**Universidad de Buenos Aires (UBA)**

**Facultades de Ciencias Económicas,**

**Cs. Exactas y Naturales e Ingeniería**

**Trabajo Final de Especialización**

**Seguridad Informática**

***Tema***

# *Análisis e implementación de medidas de seguridad en entornos BYOD.*

**Autor:** Christopher Robleto

**Tutor:** Hugo Pagola

**2017**

**COHORTE 2014**

## Declaración Jurada de origen de los contenidos

Declaración Jurada de origen de los contenidos “Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

_____

Christopher Ramón Robleto Hodgson

DNI 95.296.237

## Resumen

*Bring-your-own-Device* o Trae-tu-propio-dispositivo son estrategias de movilidad empresarial que están marcando tendencia en los últimos 10 años.

Consiste en permitir a los usuarios utilizar sus dispositivos para desarrollar tareas laborales. Esto trae consigo nuevos desafíos a la seguridad de la información, el entorno y los dispositivos.

A lo largo de este trabajo analizaremos los factores más importantes de seguridad a tener en cuenta al implementar este tipo de estrategias. Al finalizar este trabajo, se brindan recomendaciones para implementar entornos de *BYOD* seguros.

**Palabras clave:** Estrategia, Movilidad empresarial, *Bring-Your-Own-Device, Mobile Device Management*, *Mobile Application Management*,

# Tabla de contenidos

# Nómina de Abreviaturas

***COPE***: *Corporated Owned Personal Enabled,* Dispositivos propiedad de la organización habilitado para uso personal.
***COBO***: *Corporated Owned Business Only,* Dispositivo propiedad de la organización de uso exclusivo para tareas laborales.
***BYOD***: *Bring Your Own Device,* Trae tu propio dispositivo.
***APT***: *Advanced Persistent Threat,* Amenaza persistente avanzada.
***ISO***: *International Standard Organization,* Organización Internacional de Estándares.
***CBK***: *Common Body of Knowledge,* Cuerpo de conocimiento común.
***MDM***: *Mobile Device Management,* Gestión de Dispositivos Móviles.
***MAM***: *Mobile Application Management,* Gestión de Aplicaciones Móviles.
***EFSS***: *Enterprise File Sync and Sharing,* Sincronización y uso compartido de archivos empresariales.
***VPN***: *Virtual Private Network,* Redes privadas virtuales.
***NAC***: *Network Access Control,* Control de acceso de red.

# INTRODUCCION

Las estrategias de movilidad empresarial están cambiando debido al rápido avance de la tecnología y su accesibilidad. Organizaciones que anteriormente adquirían todos sus dispositivos móviles, han optado por permitir a sus usuarios utilizar sus dispositivos personales para desempeñar sus funciones laborales. Esto ha generado pérdida de control y visibilidad de la información.

Este trabajo está enfocado a brindar una guía para retomar el control de la información corporativa en organizaciones que cuentan con estrategias de *BYOD* o que están pensando implementarlas.

En esta investigación se abarcan desde los aspectos fundamentales, identificando las vulnerabilidades y amenazas a los que se está expuesto. Luego, se analizan las diferentes características de las herramientas disponibles, políticas y controles vinculados a las estrategias de *BYOD*.

En este trabajo solamente se mencionan las vulnerabilidades y amenazas, no se profundiza en metodologías de análisis de riesgo o vectores de ataques específicos. Tampoco abarca implementación de controles, ni soluciones en particular.

Para concluir este trabajo, se brindan lineamientos base, a tener en cuenta al momento de implementar entornos de *BYOD* seguros.

En el **anexo 1**, se brinda una guía de instalación de la solución **Blackberry Unified Endpoint Management**, que pueden ser utilizados por todo tipo de organizaciones, ya que cumple con todos los requisitos de soluciones MDM y MAM que aseguran los entornos *BYOD*.

# CAPÍTULO 1 FUNDAMENTOS

## 1.1 Estrategias de movilidad empresarial

En la actualidad existen diferentes tipos de estrategias para abordar los dispositivos móviles.

Dentro de las más comunes tenemos:

- ***C**ompany **O**wned **B**usiness **O**nly (COBO):* Es la estrategia de movilidad empresarial más restrictiva. Los dispositivos son propiedad de las organizaciones y están habilitados solamente para uso corporativo.
- ***C**ompany **O**wned **P**ersonal **E**nabled (COPE)*: Esta estrategia es menos restrictiva que permite la utilización de dispositivos corporativos para actividades personales.
- ***B**ring **Y**our **O**wn **D**evice (BYOD):* Es la estrategia más versátil pero menos control sobre los dispositivos ya que estos son propiedad de los usuarios.

