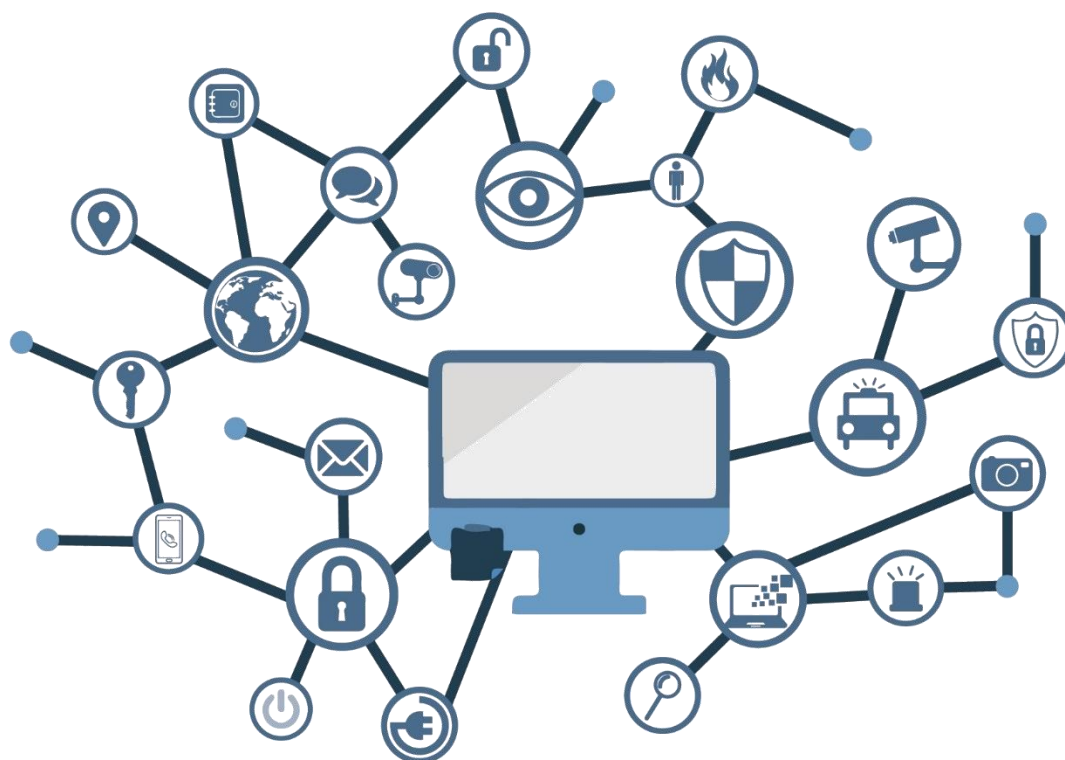


# Procedimiento de empleo seguro

## UEM MobileIron CORE



Edita:



© Centro Criptológico Nacional, 2020  
NIPO: 083-20-110-3

Fecha de Edición: Abril 2020

MobileIron ha participado en la realización y modificación del presente documento y sus anexos.

### **LIMITACIÓN DE RESPONSABILIDAD**

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

### **AVISO LEGAL**

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## **PRÓLOGO**

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

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

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

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

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

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

Abril de 2020



Paz Esteban López  
Secretaria de Estado  
Directora del Centro Criptológico Nacional

## ÍNDICE

|                                                                     |           |
|---------------------------------------------------------------------|-----------|
| <b>1 INTRODUCCIÓN .....</b>                                         | <b>5</b>  |
| 1.1 COMPONENTES Y ESCENARIOS UNA SOLUCIÓN DE MOVILIDAD .....        | 5         |
| 1.1.1 COMPONENTES .....                                             | 5         |
| 1.1.2 ESCENARIOS EN FUNCIÓN DE LA PROPIEDAD DEL DISPOSITIVO .....   | 6         |
| <b>2 PLATAFORMA UEM DE MOBILEIRON .....</b>                         | <b>7</b>  |
| <b>3 ESQUEMA DE BLOQUES PLATAFORMA UEM MOBILEIRON CORE .....</b>    | <b>9</b>  |
| <b>4 KIT DE HERRAMIENTAS DE IMPLEMENTACIÓN .....</b>                | <b>9</b>  |
| <b>5 MOBILEIRON CORE .....</b>                                      | <b>11</b> |
| 5.1 REQUISITOS DE PROCESADOR, HD Y MEMORIA DE LAS VM .....          | 11        |
| 5.2 ESPECIFICACIONES DE LA VM .....                                 | 11        |
| 5.3 ESPECIFICACIONES DE DISPOSITIVOS DE ALMACENAMIENTO .....        | 12        |
| 5.4 PRERREQUISITOS .....                                            | 12        |
| 5.5 COMPONENTES DE LA SOLUCIÓN .....                                | 14        |
| 5.6 DIAGRAMA - PROPUESTA DE ARQUITECTURA .....                      | 14        |
| 5.7 REGLAS DE RED - CORE .....                                      | 15        |
| 5.8 INSTALACIÓN .....                                               | 15        |
| 5.9 CONFIGURACIÓN .....                                             | 15        |
| <b>6 MOBILEIRON SENTRY .....</b>                                    | <b>18</b> |
| 6.1 ESPECIFICACIONES DE LA VM .....                                 | 18        |
| 6.2 ESPECIFICACIONES DE DISPOSITIVOS DE ALMACENAMIENTO .....        | 18        |
| 6.3 PRERREQUISITOS .....                                            | 19        |
| 6.4 DIAGRAMA – PROPUESTA DE ARQUITECTURA .....                      | 20        |
| 6.5 REGLAS DE RED - SENTRY .....                                    | 20        |
| 6.6 INSTALACIÓN .....                                               | 21        |
| 6.7 CONFIGURACIÓN .....                                             | 21        |
| <b>7 RECURSOS PARA NUEVOS CLIENTES .....</b>                        | <b>24</b> |
| <b>ANEXO I. EJEMPLO CHEQUEO DE SEGURIDAD SERVIDOR CORE .....</b>    | <b>25</b> |
| <b>ANEXO II. EJEMPLO CHEQUEO DE SEGURIDAD SERVIDOR SENTRY .....</b> | <b>26</b> |
| <b>ANEXO III. VISIBILIDADES CORE Y SENTRY .....</b>                 | <b>27</b> |
| III.1 REQUISITOS GENERALES CORE Y SENTRY .....                      | 27        |
| III.2 VISIBILIDADES DE CORE .....                                   | 29        |
| III.3 VISIBILIDAD DE SENTRY .....                                   | 38        |
| III.4 VISIBILIDADES DE RED .....                                    | 40        |
| III.5 VISIBILIDADES WIFI CORPORATIVA .....                          | 41        |
| <b>ANEXO IV. DISTRIBUIDORES AUTORIZADOS .....</b>                   | <b>44</b> |
| <b>ANEXO V. COMO ADQUIRIR MOBILEIRON .....</b>                      | <b>45</b> |

## 1 INTRODUCCIÓN

1. El objetivo de este documento es proporcionar una guía de despliegue y configuración de la plataforma UEM **Mobileiron CORE**, recientemente cualificado por el Centro Criptológico Nacional (CCN) y listado como tal en el Catálogo de Productos CPSTIC.
2. Las diferentes secciones están organizadas con el fin de proporcionar al lector una visión general de un hipotético proceso de despliegue de una plataforma UEM en su organización. Aunque este documento pretende ser comprensible por diferentes tipos de lectores, el rol principal al que va dirigido es al del equipo de IT de la organización, en especial su Administrador y Responsable de Sistema.
3. Las configuraciones y arquitecturas incluidas en este documento reflejan las utilizadas por el CCN durante el proceso de Cualificación y es la recomendada para despliegues que utilicen este documento como referencia. No se consideran otras configuraciones y no se pueden realizar valoraciones generales sobre el impacto en la seguridad de los cambios que se introduzcan, para la valoración de un cambio concreto sobre lo incluido en este documento puede dirigirse al CCN o al fabricante de la solución.

### 1.1 COMPONENTES Y ESCENARIOS UNA SOLUCIÓN DE MOVILIDAD

#### 1.1.1 COMPONENTES

4. Para desplegar y mantener un sistema seguro basado en dispositivos móviles es necesario disponer de los siguientes bloques funcionales:
  - Dispositivos móviles, con las capacidades y la configuración apropiada.
  - Soluciones de gestión de dispositivos móviles (MDM-Mobile Device Management, también denominadas UEMs) cualificadas y que dispongan de las funcionalidades necesarias.
  - Redes de comunicaciones, de diferentes tecnologías (3G, 4G, WiFi, ...).
  - Equipo de Administradores de dispositivos móviles de la organización donde se realiza el despliegue, así como su estructura organizativa y recursos
  - Política de seguridad de las TIC, en la que se reflejen la valoración de los sistemas, los riesgos a los que se enfrentan, las contramedidas utilizadas.
  - Usuarios de la organización, responsables del uso diario de los dispositivos.

