 38].

136. Adicionalmente, a través de Google Apps es posible gestionar la distribución de apps a los dispositivos móviles corporativos a través de "Google Play Private Channel" [Ref.- 39]. Esta plataforma permite la creación de un mercado de apps privado vía Google Play para distribuir las aplicaciones propias e internas de la organización entre sus usuarios.

137. Por otro lado, Android dispone del servicio *Google Cloud Messaging* (GCM) [Ref.- 68] que permite establecer comunicaciones a través de mensajes desde los servidores de un servicio o app concretos, como por ejemplo los servidores de la solución MDM y su agente o app asociada, hacia los dispositivos móviles gestionados (ver apartado "6.1.1. ARQUITECTURA DE GESTIÓN MDM DE ANDROID").

138. Se dispone de más información en el apartado "6.1. GESTIÓN DE ANDROID".

[4] Google Apps - My Devices [Ref.- 63]: https://www.google.com/apps/mydevices.

4.6.2 BLACKBERRY

139. La plataforma BlackBerry fue pionera al proporcionar mecanismos sofisticados, homogéneos y centralizados para la monitorización y gestión empresarial de los dispositivos móviles, concretamente a través de una arquitectura e infraestructura propietaria de BlackBerry (ver apartado "6.2.1. ARQUITECTURA DE GESTIÓN MDM DE BLACKBERRY").

140. Los mecanismos de aplicación de políticas de seguridad de BlackBerry permiten establecer políticas individuales, por grupos funcionales, por departamentos o globales a toda la organización, así como distribuir ajustes de configuración muy granulares a todos los dispositivos gestionados.

141. Recientemente las soluciones de gestión propietarias de BlackBerry (como el *Universal Device Service*) permiten la gestión de otras plataformas móviles, como Android e iOS, siguiendo la tendencia empresarial BYOD.

142. Debe tenerse en cuenta que BlackBerry ha introducido cambios muy significativos con el lanzamiento de la versión 10, en relación a versiones previas de su plataforma móvil (5.x-7.x).

143. Se dispone de más información en el apartado "6.2. GESTIÓN DE BLACKBERRY".

4.6.3 APPLE (IOS)

144. Apple promueve una solución de gestión de dispositivos móviles basada en el *Apple Push Notification Service* (APNS), con un protocolo y arquitectura propietarios para la comunicación entre los servidores de gestión, los dispositivos móviles iOS gestionados y la infraestructura propia de Apple (ver apartado "6.3.2. ARQUITECTURA DE GESTIÓN MDM DE iOS").

145. La arquitectura y mecanismos de gestión proporcionados por Apple son exclusivos para los dispositivos móviles iOS, aunque se permite la integración de soluciones MDM (multiplataforma o únicamente para iOS) de terceros para la gestión empresarial de los mismos.

146. Apple proporciona a los usuarios a nivel particular, no corporativo, desde la versión 5.x de iOS una solución básica de gestión de los dispositivos móviles a través de la plataforma iCloud [Ref.- 40] (previamente denominada MobileMe) para la gestión de dispositivos "en la nube".

147. A través de la misma los usuarios pueden de forma remota mostrar un mensaje o hacer sonar el dispositivo móvil, localizarlo, bloquear el dispositivo, o llevar a cabo el borrado remoto de datos (*wipe*).

148. Alternativamente, iCloud permite realizar copias de seguridad del correo electrónico, calendario, lista de contactos, notas, recordatorios, datos de otras apps, y, recientemente, el acceso a aplicaciones ofimáticas "en la nube" (como Pages, Numbers y Keynote).

149. Adicionalmente, Apple proporciona diferentes soluciones y herramientas para la gestión individual y local de dispositivos móviles en entornos de pequeño y mediano tamaño, por ejemplo a través de iTunes [Ref.- 35] (ver apartado "6.3.3. SOLUCIONES MDM A PEQUEÑA ESCALA PARA iOS").

150. Se dispone de más información en el apartado "6.3. GESTIÓN DE iOS".

4.6.4 MICROSOFT (WINDOWS PHONE)

151. Tradicionalmente, Microsoft, como líder de soluciones TIC a nivel empresarial, ha proporcionado capacidades de gestión para diferentes plataformas móviles a través de Microsoft Exchange, y en concreto a través de Microsoft Exchange ActiveSync (EAS o MEAS) [Ref.- 8], al considerarse éste servidor de correo electrónico y productividad un elemento común en la mayoría de entornos corporativos.

152. EAS permite disponer de capacidades de gestión, tanto al usuario final (autogestión) como al administrador TIC de la organización, a través de Outlook Web Access (OWA) o de la Exchange Management Console (EMC) respectivamente.

153. Adicionalmente, Microsoft proporciona capacidades de gestión empresarial más avanzadas a través de Microsoft System Center Mobile Device Manager (2008 y 2010, MSCMDM o SCMDM) [Ref.- 15] y System Center 2012 [Ref.- 9].

154. La principal ventaja de emplear Microsoft Exchange y EAS para la gestión de dispositivos móviles es que, asumiendo que se dispone de un entorno Microsoft Exchange previamente, sólo es necesario definir y aplicar la política de seguridad corporativa en los dispositivos móviles.

155. Sin embargo, aunque todas las plataformas móviles actuales disponen de capacidades de integración con EAS, lo hacen en diferentes grados y niveles de funcionalidad, principalmente en función de la plataforma móvil y su versión, y de la versión de Microsoft Exchange empleada (2003, 2007, 2010 ó 2013).

156. De manera general debe considerarse que la gestión de dispositivos móviles mediante EAS sólo hace uso de un conjunto mínimo y muy limitado de controles disponibles (aplicando esta situación a todas las referencias a EAS a lo largo del presente documento).

157. Esta situación dificulta el despliegue de políticas de seguridad comunes para todas las plataformas móviles, y en caso de hacerlo, éstas deben ser muy generales e imponer restricciones mínimas en los dispositivos móviles.

158. Se dispone de más información en el apartado “6.4. GESTIÓN DE WINDOWS PHONE”.

4.6.5 SOLUCIONES MDM DE TERCEROS

159. Adicionalmente a las soluciones proporcionadas por los fabricantes de las principales plataformas móviles, se dispone de soluciones MDM de otros fabricantes cuyo foco de negocio es específicamente la gestión de dispositivos móviles, o de fabricantes TIC de mayor tamaño que han incluido en sus soluciones empresariales estas capacidades.

160. Con el objetivo de comparar las distintas funcionalidades y características ofrecidas por las diferentes soluciones MDM se recomienda tanto consultar los estudios de mercado publicados por los analistas de referencia en la industria (Gartner, IDC, etc), como comparativas específicas centradas en los aspectos más específicos y/o técnicos de cada solución MDM.

161. Anualmente, o incluso con mayor frecuencia, analistas como Gartner e IDC publican diferentes estudios centrados en las diferentes soluciones MDM disponibles en el mercado:

- Gartner 2013: “Magic Quadrant for Mobile Device Management Software”. 23 May 2013. [Ref.- 10]
- Gartner 2013: “Critical Capabilities for Mobile Device Management Software”. 23 May 2013. [Ref.- 11]

- Gartner 2012: "Magic Quadrant for Mobile Device Management Software". 17 May 2012. [Ref.- 12]
- Gartner 2011: "Magic Quadrant for Mobile Device Management Software". 13 April 2011. [Ref.- 13]
- IDC 2012: "Worldwide Mobile Enterprise Management Software 2012 – 2016 Forecast and Analysis and 2011 Vendor Shares". September 2012. [Ref.- 14]
- Forrester 2012: "Market Overview: Cloud-Hosted Mobile Device Management Solutions And Managed Services". January 3, 2012. [Ref.- 55]
- Forrester 2012: "Market Overview: On-Premises Mobile Device Management Solutions, Q3 2011". January 3, 2012. [Ref.- 56]
- Info-Tech 2011: "Vendor Landscape: Mobile Device Management" [Ref.- 57]
- The Radicati Group, Inc. (December 2012): "Mobile Device Management - Market Quadrant 2012" [Ref.- 60]

162. La evolución del cuadrante mágico de Gartner para las soluciones MDM en los últimos años (2011-2013) es la siguiente:

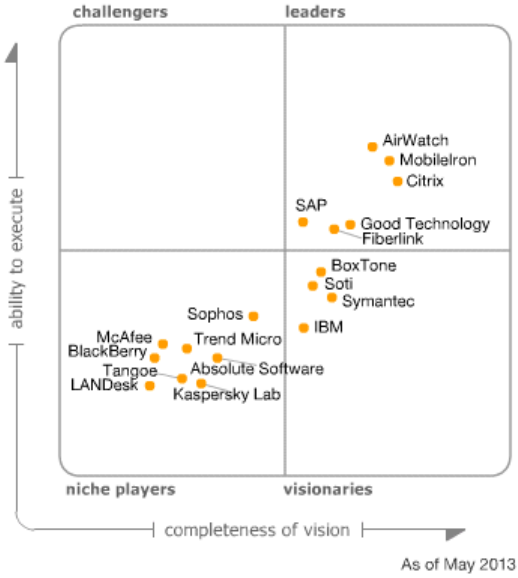

FIGURA 3.- Cuadrante mágico de Gartner para las soluciones MDM 2013 [Ref.- 10]

Figure 1. Magic Quadrant for Mobile Device Management Software

Source: Gartner (May 2012)

FIGURA 4.- Cuadrante mágico de Gartner para las soluciones MDM 2012 [Ref.- 12]

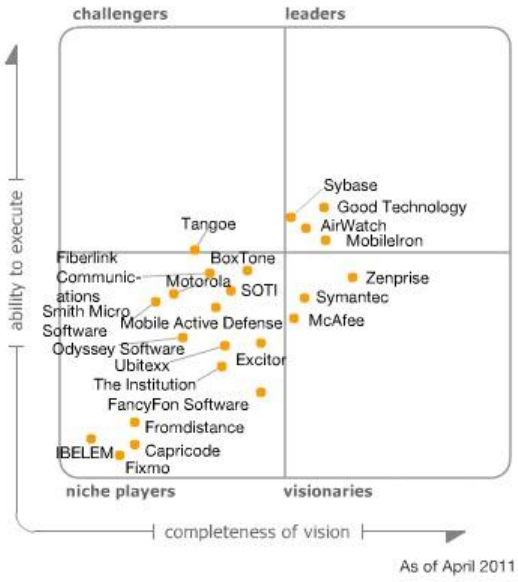

FIGURA 5.- Cuadrante mágico de Gartner para las soluciones MDM 2011 [Ref.- 13]

163. Complementando los estudios generales de mercado previos, se dispone de comparativas de referencia de terceros entre las diferentes soluciones MDM que permiten analizar de forma específica las capacidades proporcionadas por los distintos fabricantes [5]:

- Comparison of MDM Providers. Enterprise iOS: http://www.enterpriseios.com/wiki/Comparison_MDM_Providers
- Compare MDM Providers:

[5] Debido a que se publican nuevos estudios con frecuencia comparando las diferentes soluciones MDM, se recomienda emplear los buscadores de Internet para su localización, empleando el término “MDM comparison”.

http://www.mdmcomparison.com

- MDM Comparison Chart:
  http://www.bluefishwireless.net/wp-content/uploads/2012/06/Bluefish-MGMT-MDM-Comparison-Chart.pdf
- MDM Tools: Features and Functions Compared:
  https://www.computerworld.com/s/article/9238981/MDM_tools_Features_and_functions_compared

A modo de referencia y para facilitar su consulta, el Apéndice A (ver apartado “0.

164. APÉNDICE A: FABRICANTES DE SOLUCIONES MDM") incluye una lista ordenada alfabéticamente con algunos de los fabricantes de soluciones MDM actuales.

4.6.6 SOLUCIONES DE GESTIÓN BASADAS EN UN CONTENEDOR

165. Por último, dentro de los tipos de soluciones MDM es importante diferenciar dos grandes grupos: aquellas que se basan en la gestión completa de la plataforma o dispositivo móvil en base a las capacidades proporcionadas por cada uno de los fabricantes, y aquellas que se basan en la gestión de los datos, aplicaciones y servicios corporativos.

166. El segundo grupo engloba soluciones MDM de tipo contenedor (o *container* en inglés), una aproximación a la gestión de dispositivos móviles que considera la plataforma móvil como un entorno inseguro y que proporciona una app segura para llevar a cabo todas las actividades y tareas corporativas.

167. En lugar de gestionar la plataforma móvil completa y todas sus apps, la gestión se centra en una única app, que es la que tiene acceso a los datos y servicios corporativos.

NOTA: A modo de referencia se proporcionan ejemplos de soluciones MDM de tipo contenedor, como Good for Enterprise (GFE) de Good Technology (con soporte para Android, iOS, y Windows Phone), o Excitor DME (con soporte para Android e iOS).

168. Este tipo de soluciones hacen un uso extensivo de mecanismos de seguridad, proporcionando un entorno restringido o *sandbox* para proteger los datos que son gestionados por la app contenedora de la solución MDM.

169. Entre los mecanismos de seguridad empleados por la app contenedora se encuentran sistemas de autentificación adicionales a los del dispositivo móvil (y habitualmente centralizados), cifrado de datos en reposo y tránsito, es decir, al almacenarlos localmente y al enviarlos por la red, sistemas de prevención de fuga de datos que establecen restricciones para el movimiento de datos local (a través de la captura de pantalla, de la funcionalidad de copiar y pegar, del envío de datos a cuentas de correo electrónico externas, del intercambio o compartición local de datos entre apps, de las capacidades de impresión, etc), o controles de acceso en base al tiempo (sólo se puede usar la app a ciertas horas o puede expirar llegada una fecha) o a la ubicación (sólo se puede usar la app en ciertos lugares, o lo contrario, no puede ser utilizada en ciertos lugares).

170. En el caso de que la app contenedora disponga de mecanismos de autentificación, situación más habitual y recomendada, la solución MDM debería proporcionar mecanismos de gestión del código de acceso o autentificación (complejidad, longitud, renovación, etc – ver apartado "5.5.2. GESTIÓN DEL CÓDIGO DE ACCESO").

171. Algunas soluciones MDM añaden capacidades de autentificación de dos (o más) factores sobre la app contenedora, con el objetivo de proteger con mecanismos de seguridad más robustos los datos corporativos.

172. Dentro de la industria, este tipo de soluciones están teniendo más éxito en entornos BYOD, ya que toda la gestión corporativa afecta únicamente a la app contenedora y es más sencilla su implantación (y eliminación) en los dispositivos móviles personales de los usuarios, y permite establecer una separación entre datos personales y corporativos.

173. Por el contrario, la mayor desventaja identificada por parte de los usuarios es que no disponen de todas las capacidades de integración, compartición de información y facilidad de uso proporcionadas por la plataforma móvil empleada, ya que las aplicaciones a emplear para el

acceso a los datos corporativos deben ser las existentes dentro de la app contenedora (con una experiencia de usuario más restringida).

174. Así por ejemplo, los usuarios no pueden hacer uso del calendario, contactos, cliente de correo electrónico o el navegador web nativos existentes en la plataforma móvil por defecto, o instalados posteriormente por el usuario, debiendo emplear en su lugar las aplicaciones equivalentes existentes dentro de la app contenedora y su interfaz de usuario, potencialmente más seguras pero menos atractivas para el usuario.

175. Por otro lado, la app contenedora no dispone de acceso a las capacidades hardware avanzadas de cifrado para el almacenamiento de claves (por ejemplo, en iOS), ni dispone de la posibilidad de establecer restricciones o controles de acceso en el hardware y capacidades del dispositivo móvil (por ejemplo, el acceso a la cámara).

176. Debe tenerse en cuenta que los mecanismos de seguridad de la app contenedora podrían verse potencialmente vulnerados, al ejecutar ésta sobre una plataforma móvil (potencialmente) insegura, que podría ser manipulada, por ejemplo mediante la inserción de código dañino, para modificar el comportamiento de la app contenedora.

177. Otros fabricantes, aunque proporcionan soluciones MDM estándar, ofrecen como elemento adicional soluciones de tipo contenedor específicas para el acceso a ciertos servicios o contenidos, a través de apps para la navegación web o el acceso al correo electrónico.

178. Cada vez es más habitual disponer de apps complementarias a la solución MDM que actúan como contenedores seguros para el acceso a los contenidos corporativos, tanto para los servicios habituales (por ejemplo, e-mail) como para servicios más específicos del negocio a través de apps empresariales.

NOTA: A modo de referencia se proporcionan ejemplos de soluciones MDM de tipo contenedor específicas para un propósito concreto, como las proporcionadas por AirWatch (AirWatch Browser o AirWatch Email Container).

179. Existen actualmente diferentes modelos para compartimentalizar el mundo profesional y el personal dentro del mismo dispositivo móvil. Una opción es hacerlo a través de una app contenedora asociada a la solución MDM mencionada previamente. Otra opción es disponer de las capacidades de particionar el dispositivo móvil en la propia plataforma, como en el caso de BlackBerry 10 (ver apartado "4.6.6.1. BLACKBERRY 10 BALANCE"). Por último, otro modelo es el adoptado por iOS 7 centrado en compartimentalizar o aislar los datos corporativos, en lugar de crear áreas de trabajo diferenciadas (ver apartado "6.3.1. iOS 7"). Adicionalmente, la solución Samsung KNOX para Android [Ref.- 67] emplea un modelo híbrido que hace uso tanto de modificaciones en la plataforma móvil como de apps contenedoras para implementar esta compartimentalización.

4.6.6.1 *BLACKBERRY 10 BALANCE*

180. Esta idea de compartimentalizar y separar el entorno personal del profesional ha sido extendida a nivel de la propia plataforma móvil en el caso de BlackBerry con la versión 10 y una nueva arquitectura denominada BlackBerry Balance [Ref.- 46], dónde existen dos perfiles o áreas de trabajo (*work spaces*), la personal y la profesional.

181. Los mecanismos de control de acceso de BlackBerry 10 no permiten compartir datos entre estas dos áreas, manteniendo así los datos y comunicaciones corporativas seguras, y separadas de las fotos, apps y documentos personales y de su privacidad.

182. Esta separación también permite llevar a cabo el borrado remoto (*wipe*) únicamente de los datos corporativos, es decir, del área de trabajo profesional (tanto del dispositivo como de las tarjetas de almacenamiento externas), y no de la totalidad del dispositivo móvil, una característica con aplicación directa en entornos BYOD.

183. Por ejemplo, el acceso al mercado oficial de apps de BlackBerry, BlackBerry (App) World, desde el área de trabajo profesional sólo mostrará las apps aprobadas a nivel corporativo. Otras apps no aprobadas podrán ser instaladas en el área personal del dispositivo, fomentando así la implantación de entornos BYOD.

184. Adicionalmente, y con el objetivo de compartimentalizar el área de trabajo profesional y el personal en otros dispositivos móviles soportados por su solución de gestión empresarial, como Android e iOS (ver apartado "6.2.2. BLACKBERRY 10"), BlackBerry dispone de Secure Work Space [Ref.- 47], una app integrada en su entorno de gestión BlackBerry Enterprise Service 10 que proporciona un contenedor para el acceso al entorno corporativo desde dispositivos personales.

185. La aproximación adoptada es exactamente la misma descrita previamente para otras soluciones MDM de tipo contenedor de terceros (ver apartado "4.6.6. SOLUCIONES DE GESTIÓN BASADAS EN UN CONTENEDOR").

186. BlackBerry Secure Work Space permite el acceso al correo electrónico (con un visor de ficheros adjuntos), calendario, contactos (con acceso al directorio corporativo), visor de documentos, y navegación web (para el acceso a servidores web de la Intranet y contenido corporativo).

4.6.6.2 *SAMSUNG KNOX*

187. Samsung KNOX para Android [Ref.- 67] es una plataforma de seguridad diseñada para compartimentalizar los datos y apps corporativas de los personales (BYOD) en dispositivos móviles basados en Android.

188. Para ello emplea un modelo híbrido que hace uso tanto de modificaciones en la plataforma móvil como de apps contenedoras para implementar esta compartimentalización.

189. KNOX implementa seguridad en la plataforma móvil mediante una estrategia en tres niveles, empleando un gestor de arranque seguro, una arquitectura basada en zonas de confianza propia de los procesadores ARM, y un *kernel* de sistema operativo basado en SE (Security Enhancements) para Android.

190. La protección de los datos corporativos se lleva a cabo a través de una app contenedora, que permite la utilización de múltiples apps empresariales protegidas, y que hace uso de cifrado (AES-256) para el almacenamiento y transmisión de los datos (mediante VPNs por app).

191. Adicionalmente. KNOX proporciona capacidades a través de numerososas políticas predefinidas y de librerías (APIs) para su integración en las soluciones MDM de gestión empresarial, asociadas a las capacidades MDM de las soluciones Samsung SAFE.

5 CARACTERÍSTICAS Y CAPACIDADES DE LAS SOLUCIONES MDM

192. El presente apartado detalla numerosas características y funcionalidades disponibles en las diferentes soluciones MDM que existen actualmente en la industria, clasificadas en base a las múltiples capacidades que ofrecen.

193. Debe tenerse en cuenta que algunas de las características más específicas descritas a continuación no son aplicables a todas las plataformas móviles habituales, ya que no todas

ellas implementan esa funcionalidad o disponen de mecanismos que permitan la configuración y gestión de determinados aspectos del dispositivo móvil.

194. El presente apartado incluye por tanto el mayor o más completo conjunto de capacidades disponible actualmente para la gestión y protección de los dispositivos móviles.

195. Es por tanto fundamental antes de elegir una solución MDM concreta evaluar cuales de todas las características (o conjuntos de características) proporcionadas por la solución MDM aplican a cada una de las plataformas móviles soportadas por la organización.

5.1 CARACTERÍSTICAS GENERALES Y FORMATO DE LA SOLUCIÓN MDM

196. Las soluciones MDM pueden ser proporcionadas en diferentes formatos de distribución habituales en la industria, desde servicios remotos "en la nube" conocidos como SaaS (*Software as a Service*, ya sea ubicados en las dependencias de la organización o en Internet), pasando por dispositivos hardware que contienen toda la solución MDM (conocidos como *appliances*), hasta como distribución de software tradicional para los principales sistemas operativos: Windows, Unix/Linux o Mac OS X.

197. Algunas soluciones MDM adoptan aproximaciones híbridas, combinando servicios en las instalaciones de la organización con servicios "en la nube", mientras que algunos fabricantes ofrecen incluso dos soluciones diferenciadas en base a estos dos modelos de negocio o despliegue [Ref.- 60].

198. Por otro lado, algunos fabricantes ofrecen dos versiones, una solución MDM básica y otra más avanzada, que incluye todas las capacidades necesarias para organizaciones de gran tamaño (MDM, MAM, MCM, app contenedora, tienda de apps de la organización, etc), mientras que otros ofrecen cada uno de esos componentes mediante una arquitectura modular, lo que permite a las organizaciones adquirir únicamente aquellos módulos que sean realmente necesarios según sus requisitos técnicos y financieros actuales, pudiendo incrementar la funcionalidad y complejidad del entorno MDM en el futuro.

199. Alternativamente, las organizaciones interesadas en la gestión de sus dispositivos móviles pueden optar por externalizar la gestión y administración de su solución MDM a los operadores de telecomunicaciones o a las grandes empresas de la industria que ofrecen servicios TIC gestionados [Ref.- 56], aunque desde el punto de vista de seguridad no se recomienda esta solución de gestión.

200. Otros aspectos generales a considerar en la evaluación de una solución MDM son:

- El modelo de licencias, siendo habitual una licencia única (o perpetua) para la solución MDM o una licencia que debe ser renovada periódicamente (por ejemplo, mensualmente o anualmente).
- Debe tenerse en cuenta que habitualmente las licencias de las soluciones MDM suelen aplicarse por dispositivo móvil a gestionar, y no por servidor. Otra opción es aplicar las licencias por usuario, independientemente del número de dispositivos móviles asignados a éste.
- El contrato de soporte y mantenimiento, debiendo considerar si se incluyen en el mismo las actualizaciones a nuevas subversiones y versiones principales, las actualizaciones de seguridad y de resolución de errores, el tipo de acceso al servicio de soporte (e-mail, teléfono, presencial, etc), el horario de soporte (12x5, 12x7, 24x7), etc.

- Debe evaluarse si el precio de la licencia incluye el contrato de mantenimiento y soporte, habitual en licencias de suscripción temporales y abonado aparte normalmente en las licencias de un único pago o perpetuas.
- Adicionalmente, en el caso de organizaciones con presencia en múltiples países, es importante tener en cuenta en qué países dispone de presencia y de capacidades de soporte el fabricante de la solución MDM.
- Los idiomas soportados por el interfaz de autoprovisionamiento para el registro por parte de los usuarios, por el interfaz de administración y por el interfaz asociado a los diferentes servicios de la solución MDM.
- La posibilidad de personalizar el interfaz de usuario con el logo, colores y otras preferencias de la organización (*custom branding*).
- La gestión y monitorización de los procesos de auditoria de las aplicaciones y el terminal.
- La gestión y administración de los logs tanto de los terminales gestionados por las soluciones MDM como de ella misma.

201. En el caso de implantar una solución MDM en un entorno crítico o con implicaciones de negocio relevantes, muy habitual en la mayoría de organizaciones debido a la constante y creciente dependencia en los dispositivos móviles, es necesario evaluar las capacidades frente a tolerancia a fallos, carga y escalabilidad de la solución (o número máximo de dispositivos móviles soportados):

    - La solución MDM debería disponer de la posibilidad de integrar uno o varios servidores trabajando todos ellos en modo activo, o en modo activo-pasivo (*failover*).
    - Debería disponer de capacidades para ajustar, de forma automática o manual, el balanceo de carga, especialmente durante situaciones de carga elevada, ya sea al realizar tareas de gestión específicas (por ejemplo, la consulta del número de apps y versiones en todos los dispositivos móviles de la organización) o tareas de negocio en momentos puntuales (por ejemplo, en el cierre del mes).
    - Debería ser posible añadir nuevos servidores a la solución MDM en el caso en que el número de dispositivos móviles a gestionar crezca significativamente respecto a la estimación contemplada inicialmente.
    - Debería disponer de capacidades de administración independientes por cada departamento o ubicación de la organización, permitiendo la existencia de administradores independientes para cada grupo a gestionar, que pueden incluso requerir políticas de seguridad diferentes.

202. Desde un punto de vista más técnico, debe evaluarse los diferentes interfaces disponibles para la administración de la solución MDM, pudiendo disponerse de un interfaz web para acceder a través de cualquier navegador o de una aplicación cliente de escritorio tradicional. En el primer caso es importante evaluar qué navegadores web están soportados por la solución: IE, Firefox, Safari, Chrome, Opera, etc). En el segundo caso es importante evaluar sí esta aplicación cliente está disponible únicamente para sistemas operativos tradicionales (Windows, Linus/Unix, Mac OS X) o si también permite el acceso desde dispositivos móviles (Android, iOS, etc).

203. Desde el punto de vista de seguridad se recomienda llevar a cabo la gestión de los dispositivos móviles desde un entorno cliente tradicional y seguro, y no desde otros dispositivos móviles.