Para implementar cualquiera de estas estrategias es necesario tener claro cuál es el objetivo principal de la organización. La tabla 1. Nos provee una visión de cual estrategia es más conveniente en base a dichos objetivos.

| Altamente Conveniente | Ocasionalmente Conveniente | No conveniente |
|---|---|---|

| | Estrategia | | |
|---|---|---|---|
| | BYOD | COPE | COBO |
| Mantener el comportamiento actual | | | |
| Reducir costos | | | |
| Movilidad como inversión estratégica a largo plazo | | | |
| Poco apetito al riesgo | | | |
| Regulaciones exigentes | | | |

*Tabla 1. Comparativa de estrategias de movilidad y objetivos.[1]*

Podemos ver que las estrategias de *BYOD* son convenientes en entornos donde se desea mantener el comportamiento actual de los usuarios, pero no convenientes para industrias altamente reguladas o con una tolerancia baja al riesgo.

## 1.2 Beneficios

Las estrategias de BYOD presentan beneficios para la organización y sus diversas partes interesadas. Las partes interesadas las conforman el negocio, los empleados y el departamento de TI según explican Fujitsu[2] y MeruNetworks[3]

### 1.2.1 El negocio

La parte interesada con mayores beneficios es el negocio. Se logra mejorar la productividad de los empleados, la imagen del negocio para atraer a nuevos recursos humanos competentes, obliga a revisar las medidas de seguridad y reducir los activos de hardware, lo que se traduce en ahorro de costos al no tener que renovar el inventario tecnológico.

### 1.2.2 Los empleados

Los empleados son los primeros promotores para implementar estrategias de *BYOD*, porque les permite tener mayor flexibilidad y mayor integración vida-trabajo que permite trabajar desde cualquier lugar.

Además de esto, se reduce la complejidad de los empleados de utilizar dos dispositivos, uno personal y uno corporativo. Esto logra mejorar la satisfacción y el compromiso con respecto a la organización.

### 1.2.3 Departamento de TI

Esta parte interesada; normalmente obviada, también se beneficia, ya que se libera del ciclo de vida de los activos no estratégicos (celulares, las computadoras, etc.) y permite, dar un mayor enfoque de recursos a proyectos críticos. Además, reduce el entrenamiento de uso de los equipos a los usuarios, por el simple hecho que ya están acostumbrados a su uso.

## 1.3 Desafíos

Así como BYOD abre nuevos beneficios a las diferentes partes interesadas, también trae consigo nuevos desafíos de seguridad y gestión a ser abordados.

Dentro de los desafíos identificados en el CBK[4], por Wang[5] y Hewlett-Packard [6] tenemos:

### 1.3.1 Descubrimiento de dispositivos

Al implementar estrategias de *BYOD*, es esencial mantener un monitoreo y seguimiento de los dispositivos. El desafío radica en detectar dichos dispositivos dentro de las redes corporativas.

### 1.3.2 Espacio corporativo

Los dispositivos personales se convierten en extensiones de la organización, por lo tanto, deben estar de acuerdo con las políticas de seguridad.

A su vez, estos también cumplen funciones personales y es necesario que los usuarios mantengan la flexibilidad para manejar los dispositivos a su manera. Esta separación de los ambientes, se convierte en un desafío a ser afrontado por las organizaciones.

### 1.3.3 Protección de datos

Los datos de la organización pueden ser almacenados o transmitidos a través de dispositivos personales en forma de correos electrónicos, adjuntos, lista de contactos, calendarios, documentos, entre otros.

Es un desafío muy importante lograr separar estos datos y lograr restringir el acceso de estos datos por partes externas o internas no autorizadas.

### 1.3.4 Aplicación de políticas de seguridad

Combatir la renuencia de los usuarios por hacer respaldos de la información, conocer las políticas de seguridad, entre otras, es uno de los mayores desafíos que afronta la seguridad en entornos BYOD.

Muchos de estos problemas, podrían ser resueltos al implementar auditorias o imponer estándares y políticas de la organización. Sin embargo, esto se dificulta debido a que los dispositivos son propiedad de los empleados.

### 1.3.5 Mantenimiento de la seguridad y mitigación de los riesgos

La autenticación y autorización de estos dispositivos, juega un rol muy importante para proteger los sistemas de información, la privacidad y evitar fuga de información. Parte del desafío, involucra la revocación de privilegios de acceso de los empleados cuando abandonan la organización o los dispositivos son extraviados o robados.