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

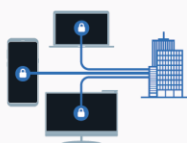
### 1.1.2 ESCENARIOS EN FUNCIÓN DE LA PROPIEDAD DEL DISPOSITIVO

6. Pese a que en la literatura de las diferentes soluciones y tecnologías se refieren a los despliegues de diferente manera y con diferentes términos, en este documento se clasifica los escenarios de despliegue según la propiedad del dispositivo (no del dato o de la información) en el momento de su despliegue y provisión. Teniendo esto en cuenta, los principales escenarios en despliegue de una solución de movilidad en una organización se pueden clasificar como:
  - BYOD - Bring Your Own Device: el dispositivo es propiedad del usuario final del mismo, no de la organización.
  - COPE - Corporate Owned Personal Enabled: el dispositivo es propiedad de la organización y se dedica a tareas profesionales, pudiendo utilizarse esporádica para comunicaciones personales del usuario final del dispositivo, previo acuerdo con la organización.
  - COBO - Corporate Owned Business Only: el dispositivo es propiedad de la organización y se dedica a tareas profesionales, pudiendo utilizarse esporádica para comunicaciones personales del usuario final del dispositivo, previo acuerdo con la organización.
7. Aunque derivado de algunas consideraciones técnicas y legales, a lo largo del documento se pueden citar otros escenarios de despliegue, los únicos considerados validos por el CCN son los ya mencionados COBO o COPE una vez analizado y concretado el riesgo asumido.

## 2 PLATAFORMA UEM DE MOBILEIRON

8. La administración unificada de puntos de conexión (UEM) de Mobileiron permite a los empleados de una organización disfrutar de un acceso fluido a aplicaciones y datos corporativos a través de dispositivos móviles, equipos de sobremesa y servicios en la nube securizados a la vez que mantienen un total control de su privacidad.
9. Asimismo, un UEM permite securizar las aplicaciones móviles de productividad como el correo electrónico, los contactos, el calendario o la lista de tareas en dispositivos, sin preocuparse por el sistema operativo en que estén basados (Android, iOS, Windows10 y macOS). El objetivo de una plataforma UEM es **implementar una política de seguridad móvil unificada**. La organización podrá configurar e implementar las mismas políticas para aplicaciones en todos los terminales de trabajo. La gestión de la VPN por aplicación permite a los usuarios acceder rápidamente a los recursos corporativos que hay detrás del firewall corporativo.
10. Entre otros, se pueden destacar los siguientes casos de uso:
  - Securitización de cualquier dispositivo: Configure y aplique políticas uniformes de seguridad de datos en dispositivos móviles y equipos de sobremesa con Android, iOS, macOS y Windows 10.
  - Correo electrónico seguro: Proporcione acceso seguro al correo electrónico, los calendarios y los contactos de la empresa a la vez que conserva la experiencia nativa del usuario móvil.
  - Aplicaciones y datos móviles securizados: Proteja los datos corporativos confidenciales en reposo del dispositivo y en movimiento en cualquier red o servicio en la nube.
  - Contenido móvil securizado: Permita el acceso seguro e inmediato a los repositorios de contenido y evite la pérdida de datos mediante el uso compartido no autorizado de archivos.
  - Compartimentación segura: Mantenga la privacidad del usuario a la vez que aplica las políticas corporativas y conserva el control de los datos empresariales en los dispositivos móviles personales y los equipos de sobremesa.

## Segurizar y administrar



### Dispositivos modernos:

Seguridad del correo electrónico  
Configuración automática  
Seguridad basada en certificados  
Borrado selectivo  
Modo *Single app*/kiosco



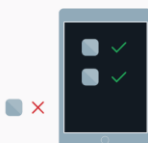
### Aplicaciones:

Aplicaciones securizadas  
Storefront de aplicaciones corporativas  
Ejecución de la autenticación del usuario  
Aislar/retirar aplicaciones corporativas



### Contenido:

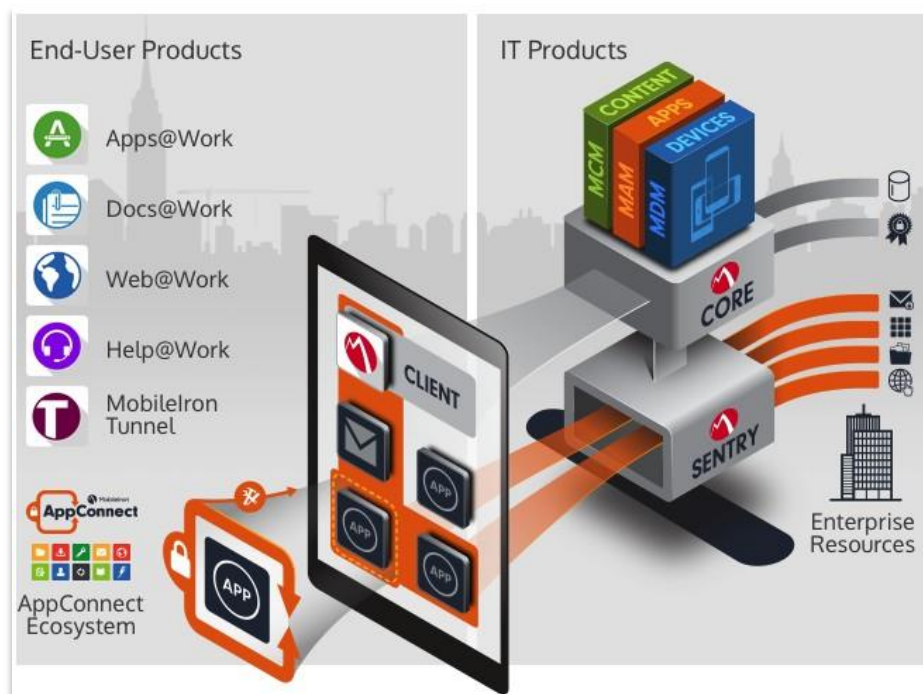
Archivos adjuntos al correo electrónico cifrados y visibles únicamente en aplicaciones autorizadas  
Navegadores web securizados  
Acceder, anotar y compartir documentos



### Modo kiosco/dispositivos de un solo uso:

Garantice la productividad restringiendo las aplicaciones que estén disponibles para ser utilizadas en un dispositivo  
Evite la instalación de aplicaciones malintencionadas en un dispositivo  
Evite el exceso de datos limitando las aplicaciones del dispositivo

### 3 ESQUEMA DE BLOQUES PLATAFORMA UEM MOBILEIRON CORE



### 4 KIT DE HERRAMIENTAS DE IMPLEMENTACIÓN

11. Use el siguiente kit de herramientas para maximizar su implementación con un socio certificado de Mobileiron.
12. La metodología de implementación está desarrollada por el equipo de Servicios Profesionales de Mobileiron para guiarle a través del proceso desde el principio hasta el final. Esta metodología es aplicable para nuevas implementaciones y despliegues de nuevas características y capacidades que impactan en su organización.
13. El kit de herramientas está organizado en 4 bloques:
14. **Planificar:** Establezca sus objetivos de implementación, evalúe los requisitos y desarrolle un completo proyecto.
15. **Diseñar:** Cree su diseño técnico y comercial para disponer de una guía durante la configuración e implementación. Establezca los requisitos de seguridad y los perfiles de usuario. Formalice un plan de comunicación para los usuarios.
16. **Implementar:** Instale y configure Core y Sentry junto a todas las integraciones con sus servicios de la organización. Configure sus aplicaciones y políticas. Pruebe la inscripción y el registro de sus dispositivos

17. **Desplegar:** Capacite a sus administradores y al servicio de asistencia interno. Informe a sus usuarios sobre cómo registrar e inscribir sus dispositivos. Experimente primero y aplique los aprendizajes a una implementación más amplia para optimizar su éxito.
18. Puede acceder a la versión completa del documento desde el siguiente link:  
<https://community.Mobileiron.com/docs/DOC-3015> \*

\* Podrá acceder al portal web de soporte de Mobileiron a través de un distribuidor certificado.

## 5 MOBILEIRON CORE

### 5.1 REQUISITOS DE PROCESADOR, HD Y MEMORIA DE LAS VM

| Máximo dispositivos | Memoria       | CPU Virtual/<br>Velocidad mínima | Capacidad de<br>almacenamiento | Almacenamiento<br>mínimo de IOPS<br>(Lectura<br>aleatoria) | Almacenamiento<br>mínimo de IOPS<br>(Escritura<br>aleatoria) |
|---------------------|---------------|----------------------------------|--------------------------------|------------------------------------------------------------|--------------------------------------------------------------|
| < 5.000             | 8 GB<br>RAM*  | Qty 2/2.13 GHz<br>procesador**   | 80 a 250 GB<br>SAS             | 400                                                        | 1000                                                         |
| < 20.000            | 16 GB<br>RAM* | Qty 4/2.13 GHz<br>procesador**   | 250 GB SAS                     | 400                                                        | 1000                                                         |
| < 50.000            | 32 GB<br>RAM* | Qty 8/2.13 GHz<br>procesador**   | 500 GB SAS                     | 400                                                        | 1000                                                         |
| < 100.000           | 64 GB<br>RAM* | Qty 16/2.13GHz<br>procesador**   | 1 TB SAS                       | 400                                                        | 1000                                                         |

\* Asignación de recursos garantizada: no se permite compartición.