204. Un elemento fundamental para la gestión de los dispositivos móviles de la organización por parte del administrador TIC es la consola de gestión, panel de control o *dashboard* de la solución MDM, qué permita tanto la realización de consultas y búsquedas, la ejecución de acciones en el entorno móvil corporativo, así como la visualización de alertas automáticas.

205. Desde el punto de vista de seguridad de la propia solución MDM, como elemento crítico en la arquitectura de la organización, es necesario analizar las capacidades de cifrado de las comunicaciones entre la solución MDM y el dispositivo móvil (OTA), incluyendo un estudio detallado de los protocolos y algoritmos de cifrado empleados.

206. Complementando los mecanismos de cifrado, es crítico también disponer de mecanismos de autentificación mutua robustos entre los dispositivos móviles y los servidores de la solución de gestión MDM.

207. Aparte de las características y funcionalidades específicas de la solución MDM, es fundamental para cualquier organización evaluar las capacidades de integración de la solución MDM con el resto de soluciones de gestión, monitorización y administración TIC ya existentes en el entorno, con el objetivo de que el proceso de implantación e integración en la arquitectura actual sea lo más sencillo y homogéneo posible.

208. El interfaz de la solución MDM puede proporcionar una API (o interfaz de programación) o SDK (o kit de desarrollo) para su integración estándar o a medida con otras soluciones de gestión y software empresarial.

209. Asimismo, y desde el punto de vista de seguridad, se recomienda evaluar las capacidades de integración de la solución MDM con las soluciones o *suites* de seguridad con capacidades de antivirus y antimalware móvil, tanto del mismo fabricante como de terceros.

5.2 REGISTRO DE LOS DISPOSITIVOS MÓVILES EN LA SOLUCIÓN MDM

210. Uno de los pasos iniciales y fundamentales a considerar en toda solución MDM es como se llevará a cabo el registro o suscripción, es decir, la incorporación inicial de los dispositivos móviles a la solución (proceso conocido como *enrollment*), para que estos pasen a estar gestionados por la organización.

211. Una vez configurada la solución MDM se debe llevar a cabo el registro de los dispositivos móviles en la misma, con el objetivo de establecer una relación entre ambos, y que el dispositivo móvil pase a estar gestionado por la organización sin ser necesaria la intervención posterior del usuario.

212. En entornos de tamaño reducido es posible realizar este proceso de forma manual, debiendo los administradores TIC plataformar (o preparar para su uso adecuado en la organización) todos y cada uno de los dispositivos móviles de manera local.

213. Normalmente en este escenario la conexión entre el dispositivo móvil y la solución MDM se realiza a través del puerto USB del servidor de gestión, estableciendo así la política de seguridad y configuración adecuada en el dispositivo móvil.

214. Se recomienda llevar a cabo este proceso antes de que los dispositivos móviles sean entregados por primera vez al usuario, como parte fundamental del proceso de configuración inicial y distribución de nuevos dispositivos móviles de la organización.

215. En entornos de mayor tamaño, por motivos de escalabilidad, puede ser el propio usuario el que puede llevar a cabo el proceso de registro del dispositivo móvil en la solución MDM (*self enrollment*) a través de un portal web o mediante la instalación de una app o agente de la propia solución MDM. Ambos métodos harán uso de la API de gestión proporcionada por el fabricante de la plataforma móvil.

216. Adicionalmente, la solución MDM debe proporcionar mecanismos que permitan al administrador TIC realizar el registro por lotes o grupos grandes de dispositivos móviles de forma sencilla.

217. El proceso de registro o *enrollment* debe ser seguro y sencillo, con el objetivo de promover y facilitar la suscripción de los dispositivos móviles a la solución MDM, configurarlos adecuadamente y asegurar el cumplimiento de la política de seguridad de la organización, apoyándose en manuales y documentación orientada al usuario final (tanto en entornos corporativos como BYOD, ver apartado "4.4. BYOD (BRING YOUR OWN DEVICE) Y BYOA (BRING YOUR OWN APP)").

218. Las soluciones MDM permiten la identificación y autentificación del usuario durante el proceso de auto-registro mediante su integración con los directorios corporativos que disponen de las credenciales corporativas del usuario.

219. Una vez el usuario ha sido identificado, el registro permite aplicar los ajustes de configuración, restricciones y controles de acceso específicos para ese usuario en base a las pautas definidas en la política de seguridad de la organización.

220. Este proceso de registro se lleva a cabo normalmente de forma remota empleando las capacidades de comunicación inalámbricas de los dispositivos móviles, vía Wi-Fi o telefonía móvil (2/3/4G), comunicaciones conocidas como OTA (*Over-the-Air*).

221. El proceso de registro o enrollment conlleva una serie de pasos, dentro de los que se incluyen:

- La autentificación del usuario: para validar que tanto el usuario como el dispositivo móvil están autorizados en la solución MDM.
- Opcionalmente, la distribución y el registro de certificados digitales para la identificación del dispositivo móvil o el usuario por la arquitectura de la organización y la solución MDM, por ejemplo, mediante SCEP (ver apartado "5.2.1. SCEP").
- La configuración del dispositivo: una vez que el servidor MDM y el dispositivo móvil pueden autentificarse mutuamente y establecer un canal de comunicación seguro (típicamente mediante SSL/TLS), se puede enviar la configuración del servidor MDM al terminal.
- A partir de ese momento es posible comenzar la gestión del terminal empezando por su configuración inicial en base a la política de seguridad definida por la organización.

222. Uno de los aspectos de seguridad más relevantes a la hora de permitir el registro del dispositivo móvil por parte del usuario es como realizar el proceso de autentificación del usuario, para asegurar que realmente cada persona registra únicamente el dispositivo móvil que le ha sido asignado o de su propiedad (Ej. BYOD), y con la configuración adecuada.

223. La autentificación de los usuarios se puede realizar a través de directorios centralizados corporativos ya existentes, como el directorio activo en entornos Microsoft, o empleando

otras soluciones de directorio, como por ejemplo servidores LDAP o a través de soluciones propietarias, en otros entornos.

224. En los entornos empresariales las soluciones basadas en el protocolo LDAP están muy extendidas para la gestión de grupos, usuarios y para el establecimiento de mecanismos de autentificación y autorización (controles de acceso).

225. La solución MDM debe disponer de capacidades de integración con servidores LDAP tanto para la autentificación de usuarios como para permitir la aplicación de diferentes políticas de seguridad por usuario, grupo, unidad organizativa (OU), o cualquier otro atributo de LDAP (ver apartado "5.4. GESTIÓN DE LA(S) POLÍTICA(S) DE SEGURIDAD CORPORATIVA(S)").

226. En el caso de emplear un portal web para el registro inicial se recomienda hacer uso de cifrado mediante HTTPS (SSL/TLS) para todas las comunicaciones, así como emplear mecanismos robustos de autentificación para asegurar que solo usuarios previamente registrados en la organización y con autorización pueden llevar a cabo el registro de los dispositivos móviles en la solución MDM.

227. Si se detectan dispositivos móviles no autorizados intentando acceder a recursos corporativos, este acceso debería ser bloqueado, y el administrador TIC debería ser notificado.

228. Pese a que la solución de monitorización puede permitir iniciar automáticamente el proceso de registro por parte del usuario en la solución MDM, pasando previamente por las autorizaciones correspondientes, no se recomienda hacer uso de estas capacidades.

229. En su lugar, debe establecerse una política de seguridad, y los procedimientos asociados, que no permitan el acceso a los recursos y datos corporativos hasta que el dispositivo móvil no esté siendo gestionado adecuadamente por la organización.

5.2.1 SCEP: SIMPLE CERTIFICATE ENROLLMENT PROTOCOL

230. El protocolo SCEP (*Simple Certificate Enrollment Protocol*), un estándar en versión borrador del IETF [Ref.- 62], ha sido diseñado para simplificar el proceso de solicitud, emisión, distribución, gestión y revocación de certificados digitales en entornos de gran tamaño (o a gran escala).

231. El proceso de registro o suscripción (*enrollment*) de los dispositivos móviles en la solución MDM puede requerir disponer de certificados digitales, y el protocolo SCEP permite su generación y distribución de manera sencilla y automática, reduciendo la sobrecarga en la realización de estas tareas manuales para el administrador TIC.

232. Por tanto, SCEP permite a los dispositivos móviles la solicitud y obtención de certificados digitales durante el proceso de registro en la solución MDM y, adicionalmente, para el acceso a otros recursos y servicios corporativos que hacen uso de certificados digitales durante el proceso de autentificación, como ActiveSync, redes Wi-Fi o redes VPN, e-mail, SharePoint, aplicaciones web, etc [6].

[6] http://blogs.gartner.com/mark-diodati/2012/07/02/mobile-device-certificate-enrollment-are-you-vulnerable/

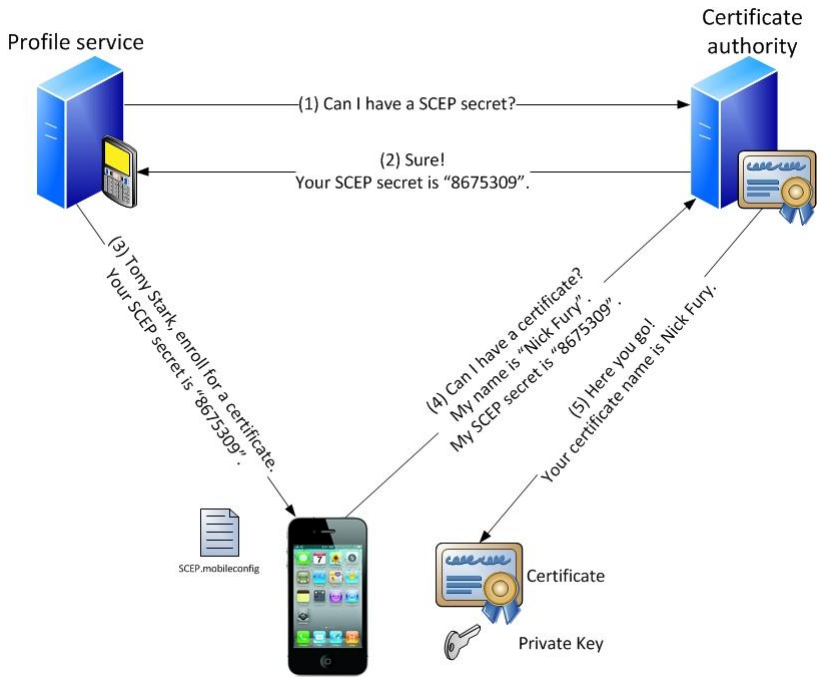

FIGURA 6.- Esquema de funcionamiento del protocolo SCEP.

233. Plataformas móviles como Android, BlackBerry o iOS disponen de soporte para SCEP, con el objetivo de facilitar la distribución de certificados vía OTA que permitan identificar los dispositivos móviles autorizados a través de los mecanismos de autentificación de los servicios corporativos (basados en certificados digitales).

234. A la hora de implantar SCEP a través de la solución MDM deben tenerse en cuenta potenciales vulnerabilidades de seguridad descubiertas en el año 2012 y asociadas al proceso de registro de los dispositivos móviles y la posibilidad de suplantar a otros usuarios (potencialmente usuarios con más privilegios) o dispositivos móviles [Ref.- 64].

5.3 INVENTARIO Y MONITORIZACIÓN

235. Una de las características más relevantes de las soluciones MDM es la monitorización automática y la generación de alertas al incumplirse la política de seguridad establecida.

236. Por un lado debe evaluarse qué tipo de alertas pueden ser generadas por la solución MDM, ya sea mediante SNMP, e-mail, SMS, etc.

237. Por otro lado debe evaluarse frente a qué tipo de eventos pueden generarse alertas, como por ejemplo cuando no es posible contactar con un dispositivo móvil, cuando el dispositivo está siendo usado en el extranjero (*roaming*), cuando se detecta un intento de instalación de una app no permitida, etc.

238. Por otro lado, otra de las principales y más básicas características de una solución MDM debería ser la posibilidad de disponer de un inventario lo más real y actualizado posible de los dispositivos móviles que gestiona, y por tanto, que existen en la organización.

239. La información que debería obtenerse para el inventario debería incluir, entre otros, el tipo de dispositivo móvil, fabricante y modelo exacto, el sistema operativo de la plataforma móvil y su versión concreta, el operador de telecomunicaciones empleado actualmente, el estado de diferentes módulos hardware y elementos asociados a su configuración, las apps instaladas en el mismo, etc.

240. Adicionalmente, la solución de inventario debe gestionar un registro con los diferentes identificadores asociados a un dispositivo móvil (si son aplicables), como por ejemplo:

- Número de serie o identificador único del dispositivo móvil según el fabricante.
- IMEI (*International Mobile Equipment Identity*).
- Número de teléfono asociado.
- IMSI (*International Mobile Subscriber Identity*), correspondiente a la tarjeta SIM.

241. La solución MDM debe proporcionar información de inventario sobre la configuración general del dispositivo móvil, así como sobre su configuración de seguridad, automatizando la detección de violaciones en la política de seguridad y tomando acciones para remediar estos incumplimientos lo antes posible, ya sea mediante notificaciones o alertas personalizables, o mediante la realización de acciones automáticas.

242. Las capacidades de inventario debería proporcionar la posibilidad de consultar en todo momento (en tiempo real y bajo demanda), o con una periodicidad establecida, cuál es el estado de un dispositivo móvil gestionado y de las apps de las que dispone actualmente.

243. Para ello deben disponer de capacidades de búsqueda en función de múltiples criterios asociados a la solución de gestión, como por ejemplo el usuario, tipo de dispositivo móvil, versión del sistema operativo, ajustes de configuración específicos, apps, etc.

244. Asimismo, las capacidades de inventario deberían almacenar un histórico de los datos recolectados a lo largo del tiempo (por ejemplo, diario, semanal mensual y anual), fundamental para poder hacer un seguimiento de la evolución en la adopción de dispositivos móviles dentro de la organización, de la evolución de la aplicación de una nueva política de seguridad o cambios sobre ésta, e identificar tendencias o extraer estadísticas que ayuden a la toma de decisiones relacionadas con el entorno móvil de la organización.

245. Complementariamente al inventario de dispositivos móviles, debería disponerse de un inventario exhaustivo de apps instaladas en todos y cada uno de los dispositivos móviles gestionados, incluyendo en el mismo la versión de la app disponible en cada dispositivo.

246. Adicionalmente, la solución MDM debe proporcionar capacidades de exportación de datos en diferentes formatos (XML, CSV, HTML, PDF, texto, etc), con el objetivo de poder generar informes y extraer la información que la solución gestiona y poder importar estos en otras soluciones de gestión y software empresarial.

247. Las capacidades para la generación de todo tipo de informes por parte de la solución MDM, asociados a sus capacidades de inventario y monitorización, deben ser evaluadas en detalle para su utilización en la gestión de los dispositivos móviles, tanto en tareas reactivas como proactivas.

248. Es especialmente interesante la disponibilidad en la solución MDM de plantillas previamente definidas por el fabricante que puedan ser utilizadas directamente por la organización o personalizadas con el menor esfuerzo posible, no siendo necesario diseñar cada nueva plantilla para un nuevo informe desde cero.

249. Las capacidades de monitorización, especialmente en entornos BYOD, deben ser capaces de filtrar los datos e información personal o propia del usuario, que puede permitir su identificación y localización, y estar afectados por las leyes de privacidad del país de aplicación.

250. Por ejemplo, la solución MDM debe permitir filtrar o no acceder a los correos electrónicos, contactos y calendarios personales, datos de apps personales, contenido de los mensajes de texto, lista de llamadas y acceso al buzón de voz, la ubicación del dispositivo móvil, etc.

251. En cualquier caso y promoviendo la transparencia de la solución MDM, es conveniente informar al usuario de la existencia de capacidades de monitorización, qué tipo de información va a ser accedida y recolectada, y obtener su autorización previa por escrito.

252. En el caso de integrar la solución MDM con soluciones de gestión de contenidos, o disponer directamente de estas capacidades en la solución MDM (ver apartado "5.5.13.5. GESTIÓN DE LOS CONTENIDOS Y DATOS MANEJADOS POR LAS APPS"), la funcionalidad de inventario y monitorización debe ser capaz de proporcionar información sobre quién tiene acceso a qué contenidos, quién ha descargado ciertos contenidos o documentos corporativos, incluyendo las versiones específicas de un documento que han sido obtenidas.

253. Las capacidades de monitorización del entorno móvil corporativo deben verse complementadas con capacidades de monitorización y registro de la propia solución MDM, pudiendo obtenerse registros detallados (o *logs*) de las diferentes acciones y actividades llevadas a cabo a través de los mecanismos de gestión, como por ejemplo cuándo y sobre qué dispositivos móviles se remite la acción para aplicar una política de seguridad concreta, o se realiza la instalación de una app determinada, o se restringe la utilización de un módulo hardware del dispositivo móvil, etc.

5.4 GESTIÓN DE LA(S) POLÍTICA(S) DE SEGURIDAD CORPORATIVA(S)

254. Las soluciones MDM empresariales deben disponer de capacidades para la configuración y aplicación de las políticas de seguridad corporativas en los dispositivos móviles gestionados.

255. Las políticas de seguridad incluyen diferentes ajustes de configuración que afectan a los múltiples elementos y componentes del dispositivo móvil, como los interfaces de comunicaciones, los módulos hardware, la utilización de apps, etc. Los detalles de configuración de los diferentes componentes son analizados en los siguientes apartados.

256. Es fundamental que la solución MDM proporcione capacidades para configurar los dispositivos móviles y aplicar la política de seguridad de forma remota independientemente de dónde se encuentre ubicado el dispositivo a gestionar, comunicación inalámbrica conocida como OTA (*Over-the-Air*) y que se puede llevar a cabo a través de redes Wi-Fi o de telefonía móvil 2/3/4G.

257. Habitualmente, la solución MDM permite la definición de perfiles de configuración que son aplicados en el dispositivo móvil en base a la política de seguridad corporativa según el tipo de dispositivo móvil, el tipo de usuario, y el nivel de acceso asociado (pudiendo emplearse los servidores LDAP corporativos).

258. La solución MDM debe permitir la definición de políticas de seguridad en los dispositivos móviles que serán aplicadas de forma permanente.

259. Adicionalmente y de manera opcional, la solución MDM puede permitir definir perfiles y políticas de seguridad temporales, con un tiempo de expiración definido (pudiendo establecer el día de comienzo y finalización de aplicación de la política de seguridad), y que se eliminarán automáticamente del dispositivo móvil llegado ese momento.

260. Estas políticas temporales pueden emplearse para disminuir o aumentar los controles, restricciones y el nivel de seguridad de un dispositivo móvil frente a diferentes escenarios,

como la realización de un viaje al extranjero, o su utilización para una tarea específica o un proyecto concreto durante un periodo de tiempo definido.

261. Las soluciones MDM pueden permitir establecer controles de acceso y la aplicación de ajustes de configuración en base a perfiles dependientes del tiempo (que aplican mayores o menores restricciones según el momento del día) o de la ubicación (la configuración del dispositivo móvil es modificada o restringida en ciertos lugares).

262. Así mismo, es necesario disponer de capacidades para la gestión de versiones de la política de seguridad establecida en los dispositivos móviles, con el objetivo de poder acomodar actualizaciones en la política según el tipo de dispositivo móvil y según evolucione la política de seguridad en la organización.

263. Complementariamente, debe definirse si hay posibilidad de devolver el dispositivo móvil a su estado previo antes de la aplicación de la política de seguridad (*rollback*), o si por el contrario, la eliminación de la política de seguridad implica un borrado completo del dispositivo, *wipe* o restauración de la configuración de fábrica.

264. Dentro de la política de seguridad corporativa pueden establecerse recomendaciones relativas a la utilización de cortafuegos (o *firewalls*) personales y soluciones antivirus y antimalware en los dispositivos móviles.

265. Se recomienda evaluar las capacidades de la solución MDM para gestionar específicamente el cortafuegos y antivirus del dispositivo móvil, aunque debe tenerse en cuenta que muchas de las plataformas móviles no disponen de capacidades para la instalación de este tipo de soluciones de seguridad, o si disponen de ellas, no son equivalentes a las existentes en dispositivos más tradicionales (por ejemplo, ordenadores portátiles o de escritorio).

5.5 CARACTERÍSTICAS DE LA(S) POLÍTICA(S) DE SEGURIDAD CORPORATIVAS

266. Los siguientes apartados proporcionan información sobre los diferentes elementos, características, capacidades y funcionalidades que deben ser contemplados por la(s) política(s) de seguridad de los dispositivos móviles de la organización y, por tanto, por los mecanismos de gestión asociados a las soluciones MDM. Cada una de estas capacidades ha sido englobada dentro de una categoría en función de la funcionalidad que proporciona.

5.5.1 RESTRICCIONES EN EL HARDWARE Y SOFTWARE DEL DISPOSITIVO MÓVIL

267. La solución MDM debe disponer de capacidades para poder restringir, con la mayor granularidad posible, los diferentes módulos y componentes hardware existentes en los dispositivos móviles, siempre que las capacidades de gestión de la plataforma móvil lo permitan.

268. Por ejemplo, debería ser posible deshabilitar aquellos elementos hardware que permiten la adquisición de información y datos, como la cámara, el módulo de localización GPS, la tarjeta de almacenamiento externa o el micrófono.

269. Igualmente, debería ser posible deshabilitar todos los interfaces de comunicaciones existentes en el dispositivo móvil, tanto cableados como inalámbricos, como el puerto USB, o los interfaces NFC, Bluetooth, Wi-Fi, telefonía móvil 2/3/4G, etc.

270. Complementariamente, al restringirse el acceso a ciertos elementos hardware del dispositivo móvil debe restringirse también el acceso a las apps o elementos software que hacen uso de ese hardware.

271. Por ejemplo, al deshabilitar la cámara del dispositivo móvil, el icono de la app asociada y disponible por defecto en todas las plataformas móviles para hacer uso de la cámara y poder hacer fotografías o grabar vídeos debería desaparecer.

272. Independientemente de su vinculación con el hardware del dispositivo móvil, las soluciones MDM pueden proporcionar capacidades para restringir el uso del software, servicios y aplicaciones disponibles por defecto en la plataforma móvil, como el navegador web, el cliente de correo electrónico, la gestión de contactos y agenda, etc.

273. Estas capacidades de gestión del software directamente asociado al hardware o disponible por defecto son independientes de las capacidades de gestión de apps de terceros de la solución MDM (ver apartado "5.5.13. GESTIÓN DE APPS").

274. Un elemento fundamental a la hora de proteger los dispositivos móviles es mantener actualizados los diferentes elementos software que componen el mismo, con el objetivo de solucionar o mitigar vulnerabilidades de seguridad públicamente conocidas que afectan a una plataforma móvil concreta, una solución MDM o una app específica.

275. Por este motivo, la solución MDM debe proporcionar capacidades avanzadas de gestión de actualizaciones del sistema operativo de la plataforma móvil, de la app contenedora o agente MDM, así como de todas las apps instaladas en el dispositivo móvil (vía mecanismos de comunicación remotos OTA).

5.5.2 GESTIÓN DEL CÓDIGO DE ACCESO

276. La solución MDM debe permitir definir la política de autentificación asociada al código (o mecanismo) de acceso necesario para desbloquear y utilizar el dispositivo móvil.

277. En primer lugar, debe ser posible verificar y establecer que es necesario disponer de un código (o mecanismo) de acceso en el dispositivo móvil, y cuál será el mecanismo de acceso concreto a emplear, ya que el nivel de seguridad no es equivalente para todos ellos.

278. Dependiendo de la plataforma móvil se dispone de diferentes implementaciones para el código (o mecanismo) de acceso, desde el PIN de cuatro dígitos más tradicional, hasta el uso de contraseñas alfanuméricas más robustas, o patrones de desbloqueo o el desbloqueo mediante la imagen de la cara del usuario, en el caso de Android.

279. La política de seguridad debe establecer que es imprescindible disponer de un código de acceso en el dispositivo móvil para poder acceder a los recursos corporativos y considerar al dispositivo móvil como gestionado, y qué éste debe estar basado en un código de acceso robusto (contraseña numérica o alfanumérica), no permitiéndose el uso de mecanismos más débiles como patrones o el reconocimiento facial.

280. El activar el código de acceso en el dispositivo móvil habilita adicionalmente diferentes mecanismos de protección de las distintas plataformas móviles, como por ejemplo las capacidades de cifrado del terminal.

281. Adicionalmente, la política de autentificación debe definir los requisitos que debe cumplir el código de acceso, incluyendo (en el caso de una contraseña):

- Longitud mínima.
- Complejidad (dentro de los cuatro conjuntos de caracteres habituales: letras minúsculas, letras mayúsculas, dígitos y símbolos).
- Periodo de expiración máximo tras el cual será necesario renovar el código de acceso.

- Periodo de renovación mínimo antes del cual no será posible modificar de nuevo el código de acceso tras su renovación.
- Mantenimiento de un histórico de códigos de acceso utilizados anteriormente para evitar su reutilización.

282. En caso de permitirse otros mecanismos de acceso diferentes, también debe ser posible definir los requisitos necesarios, como por ejemplo el número de puntos (entre 3 y 9) del patrón de desbloqueo de Android.

283. Estas capacidades de gestión detalladas de las propiedades asociadas al código de acceso empleado por el dispositivo móvil también deberían estar disponibles para el código empleado en el proceso de autentificación de apps contenedoras (ver apartado "4.6.6. SOLUCIONES DE GESTIÓN BASADAS EN UN CONTENEDOR").

284. En relación con el código de acceso y la pantalla de desbloqueo es necesario establecer el periodo de tiempo (o temporizador) de inactividad tras el cual el dispositivo móvil se bloqueará automáticamente.

285. Adicionalmente, se puede definir un periodo de tiempo (o de gracia) durante el cual no será necesario introducir de nuevo el código de acceso una vez el dispositivo se ha bloqueado, manualmente o automáticamente por falta de actividad.

286. Es posible establecer que el código de acceso sea solicitado inmediatamente después de haberse bloqueado el dispositivo móvil, es decir, que el periodo de gracia sea nulo.

287. Un mecanismo habitual en las plataformas móviles actuales, asociado al código de acceso y a la protección de los datos almacenados en el dispositivo móvil, es el que permite realizar un borrado completo del dispositivo móvil tras llevarse a cabo un número determinado de intentos de acceso fallidos.

288. La solución MDM debe disponer de capacidades para habilitar este mecanismo, así como para definir el número de intentos fallidos en función de la confidencialidad y criticidad de la información almacenada en el dispositivo móvil.

289. Algunas soluciones MDM pueden disponer de mecanismos más avanzados que, tras detectar un número determinado de intentos de acceso fallidos, bloqueen el acceso a los servicios y datos corporativos por parte del usuario (cuentas y credenciales) asociado al dispositivo móvil. Estos mecanismos deben ser habilitados en función de la política de seguridad definida.

5.5.3 PROTECCIÓN REMOTA

290. La solución MDM debe proporcionar ciertas características de seguridad que permitan la protección del dispositivo móvil y su gestión de manera remota.

291. Estas características deberían estar disponibles para el administrador TIC, pero igualmente y con el objetivo de minimizar los recursos TIC, algunas de ellas deben estar también disponibles directamente para el usuario final, si la política de seguridad de la organización así lo determina, como por ejemplo el cambio del código de acceso, la localización del dispositivo móvil y el borrado remoto de sus datos (*wipe*).