## 1.4 Requerimientos

Implementar políticas de BYOD, agrega requerimientos de seguridad a la infraestructura informática de las organizaciones. Debido a esto, es necesario que la organización cuente con un nivel de seguridad general aceptable. HP[6] nos brinda requisitos necesarios parar tener un enfoque integral de la seguridad y la gestión de BYOD:

- **Estrategia de Seguridad:** Es necesario, contar con una estrategia de seguridad de dispositivos móviles definida para poder asegurar que las políticas de BYOD estén alineadas a los procesos de negocio.
- **Seguridad en capas:** Las estrategias de *BYOD* pueden dividirse en las capas de hardware y aplicaciones, infraestructura e información. Es necesario contar con medidas de seguridad específicas para cada una de estas capas.
- **Control de acceso por identidad:** Al contar con dispositivos personales dentro de la organización, es vital lograr identificar cada dispositivo con un usuario en particular para poder controlar el acceso de los mismos.
- **Detección de dispositivos no autorizados:** Es necesario contar con mecanismos de detección de dispositivos ajenos a la organización o que no estén siendo gestionados para poder aislarlos de manera efectiva.

- **Gestión Integral:** Al incluir diferentes tipos de dispositivos, las estrategias de *BYOD* añaden complejidad a la gestión de las soluciones. Es necesario considerar implementar una solución integral, que incluya todas las tecnologías y dispositivos permitidos.
  La gestión integral, a su vez, mejora los tiempos de respuesta a incidentes, rendimientos, además de proveer mayor visibilidad, mitigación de riesgos y reducir costos operativos.

Por limitaciones en el alcance de este trabajo, no se profundizará en el funcionamiento del control de acceso ni detección de sistemas no autorizados, por ser soluciones que abarcan otras áreas.

# CAPÍTULO 2 : VULNERABILIDADES, AMENAZAS Y ATAQUES

Las grandes organizaciones, son las primeras en preocuparse por analizar y tratar los riesgos a los que están expuestos. Esto se debe, al miedo que estas se conviertan en pérdidas monetarias importantes o por estar sometidas bajo alguna regulación específica.

En Latinoamérica, la cultura de seguridad de TI, está tomando cada vez más importancia[7].

Las estrategias de *BYOD* no están exentas de vulnerabilidades, amenazas y riesgos; todo lo contrario; incorporan nuevos riesgos y amenazas por los que velar.

En este capítulo se abordan de manera general las amenazas, vulnerabilidades, riesgos y vectores de ataques que se derivan de las estas estrategias dentro de las organizaciones en la actualidad, para proporcionar un panorama de la situación real.

## 2.1 Riesgos y Amenazas

Para poder identificar las vulnerabilidades y amenazas que derivan de las estrategias de BYOD, se procedió a catalogar dichas amenazas en 3 categorías:

- **Dispositivos y Aplicaciones:** Todo aquello relacionado con el dispositivo físico y sus aplicaciones.
- **Datos:** Todo lo relacionado a los datos, tanto por acceso a los datos, como el almacenamiento del mismo.
- **Infraestructura:** Amenazas y vulnerabilidades vinculados a la infraestructura que acceden estos dispositivos.

Luego de analizar varios documentos[8]–[12] se logró identificar y separar las amenazas y vulnerabilidades en las siguientes categorías:

### 2.1.1 Dispositivos y Aplicaciones

- *Acceso Físico:* Uno de las vulnerabilidades principales no solo de los dispositivos personales, sino, de los dispositivos móviles en general, es el acceso físico a ellos. Esto se debe, a la naturaleza portable de los mismos que los hace más susceptibles a ser manipulados por terceras partes no autorizadas.

  En el caso de los dispositivos *BYOD*, al ser propiedad del usuario, no se puede forzar ningún tipo de medidas contra el uso del dispositivo por terceras partes. Esto pone en riesgo la información corporativa almacenada en dichos dispositivos.
- *Robo o extravío:* Al igual que el acceso físico, este es un riesgo inherente de los dispositivos móviles. Normalmente, el principal incentivo para el robo de los dispositivos, es su valor en el mercado.

  El robo o extravío de estos dispositivos puede significar la pérdida de información corporativa valiosa de estar almacenados localmente. Además, si combinamos esto con la falta de medidas de seguridad en el dispositivo, estamos poniendo en riesgo la confidencialidad de la información.
- *Confianza en los dispositivos:* Este riesgo se basa en el acceso los recursos internos que tienen los dispositivos personales. Algunas de las variables más importantes en este riesgo, es el nivel de acceso y el estado de los dispositivos (si está actualizado, la integridad del sistema operativo, "*jailbreak" o "rooted", etc)* y el cumplimiento de los dispositivos ya autenticados. Todas las acciones de estas variables, crean un riesgo que puede afectar pilares de la seguridad como: la confidencialidad, integridad o disponibilidad de la información.
- *Implementación de políticas:* Los dispositivos móviles, al ser propiedad privada del usuario, dificulta la aplicación de configuración y medidas de seguridad estándar de la organización. Esto pone riesgo la confidencialidad, integridad o disponibilidad de la información a la que tienen acceso estos dispositivos.
- *Versiones de sistemas operativos:* Debido a la gran cantidad de versiones de sistemas operativos utilizados en los dispositivos de los

usuarios, se torna complejo encontrar una solución práctica para el control de dichos dispositivos.