\*\* Asignación de recursos garantizada: no se permite compartir con otras máquinas virtuales

### 5.2 ESPECIFICACIONES DE LA VM

| Componentes                  | Requerimientos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disco Duro                   | Mobileiron recomienda configurar solo un disco duro en la máquina virtual. El rendimiento del sistema está directamente relacionado con el rendimiento del disco duro. Mobileiron recomienda usar solo productos de almacenamiento de nivel I de alto rendimiento.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Copia de seguridad de VMware | Mobileiron recomienda realizar copias de seguridad periódicas (.vmdk) de su <i>Mobileiron Virtual Appliance</i> como parte del mantenimiento de su sistema. Use VMware VCB u otro sistema de respaldo compatible con VMware. Se recomienda una copia de seguridad del disco virtual completo. Las instantáneas de VMware no son suficientes.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| VMware                       | <ul style="list-style-type: none"> <li>• Enlace de descarga o paquete (ISO) de Mobileiron: <a href="https://support.mobileiron.com/support/CDL.html">https://support.mobileiron.com/support/CDL.html</a></li> <li>• VMware ESXi 5.1 / 5.5 / 6.0 / 6.5</li> <li>• VM de 64 bits</li> <li>• Adaptador de red <ul style="list-style-type: none"> <li>- E1000</li> <li>- VMXNET 3</li> </ul> </li> <li>• Tipo de sistema operativo VM: <ul style="list-style-type: none"> <li>- CentOS 7.4 (64 bits)</li> </ul> </li> <li>• Configuración de la CPU: <ul style="list-style-type: none"> <li>- Acciones: Normal</li> <li>- Reserva: Especificaciones de la tabla de la página 7 de este manual</li> <li>- Límite: ilimitado (máximo asignado)</li> </ul> </li> <li>• Configuración de memoria:</li> </ul> |

| Componentes | Requerimientos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | <ul style="list-style-type: none"> <li>- Acciones: Normal</li> <li>- Reserva: Especificaciones de la tabla de la página 7 de este manual</li> <li>- Reserva alternativa: 50% de la especificación en tabla página 7*</li> <li>* La configuración de memoria alternativa no está cubierta por la garantía del producto de Mobileiron.</li> <li>- Límite: ilimitado (máximo asignado)</li> <li>• Arrancar desde el firmware de la BIOS</li> </ul> <p><b>Tenga en cuenta lo siguiente:</b></p> <ul style="list-style-type: none"> <li>• Actualmente se admiten los controladores LSI logic SAS o Paralell SCSI. Los controladores para-virtualizados no son compatibles.</li> <li>• Las configuraciones alternativas de memoria y CPU no están cubiertas por la garantía del producto de Mobileiron</li> </ul> |

### 5.3 ESPECIFICACIONES DE DISPOSITIVOS DE ALMACENAMIENTO

| Operación           | Min IOPS | Bandwidth | 90% Operaciones < xxx mS |
|---------------------|----------|-----------|--------------------------|
| Lectura Aleatoria   | 400      | 3 MBps    | 10 mS                    |
| Escritura Aleatoria | 900*     | 15 MBps   | 4 mS                     |

- Mobileiron recomienda configurar un solo disco duro por máquina virtual.
- En caso de usar un controlador RAID, este debe estar configurado correctamente para alcanzar el óptimo rendimiento de las escrituras aleatorias IOPS - (e.g. Disk Cache: Enabled, Default Write: Write Back with BBU).
- El rendimiento del Sistema está directamente relacionado al rendimiento del dispositivo de almacenamiento. Mobileiron solo recomienda el uso de productos de almacenamiento de tier1 de alto rendimiento.

### 5.4 PRERREQUISITOS

| Item                             | Descripción                                                                                                  | Notas     |
|----------------------------------|--------------------------------------------------------------------------------------------------------------|-----------|
| Acceso a servidor DNS desde Core | Para el correcto acceso a servicios internos, se recomienda que Core tenga acceso a un servidor DNS interno. | Puerto 53 |

| Item                                       | Descripción                                                                                                                                       | Notas                                                     |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Acceso a servidor NTP desde Core           | Para tareas con certificados, se recomienda que Core tenga acceso a un servidor NTP sincronizado con los servidores internos a los que se acceda. | Puerto 123                                                |
| IP pública de Core                         | Dirección IP pública fija que resuelva el FQDN de Core desde Internet                                                                             | Puerto 443 desde internet                                 |
| IP privada de Core                         | Dirección IP interna que resuelva el FQDN desde el DNS interno                                                                                    | Puerto 443 y 8443                                         |
| FQDN interno de Core                       | FQDN en un dominio externo que resuelva la IP pública de Core                                                                                     | Ex. ssc01.xyz.com en zona DNS xyz.com del dominio interno |
| FQDN externo de Core                       | FQDN en el DNS interno que resuelva la IP interna de Core. Se recomienda que sea el mismo que el externo para optimizar el tráfico interno.       | Ex. ssc01.xyz.com en dominio externo xyz.com              |
| Certificado TLS de Core                    | 1x certificado TLS de una entidad certificadora confiable desde internet, que contenga el FQDN de Core                                            | Ex. certificado con common name y SAN ssc01.xyz.com       |
| Contraseña de administrador CLI            | Su función es permitir tareas con privilegios desde la línea de comandos de la VM.                                                                |                                                           |
| Nombre de usuario administrador local      | Su función es acceder al portal de gestión de sistema para configuración.                                                                         |                                                           |
| Contraseña del usuario administrador local |                                                                                                                                                   |                                                           |
| ID de dispositivo de red                   | Por defecto A si solo hay una tarjeta de red                                                                                                      |                                                           |
| IP de Máscara de subred                    |                                                                                                                                                   |                                                           |
| IP de Gateway por defecto                  |                                                                                                                                                   |                                                           |
| Activar SSH o no.                          | Se recomienda activar para puesta en marcha                                                                                                       |                                                           |

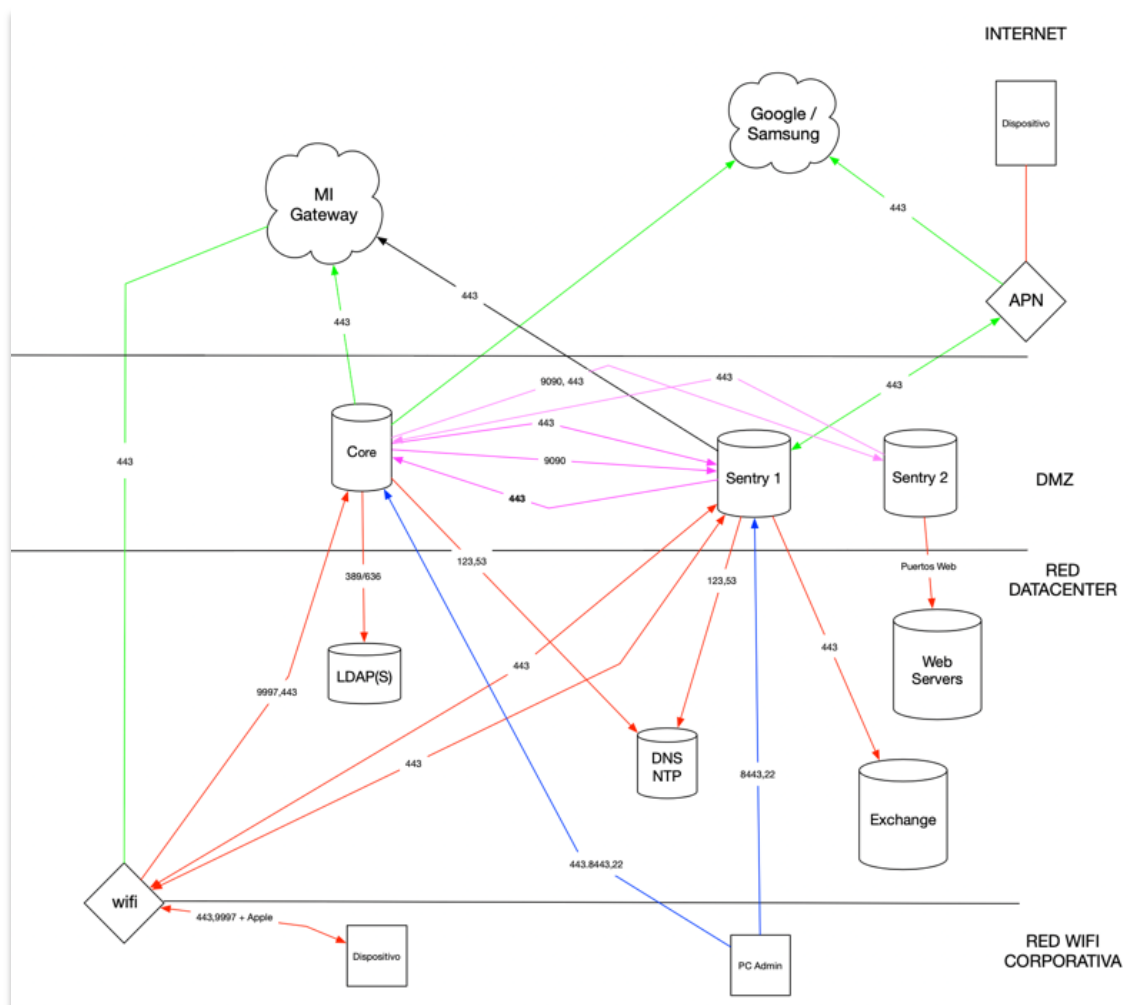
## 5.5 COMPONENTES DE LA SOLUCIÓN

22. La instalación de la solución UEM Mobileiron Core comprende los siguientes elementos:

- Mobileiron Core
- Mobileiron Sentry

23. **Mobileiron Core** es el núcleo desde donde se controla toda la solución UEM, mientras que **Mobileiron Sentry** permite dar visibilidad y acceso condicional inteligente a correo ActiveSync así como también permite el tunelizado de aplicaciones.