292. El usuario debería disponer de acceso a un portal web de autogestión, propio de la solución MDM, que le permita llevar a cabo estas acciones remotas, así como comprobar en todo momento si el dispositivo móvil cumple con la política de seguridad de la organización, y en caso de no hacerlo, el motivo asociado.

293. La solución MDM puede permitir eliminar el código de acceso de forma remota, en caso de que el usuario haya olvidado el actual y se deseé restaurar el acceso al dispositivo móvil.

294. Este tipo de funcionalidad, que puede ser muy útil en momentos puntuales, es muy crítica desde el punto de vista de seguridad, ya que permite disponer de control absoluto del dispositivo móvil desde la solución MDM.

295. Es por tanto necesario evaluar detalladamente si se desea activar estas capacidades en la solución MDM y quién tendrá acceso a las mismas, cualquier usuario (sobre sus dispositivos móviles) o únicamente el administrador TIC.

296. Igualmente, debería permitir bloquear en cualquier momento el dispositivo móvil de forma remota (en caso de que actualmente no estuviera bloqueado por haber sido usado recientemente por el usuario, no habiendo expirado el temporizador de bloqueo, y se encontrara en una ubicación insegura), empleando el código de acceso existente en la actualidad, o empleando un nuevo código de acceso (en caso de que no tuviera uno configurado, situación completamente desaconsejada desde el punto de vista de seguridad, o incluso modificando el valor actual, si la plataforma móvil lo permite).

297. Con el objetivo de recuperar el dispositivo móvil en el caso de pérdida, la solución MDM debería permitir forzar de forma remota al dispositivo móvil a emitir un sonido que permita su localización por parte del usuario o de un tercero.

298. Este escenario es similar al de llamar al número de teléfono asociado al dispositivo móvil, pero también aplica a dispositivos móviles sin capacidades de telefonía (como tabletas) o a situaciones donde el dispositivo móvil no dispone de cobertura móvil pero sí de conectividad de datos a través, por ejemplo, de una red Wi-Fi.

299. Complementariamente, debería permitir enviar un mensaje o notificación de texto (propio de las capacidades de gestión y diferente a un SMS) al dispositivo móvil que permita proporcionar información sobre su propietario y estado, con el objetivo de que si alguien lo encuentra y lee el mensaje, pueda ponerse en contacto con el propietario y devolverlo.

300. La solución MDM debe permitir eliminar toda la información almacenada en el dispositivo móvil, mediante el borrado completo del mismo y su restauración a los ajustes de fábrica, operación conocida en inglés como *wipe* (ver apartado “5.5.4. GESTIÓN Y BORRADO DE DATOS REMOTO”).

301. Una característica más avanzada para la protección remota del dispositivo móvil es el poder eliminar información parcial o selectiva del mismo, mediante el borrado de la relación de confianza entre la solución MDM y el dispositivo móvil, lo que conlleva la eliminación de los datos (por ejemplo, datos corporativos), cuentas y ajustes de configuración gestionados por el servidor MDM, sin afectar a otros datos del usuario (por ejemplo, datos personales), funcionalidad muy conveniente para entornos BYOD.

302. Algunas plataformas móviles y sus soluciones de gestión disponen de capacidades avanzadas asociadas a la introducción del código de acceso bajo amenaza, como las notificaciones de coacción (*Duress Notification Address*) de BlackBerry [Ref.- 6].

303. Dentro de las políticas asociadas al código de acceso, BlackBerry permite establecer una dirección de correo electrónico (por ejemplo, la del administrador de la solución MDM) para notificar que el usuario está introduciendo el código de acceso del dispositivo bajo coacción o amenaza física.

304. El introducir el código de acceso actual, pero posicionando el primer carácter del mismo al final (por ejemplo, para el código de acceso “secreto” el usuario introduciría “ecretos”),

permite al usuario indicar qué está bajo coacción y que se genere la notificación o alerta correspondiente.

305. Una vez el administrador de la solución MDM ha sido notificado de la situación de amenaza puede tomar medidas de protección en el dispositivo móvil gestionado, como por ejemplo eliminar todos sus datos remotamente (*wipe*).

306. Si el MDM gestiona usuarios y aplicaciones que hagan uso de datos en "nubes privadas" debe implementar la posibilidad de bloquear al usuario el acceso a los datos en estas nubes desde el dispositivo robado o perdido, o bloquear el acceso a dicho usuario.

5.5.4 GESTIÓN Y BORRADO DE DATOS REMOTO

307. Una de las características que tiene relación directa con la protección remota del dispositivo móvil (ver apartado "5.5.3. PROTECCIÓN REMOTA") es la que permite el borrado remoto completo del dispositivo (acción conocida como *wipe*).

308. La operación de borrado restaura en el dispositivo móvil los ajustes de fábrica y elimina todos los datos existentes, dejando el dispositivo móvil como si se tratase de un dispositivo nuevo recién adquirido.

309. Esta característica es muy habitual en la mayoría de soluciones MDM, incluyendo las capacidades básicas de gestión de EAS.

310. Si ninguna de las características previas de protección remota del dispositivo móvil tiene éxito y permite recuperar físicamente el dispositivo móvil, las organizaciones pueden establecer qué, con el objetivo de proteger los datos corporativos almacenados en el dispositivo, así como el acceso automático a los servicios corporativos desde éste a través de las credenciales almacenadas en él, debe llevarse a cabo un borrado completo del mismo.

311. La secuencia natural por tanto de actuación frente a un dispositivo móvil perdido o robado podría ser la siguiente si se desea balancear el equilibrio entre la posibilidad de recuperar el dispositivo móvil y proteger los datos que contiene:

- Intentar localizar la ubicación física del dispositivo móvil a través de la solución MDM (ver apartado "5.5.5. SERVICIOS DE LOCALIZACIÓN").
- Bloquear el dispositivo móvil remotamente para no permitir el acceso no autorizado al mismo.
- Llamar al número de teléfono del dispositivo, o forzar de forma remota al dispositivo móvil a emitir un sonido (a través de las capacidades de gestión) que permita su localización.
- Enviar de forma remota al dispositivo móvil un mensaje (a través de las capacidades de gestión) que permita proporcionar información del propietario para su localización o devolución.
- Llevar a cabo el borrado de datos remoto (*wipe*), selectivo o completo, del dispositivo móvil.

312. En entornos que gestionan información confidencial y sensible, la política de seguridad puede establecer un orden de actuación diferente, dando más prioridad o valor a la información que al propio hardware o recuperación del dispositivo móvil.

313. En este escenario más crítico, la secuencia de pasos a seguir podría comenzar por intentar localizar la ubicación física del dispositivo móvil, y en el caso de no tener éxito, proceder

directamente a la eliminación o borrado de datos remoto (*wipe*), selectivo o completo, del dispositivo móvil

314. En ese caso, la operación de borrado puede definirse como una de las primeras acciones a llevar a cabo para evitar el acceso a la información y datos corporativos, frente por ejemplo a los intentos de localización y recuperación del propio dispositivo móvil.

315. La operación de borrado puede ser realizada bajo demanda y de forma manual por parte del administrador TIC de la solución MDM, o cuando se cumplen ciertas condiciones, como por ejemplo tras introducir un código de acceso no válido un número determinado de veces.

316. La política de seguridad de la organización puede establecer que si los dispositivos móviles no disponen de las últimas dos versiones del sistema operativo (es decir, están significativamente desactualizados), o si no han cumplido con la política de seguridad durante más de una semana, o si se detecta que el dispositivo móvil ha sido infectado con malware, se lleve a cabo el borrado remoto de forma automática.

317. Algunas soluciones MDM proporcionan estas capacidades de borrado remoto automático si se produce una violación crítica de la política de seguridad corporativa. En entornos críticos que gestionan datos e información sensible y confidencial, deben habilitarse estas capacidades de borrado automático.

318. También es posible aplicar este procedimiento de borrado remoto antes de retirar un dispositivo móvil antiguo que vaya a ser sustituido, o que no vaya a seguir estando gestionado por la organización. Este procedimiento debe aplicarse siempre que un dispositivo móvil deje de estar gestionado por la organización.

319. Debe tenerse en cuenta que para que la operación de borrado sea efectiva, se debe cumplir una condición indispensable, qué el dispositivo móvil disponga de conectividad de datos (ya sea a través de las redes móviles 2/3/4G o de Wi-Fi) para que la solución MDM pueda enviar (mensaje *push*) la orden de borrado remoto.

320. Si un atacante obtiene acceso no autorizado a un dispositivo móvil, una de las primeras acciones que puede llevar a cabo es la extracción de la tarjeta SIM para evitar cualquier comunicación vía redes móviles 2/3/4G, especialmente en aquellos dispositivos móviles dónde es posible extraer el SIM sin extraer la batería (por ejemplo, dispositivos iOS de Apple), y por tanto sin tener que apagar necesariamente, el terminal.

321. En el caso de verse forzado a apagar el terminal, necesitaría conocer el código de acceso para poder acceder al mismo tras encenderlo de nuevo.

322. Sin embargo, un potencial atacante puede decidir apagar el dispositivo móvil antes de que se reciba la orden de borrado y podría aplicar técnicas de análisis de la memoria del dispositivo móvil para intentar extraer la información almacenada, siendo el cifrado de la misma un elemento de protección básico.

323. Respeto a las redes Wi-Fi, el atacante sólo debe situar el dispositivo móvil en una ubicación dónde no exista ninguna red Wi-Fi conocida, con el objetivo de evitar que el terminal se conecte a éstas y pueda recibir la orden de borrado.

324. En ambos casos, redes móviles 2/3/4G y redes Wi-Fi, un atacante avanzado podría situar el terminal en un entorno aislado de comunicaciones inalámbricas, como por ejemplo una jaula de Faraday, para poder interactuar con el terminal sin haberlo manipulado previamente.

325. En el caso de algunos dispositivos móviles el proceso para evitar cualquier comunicación inalámbrica es más sencillo, ya que basta con poner el dispositivo móvil en “modo avión”.

Desafortunadamente, algunos dispositivos móviles permiten habilitar este modo desde la propia pantalla de desbloqueo sin conocer el código de acceso, como por ejemplo el Nexus 7 y el Nexus 4 con Android 4.2.2 [Ref.- 53] a través del botón de activación.

326. La única solución frente a este tipo de acciones por parte de un atacante pasa por disponer de capacidades de borrado remoto en la plataforma móvil y solución MDM que permitan que el terminal inicie un borrado automáticamente (sin ninguna comunicación previa con la solución MDM) al cumplirse una condición, como por ejemplo, no haber establecido comunicación alguna con la solución MDM durante los últimos 30 días (o cualquier otro periodo de tiempo definido por la política de seguridad de la organización). Por ejemplo, estas capacidades están disponibles en los dispositivos móviles BlackBerry.

327. En cualquier caso, es fundamental que la solución MDM disponga de capacidades para verificar y confirmar si la operación de borrado remoto ha sido recibida y ejecutada con éxito en el dispositivo móvil gestionado.

328. Debe tenerse en cuenta que esta funcionalidad puede proporcionar una falsa sensación de seguridad a las organizaciones, tanto por los motivos expuestos previamente, como por el hecho de desconocer si el potencial atacante ha podido copiar los datos almacenados en el dispositivo móvil antes de realizarse el borrado remoto del mismo.

329. Para poder llevar a cabo la operación de borrado es necesario que la política de seguridad de la organización refleje claramente la autorización por parte del usuario, o incluso de forma explícita, mediante una autorización firmada específicamente con este propósito. En algunas organizaciones no se considera aceptable el poder realizar esta operación de borrado a la totalidad del dispositivo móvil (al incluir datos personales del usuario).

330. Algunas soluciones MDM disponen de capacidades de borrado remotas parciales, es decir, que permiten de forma más selectiva y granular especificar qué información será eliminada del dispositivo móvil.

331. Esta granularidad permite eliminar únicamente los datos y acceso a servicios corporativos, no afectando a los datos y acceso a servicios personales del usuario.

332. Este escenario es muy habitual en soluciones MDM de tipo contenedor (ver apartado “4.6.6. SOLUCIONES DE GESTIÓN BASADAS EN UN CONTENEDOR”), dónde únicamente se eliminan los ajustes de configuración, la app y los datos gestionados por la app contenedora o agente de la solución MDM.

333. Otras plataformas móviles como iOS no disponen de mecanismos de gestión con esta granularidad (al menos en la versión actual), por lo que algunas soluciones MDM implementan soluciones “virtuales” de borrado de datos en el acceso a los servicios corporativos.

334. Para ello, establecen políticas de acceso granulares a los datos corporativos, una especie de cortafuegos de aplicación o de datos, permitiendo o no la obtención remota de la información corporativa a cada dispositivo móvil.

335. Esta solución sin embargo no es aplicable a los datos que ya han sido almacenados en el dispositivo móvil, sino únicamente a los datos accesibles remotamente a través de servicios corporativos, como por ejemplo el correo electrónico o repositorios de documentos.

NOTA: A modo de referencia se proporciona un ejemplo de solución MDM con estas capacidades, como por ejemplo MobileIron Sentry y su integración con servidores de correo Microsoft Exchange y ActiveSync.

336. Esta característica no sólo se emplea ante la amenaza de pérdida o robo de un dispositivo móvil, sino también cuando un empleado deja la organización pero mantiene el acceso al dispositivo móvil, por ejemplo, en entornos BYOD o cuando los dispositivos móviles corporativos no son devueltos a la organización.

5.5.5 SERVICIOS DE LOCALIZACIÓN

337. Una de las funcionalidades características de los dispositivos móviles actuales es la disponibilidad de múltiples capacidades o servicios de localización que permiten obtener su ubicación física, con mayor o menor exactitud dependiendo de las condiciones y los métodos empleados.

338. Habitualmente las plataformas móviles disponen de dos tipos de mecanismos de localización que permiten obtener su ubicación actual:

- Localización de mayor precisión, en el exterior y/o espacios abiertos, a través del módulo GPS del dispositivo móvil y de los satélites GPS.
- Localización de menor precisión, pero que funciona incluso en recintos cerrados y en el interior de edificios, a través de las torres de telefonía móvil y redes Wi-Fi cercanas.

339. Los servicios de localización tienen implicaciones directas sobre la privacidad del usuario, y son utilizados extensamente por redes sociales, buscadores de Internet, y otros servicios que hacen uso o se basan en la ubicación actual del usuario.

340. La obtención no autorizada de la ubicación concreta del usuario en un momento dado facilita la realización de ataques dirigidos sobre éste y sobre las actividades que lleva a cabo en dicha ubicación.

341. Debe tenerse en cuenta qué para que las capacidades de localización remota del dispositivo móvil sean efectivas, se deben cumplir dos condiciones indispensables:

- Que el dispositivo móvil disponga de las capacidades de localización activas, preferiblemente ambos tipos (mencionados previamente).
- Que el dispositivo móvil disponga de conectividad de datos (ya sea a través de las redes móviles 2/3/4G o de Wi-Fi) para que pueda comunicar su ubicación a la solución MDM.

342. Algunas soluciones MDM no sólo permiten localizar la ubicación de un dispositivo móvil en un momento dado, por ejemplo si ha sido perdido o robado, sino que también permiten realizar un seguimiento detallado de la ubicación del dispositivo de manera periódica o permanente (*tracking*), rastreando así la ubicación y el desplazamiento del dispositivo móvil a lo largo del día.

343. Debe prestarse especial atención a las implicaciones de privacidad y posible violación de las leyes de protección de datos si se desea hacer uso de este tipo de capacidades de seguimiento del usuario.

344. La solución MDM debe disponer de capacidades para deshabilitar los servicios de localización o, al menos, poder restringir su utilización por parte de ciertas apps o elementos hardware, como por ejemplo la cámara.

345. Debe tenerse en cuenta que algunas soluciones MDM hacen uso de los servicios de localización para aplicar distintas políticas de seguridad sobre el dispositivo móvil en función

de su ubicación. Si se desea aplicar distintas políticas de seguridad según la ubicación del dispositivo móvil, es necesario habilitar estas capacidades y asegurarse que los servicios de localización están siempre activos, al ser necesarios para su correcto funcionamiento.

5.5.6 GESTIÓN DE LOS DATOS ALMACENADOS EN EL DISPOSITIVO MÓVIL

346. Adicionalmente a las capacidades de borrado remoto de datos (ver apartado "5.5.4. GESTIÓN Y BORRADO DE DATOS REMOTO") y de la protección del acceso al dispositivo móvil (ver apartado "5.5.2. GESTIÓN DEL CÓDIGO DE ACCESO"), las principales plataformas móviles actuales disponen de capacidades de cifrado de los datos que almacenan.

347. Las plataformas móviles actuales disponen de capacidades nativas para el cifrado completo del dispositivo móvil, funcionalidad asociada normalmente a la existencia de un código de acceso.

348. Por otro lado, algunas plataformas móviles también disponen de capacidades de cifrado de las tarjetas de almacenamiento externas (por ejemplo, tarjetas SD o *SD cards*).

349. Complementariamente, la plataforma móvil puede disponer de librerías específicas para el cifrado de datos por parte de las apps, de forma que éstas puedan proteger la información que gestionan dentro del *sandbox* o entorno de trabajo que tienen asociado en la plataforma móvil.

350. Las soluciones MDM deben proporcionar capacidades que permitan especificar y aplicar requisitos de cifrado sobre el dispositivo móvil y las tarjetas de almacenamiento externas por parte de la política de seguridad de la organización, con el objetivo de evitar que la información almacenada esté accesible en el caso de que un potencial atacante disponga de acceso físico no autorizado al dispositivo móvil.

351. La funcionalidad que habilita el cifrado del dispositivo móvil y las tarjetas de almacenamiento externas debe ser habilitada siempre que sea posible en función de la plataforma móvil gestionada.

352. Adicionalmente, podrían establecerse requisitos de seguridad asociados al cifrado en las propias apps, aunque su aplicación queda habitualmente en manos del desarrollador de la app, no disponiéndose de granularidad suficiente a través de los mecanismos de gestión (a menos que se haga uso de apps contenedoras o de soluciones de app *wrapping* – ver apartado "5.5.13.5. GESTIÓN DE LOS CONTENIDOS Y DATOS MANEJADOS POR LAS APPS").

353. Otro de los elementos a tener en cuenta en toda solución MDM respecto a la protección de datos es su capacidad de integración con entornos colaborativos y plataformas, soluciones y servidores empresariales para la compartición de documentos, como por ejemplo Microsoft SharePoint, facilitando el acceso seguro a contenidos corporativos.

354. Así, algunas soluciones MDM proporcionan capacidades propias de entornos colaborativos, proporcionando o integrándose con repositorios centralizados para la compartición de documentos corporativos y su acceso remoto, incluyendo la distribución segura de documentos a través de e-mail (mediante enlaces al repositorio centralizado).

5.5.7 DETECCIÓN DE JAILBREAK O ROOT

355. Uno de los procesos que pueden afectar significativamente el nivel de seguridad de los dispositivos móviles es el que permite al usuario tomar control completo del terminal y evitar o deshabilitar así los mecanismos de seguridad y protección existentes por defecto en la

plataforma móvil, así como evitar la política de seguridad definida por la organización y aplicada a través de la solución MDM.

356. Este proceso se conoce como *jailbreak* en el caso de la plataforma móvil iOS o como *root* (o *rooting*) en el caso de la plataforma móvil Android, y permite disponer de los máximos privilegios administrativos sobre el dispositivo móvil.

357. En la actualidad, otras plataformas móviles como BlackBerry o Windows Phone no tienen asociado un proceso similar que permita obtener el mismo nivel de privilegios y un control a bajo nivel de estas plataformas móviles.

358. Las soluciones MDM disponen de capacidades de detección para identificar si un dispositivo móvil gestionado ha sufrido el proceso de *jailbreak* o *root*, con el objetivo de notificar acerca de esta situación al administrador TIC.

359. La política de seguridad de la organización debe establecer que no se puede llevar a cabo este proceso en los dispositivos móviles gestionados por la organización, y la solución MDM debe detectar si el proceso ha sido realizado.

360. Para realizar la detección, la solución MDM verifica mediante distintos métodos y funciones diferentes indicadores técnicos habituales en dispositivos móviles con el *jailbreak* o *root* realizado, como por ejemplo la existencia de un servidor SSH, la ejecución de ciertos procesos a nivel de sistema operativo, la existencia de ciertos ficheros, etc.

361. La efectividad del mecanismo de detección depende de si el dispositivo móvil implementa contramedidas para evitarla. Por ejemplo, el proyecto xCon (disponible en Cydia) [Ref.- 49] para plataformas móviles iOS, dado que puede ejecutar con los máximos privilegios, implementa múltiples contramedidas para evitar la detección del proceso de *jailbreak* realizada por diferentes apps y soluciones MDM.

362. Se recomienda prestar atención a la evolución del proyecto xCon periódicamente para confirmar si implementa métodos de evasión del proceso de detección del *jailbreak* o *root* por parte de la solución MDM empleada por la organización.

363. Una vez detectada y notificada la situación, la solución MDM debe permitir al administrador TIC llevar a cabo acciones automáticas sobre el dispositivo móvil que no cumple la política de seguridad, como por ejemplo, el borrado remoto del mismo (ver apartado "5.5.4. GESTIÓN Y BORRADO DE DATOS REMOTO"), o bloquear el acceso a los recursos corporativos, como deshabilitar el acceso al buzón de correo electrónico del usuario.

5.5.8 GESTIÓN DE CERTIFICADOS DIGITALES

364. La gestión de certificados digitales en los dispositivos móviles es un elemento crítico que afecta a su nivel de seguridad, tanto para establecer el nivel de confianza con servicios remotos de terceros, como para la propia autentificación del dispositivo móvil o el usuario.

365. A la hora de evaluar las capacidades de gestión de certificados digitales de la solución MDM debe tenerse en cuenta que existen, como mínimo, dos repositorios para el almacenamiento de certificados en los dispositivos móviles:

- Certificados digitales personales: permiten almacenar los certificados propios del dispositivo móvil y/o usuario y que pueden ser utilizados como mecanismos de autentificación robusto en lugar de, por ejemplo, usuario y contraseña. El almacenamiento de este tipo de certificados incluye tanto la clave pública como la clave privada asociadas al mismo.

- Certificados digitales de las autoridades certificadoras (CA's) de confianza: permiten establecer qué CA's serán consideradas de confianza por el dispositivo móvil, incluyendo tanto CA's raíz como intermedias. La lista de CA's de confianza existente por defecto es establecida por el fabricante de la plataforma móvil.

366. Adicionalmente puede disponerse de repositorios para almacenar la confianza en servidores o servicios concretos, o por el contrario, la ausencia de confianza en servidores o CA's cuyos certificados han sido revocados por cualquier causa.

367. Las soluciones MDM pueden disponer de capacidades de gestión de certificados digitales tanto para los certificados personales como de nuevas CA's propias de la organización (o de servidores concretos de la organización) para las siguientes funcionalidades de conexión:

- Redes Wi-Fi
- Redes VPN
- Navegación web (SharePoint, aplicaciones web, etc)
- Correo electrónico (e-mail) y S/MIME
- Cuentas de Microsoft Exchange ActiveSync (EAS)
- Comunicación con la solución MDM

368. Adicionalmente a las capacidades de gestión de certificados por dispositivo móvil, la solución MDM debería proporcionar esas capacidades para las apps cliente nativas de la plataforma móvil (como por ejemplo las mencionadas previamente, e-mail o navegación web) e incluso para apps empresariales específicas.

369. Algunas soluciones MDM proporcionan capacidades de autoridad certificadora (CA)[7], encargándose de la emisión, registro y gestión de certificados digitales, mientras que otras soluciones MDM proporcionan capacidades similares a través de la integración con otras CA's externas, como por ejemplo la asociada al directorio activo de Microsoft.

370. En relación directa con el proceso de registro de los dispositivos móviles (ver apartado "5.2. REGISTRO DE LOS DISPOSITIVOS MÓVILES EN LA SOLUCIÓN MDM"), la solución MDM puede permitir la gestión de certificados para llevar a cabo el proceso de registro mediante SCEP, ya sea a través de una integración completa con un servidor SCEP externo existente dentro de la organización, o mediante la utilización de una CA propia del servidor MDM que dispone de un servidor SCEP propio.

371. Debe tenerse en cuenta que las diferentes plataformas móviles ofrecen por defecto capacidades muy variadas para la gestión de certificados digitales.

372. En la plataforma iOS, Apple no ofrece a través del interfaz de usuario capacidades para la gestión de los certificados de las CA's de confianza, ofreciendo únicamente documentación sobre la lista de CA's existentes por defecto según la versión de iOS:

- iOS 3.x: http://support.apple.com/kb/HT3580
- iOS 4.x: https://support.apple.com/kb/HT4415
- iOS 5.x & 6.x: https://support.apple.com/kb/HT5012

[7] Las referencias a lo largo de la presente guía al término CA incluyen tanto las capacidades de autoridad certificadora (CA) como de autoridad de registro (RA, *Registration Authority*).

373. En la plataforma Android, en función de la versión, las capacidades de gestión de certificados han cambiado notablemente. En la versión Android 2.x prácticamente no se disponía de capacidades para gestionar los certificados de las CA's de confianza, mientras que en Android 4.x las capacidades disponibles son muy avanzadas, incluyendo un nuevo repositorio (KeyChain API y TrustStore) a nivel del sistema que permite la gestión completa de certificados de las CA's y de usuario, incluyendo la revocación granular de certificados no válidos[Ref.- 65].

5.5.9 GESTIÓN DE LAS COMUNICACIONES

374. Desde un punto de vista genérico, la solución MDM debe gestionar los mecanismos de conectividad y la disponibilidad y estado de los diferentes interfaces de comunicaciones inalámbricas del dispositivo móvil, como NFC (*Near Field Communications*), Bluetooth, Wi-Fi, telefonía móvil 2/3/4G, etc.

375. Las organizaciones deben tener en cuenta que los dispositivos móviles se conectarán a redes de terceros (por ejemplo, para acceder a Internet) sobre las que la organización no dispone de ningún control, salvo que se implanten controles específicos en los dispositivos móviles para evitarlo.

376. La solución MDM puede permitir disponer de un mayor control sobre todas las comunicaciones de datos originadas desde el dispositivo móvil, por ejemplo, forzando el establecimiento y la utilización de una conexión VPN cifrada antes de enviar ningún tráfico, asegurando la utilización de mecanismos de autentificación mutua antes de transmitir ningún tráfico, o seleccionando el interfaz de comunicaciones a emplear en cada momento, Wi-Fi o telefonía móvil 2/3/4G.

377. Desde el punto de vista general de transmisión de datos a través de redes TCP/IP, la solución MDM debe permitir configurar un *proxy* (o *gateway*) global en el dispositivo móvil para cursar todas las comunicaciones de datos a través de la infraestructura de red de la organización, especialmente para el acceso a recursos corporativos.

378. Los siguientes apartados proporcionan ejemplos del tipo de capacidades de gestión de las comunicaciones móviles requeridas en las soluciones MDM, pero sin ser completamente exhaustivos. Se recomienda consultar las guías específicas para cada plataforma móvil con el objetivo de profundizar en todos los aspectos relacionados con la configuración y seguridad en el uso de estas tecnologías (ver referencias al final del apartado "2. OBJETO").