- *Actualizaciones de sistemas operativos:* A diferencia de los dispositivos de la organización que cuentan con un plan de actualización y mantenimiento de los dispositivos corporativos, los usuarios pueden mantener sus dispositivos desactualizados poniendo en riesgo la seguridad de los mismos.
- *Ciclo de vida de los dispositivos:* A diferencia de los dispositivos corporativos que tienen un ciclo de vida definido y deben tener un proceso de esterilización para desechar los dispositivos. Los usuarios desechar sus dispositivos sin realizar un procedimiento de este tipo poniendo en riesgo la información almacenada en ellos.
- *Incapacidad de realizar auditorías a dispositivos remotos:* Debido a problemas legales, es muy complejo que una organización pueda realizar auditorías en la configuración de los dispositivos personales.
- *Vulnerabilidades en aplicaciones móviles desarrolladas por la organización:* Al no poder controlar completamente el dispositivo, existe el riesgo que el usuario instale aplicaciones maliciosas de manera consciente o inconsciente, que permitan acceso no autorizado a los dispositivos, información almacenada o recursos a los que se tiene acceso.

### 2.1.2 Infraestructura

- *Puntos de acceso de dispositivos a la red corporativa:* Una vulnerabilidad que puede presentarse es el acceso de estos dispositivos a las redes corporativas. En caso de no aislar los dispositivos personales dentro de la organización estamos poniendo en riesgo todos los recursos conectados en la red.
- *Accesos desde dispositivos no autorizados a recursos de la organización:* Un riesgo importante compartido con los dispositivos de la organización, radica en el nivel de acceso que tienen los usuarios y estos dispositivos a las diferentes redes de la organización.
- *Tipo de implementación para accesos remotos:* Un punto muy importante a tener en cuenta, es la seguridad en las comunicaciones

que tienen estos dispositivos. En caso de no estar debidamente aseguradas mediante canales seguros, estamos poniendo en riesgo la integridad y confidencialidad de la información.

- *Vulnerabilidades en los protocolos de red utilizados:* Esto es inherente a los canales de comunicación remotos utilizados.
- *Propagación de malware por conexión de medios de almacenamiento removibles no autorizados en estaciones de trabajo corporativas:* Los dispositivos personales como *pendrives* o *smartphones* que tiene la capacidad de ser utilizados como medios de almacenamiento, pueden ser focos de infección de *malware* si no se cuentan con mecanismos que limiten el uso de estos dispositivos.

### 2.1.3 Datos

- *Almacenamiento local de información corporativa en dispositivos:* Al momento de desvinculación de un usuario de la organización, este usuario puede tener información de la organización en sus dispositivos personales, debido a que el dispositivo es propiedad del usuario, no es posible forzar un borrado remoto del dispositivo.
- *Acciones de usuarios sobre información:* Al no existir medidas de seguridad sobre los dispositivos, los usuarios pueden realizar cualquier acción sobre la información almacenada localmente. Esto se traduce en el riesgo de fuga de información, además de dificultar la identificación del vector de fuga al no tener trazabilidad.
- *Nivel de disponibilidad de la información a los dispositivos:* Información que es procesada de manera local en los dispositivos puede producir demoras en las actividades de los usuarios y afecta la disponibilidad de la información.

## 2.2 Vectores de ataques

La inclusión de estrategias de *BYOD*, ha permitido a los atacantes crear nuevos vectores de ataques, utilizando las vulnerabilidades inherentes de los dispositivos móviles. Existen varios documentos[5], [12], [13] que describen vectores de ataques ya conocidos y nuevos. A continuación, se explica brevemente, como estos vectores de ataques son utilizados en ambientes *BYOD*.