## 5.6 DIAGRAMA - PROPUESTA DE ARQUITECTURA

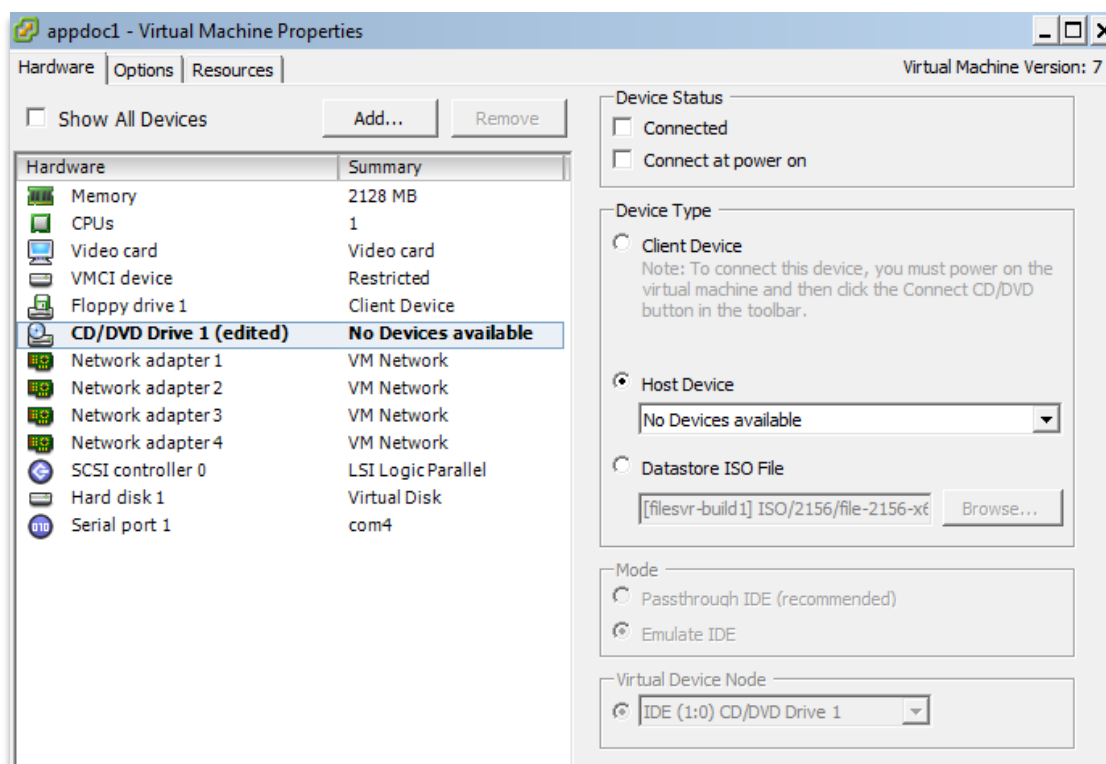


## 5.7 REGLAS DE RED - CORE

24. Ver tabla adjunta en “**anexo 8.2 Visibilidades de Core**” en página 27 así como la tabla del “**anexo 8.4 Visibilidades de red**” en la página 36

## 5.8 INSTALACIÓN

25. Una vez que tenemos creada la VM de Core y las comunicaciones están configuradas según los parámetros comentados en apartados anteriores, podemos proceder con la instalación del software.
26. Para ello, descargaremos la ISO de Core\*, y la montaremos en el DVD virtual de la VM.



## 5.9 CONFIGURACIÓN

27. Espere a que la VM se reinicie para que el programa de instalación empiece después de unos minutos.
28. Introduzca este comando para empezar la instalación:

```
vm-install
```

29. Pulse **Enter** para iniciar el proceso de instalación.
30. Después de varios minutos, el programa de instalación mostrará el mensaje de bienvenida del asistente de configuración.

```
Welcome to the MobileIron Configuration Wizard  
Use the - character to move back to the previous field  
  
Continue with configuration dialog? [yes/no]
```

31. Escriba **Yes** para mostrar el acuerdo de licencia de usuario final.
32. Desplácese y lea el acuerdo.
33. Escriba **Yes** para aceptar el contrato de licencia de usuario final.
34. Introduzca el **company name**.  
El nombre de la empresa que introduzca servirá como nombre de empresa predeterminado utilizado en la comunicación por SMS y correo electrónico.
35. Introduzca el **Nombre** de la persona de su organización que servirá como punto de contacto para las comunicaciones de Mobileiron.
36. Introduzca la **Dirección de correo electrónico** para la persona de contacto.
37. Introduzca la **Contraseña** para el modo privilegiado de CLI.  
La contraseña debe tener entre 6 y 20 caracteres.
38. Vuelva a introducir la contraseña.
39. Introduzca el nombre de usuario que desea asignar para el primer usuario administrativo. No utilice **root** o **ha\_admin**.
40. Introduzca el **Contraseña** que desea asignar al administrador. Esta contraseña debe contener al menos 8 caracteres e incluir números y letras mayúsculas.
41. **Vuelva a introducir** la contraseña de administrador.
42. Introduzca la **Letra** para la interfaz física que desea utilizar para conectarse a la red de administración.
  - a) para GigabitEthernet1
  - b) para GigabitEthernet2
43. Introduzca la **dirección IP interna** que creó para Mobileiron Core. Se asociará con la interfaz física que seleccionó en el paso anterior.
44. Introduzca el **Netmask** para su uso con la dirección IP que acaba de ingresar, por ejemplo 255.255.255.0.
45. Introduzca la **puerta de enlace de red predeterminada** para Core.
46. Introduzca el **nombre de host externo** (fully-qualified domain name) para el dispositivo.

No utilice un nombre de host interno. Los dispositivos gestionados deben poder acceder a Mobileiron Core desde Internet.

47. Introduzca el **Dirección IP** del servidor de DNS que utilizará Core.
48. Ingrese los servidores de nombres secundarios y terciarios opcionales como preferido.

Deje los campos en blanco y pulse Intro para omitir la especificación de servidores de nombres adicionales.
49. Introduzca **yes** para habilitar el acceso remoto a través de SSH.
50. Escriba **yes para** configurar un origen de NTP en el prompt de la configuración NTP.

Mobileiron recomienda que configure al menos una fuente de tiempo para garantizar la sincronización adecuada de las tareas basadas en tiempo.
51. **Revise** el script del comando visualizado.
52. Escriba **yes** para guardar los cambios.
53. Cuando se complete la configuración, el programa de instalación mostrará el mensaje de **Configuración completa**.
54. Escriba **reload** para reiniciar el sistema y habilitar el servicio del portal.
55. Escriba **yes** cuando se le solicite guardar las configuraciones del sistema.
56. Escriba **yes** cuando se le solicite guardar las configuraciones del sistema.
57. Una instalación exitosa muestra el banner de la CLI de Mobileiron Core en la consola. El script de instalación continúa, mostrando el estado en la consola. Esto puede tardar varios minutos.

## 6 MOBILEIRON SENTRY

### 6.1 ESPECIFICACIONES DE LA VM

|                     | Small configuration | Medium configuration | Large configuration |
|---------------------|---------------------|----------------------|---------------------|
| Maximum devices     | < 2000 devices      | < 8000 devices       | < 20,000 devices    |
| Memory              | 4 GB                | 6 GB                 | 8 GB                |
| Virtual CPUs**      | 1                   | 2                    | 4                   |
| Memory reservations | Reservations: 4 GB  | Reservations: 6 GB   | Reservations: 8 GB  |
| Disk                | 20 GB               | 30 GB                | 40 GB               |

VMware ESXi 5.1/5.5. ESXi 6

64-bit VM

Network adapter:

- E1000
- VMXNET3

VM OS Type: CentOS 6 (64-bit), Other Linux (64-bit), Red Hat Enterprise Linux 6 (64-bit)

This setting is intended to ensure successful installation; it does not imply that Mobileiron distributes Red Hat.

CPU Settings:

- Shares: Normal
- Reservation: 900MHz
- Limit: Unlimited (maximum assigned)