379. La protección de cualquier comunicación inalámbrica comienza con las capacidades para deshabilitar el interfaz asociado (ver apartado "5.5 – Características de la(s) Política(s) de Seguridad Corporativa").

380. Debe tenerse en cuenta que algunas plataformas móviles sí proporcionan una granularidad muy avanzada para la configuración de los interfaces de comunicaciones inalámbricos, como por ejemplo la gestión del interfaz Bluetooth en BlackBerry, mientras que otras plataformas móviles no disponen de algunas tecnologías (al menos actualmente) o de la granularidad de configuración deseada, como por ejemplo la ausencia de NFC o la limitada gestión del interfaz Bluetooth en iOS, respectivamente.

5.5.9.1 *NFC*

381. Las opciones de configuración disponibles en la actualidad en los dispositivos móviles con soporte para NFC son muy limitadas, por lo que la solución MDM debería al menos de

disponer de la capacidad para habilitar o deshabilitar el interfaz NFC, así como para gestionar los servicios asociados, como por ejemplo Android Beam.

5.5.9.2 *BLUETOOTH*

382. La solución MDM debería permitir configurar el dispositivo móvil de forma permanente como no visible u oculto, siendo necesario que durante los emparejamientos sea el otro dispositivo Bluetooth el que esté visible. Esta es la configuración recomendada desde el punto de vista de seguridad.

383. Adicionalmente, es interesante disponer de capacidades avanzadas de gestión de la configuración Bluetooth, como por ejemplo poder establecer el nombre Bluetooth del dispositivo móvil o los perfiles Bluetooth disponibles y habilitados según la política de seguridad corporativa.

384. A nivel de los perfiles Bluetooth, podría disponerse de capacidades para establecer de forma independiente los mecanismos de autentificación y autorización de cada perfil.

385. Con un mayor nivel de granularidad, podría gestionar y restringir los dispositivos Bluetooth con los que puede emparejarse el dispositivo móvil, tanto por tipo de dispositivo, como por ejemplo impresoras, ordenadores, otros dispositivos móviles, manos libres, etc, como por dispositivos Bluetooth concretos.

386. Si los emparejamientos permitidos por la organización son realizados durante la configuración inicial del dispositivo móvil, podría configurarse el mismo para restringir la posibilidad de realizar nuevos emparejamientos vía Bluetooth.

387. La solución MDM podría establecer una política de seguridad sobre el PIN empleado durante los emparejamientos Bluetooth, fijando unos requisitos mínimos sobre el mismo (longitud, complejidad, etc).

388. Al hacer uso de las capacidades Bluetooth del dispositivo móvil, se irán almacenando en la base de datos de emparejamiento referencias a todos aquellos dispositivos Bluetooth con los que se haya establecido una conexión. La solución MDM debería disponer de capacidades de gestión y borrado selectivo periódico de dicha base de datos para que únicamente contenga aquellos dispositivos con los que se establecen comunicaciones Bluetooth habitualmente.

389. La política de seguridad corporativa debería establecer que la versión de la especificación Bluetooth a emplear por los dispositivos móviles de la organización sea al menos la 2.1, ya que ésta añade mecanismos como *Secure Simple Pairing* (SSP). En caso de que un dispositivo móvil no disponga de esta versión o una superior, podría decidirse deshabilitar el interfaz Bluetooth.

5.5.9.3 *WI-FI*

390. Las comunicaciones a través de redes Wi-Fi es uno de los métodos de conectividad de datos principales empleados por los dispositivos móviles hoy en día, por lo que es muy recomendable que la solución MDM disponga de capacidades avanzadas de gestión de esta tecnología.

391. En primer lugar la solución MDM debería definir con qué tipo de redes Wi-Fi se permite al dispositivo móvil establecer una conexión, es decir, redes con infraestructura basadas en un punto de acceso, redes *ad-hoc* entre dispositivos, o ambas.

392. La política de seguridad corporativa podría ser mucho más restrictiva y definir únicamente un conjunto determinado, lista blanca, de redes Wi-Fi a las que pueden conectarse los

dispositivos móviles gestionados. La solución MDM debería disponer de capacidades para aplicar esas restricciones (si la plataforma móvil lo permite).

393. La opción recomendada desde el punto de vista de seguridad sería establecer una configuración Wi-Fi restrictiva a través de la solución MDM que sólo permita al dispositivo móvil conectarse a la red Wi-Fi corporativa, y que prohiba establecer conexiones con cualquier otra red, especialmente las redes Wi-Fi públicas sin ningún mecanismo de protección.

394. La seguridad de la red Wi-Fi corporativa debería emplear WPA2 Empresarial, y los clientes deben configurarse adecuadamente para verificar su identidad a través de los parámetros y certificados digitales correspondientes.

395. Los dispositivos móviles tienden a establecer una conexión automática con las redes Wi-Fi conocidas, por lo que desde el punto de vista de seguridad se debería poder gestionar y deshabilitar esta funcionalidad de conexión automática (si la plataforma móvil lo permite).

396. Desde un punto de vista más general, se debería establecer una política de seguridad detallada para no permitir la conexión a redes Wi-Fi inseguras, considerando como tal aquellas que hacen uso (por ejemplo) de comunicaciones sin cifrar (abiertas u *open*) o con cifrado débil (WEP).

397. La solución MDM podría también establecer una política de seguridad sobre la contraseña (clave precompartida o PSK. *Pre-Shared Key*) a emplear en la conexión a redes Wi-Fi WPA y WPA2 Personal, fijando unos requisitos mínimos sobre la misma (longitud, complejidad, etc) que de no cumplirse, no permitirían la conexión del dispositivo móvil a la red asociada.

398. Asimismo, debería permitir llevar a cabo la configuración avanzada de las redes WPA y WPA2 Empresariales, pudiendo definir y restringir los mecanismos de autentificación (EAP/802.1x) y cifrado (Ej. AES) a emplear, así como los servidores RADIUS y las CA's de confianza empleados para los mecanismos de autentificación basados en certificados digitales.

399. Al hacer uso de las capacidades Wi-Fi del dispositivo móvil, se irán almacenando en la base de datos de redes Wi-Fi conocidas (o PNL, *Preferred Network List*) referencias a todas aquellas redes Wi-Fi a las que se ha conectado previamente el dispositivo móvil. La solución MDM debería disponer de capacidades de gestión (añadir, modificar y borrar) de la PNL para que únicamente contenga aquellas redes Wi-Fi a las que se conecta el usuario habitualmente.

400. Complementando la gestión de la PNL, la solución MDM debería poder identificar que redes Wi-Fi de la PNL están configuradas como ocultas y cuales como visibles, además de poder modificar o editar su configuración para cambiar el tipo de red.

401. La solución MDM debería disponer de capacidades de gestión para restringir y configurar la funcionalidad de punto de acceso Wi-Fi existente en los dispositivos móviles actuales.

5.5.9.4 *TELEFONÍA MÓVIL 2/3/4G*

402. Respecto a las comunicaciones móviles, debería ser posible habilitar o deshabilitar de forma independiente las comunicaciones de voz (y SMS/MSM) y las comunicaciones de datos (2/3/4G).

403. La solución MDM debería permitir gestionar las capacidades de compartición de la conexión de datos con otros dispositivos (conocidas como *tethering*), incluyendo la aplicación de restricciones sobre los métodos de *tethering* permitidos (Bluetooth, Wi-Fi y/o USB) y los ajustes de seguridad de las redes de comunicaciones asociadas.

404. La opción recomendada desde el punto de vista de seguridad sería permitir únicamente hacer uso de las capacidades de *tethering* del dispositivo móvil a través del puerto USB.

405. Como elemento fundamental para la protección de este tipo de comunicaciones, debería ser posible seleccionar el tipo de red de telefonía móvil a emplear, 2G (con numerosas vulnerabilidades conocidas) ó 3/4G.

406. Esta selección del tipo de red debería ser aplicable tanto para voz (GSM o UMTS) como para datos (GPRS y EDGE, frente a UMTS y LTE).

407. Una funcionalidad complementaria que puede ser proporcionada por la solución MDM es la que permite llevar un control del gasto de los servicios de telefonía móvil (voz, SMS y datos) de cada dispositivo móvil en tiempo real.

408. Adicionalmente, la solución MDM debería poder gestionar los parámetros de conectividad en el extranjero (*roaming*), tanto para voz y SMS, como para datos.

409. En el caso de las comunicaciones a través de las redes de telefonía móvil 2/3/4G, la solución MDM puede permitir la configuración y gestión de un APN (*Access Point Name*) privado y propio de la organización, que ha sido contratado previamente al operador de telefonía.

5.5.10 GESTIÓN DE VPN

410. La solución MDM debe permitir la gestión y actualización de la configuración de las conexiones VPN de la organización en los dispositivos móviles, incluyendo tanto la configuración general de la arquitectura y servidores VPN (direcciones IP, puertos, etc) como la configuración de los secretos precompartidos y de las credenciales asociadas a la cuenta de acceso por VPN del usuario.

411. Una de las tendencias más recientes respecto al establecimiento de conexiones VPN desde dispositivos móviles es la posibilidad de establecer VPNs por app, en lugar de una VPN única y genérica para todo el sistema.

412. La posibilidad de establecer VPNs por app (o VPNs selectivas) permite proteger con más granularidad la transferencia de datos corporativos, minimizando colateralmente el consumo de batería y reduciendo el tráfico de red de apps personales (no asociadas al negocio y cuya transferencia no tiene porqué ser protegida necesariamente).

5.5.11 GESTIÓN DE CORREO ELECTRÓNICO

413. El correo electrónico o e-mail es un mecanismo de comunicación fundamental hoy en día para cualquier organización. El acceso al correo electrónico desde los dispositivos móviles puede introducir nuevas amenazas y riesgos asociados a la información confidencial y sensible intercambiada a través de este servicio.

414. Por este motivo, los clientes de e-mail en los dispositivos móviles son una de las apps iniciales dónde se comenzaron a aplicar mecanismos de seguridad más avanzados (por ejemplo, cifrado de los datos) y capacidades de contenedor, por ejemplo, para limitar la exposición de los ficheros corporativos adjuntos (ver apartado “5.5.13.5. GESTIÓN DE LOS CONTENIDOS Y DATOS MANEJADOS POR LAS APPS”).

415. Uno de los elementos a tener en cuenta en toda solución MDM es su capacidad de integración con plataformas, soluciones y servidores de correo electrónico empresariales, como por ejemplo Microsoft Exchange, Microsoft Office 365, IBM Lotus Notes/Domino o Google Apps.

416. La solución MDM debe disponer de capacidades para permitir o denegar en cualquier momento el acceso al e-mail de un usuario, por ejemplo, cuando éste deja la organización.

417. Algunas soluciones MDM más avanzadas disponen de capacidades automáticas para bloquear el acceso al correo electrónico de un usuario cuyo dispositivo móvil no ha sido registrado aún en la solución MDM o ha violado la política de seguridad de la organización.

418. Sin embargo, se recomienda que la solución MDM establezca una política de seguridad que no permita el acceso al correo electrónico corporativo, ni al resto de recursos corporativos, a dispositivos móviles que no hubieran sido registrados previamente y que por tanto estén siendo gestionados. La gestión de los dispositivos móviles permite aplicar la política de seguridad, que incluye entre otros los parámetros de configuración para el acceso al correo electrónico.

419. Adicionalmente, la solución MDM debe asegurarse de que los ajustes de configuración de acceso a los servidores de correo son seguros y hacen uso de mecanismos de cifrado para el acceso y transmisión de e-mails, por ejemplo, mediante los protocolos IMAPS, POP3S, SMTPS o HTTPS.

420. Debido a que los dispositivos móviles pueden disponer de múltiples clientes de e-mail y múltiples cuentas de correo electrónico configuradas simultáneamente, tanto personales como profesionales, es importante segregar los datos gestionados por todos ellos.

421. Complementariamente, se recomienda evaluar las capacidades de la solución MDM para impedir que se configuren cuentas de correo no corporativas adicionales, tanto en la app cliente de correo existente por defecto en la plataforma móvil, como a través de otras apps que actúan como clientes de correo (por ejemplo, no permitiendo ni siquiera la instalación de estas apps).

422. Al igual que se ha descrito previamente para otros contenidos corporativos, el acceso al servicio de e-mail y el almacenamiento de los mensajes de correo electrónico y ficheros adjuntos corporativos pueden ser aislados en una app contenedora que permita establecer medidas y protecciones adicionales de seguridad, como por ejemplo restringir las operaciones de copiar y pegar contenidos, o las opciones de impresión.

423. Una de las características principales a verificar en la app de acceso al correo electrónico es que todos los contenidos obtenidos a través de este servicio (mensajes y ficheros adjuntos) sean cifrados localmente al ser almacenados en el dispositivo móvil.

424. El acceso a los ficheros adjuntos a los mensajes de correo electrónico requiere en ocasiones disponer de apps que permitan su lectura. Esta gestión de ficheros adjuntos puede integrarse con una solución de gestión de contenidos para su almacenamiento y acceso seguro (ver apartado “5.5.13.5. GESTIÓN DE LOS CONTENIDOS Y DATOS MANEJADOS POR LAS APPS”).

425. La distribución segura de documentos adjuntos a través de e-mail se basa normalmente en la utilización de enlaces (o *links*, en lugar de incluir el propio fichero en el mensaje) que referencian al fichero dentro de la solución de gestión de contenidos corporativos.

426. Adicionalmente, la solución MDM puede establecer controles alternativos sobre los ficheros adjuntos a los mensajes de correo electrónico y no permitir la recepción o envío de ciertos ficheros según su tipo.

427. Se recomienda que la política de seguridad defina qué tipos de ficheros pueden ser intercambiados a través del servicio de correo electrónico y establecer restricciones para que sólo puedan adjuntarse o recibirse este tipo de ficheros.

428. En ocasiones, los mecanismos de gestión para las capacidades de acceso al correo electrónico (e-mail) de los dispositivos móviles se referencian como MEM (*Mobile E-mail Management*).

5.5.12 GESTIÓN DE NAVEGACIÓN WEB

429. Adicionalmente al correo electrónico, el otro servicio estándar en toda organización hoy en día es la navegación web, ya sea únicamente hacia las aplicaciones web corporativas existentes en la infraestructura de la organización, o también hacia Internet.

430. La solución MDM debe disponer de capacidades de gestión y configuración granulares del navegador web, por ejemplo, para deshabilitar el aceptar cookies de terceros o el motor de JavaScript.

431. En entornos críticos debe evaluarse el impacto asociado a deshabilitar las capacidades de JavaScript y Java en el navegador web del dispositivo móvil, así como no permitir cookies, del propio sitio web o de terceros. Está configuración más restrictiva es la recomendada desde el punto de vista de seguridad, aunque desde el punto de vista de la funcionalidad y según el tipo de sitios webs accedidos, puede ser necesario disponer de capacidades para la gestión de cookies y hacer uso de JavaScript.

432. La solución MDM puede disponer de capacidades para la creación y distribución de *web clips* (iconos con enlaces a aplicaciones web) en los dispositivos de la organización, así como gestionar la página de inicio o añadir favoritos al navegador web.

433. Adicionalmente a los controles corporativos existentes en los proxies de la organización, la solución MDM puede establecer restricciones a través de la creación de listas blancas y negras de navegación web, que permitan o denieguen el tráfico web desde los dispositivos móviles hacia Internet.

434. En ocasiones se referencian los mecanismos de gestión para las capacidades de navegación web de los dispositivos móviles como MBM (*Mobile Browsing Management*).

5.5.13 GESTIÓN DE APPS

NOTA: Las aplicaciones cliente analizadas en los dos apartados previos, correo electrónico y navegación web, son dos ejemplos concretos de apps existentes por defecto en todas las plataformas móviles actuales. Sobre ellas aplican igualmente las consideraciones de seguridad analizadas a continuación para cualquier aplicación móvil o app.

435. Uno de los elementos fundamentales a considerar en las plataformas móviles modernas, y motivo principal por el que a los terminales móviles actuales se les referencia con el término *smartphones*, es la posibilidad de instalar aplicaciones móviles o apps en los mismos, al poderse considerar a estos dispositivos como ordenadores de propósito general de reducido tamaño.

436. Las apps permiten extender las capacidades y funcionalidad existente por defecto en el dispositivo móvil hasta límites inimaginables, existiendo actualmente cientos de miles de apps disponibles en los mercados oficiales para las diferentes plataformas móviles.

437. Debe tenerse en cuenta que las plataformas móviles promueven y están diseñadas para encontrar de forma sencilla, adquirir, instalar y usar apps de los mercados de aplicaciones móviles, con los riesgos asociados, motivo por el que es fundamental imponer restricciones y controles sobre las apps disponibles.

438. Las apps pueden ser clasificadas en diferentes categorías, por ejemplo, desde apps profesionales de productividad ampliamente utilizadas en entornos corporativos, pasando por apps de acceso a servicios en Internet (como redes sociales, portales web, servicios "en la nube", etc), hasta apps de juegos o entretenimiento, o de acceso a contenidos multimedia, más utilizadas en el ámbito personal.

439. Uno de los objetivos fundamentales de la gestión de aplicaciones empresarial (MAM) es poder proporcionar a los usuarios de la organización desde el primer momento el conjunto de apps necesario para su trabajo, situación habitual con los ordenadores portátiles plataformados.

440. Cuando un usuario comienza a trabajar en la organización se le facilita un ordenador, portátil o de escritorio, ya plataformado y con todas las herramientas y aplicaciones necesarias.

441. Lo mismo debería ocurrir con los dispositivos móviles, de forma que estos sean aprovisionados con las apps necesarias en función del perfil del usuario y del departamento en el que trabaja éste dentro de la organización.

5.5.13.1 *GESTIÓN DE LOS MERCADOS PÚBLICOS DE APPS*

442. En primer lugar, la solución MDM debe permitir gestionar si se permite la instalación de apps desde los mercados públicos oficiales disponibles en Internet para cada una de las plataformas móviles, como Google Play (Android), BlackBerry World, Apple's App Store (iOS) o Microsoft Windows Phone Store, o si por el contario la instalación de apps estará circunscrita únicamente al mercado corporativo de apps de la organización.

443. En el caso de permitirse la instalación de apps desde mercados públicos, es necesario definir si se permiten únicamente los mercados oficiales vinculados al fabricante de la plataforma móvil, opción recomendada desde el punto de vista de seguridad, o también otros mercados oficiales, como el Amazon AppStore. En ningún caso se recomienda permitir la instalación de apps de mercados no oficiales.

444. En el caso de no permitirse y disponer únicamente de un mercado corporativo de apps (ver apartado "5.5.13.2. GESTIÓN DE LAS APPS Y LOS MERCADOS CORPORATIVOS DE APPS"), la solución MDM debe eliminar los iconos y apps de acceso a los mercados de apps públicos de cada plataforma, y bloquear el acceso a estos a través de un navegador web estándar.

445. Adicionalmente, para aquellas plataformas móviles que permiten de forma sencilla la instalación de apps desde mercados de terceros o desde otras fuentes, como por ejemplo páginas web, la solución MDM debe proporcionar mecanismos que permitan configurar el dispositivo móvil para restringir la obtención de apps de estas fuentes no fiables.

5.5.13.2 *GESTIÓN DE LAS APPS Y LOS MERCADOS CORPORATIVOS DE APPS*

446. Ante la innumerable cantidad de apps disponibles en los mercados oficiales de aplicaciones móviles de las diferentes plataformas, muchas organizaciones han optado por establecer controles estrictos sobre qué apps están disponibles para ser instaladas en los dispositivos móviles de los usuarios.

447. Los controles deben realizarse a través de la solución MDM mediante listas blancas (preferiblemente desde el punto de vista de seguridad) o listas negras de apps. Las primeras establecen qué conjunto de apps pueden ser instaladas en los dispositivos porque se consideran relevantes para el negocio y la productividad y no tienen implicaciones negativas

de seguridad. Las segundas establecen el modelo opuesto, qué apps se consideran no deseadas o dañinas desde el punto de vista de seguridad, prohibiendo su instalación y uso.

448. Para aquellas plataformas móviles que proporcionan más granularidad para seleccionar qué permisos están asociados a una app, como por ejemplo BlackBerry, la solución MDM debe permitir definir y asignar a la app únicamente los permisos necesarios determinados por la organización.

449. La gestión de apps debe contemplar tanto la instalación de apps corporativas en dispositivos móviles personales (habitual en entornos BYOD), como la instalación de apps personales en dispositivos móviles corporativos (habitual en entornos BYOA).

450. Por otro lado, algunas organizaciones sólo permiten (o permiten complementariamente) la instalación de apps qué han sido desarrolladas dentro de la organización, o desarrolladas por terceros sólo para la organización, con el objetivo de permitir la ejecución de procesos de negocio desde los dispositivos móviles, conocidas como *in-house* apps o *line-of-business* (LOB) apps.

451. Las diferentes plataformas móviles y algunas soluciones MDM permiten establecer y gestionar un mercado privado de aplicaciones móviles propio de la organización.

452. Estos mercados privados suelen ser referenciados como mercados corporativos de apps, o *Enterprise App Stores* [Ref.- 61]. Normalmente, las soluciones MDM proporcionan estas capacidades de gestión de apps a través de un mercado corporativo como un componente más integrado en la propia solución de gestión.

453. Uno de los elementos iniciales a evaluar respecto a la funcionalidad del mercado corporativo de apps en las soluciones MDM es el conjunto de plataformas móviles soportadas, así como la disponibilidad de funcionalidad avanzada para cada una de ellas.

454. Al igual que se mencionó inicialmente la tendencia actual asociada a la gestión integrada de los múltiples dispositivos asignados a un usuario, algunas soluciones MDM proporcionan capacidades de gestión de software y apps no sólo para las plataformas móviles, sino también para los dispositivos más tradicionales (como ordenadores portátiles y de escritorio).

455. El mercado corporativo de apps también permite llevar a cabo la gestión de licencias y la adquisición y pago de apps comerciales disponibles en los mercados públicos y oficiales, recomendándose realizar una gestión de compra de apps a nivel corporativo (o de las diferentes unidades de negocio o departamentos), en lugar de hacerlo de manera individual por parte de cada usuario, con el objetivo de obtener acuerdos más ventajosos (por ejemplo, descuentos) para la organización.

456. Este mercado incluye únicamente el catálogo personalizado de aquellas apps, oficiales y públicas (ya sean gratuitas o de pago) o privadas (*in-house*), que han sido aprobadas como válidas para su uso en los dispositivos móviles de la organización.

457. La disponibilidad de un mercado corporativo de apps no sólo permite definir qué apps estarán disponibles para los usuarios, sino también establecer controles y políticas más avanzadas para su instalación y uso en función del perfil del usuario u otros factores.

458. La solución MDM debería requerir que el usuario se autentifique para acceder al mercado corporativo de apps, siendo posible por tanto proporcionar un catálogo de apps personalizado por usuario y por dispositivo móvil.

459. Se recomienda por tanto establecer a través de la solución MDM un listado de aplicaciones permitidas (lista blanca) o prohibidas (lista negra) en los dispositivos móviles gestionados por la organización.

460. Adicionalmente es posible establecer una lista de apps requeridas por la organización, que deben estar disponibles obligatoriamente en todos los dispositivos móviles gestionados, según indique la política de seguridad de la organización.

461. Los criterios para considerar una app como aceptada o prohibida pueden ser muy diversos, y deben estar contemplados en la política de seguridad de la organización.

462. En algunos casos, puede ser necesaria una inversión relevante en tiempo y recursos para realizar un análisis detallado de una app antes de su aprobación o prohibición.

463. Este estudio puede conllevar la utilización de técnicas de análisis de código estático de la app y de técnicas de análisis del comportamiento de la misma, con el objetivo de identificar si la app almacena y transfiere datos de forma segura, o si dispone de funcionalidad adicional no deseada.

464. Un elemento fundamental a tener en cuenta antes de la aprobación de una app en algunas plataformas móviles, como por ejemplo Android, BlackBerry o Windows Phone (no en iOS, al no estar disponibles), es el conjunto de permisos y privilegios solicitados por la app. Debe evaluarse en detalle qué los permisos solicitados sean coherentes con la funcionalidad ofrecida por la app.

465. En otras ocasiones, y debido a la limitación de recursos disponibles, la decisión para incluir o no una app en una de las categorías mencionadas se basa en la reputación de la misma en los mercados oficiales de aplicaciones móviles.

466. Algunos aspectos a tener en cuenta de cara a evaluar la reputación de una app son quién es el autor o desarrollador de la misma y su propia reputación, el tiempo que la app lleva publicada y el número de versiones existentes, y los comentarios, revisiones y valoraciones de la comunidad, es decir, de otros usuarios de la app.

467. En cualquier caso, siempre deben tenerse en cuenta los términos y acuerdos de uso de cada app y de sus servicios asociados, ya que incluso los servicios asociados a proveedores de referencia en la industria puede especificar que no se garantiza la confidencialidad de los datos intercambiados por el usuario.

NOTA: Están empezando a aparecer en la industria servicios de reputación de las aplicaciones móviles, que pueden ser integrados con las soluciones MDM, con el objetivo de identificar y clasificar el riesgo de seguridad asociado a la utilización de apps disponibles en los mercados públicos o en los mercados corporativos, como por ejemplo Veracode MARS (*Mobile Application Reputation Service*)[8]. Estos servicios se basan en el análisis de las capacidades y comportamientos de las apps.

468. Pese a realizar un análisis de todos los factores mencionados previamente, no es posible asegurar que una app no contenga código malicioso sin realizar un estudio técnico detallado de la misma, por lo que las organizaciones deben disponer de mecanismos de gestión de incidentes de seguridad para gestionar este tipo de escenarios.

[8] https://www.veracode.com/products/veracode-mars.html

469. Por ejemplo, se recomienda que las organizaciones establezcan una política que no permita el uso de ninguna app que facilite la lectura de códigos QR (*Quick Response*), o de forma más general, que haga uso de la cámara, ya que estos códigos pueden ser utilizados para redirigir al dispositivo móvil a una URL o sitio web malicioso.

470. Pese a que la amenaza asociada a los códigos QR podría mitigarse con una correcta concienciación en su uso por parte de los usuarios, la organización puede decidir establecer este tipo de restricciones para proteger aún más los dispositivos móviles gestionados.

471. Si se dispone de la granularidad suficiente, dependiente de la app y plataforma móvil empleada, las apps que procesan códigos QR podrían ser configuradas a través de la solución MDM para siempre mostrar la URL contenida en el código QR antes de navegar a ella, permitiendo al usuario aceptar o rechazar la acción asociada. En cualquier caso, la decisión final estaría en manos del usuario y su criterio para identificar URLs sospechosas.

472. La solución MDM debe configurarse para que imponga restricciones que no permitan ejecutar una app determinada si el dispositivo móvil no cumple con la política de seguridad corporativa.

473. Por otro lado, la solución MDM debería disponer de granularidad suficiente para imponer restricciones en las apps respecto al uso y los permisos asociados a los servicios, módulos y elementos que constituyen la plataforma móvil, como por ejemplo la cámara, los servicios de localización, el acceso a los contactos, etc.