- *Ataques Dirigidos o Spyphones:* Hace referencia sobre aplicaciones instaladas que permiten al atacante escuchar y grabar el alrededor del dispositivo, extraer llamadas y mensajes de texto, examinar geolocalización del dispositivo y datos de aplicaciones y correos entre otras características. En dispositivos personales, es más sencillo realizar estos ataques debido a la falta de medidas de seguridad.
- *Advanced Persistent Threat (APT):* Conjunto de proceso de hacking furtivo y continúo. Este tipo de ataques, son realizados principalmente a organizaciones por atacantes con mucho conocimiento, ya que requiere mucho tiempo y encubrimiento. Los ataques APT, están dirigidos a los *endpoints* para lograr acceder a la red de la organización y de ahí poder realizar su objetivo. Las estrategias de *BYOD* puede bajar la complejidad para realizar estos ataques por falta de control de los dispositivos personales.
- *Aplicaciones maliciosas masivas:* Están dirigidas a los consumidores como pueden ser: textos *premium, dialers, SMS Spammers*, trojanos de *mobile banking* e incluso *ransomwares*. Estas aplicaciones normalmente no son consideradas muy sofisticadas y pero pueden llegar a tener un impacto mayor en la organización, ya que representan un umbral de acceso para atacantes o pueden provocar pérdida de información a nivel del dispositivo.
- *Ingeniería Social:* Los usuarios pueden ser considerados el principal vector de ataque en cualquier tipo de ambiente. Las técnicas de Ingeniería social utilizadas en entornos *BYOD*, incluyen al *phishing, vishing, baiting, pharming, spoofing* entre otras. Nunca hay que subestimar el riesgo que representa este vector de ataque.

- *Vulnerabilidades de Sistemas Operativos:* Este vector de ataque se enfoca en aprovechar las vulnerabilidades de los sistemas operativos. En los últimos años hemos escuchado de vulnerabilidades como *Heartbleed*[14] (que afecta al protocolo SSL y no al sistema operativo en específico) en 2014*, Stagefright*[15] (Afectando al sistema operativo Android) en *2015 y Quadrooter*[16] en 2016 (que afecta a 900 millones de dispositivos con chipset Qualcomm).

  En entornos *BYOD*, estos ataques tienen mayor probabilidad de suceder, al no contar con una versión estándar de sistemas operativos en los dispositivos móviles y puede repercutir en la seguridad de la organización.
- *Inyección SQL:* Este vector tiene como objetivo insertar código malicioso en las aplicaciones y sitios web. Las estrategias de *BYOD*, hacen que descubrir las causas de un ataque de inyección SQL sea más complicado [17].
- *Privacidad de Datos de la organización y el cliente:* En entornos *BYOD*, el acceso y monitoreo de los datos en los dispositivos, crea preocupaciones de la privacidad. Es muy complicado para las organizaciones, asegurar que la información de la compañía o del cliente, no sea revelada a terceros, como los miembros de la familia que utilicen el dispositivo. Esto se convierte en un ataque cuando el usuario o algún tercero utilizan el dispositivo en horarios no laborales.

## 2.3 Errores de seguridad comunes en una infraestructura BYOD

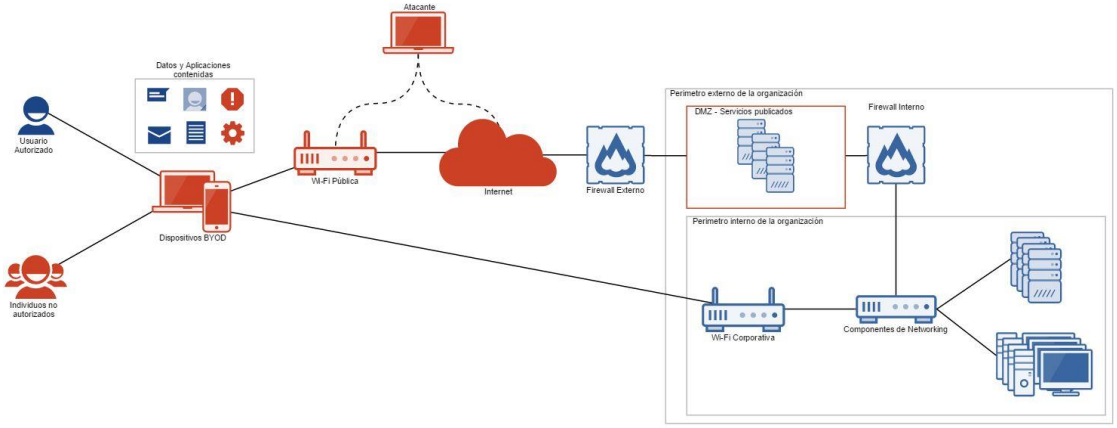



*GRÁFICO 1. Entorno no seguro de BYOD. Elaboración propia basado en Blackberry BEMS Architecture[18].*

En el gráfico 1. Podemos observar una implementación cotidiana que no tiene en cuenta la seguridad de los dispositivos móviles BYOD.