### 6.2 ESPECIFICACIONES DE DISPOSITIVOS DE ALMACENAMIENTO

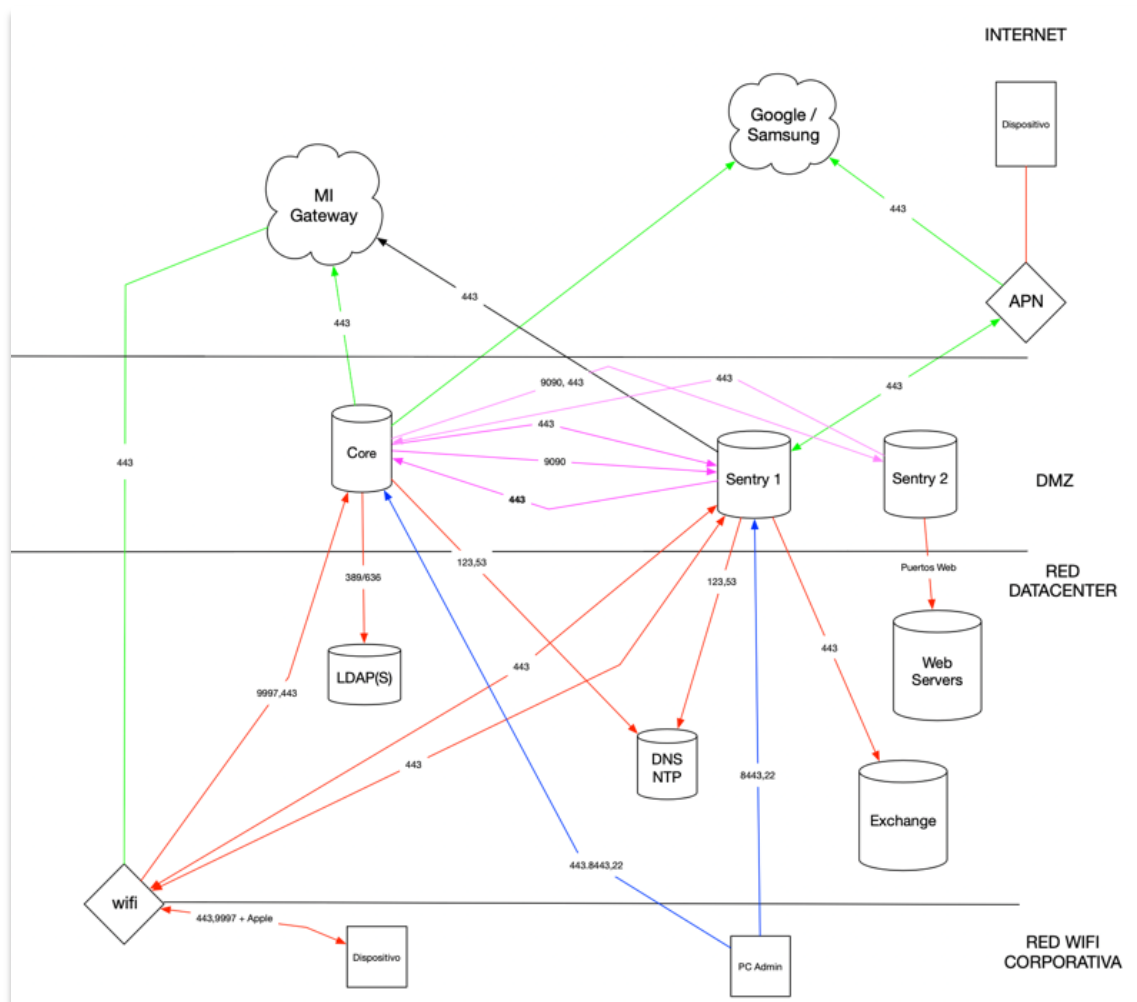
| Operation    | Min IOPS | Bandwidth | 90% Operations < xxx mS |
|--------------|----------|-----------|-------------------------|
| Random Read  | 400      | 3 MBps    | 10 mS                   |
| Random Write | 900*     | 15 MBps   | 4 mS                    |

58. Mobileiron recomienda configurar un solo disco duro por máquina virtual.
59. En caso de usar un controlador RAID, este debe estar configurado correctamente para alcanzar el óptimo rendimiento de las escrituras aleatorias IOPS - (e.g. Disk Cache: Enabled, Default Write: Write Back with BBU).
60. El rendimiento del Sistema está directamente relacionado al rendimiento del dispositivo de almacenamiento. Mobileiron solo recomienda el uso de productos de almacenamiento de tier1 de alto rendimiento.

### 6.3 PRERREQUISITOS

| Item                                       | Descripción                                                                                                                                   | Notas                                                     |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| FQDN interno de Sentry                     | FQDN en un dominio externo que resuelva la IP pública de Sentry                                                                               | Ex. mis01.xyz.com en zona DNS xyz.com del dominio interno |
| FQDN externo de Sentry                     | FQDN en el DNS interno que resuelva la IP interna de Sentry. Se recomienda que sea el mismo que el externo para optimizar el tráfico interno. | Ex. mis01.xyz.com en dominio externo xyz.com              |
| Certificado TLS de Sentry                  | 1x certificado TLS de una entidad certificadora confiable desde internet, que contenga el FQDN de Sentry                                      | Ex. certificado con common name y SAN mis01.xyz.com       |
| Contraseña de administrador CLI            | Su función es permitir tareas con privilegios desde la línea de comandos de la VM.                                                            |                                                           |
| Nombre de usuario administrador local      | Su función es acceder al portal de gestión de sistema para configuración.                                                                     |                                                           |
| Contraseña del usuario administrador local |                                                                                                                                               |                                                           |
| ID de dispositivo de red                   | Por defecto A si solo hay una tarjeta de red                                                                                                  |                                                           |
| IP de Máscara de subred                    |                                                                                                                                               |                                                           |
| IP de Gateway por defecto                  |                                                                                                                                               |                                                           |
| Activar SSH o no.                          | Se recomienda activar para puesta en marcha                                                                                                   |                                                           |

## 6.4 DIAGRAMA – PROPUESTA DE ARQUITECTURA

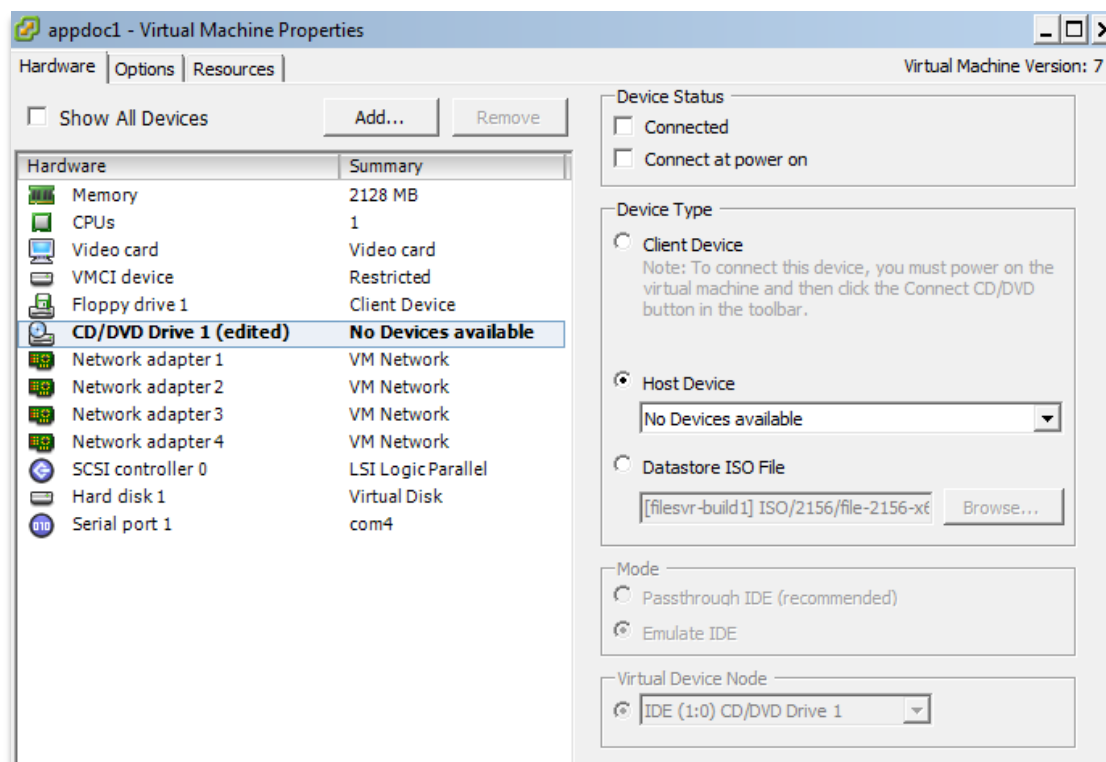


## 6.5 REGLAS DE RED - SENTRY

61. Ver tabla adjunta en anexo **"8.3 Visibilidades de Sentry"** de la página 34 con visibilidades para la VM (Virtual Machine) de Sentry.

## 6.6 INSTALACIÓN

62. Una vez tenemos creada la VM de Sentry y las comunicaciones están configuradas según los parámetros aportados en apartados anteriores, podemos proceder con la instalación del software.
63. Para ello, descargaremos la ISO de Sentry\*, y la montaremos en el DVD virtual de la VM.



## 6.7 CONFIGURACIÓN

64. Espera a que la VM se reinicie para que el programa de instalación empiece después de unos minutos.
65. Introduzca este comando para empezar la instalación:

```
vm-install
```

66. Pulse Enter para iniciar el proceso de instalación. Después de varios minutos, el programa de instalación mostrará el mensaje de bienvenida del asistente de

configuración.

```
Welcome to the MobileIron Configuration Wizard  
Use the - character to move back to the previous field  
  
Continue with configuration dialog? [yes/no]
```

67. Escriba **Yes** para mostrar el acuerdo de licencia de usuario final.
68. Desplácese y lea el acuerdo.
69. Escriba **Yes** para aceptar el contrato de licencia de usuario final.
70. Introduzca el **company name**.

El nombre de la empresa que introduzca servirá como nombre de empresa predeterminado utilizado en la comunicación por SMS y correo electrónico.
71. Introduzca el **Nombre** de la persona de su organización que servirá como punto de contacto para las comunicaciones de MobileIron.
72. Introduzca la **dirección de correo electrónico** para la persona de contacto.
73. Introduzca la **Contraseña** para el modo privilegiado de CLI.

La contraseña debe tener entre 6 y 20 caracteres.
74. Vuelva a introducir la contraseña.
75. Introduzca el nombre de usuario que desea asignar para el **primer usuario administrativo**. No utilice **root** o **ha\_admin**.
76. Introduzca la **Contraseña** que desea asignar al administrador.
77. Esta contraseña debe contener al menos 8 caracteres e incluir números y letras mayúsculas.
78. Vuelva a introducir la contraseña de administrador.
79. Introduzca el **Letra** para la interfaz física que desea utilizar para conectarse a la red de administración.
  - a) para GigabitEthernet1
  - b) para GigabitEthernet2
80. Introduzca la **dirección IP interna** que creó para MobileIron Sentry.
81. Se asociará con la interfaz física que seleccionó en el paso anterior.
82. Introduzca el **Netmask** para su uso con la dirección IP que acaba de ingresar, por ejemplo, 255.255.255.0.
83. Introduzca la **puerta de enlace de red predeterminada** para Sentry.
84. Introduzca el **nombre de host externo** (fully-qualified domain name) para el dispositivo.