474. Esta granularidad es completamente dependiente de la plataforma móvil y del modelo de permisos utilizado para las apps, siendo muy diferente la gestión de permisos por ejemplo en Android, BlackBerry e iOS.

475. En el caso en el que no sea posible la aplicación de listas blancas para la instalación de apps, como por ejemplo en entornos BYOD no restrictivos, la solución MDM debe proporcionar restricciones que permitan especificar que las apps que no hayan sido aprobadas explícitamente por la organización, en caso de poder ejecutar, no puedan acceder a datos e información sensible.

476. Adicionalmente, otra aproximación a la protección de los datos y servicios corporativos dentro de una app en los dispositivos móviles es la de hacer uso de una app contenedora (ver apartado “4.6.6. SOLUCIONES DE GESTIÓN BASADAS EN UN CONTENEDOR”).

477. Algunas soluciones MDM proporcionan kits de desarrollo (SDKs) y librerías (o APIs) para el desarrollo de apps seguras que hagan uso de las capacidades de seguridad y gestión proporcionadas por la solución MDM, como mecanismos de autentificación únicos (SSO, *Single Sign On*, certificados, etc) entre apps, mecanismos de cifrado (para el almacenamiento, OTA, etc), controles basados en la localización (*geofencing*) o facilitar el intercambio seguro de datos entre apps.

NOTA: A modo de referencia se proporcionan ejemplos de soluciones MDM con estas capacidades, como por ejemplo AirWatch SDK, MobileIron AppConnect SDK, o Good Dynamics SDK.

478. Otras soluciones MDM proporcionan una plataforma que permite englobar o envolver (*wrapping*) las apps ya existentes mediante librerías de seguridad específicas, proporcionando un entorno más seguro para apps previamente desarrolladas.

NOTA: A modo de referencia se proporcionan ejemplos de soluciones MDM con estas capacidades, como por ejemplo AirWatch App Wrapping o MobileIron AppConnect Wrapping.

479. Estas capacidades pueden ser empleadas por la organización para el desarrollo de apps propias más seguras y plenamente integradas en la solución de gestión.

5.5.13.3 *GESTIÓN EN LA DISTRIBUCIÓN DE LAS APPS*

480. La solución MDM debe permitir la distribución de apps, por ejemplo mediante la recepción automática (notificaciones *push*) por parte del usuario de un mensaje que le indica la existencia de una nueva app (o una nueva versión de una app) para su instalación (o actualización).

481. En otros casos, puede ser interesante que las apps gestionadas sean instaladas automáticamente en los dispositivos móviles gestionados por la organización sin intervención por parte del usuario.

482. En el caso de iOS, desde la versión 5.x, las apps que son gestionadas y distribuidas a través de una solución MDM se consideran apps gestionadas. Tanto las propias apps como sus datos (por ejemplo, datos corporativos) pueden ser eliminadas de los dispositivos móviles por el administrador de la solución MDM sin afectar a los datos de otras apps (por ejemplo, datos personales), funcionalidad muy conveniente especialmente en entornos BYOD.

483. La solución MDM debe proporcionar capacidades de distribución de apps granulares, en función del tipo de dispositivo móvil, del usuario asociado y del departamento al que éste pertenece en la organización, ya que éste tendrá asociadas unas necesidades de negocio y, por tanto de apps, particulares.

484. Adicionalmente a la gestión de la instalación de nuevas apps, la solución MDM debe proporcionar capacidades para la distribución de actualizaciones de apps previamente instaladas.

485. Estas capacidades deben complementarse con mecanismos de monitorización que permitan en todo momento el nivel de actualización de los dispositivos móviles de la organización para una app determinada.

486. De manera complementaria, la solución MDM debe disponer de capacidades para eliminar remotamente una app de uno o múltiples dispositivos móviles, por ejemplo, porque se identifique un comportamiento no apropiado o inseguro por parte de la organización.

5.5.13.4 *GESTIÓN DE LOS SERVICIOS ACCEDIDOS POR LAS APPS*

487. La gestión de apps tiene una relación directa con la gestión de los servicios remotos, tanto corporativos como públicos (disponibles en Internet), que pueden ser accedidos desde el dispositivo móvil.

488. Los accesos a los servicios *on-line* se realizan desde el navegador web o cliente de correo electrónico existentes por defecto en la plataforma móvil, o desde las apps instaladas posteriormente por la organización o por el usuario.

489. Mediante la restricción de las apps permitidas se restringe parcialmente el acceso a ciertos servicios corporativos, evitando el acceso a datos confidenciales, o a servicios públicos, evitando la fuga de información corporativa hacia Internet.

490. Sin embargo, debe tenerse en cuenta que muchas apps móviles actúan como navegadores web restringidos, por lo que potencialmente es también posible disponer de acceso al servicio

remoto que emplea la app haciendo uso de un navegador web estándar, siendo necesario también imponer restricciones adicionales en éste o en las redes de comunicaciones empleadas.

491. Debe tenerse en cuenta que el acceso directo desde el navegador web no está necesariamente protegido por las recomendaciones de gestión de apps descritas previamente.

492. Únicamente si se imponen restricciones en el uso del navegador web existente en la plataforma móvil (ver apartado "5.5.12. GESTIÓN DE NAVEGACIÓN WEB"), o se obliga a que toda la navegación deba transcurrir por un *proxy* o dispositivo intermedio gestionado por la organización, será posible monitorizar y aplicar controles para el acceso remoto a servicios y sitios web.

493. Debido a la importancia y criticidad de los servicios web hoy en día, desde el punto de vista de seguridad es necesario aplicar este tipo de configuración, restricciones y controles tanto en los dispositivos móviles como en la infraestructura de comunicaciones.

494. De nuevo, otra aproximación a la protección de los datos y servicios corporativos accedidos desde el navegador web en los dispositivos móviles es la de hacer uso de una app contenedora que disponga de su propio navegador web seguro (ver apartado "4.6.6. SOLUCIONES DE GESTIÓN BASADAS EN UN CONTENEDOR").

5.5.13.5 *GESTIÓN DE LOS CONTENIDOS Y DATOS MANEJADOS POR LAS APPS*

495. La gestión de contenidos y datos en los dispositivos móviles debe analizarse desde dos puntos de vista: la sincronización y realización de copias de seguridad con dispositivos locales o servicios remotos, y la gestión de contenidos corporativos asociados a las apps.

496. Muchas plataformas móviles, e incluso apps específicas, disponen de capacidades de transferencia de datos, sincronización o realización de copias de seguridad en servicios o ubicaciones remotas, o en ordenadores o dispositivos locales.

497. La interacción con equipos locales se suele llevar a cabo a través del puerto USB o mediante una conexión inalámbrica, como Bluetooth o Wi-Fi, mientras que la interacción con servicios remotos suele conllevar el envío automático de datos vía Wi-Fi o 2/3/4G a una solución de almacenamiento "en la nube".

498. Los datos corporativos pueden estar bajo riego de ser almacenados en localizaciones inseguras y externas a la organización en diferentes escenarios, como por ejemplo la conexión de un dispositivo móvil personal a un ordenador de la organización, la conexión de un dispositivo móvil de la organización a un ordenador personal, a otro dispositivo móvil personal, a un servicio remoto o a un cargador de electricidad de un tercero [Ref.- 58].

499. La solución MDM debe proporcionar capacidades para restringir con qué otros equipos puede sincronizarse el dispositivo móvil, ya sea mediante una conexión física a través del puerto USB o mediante conexión inalámbrica, y éstas deben ser aplicadas en función de la política de seguridad definida.

500. Asimismo, debería proporcionar restricciones más granulares sobre los servicios de sincronización remotos disponibles en numerosas apps, con el objetivo de gestionar si se hace o no uso de estos servicios, así como los ajustes de configuración específicos para cada uno de ellos.

501. Por ejemplo, en iOS es posible definir una política a nivel del dispositivo móvil que restrinja que los datos de apps gestionadas no sean incluidos en las copias de seguridad a través de iTunes (locales) o iCloud (remotas).

502. Desafortunadamente, es muy habitual en la actualidad que los usuarios de la organización utilicen servicios de compartición de ficheros disponibles de forma gratuita "en la nube" para intercambiar documentos corporativos. Si estos documentos no son cifrados convenientemente, los contenidos propiedad de la organización estarán expuestos a terceros.

503. Por este motivo, deben establecerse restricciones para el uso de este tipo de servicios, o en su defecto y en caso de ser necesario, la solución MDM debe proporcionar o se debe integrar con soluciones de gestión de contenidos corporativos, es decir, que proporcionen un repositorio seguro para la compartición y distribución de contenidos.

504. Estas capacidades de gestión de contenidos corporativos y compartición de documentos son referenciadas habitualmente como EFSS (*Enterprise File Synchronization and Sharing*).

505. La gestión de los dispositivos móviles puede ser integrada directamente con la gestión de contenidos de la organización, etiquetando los diferentes documentos, datos e información corporativa disponible y aplicando controles de acceso sobre los mismos desde y hacia los dispositivos móviles.

506. Existe incluso la posibilidad de crear contenidos corporativos temporales, con un tiempo de expiración definido, y que se eliminarán automáticamente del dispositivo móvil llegado ese momento.

507. Asimismo, debe bloquearse el acceso a los datos y contenidos corporativos por parte de dispositivos móviles que violen la política de seguridad de la organización, hasta que se lleven a cabo las tareas que permitan cumplir con dicha política.

508. Una tendencia cada vez más popular en las soluciones MDM es "Open In", mecanismo que permite establecer controles de acceso que definan en qué apps o servicios de la plataforma móvil es posible abrir (o acceder a) un documento concreto.

509. Estas restricciones son aplicadas habitualmente a la funcionalidad local que permite enviar o compartir un documento o datos desde una app hacia otra app en el mismo dispositivo móvil, o capacidades de la plataforma móvil, como la impresión de dicha información.

510. A través de soluciones contenedoras y de compartición y gestión de contenidos es posible cifrar los documentos intercambiados, y restringir su acceso, edición, distribución (e-mail, SharePoint, servidores de ficheros o carpetas compartidas, NFS, servidores WebDAV y otros repositorios de contenidos), y su utilización desde los dispositivos móviles sin conexión al repositorio (*offline*).

511. Los controles de acceso pueden imponer restricciones en el acceso a los contenidos con mecanismos de autentificación adicionales de dos o más factores, en función de la localización del dispositivo móvil (*geofencing*), o del tipo de conexión de datos empleada (Wi-Fi frente a 2/3/4G, por ejemplo, en escenarios de *roaming*).

512. Otra tendencia reciente para la gestión e incremento de la seguridad de los datos corporativos y privados accedidos desde los dispositivos móviles está basada en el uso de técnicas de virtualización.

513. A través de estas tecnologías se permite el acceso a la información corporativa por parte del usuario sin que los datos sean copiados en ningún momento al dispositivo móvil, ya que estos residen en los servidores corporativos y la app actúa como un simple cliente que permite su visualización.

514. Este tipo de soluciones, recomendadas desde el punto de vista de seguridad, requiere de un mayor ancho de banda para permitir una utilización de la app y un acceso a los datos fluido por parte del usuario.

515. En algunos casos, la aplicación que procesa los datos ejecuta completamente en los servidores corporativos, mientras que en otros está disponible "en la nube", opción no recomendada desde el punto de vista de seguridad. En cualquier caso, es necesario evaluar las capacidades de acceso a los datos corporativos cuando el dispositivo móvil no dispone de conexión de red (*offline*), pero es necesario acceder a la información.

5.5.13.6 *GESTIÓN DE APPS ESPECÍFICAS SEGÚN LA PLATAFORMA MÓVIL*

516. A modo de ejemplo, se proporcionan a continuación detalles específicos para la gestión de apps de una de las plataformas móviles bajo estudio, iOS.

517. Se recomienda consultar la documentación para desarrolladores del resto de plataformas móviles mencionadas, con el objetivo de obtener los detalles asociados. Por ejemplo, BlackBerry 5.x-6.x dispone de controles y permisos granulares para la gestión y desarrollo de apps, mientras que otras plataformas como Android o Windows Phone disponen de capacidades más limitadas (ver la serie CCN-STIC de guías de seguridad para dispositivos móviles, referenciadas en el apartado "2. OBJETO").

5.5.13.7 *GESTIÓN DE APPS EN DISPOSITIVOS MÓVILES IOS*

518. En el caso de iOS, para poder llevar a cabo el desarrollo de *in-house apps* y su distribución OTA (*Over-the-Air*) a través del mercado corporativo, es necesario estar registrado en el "iOS Developer Enterprise Program (iDEP)" [Ref.- 18] ($299/año), diferente del "iOS Developer Program" ($99/año), que sólo permite la publicación de apps en la AppStore oficial y pública.

519. iOS permite la distribución de apps vía OTA [Ref.- 23] mediante un servidor web interno de la organización (con autentificación y cifrado), las apps a distribuir (ficheros con extensión .ipa), un manifiesto (fichero *manifest* con extensión .plist) en formato XML, e información de configuración de red para la conexión a los servidores iTunes y OCSP de Apple.

520. La instalación de apps gestionadas se puede realizar desde el servidor MDM, pero requiere de la aceptación manual por parte del usuario (hasta la versión 7 de iOS y en ciertos escenarios – dispositivos supervisados).

521. iOS permite especificar que ciertas apps gestionadas y sus datos asociados sean eliminados bajo demanda o automáticamente cuando se elimina el perfil de configuración de la solución MDM, muy útil para apps corporativas en entornos BYOD.

522. Por otro lado, recordar que iOS también permite evitar que los datos de apps gestionadas sean incluidos en las copias de seguridad a través de iTunes o iCloud.

6 CARACTERÍSTICAS Y CAPACIDADES DE GESTIÓN DE LAS DIFERENTES PLATAFORMAS MÓVILES

523. El presente apartado describe las características principales y particulares asociadas a las capacidades de gestión de las plataformas móviles de referencia existentes actualmente: Android, BlackBerry, iOS y Windows Phone.

6.1 GESTIÓN DE ANDROID

524. Android no dispone de una herramienta o mecanismo de gestión universal, homogéneo e independiente. En su lugar, es necesario hacer uso de soluciones MDM propietarias de terceros que implementan las capacidades de gestión requeridas a través de un agente software o app que debe ser instalada en el dispositivo móvil.

525. Esta app o agente de las soluciones MDM hace uso de la *Android Device Administration API* [Ref.- 42] (disponible desde la versión Android 2.2) y debe ser instalada con permisos de administrador del dispositivo móvil en Android, en concreto, con el permiso "BIND_DEVICE_ADMIN".

526. Así por ejemplo, desde Android 2.2 es posible realizar la gestión de los dispositivos móviles Android a través de Google Apps (ver apartado "4.6.1. GOOGLE") mediante la app "Google Apps Device Policy" [Ref.- 37], que actúa como un agente para permitir la gestión de los dispositivos móviles Android de forma remota a través de los servicios de Google "en la nube".

527. El mismo modelo es empleado por los fabricantes de otras soluciones MDM, proporcionando sus propias apps o agentes, que se comunican con sus servidores MDM.

528. Esta librería o API de gestión y administración, en función de la versión de Android, define el tipo de operaciones y acciones disponibles para este tipo de agentes de gestión.

529. Por otro lado, y como ejemplo específico, existen fabricantes de dispositivos móviles basados en Android, como Samsung, que proporcionan sus propias librerías y APIs de gestión empresarial a través de las soluciones Samsung SAFE y KNOX [Ref.- 67].

530. El modelo de gestión de Android ofrece más flexibilidad a los fabricantes de soluciones MDM para implementar controles y capacidades adicionales, sin embargo, éstas siguen estando limitadas por la funcionalidad expuesta por Android a través de la API de gestión.

NOTA: Por ejemplo, desde iOS 5.x se dispone en APNS de la capacidad de configurar una política de seguridad que no permita el establecimiento de conexiones a través de HTTPS con servicios en los que no es posible validar el certificado digital, funcionalidad no disponible en la API de Android para la versión 4.0, Ice Cream Sandwich (ICS).

531. Por tanto, la gestión de los dispositivos móviles Android se puede realizar a través de EAS,a través de soluciones MDM propietarias o con Google Apps.

532. La configuración inicial que permite la integración y la obtención de los datos del servidor MDM para realizar el proceso de registro en dispositivos móviles Android se lleva a cabo normalmente a través de la instalación de una app asociada a la solución MDM.

6.1.1 ARQUITECTURA DE GESTIÓN MDM DE ANDROID

533. Las soluciones MDM de gestión de la plataforma Android no disponen obligatoriamente de una arquitectura universal, ya que dependen de la implementación realizada por el fabricante de la solución y su app o agente de gestión.

534. Sin embargo, Google proporciona un servicio gratuito, denominado *Google Cloud Messaging* (GCM) [Ref.- 68] (inicialmente se denominó C2DM, *Cloud to Device Messaging*), para el envío de mensajes desde los servidores de la solución MDM hacia los dispositivos móviles Android gestionados, y en concreto hacia al app o agente de gestión de la solución MDM, y

viceversa (permite recibir mensajes del dispositivo móvil empleando la misma conexión a través de CCS, analizado posteriormente).

535. El servicio GCM, aunque puede ser empleado por cualquier servidor y app de terceros de Android (no necesariamente para la gestión empresarial del terminal a través de las soluciones MDM), es ampliamente utilizado como plataforma para el envío de notificaciones *push* por los fabricantes de las soluciones MDM que disponen de soporte para los dispositivos móviles Android.

536. Alternativamente a las soluciones de Google, la solución MDM puede optar por emplear servidores *push* propios, como por ejemplo los utilizados por el servicio de notificaciones push de Samsung, y la app *Samsung Push Service*.

537. En la arquitectura GCM el cliente es el agente o app de gestión que ejecuta en el dispositivo móvil Android (que debe disponer al menos de la versión 2.2 o superior, y disponer de una cuenta de Google configurada en versiones previas a la 4.0.4 [Ref.- 68]), y que debe registrarse en GCM y recibir como resultado un identificador de registro. El servidor MDM implementa el protocolo GCM y se comunica con la app instalada en el dispositivo móvil a través de los servidores de conexión GCM de Google, y los servidores de conexión GCM se encargan de encolar, almacenar y reenviar (cuando el dispositivo móvil está disponible u *online*) las notificaciones entre los servidores MDM y las apps:

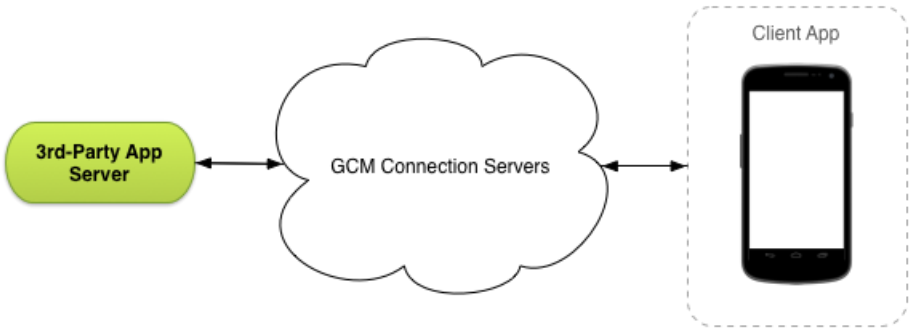

FIGURA 7.- Arquitectura de notificaciones *push* de *Google Cloud Messaging* [Ref.- 68].

538. La comunicación entre el servidor MDM y los servidores de conexión de GCM se realiza mediante HTTP [Ref.- 70], empleando conexiones cifradas HTTPS, mediante peticiones POST basadas en JSON o texto plano, hacia el servidor "https://android.googleapis.com/gcm/send.".

539. La autentificación se realiza a través de cabeceras HTTP mediante el identificador de API (API key).

540. Es necesario configurar adecuadamente los cortafuegos perimetrales corporativos para permitir el tráfico desde los servidores MDM hacia GCM en el puerto 443/tcp (HTTPS).

541. Desde el 2013 (conferencia Google IO 2013) GCM está integrado con Google Play Services, lo que permite sincronizar el estado de las notificaciones GCM entre diferentes dispositivos móviles Android de un mismo usuario.

542. Adicionalmente, debe permitirse el tráfico con GCM desde los dispositivos móviles Android para que puedan recibir las notificaciones, y en concreto los puertos TCP 5228, 5229, y 5230. Normalmente GCM sólo usa el puerto 5228, pero a veces se hace uso de los puertos 5229 y 5230. Dado que GCM no hace uso de un conjunto específico de direcciones IP, es necesario permitir en los cortafuegos conexiones salientes a todos los rangos de direcciones contenidos en el sistema autónomo (ASN) de Google número 15169 [Ref.- 70].

543. Adicionalmente, la utilización del servicio de GCM *Cloud Connection Server* (CCS) [Ref.-69] por parte de los servidores de la solución MDM permite a través de una conexión TCP permanente con los servidores de Google mediante el protocolo XMPP la comunicación con los dispositivos móviles Android, permitiendo conexiones rápidas y bidireccionales, es decir, también permite el envío de mensajes desde el dispositivo móvil hacia el servidor (*upstream*).

544. Este mecanismo de comunicación mediante XMPP puede ser usado por los servidores MDM simultáneamente a las comunicaciones estándar de GCM mediante HTTP.

545. De cara a permitir las comunicaciones del servidor MDM hacia Google, el servidor CCS está disponible en "http://gcm.googleapis.com" en el puerto 5235/tcp, siendo necesario hacer uso de cifrado mediante TLS (*Transport Layer Security*).

546. La autentificación empleada en CSS hace uso de mecanismos basados en SASL (PLAIN) empleando el identificador del emisor en GCM y el identificador de API (API key) como contraseña.

547. En general, la comunicación entre el dispositivo móvil, en concreto la app de gestión empresarial, y los servidores MDM se realiza habitualmente a través de HTTPS, con el objetivo de autentificar y cifrar la comunicación.

548. Sin embargo, algunas soluciones MDM pueden implementar sus propios mecanismos de comunicación empleando protocolos propietarios. Si este es el caso, se recomienda analizar en detalle los mecanismos de seguridad existentes en dichos protocolos.

6.2 GESTIÓN DE BLACKBERRY

549. El modelo de gestión empresarial de BlackBerry permite la aplicación granular de controles y ajustes de configuración sobre los dispositivos móviles gestionados, como por ejemplo la gestión individual de perfiles Bluetooth, forzar el cifrado completo del dispositivo móvil, establecer códigos de acceso y sus requisitos, habilitar y deshabilitar las diferentes funcionalidades hardware de los dispositivos móviles, distribuir certificados digitales, etc.

550. La gestión de los dispositivos móviles BlackBerry se puede realizar a través de las soluciones propietarias de BlackBerry, o a través de EAS.

551. La configuración inicial que permite la integración y la obtención de los datos del servidor MDM para realizar el proceso de registro en dispositivos móviles BlackBerry puede llevarse a cabo a través de su activación previa en BES y del establecimiento y utilización de las credenciales asignadas al usuario.

6.2.1 ARQUITECTURA DE GESTIÓN MDM DE BLACKBERRY

552. La arquitectura propietaria de BlackBerry, existente en sus centros de operaciones o infraestructura, se comunica por un lado con los dispositivos móviles a gestionar, y por otro con los servidores empresariales de gestión de las organizaciones, denominados BES (*BlackBerry Enterprise Server*).

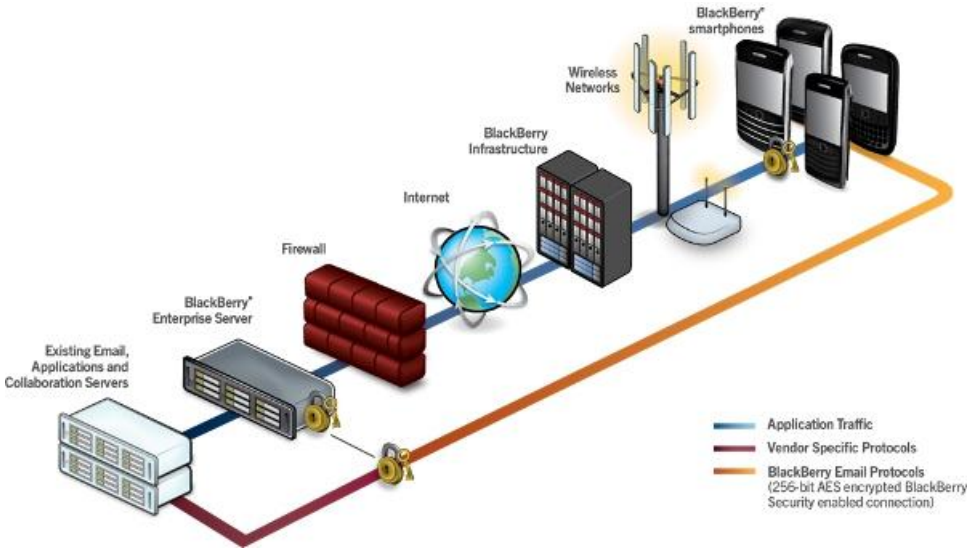

FIGURA 8.- Arquitectura de gestión de BlackBerry [Ref.- 45].

553. Los dispositivos móviles gestionados BlackBerry hacen uso del protocolo *Mobile Data Service* (MDS) para establecer comunicaciones cifradas (mediante 3DES o AES) entre ellos, la infraestructura de BlackBerry y los servidores MDM empresariales (o BES).

554. El protocolo MDS hace uso del puerto 3101/tcp para sus comunicaciones a través de redes móviles (2/3/4G) y el puerto 4101/tcp a través de redes Wi-Fi [Ref.- 43].

555. Desde el punto de vista de los cortafuegos perimetrales corporativos es necesario permitir el tráfico saliente hacia el puerto 3101/tcp desde el servidor BES hacia la infraestructura de BlackBerry.

556. Debe tenerse en cuenta que la mayoría de comunicaciones de los dispositivos BlackBerry transitan a través de la infraestructura de BlackBerry incluyendo el correo electrónico, la gestión del calendario y los contactos, y los controles de monitorización y configuración de las políticas empresariales.

557. Las únicas comunicaciones que habitualmente no pasan por la infraestructura de BlackBerry son la mensajería instantánea entre dispositivos móviles BlackBerry (conocida como "PIN to PIN", *Personal Identification Number*), los SMS y las comunicaciones de voz.

6.2.2 BLACKBERRY 10

558. Desde el lanzamiento del BlackBerry Playbook se hace un uso más intensivo de Exchange ActiveSync para las comunicaciones de mensajería en la arquitectura de BlackBerry [Ref.- 45].

559. Con la introducción de BlackBerry 10, una plataforma móvil completamente renovada respecto a BlackBerry 4.x-7.x, la arquitectura de gestión también ha sido rediseñada, basada actualmente en *BlackBerry Management Studio* (BMS; previamente BlackBerry Mobile Fusion - BMF) y sustituyendo BES (*BlackBerry Enterprise Server 5.x-7.x*) por BES (*BlackBerry Enterprise Service 10.x*)[9] [Ref.- 44].

560. Los dispositivos BlackBerry 10 disponen del *Enterprise Management Agent* (EMA), el componente o agente asociado al entorno profesional que se comunica con el servicio BES

[9] Ambos productos emplean el mismo acrónimo (BES) pero con distinto significado.