Las figuras azules representan los componentes visibles o autorizados de la organización, mientras que las figuras rojas representan individuos o situaciones fuera del control de la organización.

Podemos observar que a los dispositivos BYOD, pueden acceder terceras partes no autorizadas como familiares, amigos, entre otros, ya sea con autorización del usuario o por el robo o extravío del dispositivo.

Dentro de los dispositivos, no existe una separación de los datos personales y corporativos, lo que puede generar fuga de información por alguna acción del usuario o al desvincularse de la organización. Además, el dispositivo puede estar comprometido por alguna aplicación maliciosa o configuración del usuario.

En caso de no utilizar ningún tipo de mecanismo de cifrado para las comunicaciones, el tráfico entre el dispositivo y la organización puede estar comprometido.

Todos los servicios deben estar publicados para estar disponibles para estos dispositivos, incrementando la superficie de ataque expuesta.

Los dispositivos personales se conectan a la misma red inalámbrica que el resto de los dispositivos logrando acceder a todos los recursos internos.

# CAPÍTULO 3 REQUERIMIENTOS DE SEGURIDAD

## 3.1 Estándares

### 3.1.1 ISO 27002

Dejan Kusotic[17] identifica los controles de la ISO 27002 que tienen mayor relevancia para las políticas de *BYOD*. Estos controles son:

***A.6.2.1 Política de dispositivos móviles.***

Medidas de seguridad a ser adoptadas para manejar el riesgo introducido por los dispositivos móviles en entornos no protegidos[20].

Respecto a *BYOD,* la política de dispositivos móviles debe especificar que el uso de dispositivos personales está permitido y menciona los siguientes puntos a considerar:

- Separación de entornos privado y corporativo en el dispositivo para proteger la información.
- Proveer acceso a la información corporativa luego que el usuario firme un acuerdo de usuario final donde se definen sus deberes, renuncia a la propiedad de datos corporativos, permite borrado remoto de los datos en caso de robo o pérdida del dispositivo.
- Tener en cuenta la legislación nacional sobre privacidad.

***A.6.2.2 Teleworking.***

Este control trata sobre la protección de acceso, procesamiento y almacenamiento de información en sitios de *teleworking*.

Con respecto a los dispositivos personales considera lo siguiente:

- Tener en cuenta los requerimientos de seguridad de las comunicaciones para el acceso remoto, la sensibilidad de la información que será accedida y los sistemas internos.
- La amenaza de acceso no autorizado a la información o recursos por otras personas.
- El aprovisionamiento de escritorios virtuales para prevenir el procesamiento y almacenamiento de información en los dispositivos personales.

- Políticas y procedimientos para prevenir disputas sobre los derechos de propiedad intelectual desarrollada en los dispositivos personales.
- Acuerdos sobre software licenciado requerido para el desarrollo de las actividades laborales en dispositivos personales.

***A.13.2.1 Procedimientos y políticas de transferencia de información.***

Proteger la transferencia de información en los diferentes tipos de comunicación.

No menciona directamente los dispositivos personales, pero habla acerca de las medidas de seguridad al transmitir la información que debe ser tomado implementado por toda la organización.

***A.13.2.3 Mensajería Electrónica.***

Protección de la información involucrada en mensajeria electrónica.

Al igual que el control anterior, debe ser implementado por toda la organización.

Según Dejan, estos 4 controles pueden ser definidos en la política de *BYOD*. Se profundiza más acerca de esto en el punto Política de BYOD.

**3.1.2 *Common Body of Knowledge***

Según Steward[4], el *CBK* menciona los siguientes puntos o controles técnicos a tener en cuenta al implementar *BYOD*:

***3.1.2.1 Autenticación e identificación de dispositivos.***

Un método para lograr estos es conocido como *device fingerprinting.* Los usuarios registran sus dispositivos que luego son asociados con sus cuentas de usuario. Durante el proceso de registro, el sistema de autenticación captura características del dispositivo como Sistema operativo, explorador de internet, zona horaria, entre otras.

Cuando un usuario ingresa desde el dispositivo, el sistema de autenticación revisar la cuenta del usuario en busca del dispositivo registrado.

Las herramientas de *Mobile Device Management (MDM) o Mobile Application Management* cuentan con esta funcionalidad. Estas herramientas están detalladas en el siguiente capítulo.

#### *3.1.2.2 Propiedad de la información.*

Para cubrir este punto, el *CBK* menciona la necesidad de segmentar el almacenamiento del dispositivo para lograr separar los datos personales de los corporativos. No todos los dispositivos cuentan con esta capacidad nativa, por lo que se recomienda utilizar algún tipo de herramienta que agregue esta capacidad.