No utilice un nombre de host interno. Los dispositivos gestionados deben poder acceder a Mobileiron Sentry desde Internet.

85. Introduzca la **dirección IP** del servidor de DNS que utilizará Sentry.
86. Ingrese los servidores de nombres secundarios y terciarios opcionales como preferido.
87. Deje los campos en blanco y pulse Intro para omitir la especificación de servidores de nombres adicionales.
88. Introduzca **yes** para habilitar el acceso remoto a través de SSH.
89. Escriba **yes para** configurar un origen de NTP en el prompt de la configuración NTP.

Mobileiron recomienda que configure al menos una fuente de tiempo para garantizar la sincronización adecuada de las tareas basadas en tiempo.

90. **Revise** el script de comando visualizado.
91. Escriba **yes** para guardar los cambios.
92. Cuando se complete la configuración, el programa de instalación mostrará el mensaje de **Configuración completa**.
93. Escriba **reload** para reiniciar el sistema y habilitar el servicio del portal.
94. Escriba **yes** cuando se le solicite guardar las configuraciones del sistema.
95. Escriba **yes** cuando se le solicite guardar las configuraciones del sistema.
96. Una instalación exitosa muestra el banner de la CLI de Mobileiron Sentry en la consola. El script de instalación continúa, mostrando el estado en la consola. Esto puede tardar varios minutos.

## 7 RECURSOS PARA NUEVOS CLIENTES

97. Los siguientes artículos y guías están disponibles online y pueden ser de utilidad para ampliar lo expuesto en el presente documento:

- **Recursos de despliegue:**  
<https://community.Mobileiron.com/docs/DOC-2625>
- **Crea tu proyecto de despliegue:**  
<https://community.Mobileiron.com/docs/DOC-3015>
- **Como formarse en Mobileiron University (MIU):**  
<https://community.Mobileiron.com/docs/DOC-2671>
- **Encuentra respuestas en los foros de soporte:**  
<https://community.Mobileiron.com/community/support-forums>
- **Link a la descarga de software de Mobileiron:**  
<https://support.Mobileiron.com/support/CDL.html>
- **Comprobar seguridad de un despliegue:**  
<https://shc.Mobileiron.net>

## ANEXO I. EJEMPLO CHEQUEO DE SEGURIDAD SERVIDOR CORE



## Security Health Check

[Home](#)

## Scan Results

**Hostname:** Core external FQDN

**Ports:** 443, 8443 and 9997

## Scan Results:

The following issues have been identified:

| Issue | Recommended Fix |
|-------|-----------------|
|       |                 |

## Additional Details on the Tests:

| Test Name                                                                | Port | Result |
|--------------------------------------------------------------------------|------|--------|
| <b>Certificates</b>                                                      |      |        |
| Trusted SSL Certificates                                                 | 443  | Pass ✓ |
|                                                                          | 9997 | Pass ✓ |
| No other Certificate Authority warnings                                  | 443  | Pass ✓ |
|                                                                          | 9997 | Pass ✓ |
| Hostname verified in certificate                                         | 443  | Pass ✓ |
|                                                                          | 9997 | Pass ✓ |
| <b>ATS</b>                                                               |      |        |
| ATS - SSL Certificate has SHA digest of at least 256                     | 443  | Pass ✓ |
| ATS - Forward Secrecy ciphers supported                                  | 443  | Pass ✓ |
| ATS - Leaf Certificate signed with at least 2048 RSA or 256 ECC bits     | 443  | Pass ✓ |
| ATS - Trusted SSL Certificates                                           | 443  | Pass ✓ |
| ATS - TLSv1.2 is supported                                               | 443  | Pass ✓ |
| <b>ACL</b>                                                               |      |        |
| Restrict access of Core System Manager portal to internal networks only. | 443  | Pass ✓ |
|                                                                          | 8443 | Pass ✓ |
| Restrict Access to Sentry Service Port on Core                           | 443  | Pass ✓ |
|                                                                          | 8443 | Pass ✓ |
| Restrict access of Core Admin Portal to internal networks only           | 443  | Pass ✓ |
|                                                                          | 8443 | Pass ✓ |

| Port | Expiration Date                                              |
|------|--------------------------------------------------------------|
| 443  | Mon, 27 Apr 2020 23:59:59 UTC (expires in 3 months 17 days ) |
| 9997 | Mon, 27 Apr 2020 23:59:59 UTC (expires in 3 months 17 days ) |

Validez del Certificado TLS expuesto para encintar las comunicaciones entre dispositivo y servidor Core

[Home](#)

## ANEXO II. EJEMPLO CHEQUEO DE SEGURIDAD SERVIDOR SENTRY



# Security Health Check

[Home](#)

## Scan Results

Hostname: Sentry External FQDN  
Ports: 443

Scan Results:  
No issues identified.

**Additional Details on the Tests:**

| Test Name                                                            | Port | Result |
|----------------------------------------------------------------------|------|--------|
| <b>Certificates</b>                                                  |      |        |
| Trusted SSL Certificates                                             | 443  | Pass ✓ |
| No other Certificate Authority warnings                              | 443  | Pass ✓ |
| Hostname verified in certificate                                     | 443  | Pass ✓ |
| <b>ATS</b>                                                           |      |        |
| ATS - SSL Certificate has SHA digest of at least 256                 | 443  | Pass ✓ |
| ATS - Forward Secrecy ciphers supported                              | 443  | Pass ✓ |
| ATS - Leaf Certificate signed with at least 2048 RSA or 256 ECC bits | 443  | Pass ✓ |
| ATS - Trusted SSL Certificates                                       | 443  | Pass ✓ |
| ATS - TLSv1.2 is supported                                           | 443  | Pass ✓ |

| Port | Expiration Date                                              |
|------|--------------------------------------------------------------|
| 443  | Mon, 27 Apr 2020 23:59:59 UTC (expires in 3 months 17 days ) |

## ANEXO III. VISIBILIDADES CORE Y SENTRY

### III.1 REQUISITOS GENERALES CORE Y SENTRY

| Requisitos                                                                                             | Notas                                                                                            |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| 1 IP privada para Core                                                                                 |                                                                                                  |
| 1 IP privada para Sentry                                                                               |                                                                                                  |
| 1 IP privada para Sentry2, etc                                                                         |                                                                                                  |
| Dirección IP de la puerta de enlace predeterminada para Core                                           |                                                                                                  |
| Dirección IP de la puerta de enlace predeterminada para Sentry1                                        |                                                                                                  |
| Dirección IP de la puerta de enlace predeterminada para Sentry2, etc                                   |                                                                                                  |
| Dirección IP de servidor DNS                                                                           |                                                                                                  |
| Dirección IP de servidor NTP                                                                           |                                                                                                  |
| 1 Entrada A en el DNS externo para la URL elegida para Core que resuelva la IP pública                 | ex. ssc01.x.y.z donde x.y.z es el dominio externo de su propiedad                                |
| 1 Entrada A en el DNS externo para la URL elegida para Sentry1 que resuelva su IP pública              | ex. misc01.x.y.z donde x.y.z es el dominio externo de su propiedad                               |
| 1 Entrada A en el DNS externo para la URL elegida para Sentry2 que resuelva su IP pública              | ex. mics02.x.y.z donde x.y.z es el dominio externo de su propiedad                               |
| 1 Entrada A en el DNS interno para la URL elegida para Core que resuelva su IP privada                 | Hay que replicar la zona externa internamente para que la conexión desde la red wifi sea optima. |
| 1 Entrada A en el DNS interno para la URL elegida para Sentry1 que resuelva su IP privada              | Hay que replicar la zona externa internamente para que la conexión desde la red wifi sea optima. |
| 1 Entrada A en el DNS interno para la URL elegida para Sentry2 que resuelva su IP privada              | Hay que replicar la zona externa internamente para que la conexión desde la red wifi sea optima. |
| 1 certificado TLS confiable desde internet que contenga la URL de Core                                 | Para proteger las comunicaciones de Core                                                         |
| 1 certificado TLS confiable desde internet que contenga la URL de Sentry1                              | Para proteger las comunicaciones de Sentry 1                                                     |
| 1 certificado TLS confiable desde internet que contenga la URL de Sentry2                              | Para proteger las comunicaciones de Sentry 2                                                     |
| Admin PC con acceso a la consola de cada máquina virtual de Core y Sentry para realizar la instalación |                                                                                                  |
| Borrar y volver a crear los discos duros de cada VM de la lista, dejándolos vacíos.                    |                                                                                                  |

| Requisitos                                                                                                  | Notas |
|-------------------------------------------------------------------------------------------------------------|-------|
| Se debe tener acceso para montar archivos ISO dentro de cada VM de Core y Sentry, para instalar el software |       |
| 1 cuenta de Gmail de consumo para realizar la integración con Android Enterprise                            |       |
| 1 cuenta AppleID para realizar la configuración del servicio APNS de iOS                                    |       |