10.x para llevar a cabo todas las tareas de gestión, a través de una red VPN corporativa o una red Wi-Fi, el protocolo MDS y la infraestructura de BlackBerry.

561. La nueva arquitectura de gestión dispone de soporte para otras plataformas móviles, como Android e iOS, a través del componente *Universal Device Service* (UDS), y hace por tanto un uso más extensivo de comunicaciones HTTPS (443/tcp), junto al protocolo MDS propietario de BlackBerry.

562. Las soluciones MDM con soporte para dispositivos móviles BlackBerry, aunque pueden disponer de algunas capacidades nativas, normalmente se integran con el servidor BES ya existente para disponer de todas las capacidades de gestión disponibles a través de éste.

6.3 GESTIÓN DE iOS

563. La gestión y configuración avanzada de los dispositivos móviles iOS se realiza a través de perfiles de configuración, empleando ficheros XML (con la extensión .mobileconfig), que aprovechan las capacidades de gestión de la API de iOS definidas por Apple.

564. Los perfiles de configuración permiten establecer la política de seguridad corporativa en los dispositivos móviles iOS, así como habilitar restricciones en el uso de los mismos y ajustar diferentes parámetros de configuración.

565. Las capacidades de los perfiles de configuración están definidas en la especificación correspondiente creada por Apple [Ref.- 16], y varían en función de la versión de iOS, añadiéndose normalmente nuevas capacidades en las versiones más actualizadas de iOS (como por ejemplo en iOS 7; ver apartado "6.3.1. iOS 7").

566. Las capacidades de gestión de los dispositivos iOS para las soluciones MDM están definidas en la especificación correspondiente creada por Apple [Ref.- 17], sólo disponible para ciertas compañías proveedoras de soluciones MDM, aprobadas previamente por Apple.

567. Las soluciones MDM para iOS [Ref.- 25] en entornos empresariales, con el objetivo de aprovechar todos los mecanismos de protección disponibles en esta plataforma móvil y su integración con los sistemas de la organización [Ref.- 24], se basan en una arquitectura de gestión propia de Apple.

568. La gestión de dispositivos móviles iOS vía MDM tiene en cuenta la privacidad del usuario final, por lo que la solución MDM tiene acceso a datos como el nombre y modelo del dispositivo, número de teléfono y de serie, versión de iOS, apps instaladas, etc…, pero no dispone de acceso al correo electrónico, contactos y calendario, a los mensajes (SMS e iMessage), registro de llamadas, o ubicación del dispositivo (opcionalmente).

569. La soluciones MDM para iOS permiten llevar a cabo tres tipos de tareas principales [Ref.- 28] tras su registro inicial:

- Modificar y actualizar los ajustes de configuración de manera remota a través de la instalación, actualización y eliminación de perfiles de configuración y aprovisionamiento.

  El conjunto de ajustes de configuración disponibles está definido por Apple en función de la versión de iOS [Ref.- 28].

- Monitorizar el cumplimiento de las políticas corporativas a través de la realización de consultas sobre el dispositivo móvil.

  El tipo de información y consultas que pueden ser realizadas a través de la solución MDM está definido por Apple en función de la versión de iOS [Ref.-

28], y el servidor MDM puede determinar con qué frecuencia obtiene esta información.

- Gestionar las apps y el propio dispositivo móvil, pudiendo eliminar temporalmente el código de acceso si el usuario lo ha olvidado (debiendo fijarse uno nuevo en los siguientes 60 minutos), bloquear la pantalla de acceso o eliminar los datos almacenados en el dispositivo (*wipe*). Adicionalmente, si el dispositivo móvil no cumple con la política de la organización, ha sido robado o perdido, o el usuario deja la organización, es posible eliminar el perfil de configuración de la solución MDM, eliminando así todas las cuentas, datos, apps, y configuraciones asociadas [Ref.- 28]. Alternativamente es posible eliminar perfiles de configuración y aprovisionamiento individualmente, mientras el dispositivo móvil sigue estando gestionado.

  Los comandos de gestión que pueden ser ejecutados a través de la solución MDM están definidos por Apple en función de la versión de iOS [Ref.- 28].

570. Hasta la versión 6 de iOS, las soluciones MDM no disponen de mecanismos para evitar o detectar la instalación de perfiles de configuración adicionales por parte del usuario. Mediante estos perfiles es posible instalar, por ejemplo, certificados de desarrollador de apps en el dispositivo móvil y ejecutar, por tanto, apps no provenientes del mercado oficial de Apple.

571. Desde un punto de vista global, la especificación de gestión vía MDM de iOS permite la gestión de cuentas para el acceso a servicios corporativos, la gestión de la configuración de los dispositivos móviles, la ejecución de acciones para incrementar la seguridad del dispositivo, la instalación, gestión y eliminación de apps (públicas e *in-house*), la consulta inmediata o planificada de información sobre el dispositivo, su configuración de red y seguridad, y apps, etc.

572. A la hora de elegir una solución MDM es necesario evaluar cuáles de las diferentes capacidades disponibles en la API de iOS pueden ser configuradas y gestionadas por la solución MDM, como por ejemplo la política de seguridad del código de acceso, restricciones en el uso del hardware del dispositivo (como la cámara, la realización de llamadas, etc), restricciones en los servicios avanzados del dispositivo (Siri, FaceTime, capturas de pantalla, etc), configuración de las redes Wi-Fi, configuración de las redes VPN (L2TP, Cisco Anyconnect, Juniper, F5, etc), políticas de voz y datos en el extranjero (*roaming*), configuración de la cuenta de MS Exchange, controlar el acceso a iCloud, etc.

573. Debido a que el conjunto de capacidades de gestión de los dispositivos móviles iOS está limitado por la funcionalidad disponible en la API y la especificación de los perfiles de configuración definida por Apple, las soluciones MDM sólo pueden implementar (como máximo) ese conjunto de capacidades. Por este motivo, la funcionalidad de las soluciones MDM para iOS es muy similar entre diferentes fabricantes.

574. Algunas soluciones MDM permiten tanto la instalación de apps gestionadas (oficiales y públicas, e *in-house*), como su eliminación, e incluso poder especificar para qué apps no se debe realizar una copia de seguridad a través de iTunes o iCloud.

575. En resumen, la gestión de los dispositivos móviles iOS se puede realizar de forma local y manual, a través de EAS o a través de APNS (*Apple Push Notification Service*; ver apartado "6.3.2. ARQUITECTURA DE GESTIÓN MDM DE iOS").

576. La configuración inicial que permite la integración y la obtención de los datos del servidor MDM para realizar el proceso de registro en dispositivos móviles iOS puede llevarse a cabo a

través de un perfil de configuración (y su distribución a los usuarios), o a través de la instalación de una app asociada a la solución MDM.

6.3.1 iOS 7

577. Las capacidades de gestión a través de las soluciones MDM en iOS 7 han sido extendidas respecto a versiones previas, añadiéndose nuevas restricciones, consultas sobre qué funcionalidad está activa en el dispositivo móvil, y comandos de gestión.

578. iOS 7 [Ref.- 7] añade nuevas opciones de configuración, acciones y consultas a través de los mecanismos de gestión empresarial (MDM), como la configuración remota de apps gestionadas, la instalación de fuentes personalizadas, la configuración de opciones de accesibilidad e impresoras AirPrint, junto a la gestión de AirPlay y a la definición de destinos permitidos y/o protegidos por contraseña.

579. Versiones previas de iOS (Ej. iOS 6) permitían la instalación de apps gestionadas a través de la solución MDM, así como su posterior eliminación, o poder prevenir la realización de copias de seguridad a través de iCloud para evitar la fuga de datos corporativos.

580. iOS 7 añade nuevas capacidades para instalar apps silenciosamente en dispositivos móviles supervisados, e incluso configurar las apps remotamente (vía OTA), modificando así su comportamiento. Adicionalmente, la nueva API para las soluciones MDM dispone de comandos para obtener datos del usuario directamente (a través de los protocolos de comunicaciones MDM) de las apps y su *sandbox* asociado (mecanismo denominado *feedback*) [Ref.- 48].

581. Adicionalmente se ha automatizado el proceso de registro en la solución MDM para los dispositivos móviles iOS propiedad de la organización (no válido en entornos BYOD) durante el proceso de activación de los mismos (*streamlined device enrollment*) [Ref.- 48].

582. El nuevo proceso de registro permite a las organizaciones definir previamente como debe realizarse el registro en su solución MDM (pudiendo definir distintos criterios para dispositivos diferentes) e integrar las configuraciones asociadas (como la URL de registro del servidor MDM) en el proceso estándar de obtención de fábrica y activación de los dispositivos móviles iOS.

583. Estas gestiones se realizan a través de un nuevo servicio de Apple “en la nube” asociado a la compra y registro de dispositivos móviles iOS.

584. Cuando un nuevo dispositivo móvil iOS es recibido por la organización (vía Apple), y es activado por el usuario siguiendo los pasos del proceso de activación estándar, el usuario será preguntado por sus credenciales para proceder automáticamente al proceso de registro en la solución MDM.

585. Es posible incluso establecer que el registro en la solución MDM sea un paso obligatorio que de no ser completado, no permitirá la activación del dispositivo móvil.

586. iOS 7 ha comenzado la adopción de un modelo para poder compartimentalizar la parte profesional y personal del dispositivo móvil, y su adecuación a entornos BYOD, basado en proteger los datos corporativos y no permitir acceso a estos desde apps no aprobadas por la organización.

587. Para ello, iOS 7 emplea la tecnología denominada “Managed Open In” que permite controlar qué apps y cuentas pueden emplearse para abrir documentos y ficheros adjuntos corporativos.

588. Mediante controles de acceso en los propios documentos (datos) es posible definir dónde un documento puede ir (a qué app) o como se puede compartir, limitando así el acceso a los documentos de la organización únicamente desde las apps corporativas, y también evitando el acceso a documentos personales desde las apps gestionadas.

589. Asimismo, iOS 7 proporciona una solución de autentificación única empresarial, denominada *Enterprise Single Sign On* (SSO), para compartir y reutilizar las credenciales del usuario entre diferentes app. El modelo de integración empleado previamente en iOS 6 para compartir las credenciales de acceso a Twitter y Facebook se ha extendido a lo largo de todo el sistema y todas las apps.

590. Las credenciales para distintos servicios son almacenadas en un punto único del sistema, desde el que pueden ser (re)utilizadas por diferentes apps, siendo posible definir su uso en base a prefijos de URLs o identificadores de apps concretos.

591. Adicionalmente, iOS 7 incorpora la posibilidad de establecer una conexión VPN por app en lugar de disponer de una VPN global para todo el sistema, de forma que cuando la app gestionada es iniciada, se establece automáticamente una conexión VPN hacia la organización para la transmisión de los datos corporativos, contribuyendo así a la separación y protección de la transmisión de datos corporativos y personales.

592. Además, en la versión 7 los mecanismos de protección de datos nativos de iOS mediante cifrado están disponibles automáticamente para todas las apps, con el objetivo de proteger los datos corporativos almacenados por apps de terceros (hasta el primer desbloqueo con el código de acceso tras reiniciar el dispositivo).

6.3.2 ARQUITECTURA DE GESTIÓN MDM DE iOS

593. La gestión de dispositivos móviles iOS a través de las soluciones MDM debe hacer uso del *Apple Push Notification Service* (APNS), mecanismo de comunicación que permite al servidor MDM iniciar una conexión con el dispositivo móvil a gestionar.

594. APNS emplea la infraestructura diseñada por Apple que consiste en una serie de servidores que permiten la comunicación y el envío de mensajes (o notificaciones) entre los dispositivos móviles gestionados y los servidores de gestión o MDM de la organización.

595. En teoría, la notificación *push* es silenciosa desde el punto de vista del dispositivo móvil y no contiene datos confidenciales, sino que se emplea como mecanismo de notificación para que el dispositivo móvil contacte con el servidor MDM y compruebe las acciones pendientes de realizar.

596. Por tanto, la conexión entre el servidor MDM y el dispositivo móvil gestionado debe transcurrir obligatoriamente a través de la infraestructura y los servidores de Apple, situación que debe ser tenida en cuenta desde dos puntos de vista: confidencialidad, confiando en las comunicaciones y datos enviados por la solución MDM a través de Apple, y disponibilidad, confiando en que la infraestructura de Apple esté siempre disponible para poder realizar la gestión de los dispositivos corporativos.

597. Una vez se ha establecido la conexión entre el servidor MDM y el dispositivo móvil, se hace uso de las capacidades definidas en la especificación o *framework* correspondiente de iOS, diseñado para mantener una comunicación sin afectar significativamente el rendimiento o el consumo de batería.

598. Para que el APNS funcione adecuadamente es necesario permitir comunicaciones TCP/IP específicas entre el dispositivo móvil, la infraestructura de Apple (reflejada como APNS en la

imagen inferior [Ref.- 25]) y asociada a la clase A "17.0.0.0/8" (donde se encuentran los servidores de Apple para el servicio haciendo uso de técnicas de balanceo de carga), y el servidor MDM de la organización, a través de los cortafuegos perimetrales corporativos [Ref.- 27]:

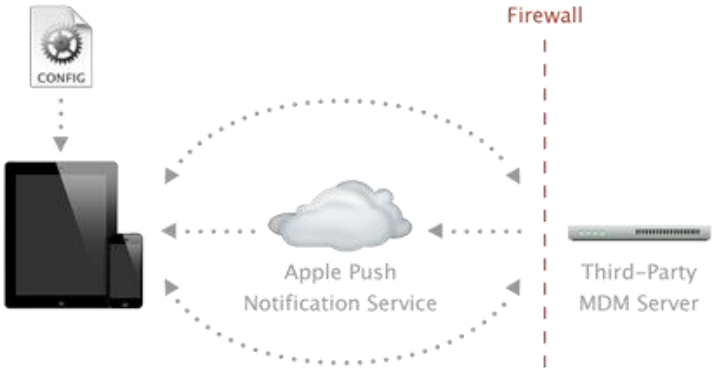

FIGURA 9.- Arquitectura de gestión de iOS [Ref.- 25]

599. Las comunicaciones TCP/IP necesarias, ya sea a través de redes Wi-Fi o de telefonía móvil (2/3/4G), para la gestión de dispositivos móviles iOS mediante APNS son [Ref.- 26]:

- Registro o suscripción (*enrollment*) en la solución MDM: iniciada por el dispositivo móvil hacia los servidores "[NN-]courier.push.apple.com" de Apple.
  - APNS emplea por defecto el puerto 5223/tcp y los contenidos se codifican a través del protocolo de mensajería XMPP (Extensible Messaging and Presence Protocol), con cifrado mediante SSL/TLS.
- Envío de mensajes (notificación *push*) vía APNS: iniciada por el servidor MDM hacia los servidores "gateway.[sandbox.]push.apple.com" de Apple.
  - Puertos 2195/tcp (notificaciones) y 2196/tcp (*feedback*) con los contenidos en formato JSON (JavaScript Object Notation) y binario, con cifrado mediante SSL/TLS.
  - El servidor de Apple con el término "sandbox" en su nombre está asociado al envío de notificaciones *push* en entornos de desarrollo.
- Comunicación desde el dispositivo móvil hacia el servidor MDM tras recibir la notificación (*push*): HTTPS (443/tcp).

600. La autentificación mutua entre las diferentes entidades que participan en las comunicaciones descritas previamente se realiza mediante certificados digitales (SSL/TLS).

601. Todos los datos de configuración de la solución MDM son proporcionados al dispositivo móvil a través de un perfil de configuración. Cuando el perfil es instalado, el dispositivo se registra (*enrollment*) en la solución MDM y pasa a estar gestionado. Cuando el servidor MDM quiere realizar una tarea o consulta en el dispositivo, envía un mensaje (notificación *push*) vía APNS, instando al dispositivo a qué compruebe las acciones pendientes de realizar. En ese momento, el dispositivo se conecta directamente al servidor MDM a través de HTTPS para recibir la consulta o las tareas a ejecutar.

602. Para hacer uso de una solución MDM para la gestión de dispositivos móviles iOS es necesario instalar un certificado digital en el propio servidor MDM, proporcionado por el fabricante de

la solución MDM y Apple[10] (*Apple Push Certificates Portal*), y necesario para establecer comunicaciones SSL/TLS con Apple a través del *Apple Push Notification Service* (APNS).

603. La obtención del certificado requiere iniciar una solicitud a través del fabricante de la solución MDM, que devolverá una *Certificate Signing Request* (CSR) firmada. Empleando la CSR y a través del *Apple Push Certificates Portal*, es posible solicitar el certificado empleando el Apple ID de la organización. Una vez obtenido, el certificado puede ser instalado en el servidor MDM para hacer uso del *Apple Push Notification Service* (APNS).

6.3.3 SOLUCIONES MDM A PEQUEÑA ESCALA PARA iOS

604. Apple distribuye un conjunto de herramientas de gestión de dispositivos móviles iOS para entornos de tamaño reducido (o a pequeña escala) [Ref.- 19], incluyendo *iPhone Configuration Utility* (iPCU), *Apple Configurator* y *Profile Manager*, disponible únicamente para Mac OS X Server.

605. Apple proporciona la herramienta iPhone Configuration Utility (iPCU) [Ref.- 20], qué también aplica a dispositivos iPad y iPod Touch pese a su nombre, para la configuración de las capacidades avanzadas y empresariales de dispositivos móviles iOS a través de perfiles de configuración y de aprovisionamiento.

606. Los perfiles de aprovisionamiento (ficheros con la extensión .mobileprovision) permiten la distribución de *in-house* apps o apps públicas oficiales que han sido adquiridas individualmente o por lotes.

607. Estos perfiles autorizan la instalación y uso de apps de ciertos desarrolladores, como la propia organización, en los dispositivos móviles gestionados.

608. iPCU está disponible para ordenadores basados en Mac OS X y en Windows, y permite la gestión local, a través del puerto USB, de dispositivos móviles iOS.

609. iPCU permite tanto la creación de perfiles de configuración como su distribución a través de diferentes métodos, incluyendo la conexión mediante USB del dispositivo móvil a gestionar (método que conlleva la firma y el cifrado del perfil), el envío del perfil a través de correo electrónico o su distribución mediante un servidor web.

610. Por defecto, los perfiles de configuración son firmados por iPCU para poder verificar su procedencia y autenticidad, junto a su integridad (para evitar modificaciones del perfil), mediante los certificados digitales de iPCU. Por tanto, la gestión de dispositivos móviles iOS mediante iPCU requiere que al menos una primera vez se haya realizado la conexión a través de USB del dispositivo al ordenador con iPCU, de forma que se establezca una relación de confianza entre ambos a través del intercambio de estos certificados digitales. Posteriormente es posible distribuir nuevos perfiles de forma remota, o previamente si los perfiles no son firmados ni cifrados (opción no recomendada desde el punto de vista de seguridad).

611. Se recomienda realizar la distribución de los perfiles de configuración a través de USB, opción más segura y que no requiere distribuir remotamente el fichero .mobileconfig.

612. Los ficheros .mobileconfig pueden contener información muy sensible, como credenciales, asociadas a la configuración de las cuentas de correo electrónico, redes Wi-Fi, conexiones VPN, etc. Es importante tener en cuenta que el fichero .mobileconfig es un fichero XML de texto sin cifrar, salvo que sea generado para un dispositivo concreto, en cuyo caso sí puede ser

[10] Apple Push Certificates Portal: https://identity.apple.com/pushcert/.

cifrado para ese dispositivo, opción más recomendada desde el punto de vista de seguridad para la distribución remota de perfiles.

613. Sin embargo, la distribución de un perfil de configuración cifrado para un dispositivo concreto dificulta la distribución de un mismo perfil a múltiples dispositivos en entornos de mediano o gran tamaño, ya que es necesario generar una versión del perfil cifrada para cada uno de los dispositivos a gestionar.

614. Una vez un perfil de configuración ha sido instalado, sólo puede ser actualizado por otro perfil con el mismo identificador (definido con notación DNS inversa en los ajustes generales del perfil) y que ha sido firmado por la misma instancia de iPCU.

615. Adicionalmente, la posibilidad de eliminar el perfil de configuración del dispositivo se define en su configuración de seguridad, pudiendo eliminarse por parte del usuario (opción no recomendada si se desea aplicar permanentemente la política de seguridad de la organización), eliminarse con autorización o contraseña (debiendo tener en cuenta que el perfil de configuración puede no estar cifrado y por tanto la contraseña estaría almacenada en claro y fácilmente accesible), o nunca, es decir, para eliminar el perfil de configuración es necesario restaurar el dispositivo móvil a los ajustes de fábrica (opción más segura).

616. En resumen, se deberían emplear perfiles de configuración que requieran conocer una contraseña para su eliminación, o que no puedan ser eliminados nunca, y su distribución se deberían realizar a través de USB, o mediante perfiles cifrados individuales si se lleva a cabo de forma remota. En el caso de emplear un servidor web para su distribución, debería ser un servidor web interno de la organización con mecanismos robustos de autentificación (sólo con acceso a los usuarios de dispositivos móviles autorizados) y cifrado (HTTPS).

617. Complementariamente, los perfiles de configuración de iOS pueden ser distribuidos vía OTA a través de las soluciones MDM comerciales o de Profile Manager (referenciado posteriormente). Las soluciones MDM permiten la gestión completa de los perfiles de configuración, incluyendo su eliminación y actualización.

618. Por otro lado, Apple proporciona la herramienta Apple Configurator [Ref.- 21], disponible a través de la Mac App Store, una herramienta de gestión que define tres tipos de flujos de trabajo o tareas: preparación o configuración de los dispositivos móviles iOS (preparar), gestión de dispositivos supervisados (supervisar), y asignación de dispositivos a usuarios (asignar).

619. La herramienta se ha diseñado principalmente para entornos empresariales de tamaño reducido como solución MDM [11] para la configuración de ajustes y apps en dispositivos móviles iOS, para la supervisión de dispositivos en centros de formación (aulas y laboratorios) y para la personalización de dispositivos con los datos y documentos de usuarios específicos.

620. Las principales ventajas de Apple Configurator frente a iPCU es que permite, también a través del puerto USB, la gestión simultánea de varios dispositivos, y la gestión de dispositivos supervisados.

621. Los dispositivos móviles iOS pueden configurarse como supervisados, es decir, dispositivos de uso controlado y limitados a una configuración estándar. Para ello se establece una relación de confianza entre el dispositivo y el ordenador con Apple Configurator (mediante certificados digitales de supervisión, SHIC - *Supervisory Host Identity Certificate*) y dónde es

[11] http://www.enterpriseios.com/wiki/Apple_Configurator_vs_MDM

posible, por ejemplo, restringir el emparejamiento o sincronización con otros ordenadores e iTunes, pudiendo así gestionar y limitar los contenidos multimedia, apps, copias de seguridad, etc.

622. Los dispositivos supervisados pueden gestionarse por grupos, con configuraciones comunes y asignación de nombres secuenciales, y pueden ser restaurados de forma rápida, incluyendo tanto la instalación de apps y ajustes de configuración, como la eliminación de datos previos.

623. La asignación de dispositivos a usuarios permite la gestión por usuarios y grupos, y la realización de copias de seguridad y restauración (incluso en otro dispositivo diferente) personalizadas, tanto de ajustes de configuración como de apps y datos, para usuarios concretos.

624. Apple Configurator permite la distribución de apps (o libros) de pago empleando códigos o bonos de pago (*redemption codes*, o URLs) adquiridos a través del *Volume Purchase Program* (VPP) de Apple [Ref.- 23]. Este programa permite la adquisición de apps (y libros) por lotes, asociadas a compras por volumen, junto a apps privadas, personalizadas y específicas para negocios (B2B) no disponibles en la App Store pública, para su posterior distribución e instalación en los dispositivos móviles de la organización (sin que los usuarios tengan que pagar individualmente por ellas).

625. En iOS 7 [Ref.- 7] [Ref.- 48] se permite la asignación temporal y remota (OTA) de apps (y libros) a usuarios a través del VPP, mientras que la organización mantiene la propiedad y el control de las licencias, pudiendo revocar las mismas en todo momento y/o asignarlas a otro usuario.

626. Se emplea por tanto más el concepto de licencia en lugar de código de pago en iOS 7 (frente a versiones previas), y se puede vincular (si se desea) su uso al proceso de instalación o eliminación de apps a través de la solución MDM.

627. Por último, Apple distribuye Profile Manager [Ref.- 22] como parte de Mac OS X Server (desde la versión Lion o superior), que a diferencia de las dos opciones previas, es un servidor MDM completo para entornos de tamaño reducido.

628. Profile Manager disponer de un portal web para la administración, monitorización y configuración de la solución MDM, un portal web de autoservicio para los usuarios, a través del cual pueden registrar sus dispositivos en la solución MDM y obtener las configuraciones adecuadas, y el propio módulo de servidor MDM qué permite la gestión remota de los dispositivos móviles iOS a través de APNS.

629. Profile Manager es una solución limitada en comparación a las soluciones MDM específicas de terceros, ya que no permite, por ejemplo, la monitorización de los dispositivos móviles, ni la generación de eventos de un dispositivo móvil concreto.

6.4 GESTIÓN DE WINDOWS PHONE

630. La plataforma móvil Windows Phone 7 estaba principalmente orientada al consumidor final, y por tanto presentaba carencias notables respecto a las capacidades de gestión empresarial y los mecanismos de seguridad disponibles.

631. Windows Phone 8, sin embargo, ha sido diseñada como una plataforma móvil que conjuga los requisitos personales y empresariales, incluyendo características necesarias desde el punto de vista de seguridad y de los mecanismos de gestión empresariales.

632. Windows Phone 8 dispone de capacidades para su integración directa con las plataformas de gestión empresarial de Microsoft, como Office 365, Microsoft Exchange y EAS [Ref.- 52].

633. Adicionalmente, Windows Phone 8 dispone de soporte para *Enterprise Device Management Protocol* [Ref.- 51] y su integración con soluciones MDM de terceros.

634. Windows Phone 8 dispone por defecto de un agente de gestión que, a través de este protocolo de gestión, puede comunicarse con los servidores MDM y llevar a cabo el proceso de registro inicial en la solución MDM (*enrollment*) mediante MS-XCEP, la instalación de una app de tipo *Company Hub* que permita el acceso al mercado de apps privado de la organización y la posterior instalación de nuevas apps aprobadas por la organización, así como la consulta de información y configuración del dispositivo móvil según las políticas de seguridad corporativas.

635. La comunicación entre Windows Phone 8 (y su agente o cliente DM, *Device Management*) y el servidor MDM se lleva a cabo a través del protocolo DM SyncML sobre HTTPS (u OMA DM XML).

636. Por un lado, el diseño de Windows Phone 8 está orientado a homogeneizar las plataformas cliente de acceso empleadas por los usuarios en entornos Microsoft, y presenta una notable tendencia a poder aplicar los mecanismos de gestión empresarial habituales en dispositivos tradicionales como las políticas de grupo (*Group Policy Objects*, GPOs) a través del directorio activo (DA) o hacer uso de plataformas como *Windows Server Update Services* (WSUS) para la distribución de actualizaciones de software.