A su vez, es necesario que los usuarios firmen la política de *BYOD* o un acuerdo de usuario final para evitar disputas legales sobre la información.

#### *3.1.2.3 Consideración de infraestructura.*

Al implementar *BYOD,* es necesario que la organización evalué su diseño de red y seguridad, arquitectura e infraestructura. Si un usuario trae su dispositivo personal el número de equipos en la red puede duplicarse, sin contar que se debe analizar el aislamiento de la comunicación, Manejo de prioridad de datos, incremento en el consumo de ancho de banda o incremento de carga de monitoreo en herramientas *IPS*/*IDS*.

Gran parte de los dispositivos móviles, sino todos, tienen capacidades de comunicación inalámbrica. Por tanto, es necesario contar con una infraestructura inalámbrica robusta para poder soportar la congestión e interferencia en estas comunicaciones.

#### *3.1.2.4 Cumplimiento de dispositivos.*

Es necesario definir como serán gestionados los dispositivos al momento del registro. En este proceso debe incluir tareas como instalación de aplicaciones de productividad, seguridad y de gestión, además de implementación de configuraciones de seguridad acordes a las políticas definidas por la organización.

#### *3.1.2.5 Preocupaciones Legales.*

El *CBK* menciona que los abogados de la organización deben evaluar la responsabilidad y el riesgo de fuga de información. Puede ser posible que estas estrategias no sean costo-efectivas para cierto tipo de organizaciones más reguladas.

Otro punto legal a tener en cuenta es la privacidad y monitoreo de los dispositivos. Cuando un dispositivo personal es utilizado para desarrollar funciones laborales, el usuario normalmente pierde una parte o toda la privacidad de sus dispositivos.

Los dispositivos *BYOD* deben ser considerados como cuasi-propiedad de la organización.

## 3.2 Políticas

Para implementar una estrategia de BYOD segura, es necesario definir una política propia que abarque todos los puntos relevantes de la estrategia.

Al mismo tiempo, esta estrategia requiere apoyo de otras políticas de seguridad descritas más adelante.

### 3.2.1 Política de BYOD

Según el marco CBK[4] e ISO 27001[19]–[21], Para definir una política de BYOD se debe tener en cuenta los siguientes puntos:

- Estar basada en riesgos identificados por el uso de dispositivos personales.
- Aclarar los derechos de propiedad de los datos corporativos y las acciones permitidas con esta información. Se hace referencia a la política de uso aceptable y acuerdo de usuario.
- Métodos de autenticación de dispositivos y usuarios aprobados por la organización.
- Acceso de la información según su clasificación.
- Derechos de propiedad de la información en los dispositivos, incluyendo derechos de respaldo, obtención, acceso, modificación y eliminación.
- Derechos sobre el dispositivo en caso de investigación o control.
- Instalación de medidas de seguridad.
- Métodos de respaldo de información.
- Cifrado de la información almacenada en el dispositivo.
- Cifrado de las comunicaciones.
- Asuntos de privacidad.

- Separación de ambientes de trabajo y personal si no se dispone de una medida de seguridad de este tipo.
- Mención de políticas relacionadas con BYOD.

### 3.2.2 Política de Nivel de cumplimiento Aceptable

Esta política suele estar incluida dentro de la política de *BYOD* pero al estar separada puede tener tiempos de revisión más cortos.

A continuación, se presenta un ejemplo para definir un nivel de cumplimiento básico para los dispositivos personales:

| **Funcionalidades** | **Status** |
|---|---|
| SO liberado (*root o Jailbreak)* | No aceptable. |
| Permitir versiones de SO no homologadas | No aceptable. |
| Permitir modelo de dispositivo no homologados | No aceptable. |
| Tiempo sin comunicación de dispositivo a la infraestructura de la organización | 30 días. |
| Aplicaciones obligatorias no instaladas | No aceptable. |
| Aplicaciones no homologadas instaladas | Aceptable con restricciones. |
| Aplicaciones restringidas instaladas | No aceptable. |
| Almacenamiento cifrado | Recomendable |
| Uso de autenticación al dispositivo | Obligatorio. |
| Complejidad de contraseña | Alfanumérica. |
| Longitud de contraseña | 8 a 32 caracteres. |
| Tiempo de bloqueo de dispositivo | 1 minuto. |

| | |
|---|---|
| Borrado remoto habilitado | Obligatorio si no esta cifrado. |
| Segregación de entorno de trabajo y personal | Aceptable. |

### 3.2.3 Política de uso aceptable y acuerdo de usuario

Debe hacer referencia a la política de uso aceptable de la organización o se debe generar una política que aborde los siguientes aspectos:

- Entendimiento sobre propiedad de la información corporativa.
- Cumplimiento de dispositivo (Versiones, Sistemas operativo, configuraciones varias).
- Acciones no permitidas al usuario.
- Recursos o aplicaciones permitidas.
- Reembolsos a usuarios (En caso de estar definido).
- Medidas de seguridad a implementar.
- Riesgos y responsabilidades.
- Autorización de acciones administrativas sobre el dispositivo por parte del área de soporte de la empresa (En caso de estar definido).
- Acuerdo de usuario.