## III.2 VISIBILIDADES DE CORE

| TRÁFICO         | ORIGEN              | PUERTO                                        | DESTINO    | SERVICIO           | DESCRIPCIÓN                                                                                                                |
|-----------------|---------------------|-----------------------------------------------|------------|--------------------|----------------------------------------------------------------------------------------------------------------------------|
| Internet a Core | INTERNET            | HTTPS 443                                     | Core       | MDM                | Este es el puerto desde el que se conectan los terminales con el servidor UEM para intercambio de postura, políticas, etc. |
| Internet a Core | INTERNET            | TCP 9997                                      | Core       | TLS Sync           | Este puerto es usado por el cliente de Android para la sincronización de configuraciones, políticas, etc mediante TLS      |
| Internet a Core | accounts.google.com | HTTPS 443                                     | Core       | Android Enterprise | Necesario para el envío de configuraciones y políticas a través de la API de Android Enterprise                            |
| Internet a Core | www.googleapis.com  | HTTPS 443                                     | Core       | Android Enterprise | Necesario para el envío de configuraciones y políticas a través de la API de Android Enterprise                            |
| Core a Internet | Core                | HTTPS 443<br>TCP 2195<br>TCP 2196<br>TCP 2197 | 17.0.0.0/8 | iOS                | Necesario para el envío de configuraciones y políticas a través de la API de Apple                                         |

| TRÁFICO         | ORIGEN | PUERTO    | DESTINO                                  | SERVICIO           | DESCRIPCIÓN                                                                                                           |
|-----------------|--------|-----------|------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------|
| Core a Internet | Core   | HTTPS 443 | api.push.apple.com                       | iOS                | Necesario para el envío de configuraciones y políticas a través de la API de Apple                                    |
| Core a Internet | Core   | TCP 2195  | gateway.push.apple.com                   | iOS                | Necesario para el envío de configuraciones y políticas a través de la API de Apple                                    |
| Core a Internet | Core   | TCP 2196  | feedback.push.apple.com                  | iOS                | Necesario para el envío de configuraciones y políticas a través de la API de Apple                                    |
| Core a Internet | Core   | TCP 2197  | api.push.apple.com                       | iOS                | Necesario para el envío de configuraciones y políticas a través de la API de Apple                                    |
| Core a Internet | Core   | HTTPS 443 | api.push.apple.com                       | iOS                | Necesario para el envío de configuraciones y políticas a través de la API de Apple                                    |
| Core a Internet | Core   | HTTPS 443 | support.Mobileiron.com (199.127.90.0/23) | Mobileiron Gateway | Necesario para actualizaciones de servidor y para subir los logs de manera segura a la web de soporte del fabricante. |
| Core a Internet | Core   | HTTPS 443 | app-gw.Mobileiron.com                    | Mobileiron Gateway | Necesario para algunos servicios básicos sobre dispositivos iOS                                                       |

| TRÁFICO         | ORIGEN | PUERTO               | DESTINO                                         | SERVICIO              | DESCRIPCIÓN                                                                                         |
|-----------------|--------|----------------------|-------------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------------|
| Core a Internet | Core   | HTTPS 443            | coresms.<br>Mobileiron.com                      | Mobileiron Gateway    | Necesario para enviar SMS para alertas e invitaciones                                               |
| Core a Internet | Core   | HTTPS 443            | coreapns.<br>Mobileiron.com                     | Mobileiron Gateway    | Necesario para envío de notificaciones Push desde Core                                              |
| Core a Internet | Core   | HTTPS 443            | clm.<br>Mobileiron.com                          | Mobileiron Gateway    | Necesario para envío de notificaciones Push desde Core                                              |
| Core a Internet | Core   | HTTPS 443            | supportcdn.<br>Mobileiron.com                   | Mobileiron Gateway    | Necesario para sistema distribuido de actualizaciones de sistema                                    |
| Core a Internet | Core   | HTTPS 443            | core-gcm.<br>Mobileiron.com                     | Mobileiron Gateway    | Necesario para el envío de notificaciones Push a Android                                            |
| Core a Internet | Core   | HTTPS 443            | corefcm.<br>Mobileiron.com<br>(199.127.90.0/23) | Mobileiron Gateway    | Necesario para el envío de notificaciones Push a Android                                            |
| Core a Internet | Core   | HTTPS 443<br>TCP 443 | appconfig.cdn.<br>Mobileiron.com                | Repositorio AppConfig | Necesario para la actualización automática de plantillas de configuración de apps de iOS y Android. |

| TRÁFICO         | ORIGEN | PUERTO    | DESTINO                 | SERVICIO       | DESCRIPCIÓN                                                                                                                                                     |
|-----------------|--------|-----------|-------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Core a Internet | Core   | HTTPS 443 | vpp.itunes.apple.com    | Apple VPP      | Necesario para el programa de compras por volumen de apps de Apple. Esto sirve para que los usuarios no requieran de un AppleID para instalar apps gestionadas. |
| Core a Internet | Core   | HTTPS 443 | www.apple.com           | Apple VPP      | Necesario para el programa de compras por volumen de apps de Apple. Esto sirve para que los usuarios no requieran de un AppleID para instalar apps gestionadas. |
| Core a Internet | Core   | HTTPS 443 | secure-metrix.apple.com | Apple VPP      | Necesario para el programa de compras por volumen de apps de Apple. Esto sirve para que los usuarios no requieran de un AppleID para instalar apps gestionadas. |
| Core a Internet | Core   | HTTPS 443 | itunes.apple.com        | Apple AppStore | Necesario para buscar e importar apps públicas de iOS a Core.                                                                                                   |
| Core a Internet | Core   | HTTPS 443 | *.phobos.apple.com      | Apple AppStore | Necesario para buscar e importar apps públicas de iOS a Core.                                                                                                   |

| TRÁFICO         | ORIGEN | PUERTO    | DESTINO                   | SERVICIO             | DESCRIPCIÓN                                                                              |
|-----------------|--------|-----------|---------------------------|----------------------|------------------------------------------------------------------------------------------|
| Core a Internet | Core   | HTTPS 443 | *.mzstatic.com            | Apple AppStore       | Necesario para buscar e importar apps públicas de iOS a Core.                            |
| Core a Internet | Core   | HTTPS 443 | api.mqcdn.com             | Apple AppStore       | Necesario para buscar e importar apps públicas de iOS a Core.                            |
| Core a Internet | Core   | HTTPS 443 | developer.mapquest.com    | API de liocalización | Necesario para que el administrador pueda localizar dispositivos.                        |
| Core a Internet | Core   | TCP 80    | hoedus.Mobileiron.com     | Google Play          | Necesario para hacer búsquedas de apps de Google Play para Android Enterprise            |
| Core a Internet | Core   | HTTPS 443 | lh1.googleusercontent.com | Google Play          | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise |
| Core a Internet | Core   | HTTPS 443 | lh2.googleusercontent.com | Google Play          | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise |
| Core a Internet | Core   | HTTPS 443 | lh3.googleusercontent.com | Google Play          | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise |

| TRÁFICO         | ORIGEN | PUERTO    | DESTINO                   | SERVICIO    | DESCRIPCIÓN                                                                              |
|-----------------|--------|-----------|---------------------------|-------------|------------------------------------------------------------------------------------------|
| Core a Internet | Core   | HTTPS 443 | lh4.googleusercontent.com | Google Play | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise |
| Core a Internet | Core   | HTTPS 443 | lh5.googleusercontent.com | Google Play | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise |
| Core a Internet | Core   | HTTPS 443 | lh6.googleusercontent.com | Google Play | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise |
| Core a Internet | Core   | HTTPS 443 | lh1.ggpht.com             | Google Play | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise |
| Core a Internet | Core   | HTTPS 443 | lh2.ggpht.com             | Google Play | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise |
| Core a Internet | Core   | HTTPS 443 | lh3.ggpht.com             | Google Play | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise |

| TRÁFICO         | ORIGEN | PUERTO    | DESTINO                           | SERVICIO            | DESCRIPCIÓN                                                                                                |
|-----------------|--------|-----------|-----------------------------------|---------------------|------------------------------------------------------------------------------------------------------------|
| Core a Internet | Core   | HTTPS 443 | lh4.ggpht.com                     | Google Play         | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise                   |
| Core a Internet | Core   | HTTPS 443 | lh5.ggpht.com                     | Google Play         | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise                   |
| Core a Internet | Core   | HTTPS 443 | lh6.ggpht.com                     | Google Play         | Necesario para importar imágenes e iconos de apps de Google Play para Android Enterprise                   |
| Core a Internet | Core   | HTTPS 443 | Internet                          | Client TLS          | Necesario para enviar configuraciones, comandos y políticas a dispositivos Android con autenticación mutua |
| Core a Internet | Core   | HTTPS 443 | deviceservices-external.apple.com | iOS Activation Lock | Necesario para activar y desactivar la protección antirrobo de dispositivos iOS                            |
| Core a Internet | Core   | HTTPS 443 | mdmenrollment.apple.com           | Apple DEP           | Necesario para el programa de autoregistro de dispositivos iOS                                             |

| TRÁFICO                  | ORIGEN | PUERTO  | DESTINO                              | SERVICIO  | DESCRIPCIÓN                                                                                                                                              |
|--------------------------|--------|---------|--------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Core a Internet          | Core   | TCP 443 | api.mqcdn.com                        | MapQuest  | Necesario para pintar en el mapa la localización del dispositivo a ser localizado                                                                        |
| Core a Internet          | Core   | TCP 443 | webapi.teamviewer.com                | Help@Work | Necesario para utilizar la API de control remoto para dispositivos Android                                                                               |
| Core a Red de Servidores | Core   | TCP 636 | Dirección URL o IP de servidor LDAPS | LDAPS     | Necesario para dar visibilidad al Directorio Activo o fuente de LDAPS en Core, validar contraseñas, etc.                                                 |
| Core a Red de Servidores | Core   | TCP 25  | Dirección URL o IP de servidor SMTP  | SMTP      | Necesario para envío de alertas e invitaciones por email                                                                                                 |
| Core a Red de Servidores | Core   | UDP 53  | Dirección URL o IP de Servidor DNS   | DNS       | Necesario para que Core tenga resolución DNS, incluida la de servidores LDAPS, etc.                                                                      |
| Core a Red de Servidores | Core   | UDP 123 | Dirección URL o IP de Servidor NTP   | NTP       | Necesario para sincronizar la hora con el sistema de servidores interno. Es importante cuando se utilizan certificados emitidos mediante protocolo SCEP. |

| TRÁFICO                  | ORIGEN | PUERTO                  | DESTINO                             | SERVICIO      | DESCRIPCIÓN                                                                                                                     |
|--------------------------|--------|-------------------------|-------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------|
| Core a Red de Servidores | Core   | HTTPS 443               | Dirección URL o IP de Servidor SCEP | SCEP          | Necesario si se va distribuir certificados emitidos mediante una Autoridad de Certificación Interna, mediante el protocolo SCEP |
| Core a Sentry            | Core   | HTTPS 9090<br>HTTPS 443 | Sentry                              | Sentry config | Necesario para intercambio de información entre Core y Sentry                                                                   |