637. Por otro lado, Microsoft también apuesta por su solución de gestión “en la nube” (o integrada con *System Center Configuration Manager*, DA o Exchange 2010) y multiplataforma (Windows RT, Windows 8, Windows Phone 8, iOS, y Android), denominada Windows Intune [Ref.- 50].

638. Por tanto, la gestión de los dispositivos móviles Windows Phone 8 se puede realizar a través de EAS o del *Enterprise Device Management Protocol*, con tendencia a la aplicación de mecanismos de gestión similares a los empleados por las políticas de grupo (GPOs) en entornos tradicionales Microsoft Windows.

639. La configuración inicial que permite la integración y la obtención de los datos del servidor MDM para realizar el proceso de registro en dispositivos móviles Windows Phone puede llevarse a cabo a través del *Enterprise Device Management Protocol* o manualmente.

7 LISTADO RESUMEN DE CARACTERÍSTICAS DE LAS SOLUCIONES MDM

640. Este apartado proporciona un listado resumen de las características comunes y recomendadas en las soluciones MDM actuales, analizadas a lo largo de la presente guía, y que deben ser evaluadas antes de la adquisición de una solución MDM.

641. Las mismas han sido clasificadas en dos categorías, en función del nivel de seguridad del entorno u organización dónde serán aplicadas, de su complejidad y de la sensibilidad y criticidad de la información que gestionan, denominadas características básicas y avanzadas.

642. Las características básicas engloban los requisitos mínimos que toda solución MDM debe proporcionar para proteger a los dispositivos móviles y poder así aplicar los mecanismos de seguridad necesarios.

643. La clasificación realizada es sólo una referencia que permita a las organizaciones analizar la variedad y complejidad de las diferentes características ofrecidas por las soluciones MDM, pero queda en mano de las propias organizaciones evaluar en detalle y determinar cuáles de todas las funcionalidades disponibles son requisito indispensable para la organización en

función de su política de seguridad, independientemente del nivel en el que se hayan englobado en la presente guía.

644. Debe tenerse en cuenta que algunas de las características mencionadas sólo aplican a ciertas soluciones MDM en función del modelo o formato empleado por éstas, como por ejemplo los mecanismos de protección del dispositivo móvil más asociados a soluciones MDM puras, frente a mecanismos de protección de los datos corporativos en entornos BYOD, más asociados a soluciones basadas en una app contenedora.

645. Antes de proporcionar la clasificación de las diferentes características en las dos categorías previamente mencionadas se resumen el resto de consideraciones generales que deben ser tenidas en cuenta antes de la adquisición de una solución MDM.

7.1 CONSIDERACIONES GENERALES

Modelo de gestión de dispositivos y apps móviles

- Dispositivos móviles aprobados: (dispositivos gestionados frente a no gestionados)
  - Dispositivos móviles corporativos únicamente.
  - COPE (*Corporataly-Owned, Personally-Enabled*).
  - CYOD (*Choose Your Own Device*).
  - BYOD (*Bring Your Own Device*).
- Apps móviles aprobadas: (apps gestionadas frente a no gestionadas)
  - Apps corporativas únicamente.
  - BYOA (*Bring Your Own App(lication)*).

Plataformas soportadas

- Plataformas móviles principales soportadas: Android, BlackBerry, iOS y Windows Phone.
- Plataformas móviles adicionales soportadas: Symbian y Windows Mobile.
- Soporte para APIs de seguridad empresariales (ej. Samsung KNOX o SAFE).
- Otras plataformas tradicionales soportadas:
  - Ordenadores portátiles, de escritorio, de pantalla táctil, etc (Windows XP/7/8/RT…, Linux y Mac OS X).
  - Impresoras, dispositivos embebidos o módulos M2M.
- Identificación de las plataformas móviles que deben ser gestionadas:
  - ¿Se hará uso de una única solución MDM multiplataforma o de la integración de múltiples soluciones MDM (algunas de ellas específicas para determinadas plataformas móviles)?

Características generales de la solución MDM

- Formato de la solución MDM: arquitectura de gestión tradicional en la propia organización (*on-premises*), servicios remotos a través de arquitecturas "en la nube" (*cloud computing, SaaS* – en la propia organización o en Internet), o un modelo híbrido.
- Modelo de la solución MDM: gestión completa del dispositivo móvil, gestión mediante una app contenedora, o ambas.
- Arquitectura modular o monolítica (incluyendo todas las capacidades MDM, MAM, MCM, etc).
- Modelo de licencias:
  - Licencias periódicas o perpetuas.
  - Por dispositivo móvil o por usuario.
- Características del contrato de soporte y mantenimiento (¿incluido en la licencia?).

- Características frente a tolerancia a fallos, carga y escalabilidad de la solución MDM.
- Características de administración de la solución MDM: interfaz web o aplicación cliente.
  - Realización de consultas y búsquedas, ejecución de acciones, visualización de alertas automáticas, etc.
- Capacidades de gestión de la solución MDM: (una o varias)
  - Gestión del dispositivo móvil (MDM)
  - Gestión de apps (MAM)
  - Gestión de contenidos (MCM)
- Integración de soluciones MDM:
  - Varias soluciones MDM particulares para cada plataforma móvil.
  - Una solución MDM multiplataforma única.
- Integración de la solución MDM con los sistemas de control de tráfico de red Wi-Fi: NAC y WIPS.
- Integración de la solución MDM con otros entornos de gestión, monitorización y administración TIC empresariales y con el servidor de correo, directorio activo u otros directorios corporativos (LDAP), *suites* de seguridad (antivirus y antimalware), etc.

Política de seguridad corporativa para los dispositivos móviles

- Requisito imprescindible (ver apartado "4.1. NORMA DE SEGURIDAD PARA LOS DISPOSITIVOS MÓVILES").

NOTA: La siguiente lista de recomendaciones aplican a cualquier app contenedora, ya sea ésta el elemento de gestión principal de la solución MDM, o un elemento complementario que proporciona un mayor nivel de seguridad al resto de capacidades de la solución MDM. Las capacidades listadas se engloban en las dos categorías mencionadas previamente, básicas y *avanzadas* (en letra cursiva para facilitar su diferenciación).

Soluciones de gestión basadas en una app contenedora

- Mecanismos de autentificación adicionales de la app contenedora:
  - *Gestión de los mecanismos de autentificación (complejidad, longitud, periodo de expiración y renovación, histórico, etc).*
  - *Mecanismos de autentificación de dos (o más) factores.*
- Cifrado de datos en reposo (al almacenarlos localmente).
- Cifrado de datos en tránsito (al enviarlos por la red).
- Sistemas de prevención de fuga de datos, imponiendo restricciones para el movimiento de datos local:
  - *Captura de pantalla.*
  - *Funcionalidad de copiar y pegar.*
  - *Envío de datos a cuentas de correo electrónico externas.*
  - *Intercambio o compartición local de datos entre apps.*
  - *Capacidades de impresión.*
- *Controles de acceso en base al tiempo (sólo se puede usar la app a ciertas horas o puede expirar llegada una fecha).*
- *Controles de acceso en base a la ubicación (sólo se puede usar la app en ciertos lugares, o lo contrario, no puede ser utilizada en ciertos lugares).*
- Funcionalidad de la app contenedora:
  - E-mail
  - Navegación web
  - Calendario

- Contactos
- Aplicaciones específicas del negocio

7.2 CARACTERÍSTICAS BÁSICAS DE LA SOLUCIÓN MDM

7.2.1 REGISTRO DE LOS DISPOSITIVOS MÓVILES EN LA SOLUCIÓN MDM

- Mecanismo de registro (*enrollment*): servicio remoto o portal web, o instalación de app o agente.
- Automatización del proceso de registro por lotes (o grupos) para el administrador TIC.
- Autentificación del usuario y del dispositivo móvil: directorio corporativo.
- Capacidades de auto-registro (*self enrollment*) del dispositivo móvil por parte del usuario:
  - Portal web para el proceso de registro, complementado con documentación y manuales de usuario.

7.2.2 INVENTARIO Y MONITORIZACIÓN

Inventario de los dispositivos y apps móviles

- Inventario de los dispositivos móviles (*hardware* y *software*):
  - Fabricante y modelo.
  - Capacidades hardware.
  - Versión de sistema operativo.
- Registro de identificadores de los dispositivos móviles: número de serie, IMEI, número de teléfono, IMSI, etc.
- Capacidades de consulta y búsqueda:
  - Tiempo real (actualizadas permanentemente) y bajo demanda.
  - Históricos (estadísticas).
  - Periodicidad establecida.
- Criterios de consulta: (ejemplos)
  - Nombre de usuario.
  - Nombre del grupo de usuarios.
  - Tipo de dispositivo o plataforma móvil.
  - Versión de sistema operativo.

Monitorización de los dispositivos y apps móviles

- Detección de violaciones en la política de seguridad de la organización.
- Acciones tras la detección de una violación en la política de seguridad:
  - Generación de alertas automáticas: consola de la solución MDM, SNMP, e-mail, SMS, etc.
    - Alertas personalizables.
- Panel de control (*dashboard*) con información en tiempo real.
- Capacidad de Establecer auditorias de los usos de las aplicaciones móviles.
- Monitorización de:
  - La versión de sistema operativo y actualizaciones de seguridad instaladas en los dispositivos móviles.
- La política de seguridad aplicada en los dispositivos móviles por usuario individual y/o por grupo de usuarios y/o por dispositivo móvil.Capacidades de monitorización y registro (logs) de la propia solución MDM.

Generación de informes y estadísticas

- Generación de informes bajo demanda o planificados:
  - Formatos: XML, CSV, HTML, PDF, texto, etc.
- Generación de estadísticas a nivel de dispositivo móvil.
- Generación de estadísticas a nivel de app.

7.2.3 CONFIGURACIÓN DE LOS DISPOSITIVOS MÓVILES

Gestión y restricciones del hardware del dispositivo móvil

- Deshabilitar la cámara.
- Deshabilitar el módulo GPS y las capacidades de localización (vía satélites GPS, redes Wi-Fi y torres de telefonía móvil).
- Deshabilitar el interfaz NFC.
- Deshabilitar el interfaz Bluetooth.
- Deshabilitar el interfaz Wi-Fi.

7.2.4 MECANISMOS DE SEGURIDAD

Gestión de las políticas de seguridad corporativas

- Definición y asignación de políticas de seguridad (vía OTA) por dispositivo móvil y/o por tipo de dispositivo móvil y/o por usuario individual y/o por grupo de usuarios.
- Gestión de versiones de la política de seguridad.

Mecanismos de protección y seguridad

- Forzar la utilización de un código (o mecanismo) de acceso al dispositivo móvil.
- Definir el tipo de código (o mecanismo) de acceso a emplear:
  - PIN, contraseña, patrón de desbloqueo o desbloqueo mediante una imagen.
- Definir los requisitos del código (o mecanismo) de acceso:
  - Longitud, complejidad, periodo de expiración y renovación, histórico, etc.
- Definir el periodo de tiempo de inactividad para el bloqueo automático del dispositivo móvil.
- Definir el periodo de gracia en el que no será necesario introducir un código de acceso tras el bloqueo (automático o manual) del dispositivo móvil.
- Definir el número de intentos de acceso fallidos para llevar a cabo el borrado completo (*wipe*) del dispositivo móvil.
- Bloqueo remoto del dispositivo móvil.
- Deshabilitar el código de acceso actual remotamente.
- Borrado remoto completo (*wipe*) del dispositivo móvil.
- Capacidad de localización de la ubicación física del dispositivo móvil:
  - Puntual.
  - Seguimiento permanente (*tracking*).
- Cifrado completo del dispositivo móvil.
- Cifrado de las tarjetas de almacenamiento externas (ej. *SD card*).
- Gestión de certificados digitales:
  - Certificados digitales personales y certificados digitales de confianza (CA's).
  - Certificados digitales para servicios concretos.
  - Gestión de certificados digitales revocados.

  - Funcionalidad de los certificados digitales: redes Wi-Fi y VPN, navegación web, e-mail y S/MIME, EAS, comunicación con la solución MDM, etc
  - Gestión de certificados a nivel de sistema y/o por app individual.
- Capacidades de CA en la solución MDM:
  - Emisión, registro y gestión de certificados digitales propia.
  - Integración con otras CA's externas.
  - Servidor SCEP propio o integración con servidor SCEP externo.
- Gestión de actualizaciones del sistema operativo de la plataforma móvil (vía OTA).
- Gestión de actualizaciones de la app contenedora o agente MDM (vía OTA).
- Gestión de actualizaciones de todas las apps instaladas en el dispositivo móvil (vía OTA).

7.2.5 GESTIÓN DE LAS COMUNICACIONES

- Configuración de los ajustes de conectividad para las diferentes tecnologías e interfaces de comunicaciones inalámbricas:
  - NFC.
  - Bluetooth.
  - Redes Wi-Fi.
  - Redes de telefonía móvil 2/3/4G (APNs).
  - Redes VPN.
- Configuración de un proxy global para todas las comunicaciones de datos.
- Cifrado de las comunicaciones entre la solución MDM y el dispositivo móvil (OTA):
  - Análisis de los protocolos y algoritmos de cifrado empleados.

Bluetooth

- Restringir el estado del interfaz Bluetooth a no visible u oculto.
- Gestión de la configuración Bluetooth: nombre, etc.

Wi-Fi

- Definir el tipo de redes Wi-Fi permitidas: infraestructura, *ad-hoc*, o ambas.
- Gestión avanzada de la configuración de las redes WPA y WPA2 Empresariales.

Telefonía móvil 2/3/4G

- Habilitar o deshabilitar de forma independiente las comunicaciones de voz (y SMS/MSM) y las comunicaciones de datos (2/3/4G).
- Control del gasto de los servicios de telefonía móvil.
- Permitir la configuración y gestión de un APN (*Access Point Name*) privado.

VPNs

- Gestión de la configuración de las conexiones VPN globales al dispositivo móvil.

7.2.6 GESTIÓN DE APPS

Gestión de correo electrónico

- Capacidades de integración con plataformas, soluciones y servidores de correo electrónico empresariales.
- Configuración segura de las cuentas de correo electrónico (e-mail).

Gestión de apps (MAM)

- Gestión del uso y limitaciones para la instalación de apps desde los mercados públicos oficiales:
  - Mercados oficiales de los fabricantes y/o mercados oficiales de terceros.
  - Restringir la instalación de apps de mercados de terceros no oficiales y fuentes no fiables.
- Gestión y autorización de apps: listas blancas, listas negras y lista de apps requeridas por la organización.
- Gestión del mercado corporativo de apps de la organización:
  - Conjunto de plataformas móviles soportadas: ¿disponibilidad de funcionalidad avanzada para cada una de ellas?
  - Gestión única (o complementaria) de *in-house* apps o *line-of-business* (LOB) apps.
  - Capacidades para la distribución de actualizaciones de apps previamente instaladas.
  - Establecer controles y políticas más avanzadas para la disponibilidad, instalación y uso de apps en función del perfil del usuario.
    - Disponibilidad y distribución de apps individuales o conjuntos de apps por usuario individual y/o por grupo y/o por dispositivo móvil y/o por tipo de dispositivo móvil.
- Gestión de apps corporativas en dispositivos móviles personales y gestión de apps personales en dispositivos móviles corporativos.

Gestión de contenidos y datos corporativos (MCM)

- Capacidades para restringir con qué otros equipos locales puede sincronizarse el dispositivo móvil (USB o conexión inalámbrica).
- Capacidades de prevención de fuga de datos (*Data Loss Prevention*, DLP):
  - Datos gestionados por las apps.
  - Sincronización desde las apps hacia servicios "en la nube".
  - Ficheros adjuntos en correos electrónicos (e-mail).

7.3 CARACTERÍSTICAS AVANZADAS DE LA SOLUCIÓN MDM

7.3.1 REGISTRO DE LOS DISPOSITIVOS MÓVILES EN LA SOLUCIÓN MDM

- Soporte para el protocolo SCEP (*Simple Certificate Enrollment Protocol*).
- Portal web para la autogestión (*self management*) del dispositivo móvil por parte del usuario:
  - Cambio del código de acceso.
  - Bloqueo remoto del dispositivo móvil.
  - Borrado remoto del dispositivo móvil (*wipe*).

7.3.2 INVENTARIO Y MONITORIZACIÓN

Inventario de los dispositivos y apps móviles

- Inventario de los dispositivos móviles (*hardware* y *software*):
  - Operador de telecomunicaciones.
  - Estado de la configuración: general y de seguridad.
  - Estado de los módulos o componentes hardware.
- Inventario de las apps:
  - Distribución de las apps y versiones específicas instaladas por dispositivo móvil.
- Inventario de los contenidos corporativos:
  - Distribución de los contenidos corporativos y versiones específicas.
- Criterios de consulta: (ejemplos)
  - Nombre y versión especifica de la app.
  - Operador de telecomunicaciones.
  - Términos de búsqueda flexibles.

Monitorización de los dispositivos y apps móviles

- Acciones tras la detección de una violación en la política de seguridad:
  - Notificación automática al dispositivo móvil del usuario o administrador TIC.
  - Eliminación remota de datos selectiva o completa (*wipe*).
  - Restricción del acceso del dispositivo móvil a los servicios y datos corporativos.
  - Respuesta automática ante alertas: ejecución de acciones personalizables.
- Generación de alertas frente a eventos personalizables (cuando no es posible contactar con un dispositivo móvil, cuando el dispositivo está siendo usado en el extranjero (*roaming*), cuando se detecta un intento de instalación de una app no permitida, etc).
- Capacidades de monitorización para diferenciar y filtrar datos personales de datos corporativos.
- Monitorización de:
  - Los ajustes de configuración individuales de los dispositivos móviles.
  - El uso de las comunicaciones móviles: NFC, Bluetooth, Wi-Fi, 2/3/4G, etc.
  - El nivel de actualización de los dispositivos móviles de la organización para una app determinada.
  - El uso de cada app y del almacenamiento y transferencia de los contenidos corporativos gestionados por la app.
  - Contenidos y datos corporativos, incluyendo la versión de cada documento.
- Capacidades de análisis del rendimiento del dispositivo móvil, incluyendo apps, redes Wi-Fi y redes de telefonía móvil, y notificación mediante alertas proactivas.
- Recepción de los logs de los dispositivos móviles.

Generación de informes y estadísticas

- Generación de informes bajo demanda o planificados:
  - Disponibilidad de plantillas predefinidas.
- Generación de estadísticas a nivel de contenidos.

7.3.3 CONFIGURACIÓN DE LOS DISPOSITIVOS MÓVILES

Gestión y restricciones del hardware del dispositivo móvil

- Deshabilitar el micrófono.
- Deshabilitar las tarjetas de almacenamiento externas (ej. *slot SD card*).

- Deshabilitar o restringir las capacidades de conexión a través del puerto USB:
  - Lista de equipos permitidos a través de la conexión USB.
- Deshabilitar el interfaz de telefonía móvil (2/3/4G):
  - SMS/MMS y voz.
  - Datos.
  - Datos compartidos con otros dispositivos (*tethering*).

Gestión del software (apps y servicios) existente por defecto en el dispositivo móvil

- Deshabilitar apps y servicios disponibles por defecto en la plataforma móvil:
  - Navegador web, cliente de correo electrónico, gestión de contactos y calendario, etc.
- Deshabilitar apps (existentes por defecto o de terceros) que permiten la grabación de voz y su envío a través de Internet.
- Gestión de otros dispositivos conectados directamente al dispositivo móvil (vía conexión inalámbrica, como por ejemplo Bluetooth, o vía USB):
  - Impresoras, escáneres, proyectores, ordenadores, manos libres, altavoces, etc.

7.3.4 MECANISMOS DE SEGURIDAD

Gestión de las políticas de seguridad corporativas

- Definición de políticas de seguridad permanentes o temporales (con fecha de comienzo y expiración).
- Definición de políticas de seguridad dependientes del tiempo o de la ubicación.
- Portal web de autogestión que permita al usuario comprobar si sus dispositivos móviles cumplen con la política de seguridad de la organización, y en caso de no hacerlo, el motivo asociado.
- Modelo de eliminación de la política de seguridad: estado previo (*rollback*) o borrado completo (*wipe*).

Mecanismos de protección y seguridad

- Definir el número de intentos de acceso fallidos para bloquear el acceso del dispositivo móvil, y/o el usuario asociado, a los servicios y datos corporativos.
- Modificar el valor del código de acceso actual remotamente.
- Forzar de forma remota al dispositivo móvil a emitir un sonido (a través de las capacidades de gestión) que permita su localización.
- Enviar de forma remota al dispositivo móvil un mensaje (a través de las capacidades de gestión) que permita proporcionar información del propietario para su localización o devolución.
- Borrado remoto selectivo de datos del dispositivo móvil.
- Establecimiento de otros escenarios automáticos para realizar el borrado remoto, selectivo o completo, del dispositivo móvil, como por ejemplo disponer de un sistema operativo significativamente desactualizado o incumplir la política de seguridad durante más de un periodo de tiempo determinado.
- Capacidades para iniciar un borrado remoto automático si el dispositivo móvil no ha establecido comunicación alguna con la solución MDM durante un periodo de tiempo determinado.
- Solución “virtual” de borrado de datos en el acceso a los servicios corporativos, no permitiendo su acceso a través de un cortafuegos de aplicación o de datos, por ejemplo, al correo electrónico.

- Capacidad para deshabilitar o restringir la utilización de los servicios de localización por app o elemento hardware (por ejemplo, desde la cámara).
- Definición de políticas de cifrado de datos a nivel de apps.
- Capacidad de integración con entornos colaborativos y plataformas, soluciones y servidores empresariales para la compartición de documentos.
- Mecanismos de detección del proceso de *jailbreak* (iOS) o *root* (Android).
- Ejecución de acciones automáticas tras la identificación del proceso de *jailbreak* o *root*.
- Capacidades de integración con cortafuegos y soluciones antivirus/antimalware para dispositivos móviles (*con limitaciones significativas de las plataformas móviles*).

7.3.5 GESTIÓN DE LAS COMUNICACIONES

- Gestión de las comunicaciones de datos: sólo a través de redes Wi-Fi frente a redes de telefonía móvil 2/3/4G:
  - ¿Cuándo, dónde y por qué?

NFC

- Capacidad para habilitar o deshabilitar el interfaz NFC, así como para gestionar los servicios asociados, como por ejemplo Android Beam.

Bluetooth

- Restringir y configurar los perfiles Bluetooth disponibles.
  - Configuración independiente de los mecanismos de autentificación y autorización de cada perfil.
  - Restringir la posibilidad de realizar nuevos emparejamientos vía Bluetooth.
- Gestión de los dispositivos Bluetooth emparejados (ej. impresoras, manos libres, etc).
- Política de seguridad sobre el PIN empleado durante los emparejamientos Bluetooth: requisitos mínimos de longitud, complejidad, etc.
- Capacidades de gestión y borrado selectivo periódico de la base de datos de dispositivos emparejados.
- Requisitos relativos a la versión de la especificación Bluetooth a emplear (versión 2.1 o superior: SSP).

Wi-Fi

- Definir un conjunto determinado, lista blanca, de redes Wi-Fi a las que pueden conectarse los dispositivos móviles gestionados.
- Deshabilitar el establecimiento automático de conexiones a redes Wi-Fi conocidas.
- Restringir la conexión a redes Wi-Fi inseguras: sin cifrado (abiertas) o con cifrado WEP.
- Política de seguridad sobre la contraseña empleada para la conexión a redes WAP y WPA2 Personal: requisitos mínimos de longitud, complejidad, etc.
- Gestión de la base de datos de redes Wi-Fi conocidas (PNL).
  - Identificar y permitir editar qué redes Wi-Fi son ocultas y cuáles son visibles.
- Gestión de la funcionalidad de punto de acceso Wi-Fi del dispositivo móvil.

Telefonía móvil 2/3/4G

- Datos compartidos con otros dispositivos (*tethering*):
  - Restringir los métodos de *tethering* permitidos (Bluetooth, Wi-Fi y/o USB) y los ajustes de seguridad de las redes de comunicaciones asociadas.

- Seleccionar el tipo de red de telefonía móvil: 2G ó 3/4G (tanto para voz como para datos).
- Gestionar los parámetros de conectividad en el extranjero (*roaming*):
  - Voz y SMS
  - Datos

VPNs

- Gestión de conexiones VPN por app (o VPNs selectivas).

7.3.6 GESTIÓN DE APPS

Gestión de correo electrónico

- Cifrado local de los mensajes de correo electrónico.
- Cifrado local de los ficheros adjuntos a los mensajes de correo electrónico.
- Gestión de ficheros adjuntos integrada con una solución de gestión de contenidos para su almacenamiento y acceso seguro.
- Controles sobre los ficheros adjuntos para no permitir su recepción o envío según su tipo.
- Bloquear las operaciones de copiar y pegar, o las operaciones de impresión, desde el cliente de correo electrónico.
- Bloquear el acceso a la cuenta de correo electrónico del usuario si su dispositivo móvil no cumple la política de seguridad corporativa o si éste deja la organización.

Gestión de navegación web

- Configuración granular del navegador web, por ejemplo, para deshabilitar ajustes como el aceptar cookies de terceros o el motor de JavaScript.
- Capacidades para la creación y distribución de *web clips*.
- Permitir la creación de listas blancas y negras de navegación web.

Gestión de apps (MAM)

- Gestión del mercado corporativo de apps de la organización:
  - Gestión de licencias y compras.
  - Distribución automática de apps por intervalos de tiempo (ej. cada "x" horas), o por evento (ej. al producirse una situación determinada).
  - Instalación automática de las apps gestionadas en los dispositivos móviles sin intervención por parte del usuario.
  - Eliminación remota de una app de uno o múltiples dispositivos móviles.
- Gestión y autorización de los permisos necesarios para una app determinada (según la plataforma móvil).
- Gestión de software y apps no sólo para las plataformas móviles, sino también para los dispositivos más tradicionales.
- Integración con servicios de reputación de las aplicaciones móviles.
- Bloqueo de la ejecución de una app si el dispositivo móvil no cumple con la política de seguridad corporativa.
- Disponibilidad de kits de desarrollo (SDKs) y librerías (o APIs) para el desarrollo de apps seguras:
  - Autentificación, cifrado, *geofencing*, intercambio seguro de datos, etc.
- Disponibilidad de plataformas que permite englobar o envolver (*wrapping*) las apps ya existentes mediante librerías de seguridad específicas.

Gestión de contenidos y datos corporativos (MCM)

- Deshabilitar la realización de copias de seguridad hacia servicios "en la nube" o hacia dispositivos locales (USB o conexión inalámbrica):
  - Posibilidad de diferenciar entre datos corporativos y personales.
- Integración con soluciones de gestión de contenidos corporativos que proporcionen un repositorio seguro para la compartición y distribución de contenidos:
  - Creación de contenidos corporativos temporales, con un tiempo de expiración definido.
  - Distribución automática de datos corporativos (*push*) asociados a una por intervalos de tiempo (ej. cada "x" horas), o por evento (ej. al producirse una situación determinada).
  - Bloqueo del acceso a los datos y contenidos corporativos por parte de dispositivos móviles que violen la política de seguridad de la organización.
- Bloquear las operaciones de copiar y pegar, de impresión, o de compartición de datos entre apps.
- Capacidades de gestión de la funcionalidad "Open In": controles de acceso para definir en qué apps o servicios de la plataforma móvil es posible abrir (o acceder a) un documento concreto.
- Contenedor cifrado para almacenar documentos sensibles.
- Capacidades de gestión de la utilización de contenidos desde los dispositivos móviles sin conexión al repositorio compartido (*offline*).
- Restricciones en el acceso a los contenidos: autentificación de dos o más factores, *geofencing*, o según el tipo de conexión de datos empleada.
- Acceso virtualizado a aplicaciones, servicios o escritorios remotos corporativos.