### III.3 VISIBILIDAD DE SENTRY

| TRÁFICO                           | ORIGEN   | PUERTO                 | DESTINO                                         | SERVICIO                                                                                       | DESCRIPCIÓN                                                                                                                                                  |
|-----------------------------------|----------|------------------------|-------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Internet a Sentry</b>          | INTERNET | HTTPS 443              | Sentry                                          | Correo ActiveSync<br>Reverse Proxy<br>Terminador VPN para Mobileiron Tunnel para iOS y Android | Reverse Proxy con acceso condicional para acceder a los servicios internos de manera segura.                                                                 |
| <b>Sentry a Internet</b>          | Sentry   | HTTPS 443              | support.<br>Mobileiron.com<br>(199.127.90.0/23) | Actualizaciones de servidor                                                                    | Necesario para actualizaciones de servidor y para subir logs de servidor en caso de incidencia de manera segura a la web de soporte                          |
| <b>Sentry a Core</b>              | Sentry   | HTTPS 443              | Core                                            | Sentry config                                                                                  | Necesario para intercambio de información entre Core y Sentry                                                                                                |
| <b>Sentry a Red de Servidores</b> | Sentry   | TCP 445<br>TCP 139     | Servidores de unidades de red SMB               | Unidades de red                                                                                | Necesario para que los dispositivos accedan a las unidades de red de los servidores de ficheros internos, si aplica.                                         |
| <b>Sentry a red de Servidores</b> | Sentry   | HTTP 80<br>o HTTPS 443 | Dirección URL o IP de Servidor SCEP             | SCEP                                                                                           | Necesario para comprobar si el certificado que presentan los dispositivos es válido, en tanto este haya sido emitido por el servidor de certificados interno |

| TRÁFICO                           | ORIGEN | PUERTO               | DESTINO                                       | SERVICIO          | DESCRIPCIÓN                                                                                                     |
|-----------------------------------|--------|----------------------|-----------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Sentry a red de Servidores</b> | Sentry | Puertos web internos | Dirección URL o IP de Servidores Web internos | Navegación Segura | Necesario para que los dispositivos que conecta a través de Sentry puedan llegar a los servidores web internos. |
| <b>Sentry a red de Servidores</b> | Sentry | HTTPS 443            | Direcciones URL o IP de Servidores Exchange   | Correo ActiveSync | Necesario para sincronizar correo ActiveSync en los dispositivos que conectan a través de Sentry                |
| <b>Sentry a red de Servidores</b> | Sentry | UDP 53               | Dirección URL o IP de Servidor DNS            | DNS               | Necesario para que Sentry tenga resolución DNS, incluida la de servidores internos                              |
| <b>Sentry a Red de Servidores</b> | Sentry | UDP 123              | Dirección URL o IP de Servidor NTP            | NTP               | Necesario para sincronizar la hora con el sistema de servidores interno.                                        |
| <b>Sentry a Red de Servidores</b> | Sentry | TCP 25               | Dirección URL o IP de servidor SMTP           | SMTP              | Necesario para envío de alertas or correo electrónico                                                           |

### III.4 VISIBILIDADES DE RED

| TRÁFICO                        | ORIGEN          | PUERTO     | DESTINO | SERVICIO                                  | DESCRIPCIÓN                                                                                                                           |
|--------------------------------|-----------------|------------|---------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>ADMIN PC A CORE</b>         | Red PC Admin    | HTTPS 8443 | Core    | Administración de dispositivos            | Necesario para que el administrador pueda acceder al portal de administración de dispositivos y a la consola de configuración de Core |
| <b>ADMIN PC A CORE</b>         | Red PC Admin    | SSH 22     | Core    | SSH                                       | Necesario para conectar a la línea de comandos de Core                                                                                |
| <b>ADMIN PC A SENTRY</b>       | Red PC Admin    | SSH 22     | Sentry  | SSH                                       | Necesario para conectar a la línea de comandos de Sentry                                                                              |
| <b>ADMIN PC A SENTRY</b>       | Red PC Admin    | HTTPS 8443 | Sentry  | Portal de configuración interna de Sentry | Necesario para configurar los valores de red, cifrado etc de Sentry                                                                   |
| <b>Red PCs Usuarios a Core</b> | Red PC Usuarios | HTTPS 443  | Core    | Portal de autogestión del usuario         | Necesario para que los usuarios accedan al portal de autogestión                                                                      |

### III.5 VISIBILIDADES WIFI CORPORATIVA

| TRÁFICO                      | ORIGEN                | PUERTO                                           | DESTINO                      | SERVICIO                           | DESCRIPCIÓN                                                                                                                                                                 |
|------------------------------|-----------------------|--------------------------------------------------|------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | TCP 5223                                         | 17.0.0.0/8                   | APNS iOS                           | Necesario para el funcionamiento de dispositivos iOS dentro de la red wifi corporativa.                                                                                     |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | TCP 5223                                         | ax.init.<br>itunes.apple.com | APNS iOS                           | Necesario para el funcionamiento de dispositivos iOS dentro de la red wifi corporativa.                                                                                     |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | TCP 5224                                         | ocsp.apple.com:              | APNS iOS                           | Necesario para el funcionamiento de dispositivos iOS dentro de la red wifi corporativa.                                                                                     |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS<br>443<br>TCP 5228<br>TCP 5229<br>TCP 5230 | Bloque Google<br>ASN 15169   | GCM y FCM<br>Android<br>Enterprise | Necesario para el funcionamiento de dispositivos Android Enterprise dentro de la red wifi corporativa                                                                       |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS<br>443                                     | www.<br>googleapis.<br>com   | GCM y FCM<br>Android<br>Enterprise | Necesario para el funcionamiento de dispositivos Android Enterprise dentro de la red wifi corporativa.<br><a href="https://ipinfo.io/AS15169">https://ipinfo.io/AS15169</a> |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS<br>443                                     | accounts.<br>google.com      | GCM y FCM<br>Android<br>Enterprise | Necesario para el funcionamiento de dispositivos Android Enterprise dentro de la red wifi corporativa                                                                       |

| TRÁFICO                      | ORIGEN                | PUERTO    | DESTINO                        | SERVICIO                     | DESCRIPCIÓN                                                                                   |
|------------------------------|-----------------------|-----------|--------------------------------|------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS 443 | api.polariskit.com             | Servidor licencias Docs@Work | Necesario para activar la licencia de Polaris Office incluida dentro del cliente de Docs@Work |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS 443 | enterprise.infraware.net       | Servidor licencias Docs@Work | Necesario para activar la licencia de Polaris Office incluida dentro del cliente de Docs@Work |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS 443 | pspdfkit-license-service-1.com | Servidor licencias Docs@Work | Necesario para activar la licencia de Polaris Office incluida dentro del cliente de Docs@Work |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS 443 | pspdfkit-license-service-2.com | Servidor licencias Docs@Work | Necesario para activar la licencia de Polaris Office incluida dentro del cliente de Docs@Work |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS 443 | pspdfkit-license-service-3.com | Servidor licencias Docs@Work | Necesario para activar la licencia de Polaris Office incluida dentro del cliente de Docs@Work |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS 443 | pspdfkit-license-service-4.com | Servidor licencias Docs@Work | Necesario para activar la licencia de Polaris Office incluida dentro del cliente de Docs@Work |

| TRÁFICO                      | ORIGEN                | PUERTO                | DESTINO  | SERVICIO                  | DESCRIPCIÓN                                                                                |
|------------------------------|-----------------------|-----------------------|----------|---------------------------|--------------------------------------------------------------------------------------------|
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS 443<br>TCP 5938 | Internet | Control Remoto de Android | Necesario para el control remoto de dispositivos Android dentro de la red wifi corporativa |
| <b>Red Wifi dispositivos</b> | Red Wifi dispositivos | HTTPS 9997            | Core     | TLS Client                | Puerto de autenticación mutua TLS para Android                                             |

Todos los puertos descritos en esta tabla (excepto los UDP) deben ser bidireccionales para permitir el intercambio de información entre sistemas

## ANEXO IV. DISTRIBUIDORES AUTORIZADOS

Listado de las empresas en España que se han certificado para la implementación y configuración de la plataforma UEM de Mobileiron en versión on-premise (Mobileiron CORE)



## ANEXO V. COMO ADQUIRIR MOBILEIRON

98. La instalación, mantenimiento y soporte de la plataforma UEM de Mobileiron requiere de los servicios profesionales de un partner certificado por Mobileiron.

99. Para más información, póngase en contacto con Mobileiron a través de:

Mobileiron Iberia

Calle Campoamor 14

28004 Madrid

Spain

+34 910496676

iberia@Mobileiron.com