8 APÉNDICE A: FABRICANTES DE SOLUCIONES MDM

Lista ordenada alfabéticamente con algunos de los fabricantes de soluciones MDM actuales (teniendo en cuenta que no es exhaustiva; más referencias en [Ref.- 10] - [Ref.- 14]):

Absolute Software
Afaria (SAP/Sybase)
AirWatch
Amtel
BlackBerry
BoxTone
Dialogs Smartman (Sophos)
Excitor
FancyFon
Fiberlink MaaS360
Good Technology
IBM Tivoli
Kaseya
Kaspersky Lab
LANDesk
McAfee
Meraki
Mobile Active Defense
MobileIron
Odyssey (Symantec)
RhoGallery
Sophos Mobile Control
Soti
Symantec
Tangoe
Trend Micro
Unwired Revolution DeviceLink
Zenprise (Citrix)

9 APENDICE B: LISTA DE RECOMENDACIONES DE SEGURIDAD PARA LA GESTIÓN DE DISPOSITIVOS MÓVILES

La siguiente tabla incluye una lista con las diferentes características de las soluciones MDM y las recomendaciones descritas a lo largo de la presente guía, incluyendo tanto los ajustes de configuración de gestión o seguridad disponibles, como los valores más recomendados (siempre teniendo en cuenta que los valores a aplicar serán dependientes de la política de seguridad definida por la organización).

AJUSTE DE CONFIGURACIÓN	VALOR RECOMENDADO
Consideraciones generales	
Modelo de gestión de dispositivos y apps móviles	
Dispositivos móviles aprobados	Corporativos COPE CYOD BYOD
Apps móviles aprobadas	Corporativas BYOA
Plataformas soportadas	
Plataformas soportadas	Android (obligatorio) BlackBerry (obligatorio) iOS (obligatorio) Win Phone (*recomendado*) *Win Mobile* (*recomendado*) *Symbian* (*recomendado*) Otros (*recomendado*)
Soporte para APIs de seguridad empresariales	Obligatorio
Otras plataformas tradicionales soportadas	Windows Linux Mac OS X
Características generales de la solución MDM[12]	
Formato de la solución MDM	On-premises En la nube (*cloud*) Híbrido
Modelo de la solución MDM	Dispositivo móvil App contenedora Ambas
Arquitectura de la solución MDM con capacidades de gestión...	MDM MAM MCM
Soluciones de gestión basadas en una app contenedora	

[12] Ver resumen de las capacidades adicionales de las soluciones MDM en el apartado "**¡Error! No se encuentra el origen de la eferencia.**. **¡Error! No se encuentra el origen de la referencia.**", no incluidas en la presente tabla.

Mecanismos de autentificación adicionales de la app contenedora	Código de acceso
Gestión de los mecanismos de autentificación de la app contenedora	Complejidad Longitud Expiración Histórico
Mecanismos de autentificación de dos (o más) factores	*Recomendado*
Cifrado de datos en reposo (al almacenarlos localmente)	Obligatorio
Cifrado de datos en tránsito (al enviarlos por la red)	Obligatorio
Sistemas de prevención de fuga de datos	Obligatorio
Controles de acceso en base al tiempo o a la ubicación	*Recomendado*
Funcionalidad de la app contenedora	E-mail Navegación web Calendario Contactos Apps negocio
Registro de los dispositivos móviles en la solución MDM	
Mecanismo de registro (*enrollment*)	Portal web App o agente
Automatización del proceso de registro por lotes (o grupos)	*Recomendado*
Autentificación del usuario y del dispositivo móvil	Obligatorio
Capacidades de auto-registro (*self enrollment*) del dispositivo móvil	Obligatorio
Soporte para el protocolo SCEP (*Simple Certificate Enrollment Protocol*)	*Recomendado*
Portal web para la autogestión (*self management*) del dispositivo móvil por parte del usuario	*Recomendado*
Inventario	
Inventario de los dispositivos móviles (*hardware* y *software*)	Obligatorio
Registro de identificadores de los dispositivos móviles	Obligatorio
Capacidades de consulta y búsqueda	Obligatorio
Inventario de las apps	Obligatorio
Inventario de los contenidos corporativos	*Recomendado*
Monitorización	
Detección de violaciones en la política de seguridad de la organización	Obligatorio
Acciones tras la detección de una violación en la política de seguridad	*Recomendado*
Monitorización detallada de ajustes, uso de capacidades, etc	*Recomendado*
Generación de alertas frente a eventos personalizables	Obligatorio
Generación de informes y estadísticas	*Recomendado*
Gestión y restricciones del hardware del dispositivo móvil	
Deshabilitar: cámara, módulo GPS, NFC, Bluetooth, Wi-Fi, micrófono, tarjetas almacenamiento externas, puerto USB, telefonía móvil, etc	*Recomendado*
Gestión del software existente por defecto	
Deshabilitar apps y servicios disponibles por defecto	Obligatorio
Gestión de otros dispositivos conectados directamente al dispositivo	*Recomendado*
Gestión de las políticas de seguridad corporativas	
Definición y asignación granular de políticas de seguridad	Obligatorio

Gestión de versiones de la política de seguridad	Obligatorio
Definición de políticas de seguridad permanentes o temporales, dependientes del tiempo o de la ubicación	*Recomendado*
Capacidades de gestión de eliminación de la política de seguridad	Obligatorio
Mecanismos de protección y seguridad	
Imposibilidad del usuario de actuar sobre las acciones del MDM (enrrollment, aplicación de políticas, eliminación del agente) sin autorización del administrador.	Obligatorio[13]
Forzar la utilización de un código (o mecanismo) de acceso	Obligatorio
Tipo de código (o mecanismo) de acceso a emplear	Contraseña (*recomendado*) PIN (obligatorio)
Requisitos de la contraseña de acceso (*recomendado*): - Longitud: - Complejidad: - Periodo de expiración y renovación: - Histórico	 6 caracteres Números y letras Anual Últimos tres
Requisitos del PIN de acceso (obligatorio): - Longitud: - Complejidad: - Periodo de expiración y renovación: - Histórico	 6 caracteres Números Anual Últimos tres
Periodo de tiempo de inactividad para el bloqueo automático del dispositivo móvil	1-5 minutos
Definir el periodo de gracia en el que no será necesario introducir un código de acceso tras el bloqueo (automático o manual) del dispositivo móvil	1 minuto
Definir el número de intentos de acceso fallidos para llevar a cabo el borrado completo (*wipe*) del dispositivo móvil	Obligatorio
Número de intentos de acceso fallidos para bloquear el acceso del dispositivo móvil, y/o el usuario, a los servicios y datos corporativos	Obligatorio
Bloqueo remoto del dispositivo móvil	*Recomendado*
Borrado remoto selectivo de datos del dispositivo móvil	Obligatorio
Borrado remoto completo (*wipe*) del dispositivo móvil	Obligatorio
Capacidades para iniciar un borrado remoto automático si no ha establecido conexión alguna con la solución MDM durante un periodo de tiempo	*Recomendado*
Forzar de forma remota al dispositivo móvil a emitir un sonido (a través de las capacidades de gestión) que permita su localización	*Recomendado*
Enviar de forma remota al dispositivo móvil un mensaje de notificación	*Recomendado*
Capacidad para deshabilitar o restringir la utilización de los servicios de localización por app o elemento hardware	Obligatorio
Capacidad de localización de la ubicación física del dispositivo	Obligatorio

[13] Puede no ser posible para ciertos sistemas operativos móviles.

móvil	
Cifrado completo del dispositivo móvil	Obligatorio
Cifrado de las tarjetas de almacenamiento externas	Obligatorio
Gestión de certificados digitales	Obligatorio
Gestión de actualizaciones del SO de la plataforma móvil (vía OTA)	Obligatorio
Gestión de actualizaciones de la app contenedora MDM (vía OTA)	Obligatorio
Gestión de actualizaciones de todas las apps instaladas (vía OTA)	Obligatorio
Mecanismos de detección del proceso de *jailbreak* (iOS) o *root* (Android)	Obligatorio
Ejecución de acciones automáticas tras la identificación del proceso de *jailbreak* o *root*	Obligatorio
Capacidades de integración con cortafuegos y soluciones antivirus/antimalware para dispositivos móviles	*Recomendado*
Gestión de las comunicaciones	
Configuración de los ajustes de conectividad	NFC Bluetooth Wi-Fi Telefonía móvil VPN
Configuración de un proxy global para todas las comunicaciones de datos	Obligatorio[14]
Cifrado de las comunicaciones entre la solución MDM y el dispositivo móvil (OTA)	Obligatorio
Gestión de las comunicaciones de datos: Wi-Fi vs. telefonía móvil	*Recomendado*
NFC	
Gestión del interfaz NFC y los servicios asociados	*Recomendado*
Bluetooth	
Restringir el estado del interfaz Bluetooth a no visible u oculto	Obligatorio
Gestión de la configuración Bluetooth	Obligatorio
Restringir y configurar los perfiles Bluetooth disponibles	*Recomendado*
Gestión de los dispositivos Bluetooth emparejados	*Recomendado*
Política de seguridad sobre el PIN de emparejamientos Bluetooth	*Recomendado*
Wi-Fi	
Definir el tipo de redes Wi-Fi permitidas	Obligatorio
Gestión avanzada de las redes WPA(2) Empresariales	Obligatorio
Definir listas blancas de redes Wi-Fi	*Recomendado*
Restringir la conexión a redes Wi-Fi inseguras	*Recomendado*
Gestión de la base de datos de redes Wi-Fi conocidas (PNL)	Obligatorio
Gestión de la funcionalidad de AP Wi-Fi del dispositivo móvil	*Recomendado*
Telefonía móvil	
Gestión independiente las comunicaciones de voz y datos	Obligatorio
Permitir la configuración y gestión de un APN privado	Obligatorio
Gestión de *tethering*	*Recomendado*
Seleccionar el tipo de red de telefonía móvil: 2G ó 3/4G (voz y datos)	*Recomendado*
VPNs	

[14] Puede no ser posible para ciertos sistemas operativos móviles.

Gestión de la configuración de las conexiones VPN	Obligatorio
Gestión de conexiones VPN por app (o VPNs selectivas)	*Recomendado*
Gestión de apps	
Gestión de correo electrónico	
Configuración segura de las cuentas de correo electrónico (e-mail)	Obligatorio
Cifrado local de los mensajes (y ficheros adjuntos) de correo electrónico	Obligatorio
Gestión de ficheros adjuntos integrada con una solución de gestión de contenidos (MCM) y según su tipo	*Recomendado*
Bloquear las operaciones de copiar y pegar, o las operaciones de impresión, desde el cliente de correo electrónico	*Recomendado*
Bloquear el acceso a la cuenta de correo electrónico del usuario si su dispositivo móvil no cumple la política de seguridad corporativa	*Recomendado*
Gestión de navegación web	
Configuración granular del navegador web	Obligatorio
Permitir la creación de listas blancas y negras de navegación web	*Recomendado*
Gestión de apps (MAM)	
Gestión del uso y limitaciones para la instalación de apps desde los mercados públicos oficiales (principal y terceros)	Obligatorio
Gestión y autorización de apps: listas blancas y listas negras	Obligatorio
Gestión del mercado corporativo de apps de la organización	*Recomendado*
Bloqueo de la ejecución de una app si el dispositivo móvil no cumple con la política de seguridad corporativa	*Recomendado*
Gestión de contenidos y datos corporativos (MCM)	
Capacidades para restringir con qué otros equipos locales puede sincronizarse el dispositivo móvil (USB o conexión inalámbrica)	Obligatorio
Capacidades de prevención de fuga de datos	Obligatorio
Deshabilitar la realización de copias de seguridad hacia servicios “en la nube” o hacia dispositivos locales	Obligatorio
Integración con soluciones de gestión de contenidos corporativos que proporcionen un repositorio seguro para la compartición y distribución de contenidos	*Recomendado*
Bloquear las operaciones de copiar y pegar, de impresión, o de compartición de datos entre apps	Obligatorio
Capacidades de gestión de la funcionalidad “Open In”	*Recomendado*
Contenedor cifrado para almacenar documentos sensibles	Obligatorio

10 REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:

Referencia	Título, autor y ubicación
[Ref.- 1]	"Guía CCN-STIC-450: Seguridad de dispositivos móviles". CCN-CERT. 2010. URL: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/450-Seguridad_Dispositivos_Moviles/450_SEGURIDAD_EN_DISPOSITIV.PDF
[Ref.- 2]	Android. Google. URL: http://www.android.com Android Open Source Project (AOSP). URL: http://source.android.com
[Ref.- 3]	BlackBerry. URL: http://www.blackberry.com
[Ref.- 4]	iOS. Apple. URL: http://www.apple.com/iphone/ios/
[Ref.- 5]	Windows Phone. Microsoft. URL: http://www.windowsphone.com
[Ref.- 6]	"Duress Notification Address IT policy rule". BlackBerry. URL:http://docs.blackberry.com/en/admin/deliverables/4222/Duress_Notification_Address_204132_11.jsp
[Ref.- 7]	"iOS 7 and business". Apple. URL: https://www.apple.com/ios/ios7/business/
[Ref.- 8]	"Microsoft Exchange ActiveSync". Exchange 2013. Microsoft. URL: http://technet.microsoft.com/es-es/library/aa998357%28v=exchg.150%29.aspx
[Ref.- 9]	"Microsoft System Center Mobile Device Manager (MSCMDM)". Microsoft. URL: http://technet.microsoft.com/es-es/systemcenter/bb968863.aspx URL: https://blogs.technet.com/b/keithmayer/archive/2012/12/03/managing-mobile-devices-with-system-center-2012-configuration-manager-sp1-and-windows-intune.aspx
[Ref.- 10]	"Magic Quadrant for Mobile Device Management Software". Gartner. May 23, 2013. ID:G00249820. URL:https://www.gartner.com/technology/reprints.do?id=1-1FRIMH0&ct=130523&st=sb
[Ref.- 11]	"Critical Capabilities for Mobile Device Management Software". Gartner. May 23, 2013. ID:G00250008. URL:https://www.gartner.com/technology/reprints.do?id=1-1FRIMJB&ct=130523&st=sb
[Ref.- 12]	"Magic Quadrant for Mobile Device Management Software". Gartner. May 17, 2012. ID:G00230508. URL:https://dell.symantec.com/system/files/Magic_Quadrant_for_Mobile_Device_Management_Software.pdf URL:https://enterprisemobilitymobi.wordpress.com/2012/05/18/gartner-2012-magic-quadrant-for-mdm/
[Ref.- 13]	"Magic Quadrant for Mobile Device Management Software". Gartner. April 13, 2011. ID: G00211101. URL:http://www.sap.com/campaigns/2011_04_mobility/assets/GartnerReport_MDM_MQ_April2011.pdf URL: http://icomm.co/icomm-services/mobility-services/mobile-device-management/
[Ref.- 14]	"Worldwide Mobile Enterprise Management Software 2012 – 2016 Forecast and Analysis and 2011 Vendor Shares". IDC. Septiembre 2012. URL: http://idcdocserv.com/236835e
[Ref.- 15]	"White Paper: A Technical Comparison of Mobile Management Solution Features and Functions". SCMDM 2008. Microsoft. URL: http://download.microsoft.com/download/E/E/5/EE517330-67B4-4057-961F-D883FBC34F39/MDM%20Technical%20Comparison%20White%20Paper_CR_Final.pdf
[Ref.- 16]	"Configuration Profile Key Reference" (antes "iPhone Configuration Profile Reference"). Apple. URL: http://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/
[Ref.- 17]	"iOS MDM Specification". Apple. URL:http://adcdownload.apple.com//Documents/mobile_device_management_protocol/mobiledevicemanagementprotocol.pdf

Referencia	Título, autor y ubicación
[Ref.- 18]	"iOS Developer Enterprise Program (iDEP)". Apple. URL: https://developer.apple.com/programs/ios/enterprise/
[Ref.- 19]	"iPhone Support: Enterprise". Apple. URL: https://www.apple.com/support/iphone/enterprise/
[Ref.- 20]	"iPhone Configuration Utility (iPCU)". Apple. URL: http://support.apple.com/kb/DL1465 (Mac OS X) URL: http://support.apple.com/kb/DL1466 (Windows) URL: https://help.apple.com/iosdeployment-ipcu/mac/1.0/
[Ref.- 21]	"Apple Configurator". Apple. URL: https://help.apple.com/configurator/mac/1.3/?lang=es (ver [Ref.- 19]) URL: https://support.apple.com/kb/HT5769 (v1.3)
[Ref.- 22]	"Profile Manager". Apple. URL: https://www.apple.com/support/lionserver/profilemanager/ URL: https://help.apple.com/profilemanager/mac/10.7/
[Ref.- 23]	"Volume Purchase Program (VPP)". Apple. URL: https://www.apple.com/business/vpp/ URL: https://help.apple.com/iosdeployment-apps/ URL: https://www.apple.com/iphone/business/it-center/apps.html
[Ref.- 24]	"iPhone in Business – IT Center". Apple. URL: https://www.apple.com/iphone/business/it-center/ URL: https://www.apple.com/iphone/business/it-center/deployment.html URL: https://www.apple.com/iphone/business/it-center/security.html
[Ref.- 25]	"iPhone in Business – MDM". Apple. URL: https://www.apple.com/iphone/business/it-center/deployment-mdm.html URL: https://www.apple.com/iphone/business/it-center/byod.html
[Ref.- 26]	"Well known TCP and UDP ports used by Apple software products". Apple. URL: https://support.apple.com/kb/ts1629
[Ref.- 27]	"Unable to use Apple Push Notification service (APNs)". Apple. URL: https://support.apple.com/kb/ts4264 URL: https://developer.apple.com/library/ios/#technotes/tn2265/_index.html
[Ref.- 28]	"Deploying iPhone and iPad – (iPhone in Business) Mobile Device Management". Apple. URL: http://itstreaming.apple.com/podcasts/iphoneinbusiness/ds/iPhone_MDM.pdf URL: https://www.apple.com/iphone/business/docs/iOS_6_MDM_Sep12.pdf
[Ref.- 29]	"Zune para Windows" (Windows Phone 7). Microsoft. URL: http://www.windowsphone.com/es-es/how-to/wp7/zune-software
[Ref.- 30]	"Windows Phone 7 Connector para Mac OS X" (Windows Phone 7). Microsoft. URL: http://www.windowsphone.com/es-es/how-to/wp7/mac-connector
[Ref.- 31]	"Aplicación de Windows Phone" (para ordenadores y Mac). Microsoft. URL:http://www.windowsphone.com/es-ES/How-to/wp8/windows-phone-app-for-desktop URL: http://www.windowsphone.com/es-es/how-to/wp8/windows-phone-app-for-mac URL: http://www.windowsphone.com/es-ES/how-to/wp8/start/syncing-and-moving
[Ref.- 32]	"Android SDK". Google. URL: https://developer.android.com/sdk/index.html
[Ref.- 33]	"BlackBerry Desktop Software" (para PC y Mac). BlackBerry. URL: http://es.blackberry.com/software/desktop.html
[Ref.- 34]	"BlackBerry Link" (para PC y Mac). BlackBerry. URL: http://es.blackberry.com/software/desktop/blackberry-link.html
[Ref.- 35]	"iTunes". Apple. URL: https://www.apple.com/es/itunes/
[Ref.- 36]	"Google Apps" (for Business, etc). Google URL: https://www.google.com/apps/
[Ref.- 37]	"Google Apps Device Policy". Google. URL: https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent&hl=es
[Ref.- 38]	"Google Apps Mobile Management". Google. URL: https://support.google.com/a/bin/answer.py?hl=es&answer=1734200 URL: https://www.youtube.com/watch?v=TtDYpU4V4UQ

Referencia	Título, autor y ubicación
[Ref.- 39]	"A new way to distribute your internal Android apps". Google. URL: http://googleenterprise.blogspot.com.es/2012/12/a-new-way-to-distribute-your-internal.html
[Ref.- 40]	"iCloud". Apple. URL: https://www.icloud.com
[Ref.- 41]	"Mobile Device Security Checklist". SANS. URL: https://www.sans.org/score/mobile-device-checklist.php
[Ref.- 42]	"Device Administration" (API). Google. URL: https://developer.android.com/guide/topics/admin/device-admin.html
[Ref.- 43]	"BlackBerry Enterprise Service 10 version 10.1 Architecture and Data Flows". BlackBerry.URL:http://docs.blackberry.com/en/admin/deliverables/52723/BlackBerry_Enterprise_Service_10_version_10.1_Architecture_and_Data_Flow_Quick_Reference-en.pdf
[Ref.- 44]	"BlackBerry Enterprise Server 5 to BlackBerry Enterprise Service 10.1 – Going Under The Covers". BlackBerry. URL: https://bblive.blackberryconferences.net/2013/connect/fileDownload/session/057C33D60B1985BAD477FE9C019A74CE/BPD03_BBLive-BPD03.pdf
[Ref.- 45]	"Does RIM Compromise on Security by Using ActiveSync? The answer is No, and here's why…". BlackBerry. Agosto 2012. URL: http://bizblog.blackberry.com/2012/08/rim-activesync-security/
[Ref.- 46]	"BlackBerry Balance". BlackBerry. URL: http://ca.blackberry.com/business/software/blackberry-balance.html
[Ref.- 47]	"Secure Work Space for iOS and Android Now Available with BlackBerry Enterprise Service 10". BlackBerry. Junio 2013. URL: http://bizblog.blackberry.com/2013/06/secure-work-space-ios-android-bes-10/
[Ref.- 48]	"Managing Apple Devices" (session 300). Apple. WWDC 2013. Julio 2013. URL: https://developer.apple.com/wwdc/videos/ URL: https://developer.apple.com/wwdc/videos/index.php?id=300
[Ref.- 49]	"xCon". Cydia. URL: http://theiphonewiki.com/wiki/XCon URL: https://github.com/n00neimp0rtant/xCon-Issues/issues
[Ref.- 50]	"Windows Intune". Microsoft. URL: https://www.microsoft.com/en-us/windows/windowsintune/explore.aspx
[Ref.- 51]	"Windows Phone 8 Enterprise Device Management Protocol". Microsoft. Junio 2013. URL: https://www.microsoft.com/en-us/download/details.aspx?id=36831 (v1.3)
[Ref.- 52]	"Windows Phone 8 Device Management Overview". Microsoft. Octubre 2012. URL: http://blogs.msdn.com/cfs-filesystemfile.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-01-5506/1832.20_2C00_205.01_5F00_WP8_5F00_MobileDeviceManagementOverview_5F00_102912_5F00_CR.pdf
[Ref.- 53]	"Risk Management of Enterprise Mobility Including Bring Your Own Device". DoD. Australian Government. Junio 2013. URL: http://dsd.gov.au/publications/csocprotect/Enterprise_Mobility_BYOD.pdf
[Ref.- 54]	"Companies Weigh BYOD vs. COPE, But What Really Protects Data?". Wired. May 2013. URL: http://www.wired.com/insights/2013/05/companies-weigh-byod-vs-cope-but-what-really-protects-data/
[Ref.- 55]	"Market Overview: Cloud-Hosted Mobile Device Management Solutions And Managed Services". Forrester. January 3, 2012. URL: http://www.air-watch.com/downloads/analyst-reports/forrester-cloud-hosted-mdm-market-overview-2012.pdf
[Ref.- 56]	"Market Overview: On-Premises Mobile Device Management Solutions, Q3 2011". Forrester. January 3, 2012. URL: http://www.air-watch.com/resources/analyst-reports/forrester-market-overview-on-premise-mdm/download
[Ref.- 57]	"Vendor Landscape: Mobile Device Management". Info-Tech Research Group. 2011. URL: http://www.air-watch.com/downloads/analyst-reports/info-tech-mdm-vendor-landscape-2011.pdf

Referencia	Título, autor y ubicación
[Ref.- 58]	"Guidelines for Managing the Security of Mobile Devices in the Enterprise". NIST Special Publication 800-124 Revision 1. Junio 2013. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
[Ref.- 59]	"Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)". NIST Special Publication 800-164 (Draft). Octubre 2012. URL: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf
[Ref.- 60]	"Mobile Device Management - Market Quadrant 2012". The Radicati Group, Inc. Diciembre 2012. URL: http://www.air-watch.com/downloads/analyst-reports/2012-12-20-Radicati-MDM-Market-Quadrant.pdf
[Ref.- 61]	"Enterprise App Stores Can Increase the ROI of the App Portfolio". Gartner. Feb 4, 2013. URL: http://www.gartner.com/technology/reprints.do?id=1-1EL8YUQ&ct=130321&st=sb
[Ref.- 62]	"SCEP (Simple Certificate Enrollment Protocol". IETF. 2012. URL: https://tools.ietf.org/html/draft-nourse-scep-23
[Ref.- 63]	"Manage my devices". Google Mobile. URL: https://support.google.com/a/users/answer/1235372
[Ref.- 64]	"Simple Certificate Enrollment Protocol (SCEP) does not strongly authenticate certificate requests" (Vulnerability Note VU#971035). CSS. Junio 2012. URL: http://www.css-security.com/scep/ URL: http://www.kb.cert.org/vuls/id/971035
[Ref.- 65]	Android 4.x KeyChain API, TrustStore, y blacklisting. "Android Explorations". Nikolay Elenkov. URL: http://nelenkov.blogspot.com.es/2011/11/using-ics-keychain-api.html URL: http://nelenkov.blogspot.com.es/2011/12/ics-trust-store-implementation.html URL: http://nelenkov.blogspot.com/2012/07/certificate-blacklisting-in-jelly-bean.html
[Ref.- 66]	"Guía CCN-STIC-406: Seguridad en redes inalámbricas". CCN-CERT. 2013. URL: https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=188&lang=es
[Ref.- 67]	"Samsung KNOX". URL: https://www.samsung.com/global/business/mobile/solution/security/samsung-knox
[Ref.- 68]	"Google Cloud Messaging (GCM)". Google. URL: https://developer.android.com/google/gcm/index.html URL: https://developer.android.com/google/gcm/gcm.html
[Ref.- 69]	"GCM Cloud Connection Server". Google. URL: https://developer.android.com/google/gcm/ccs.html
[Ref.- 70]	"GCM HTTP Connection Server". Google. URL: https://developer.android.com/google/gcm/http.html
[Ref.- 71]	"Administración de dispositivos"Google Apps Bussines. URL: http://support.google.com/a/bin/answer.py?hl=en&answer=1734200
[Ref.- 72]	"Google Apps For Bussines" Google. URL: http://www.google.com/intx/es/enterprise/apps/business/
[Ref.- 73]	"Google Device Manage". Google. URL: https://www.google.com/android/devicemanager