### 3.2.4 Políticas relacionadas

Otras políticas que BYOD tiene relación y que se pueden ser tomadas como referencia al momento de definir la estrategia de BYOD a utilizar son:

- Política de Clasificación de Información.
- Política de Control de acceso.
- Política de Respaldos.
- Política de Contraseñas.
- Política de Seguridad de la Información.

## 3.3 Controles

Una vez identificadas las vulnerabilidades, procedemos a definir controles definidos [3], [22]–[29] para mitigar o reducir los mismos.

Se decidió realizar tablas que permitan ajustar estos requerimientos a los controles existentes dentro de las organizaciones, para facilitar su asimilación.

En el **ANEXO 3: Listado de controles** se encuentra la lista detallada de controles.

En las tablas 2-4 podemos observar estos controles divididos en las categorías definidas previamente.

### 3.3.1 Dispositivos y aplicaciones

| Vulnerabilidad | Controles |
|---|---|
| | Definir política de acuerdo de uso aceptable. |
| | Definir nivel de cumplimiento del dispositivo. |
| | Implementar mecanismos autenticación de dispositivo. |
| | Implementar mecanismos autenticación de dispositivo. |
| | Implementar cifrado del dispositivo o contenedor. |
| | Definir política de acuerdo de uso aceptable. |
| | Implementar mecanismos de control del hardware del dispositivo. |
| | Implementar mecanismos de identificación de dispositivos. |
| | Definir política de acuerdo de uso aceptable. |
| | Definir nivel de cumplimiento del dispositivo. |
| | Implementar configuraciones de seguridad acordes a políticas. |
| | Implementar aislamiento local de espacio corporativo y personal. |
| | Implementar cifrado del dispositivo o contenedor. |
| | Implementar mecanismos de borrado remoto del contenedor de datos. |
| | Definir nivel de cumplimiento del dispositivo. |
| | Implementar mecanismos de identificación de dispositivos. |
| | Definir nivel de cumplimiento del dispositivo. |
| | Implementar mecanismos de identificación de dispositivos. |
| Incapacidad de realizar auditorías a dispositivos remotos | Implementar aislamiento local de espacio corporativo y personal. |
| | Definir política de acuerdo de uso aceptable. |
| | Implementar catálogo de aplicaciones empresariales. |
| | Implementar mecanismos de listas blancas y negras de aplicaciones. |
| Vulnerabilidades en aplicaciones internas | Definir ciclo de vida de aplicaciones. |

*Tabla 2.Vulnerabilidades y Controles – Dispositivos y Aplicaciones. Elaboración propia.*

### 3.3.2 Infraestructura

| Vulnerabilidad | Controles |
|---|---|
| | Definir políticas de control de acceso. |
| | Implementar mecanismos de identificación de dispositivos. |
| | Implementar mecanismos autenticación de dispositivo. |
| | Implementar mecanismos de descubrimiento de dispositivos, incluyendo dispositivos no tradicionales conectados a la red. |
| | Implementar mecanismos de aislamiento de dispositivos en la red. |
| | Implementar mecanismos de cuarentena en caso de no cumplimiento. |
| | Definir políticas de control de acceso. |
| | Implementar mecanismos autenticación de dispositivo. |
| | Implementar mecanismos de control de acceso granular. |
| | Implementar mecanismos de aislamiento de dispositivos en la red. |
| Tipo de implementación para accesos remotos | Implementar mecanismos de comunicación segura. |
| Vulnerabilidades en los protocolos de red utilizados | Definir políticas de control de acceso. |
| Propagación de malware | Definir nivel de cumplimiento del dispositivo. |

*Tabla 3. Vulnerabilidades y Controles – Infraestructura. Elaboración propia.*

### 3.3.3 Datos

| Vulnerabilidad | Controles. |
|---|---|
| | Implementar aislamiento local de espacio corporativo y personal. |
| | Implementar cifrado del dispositivo o contenedor. |
| | Implementar mecanismos de borrado remoto del contenedor de datos. |
| | Implementar aislamiento local de espacio corporativo y personal. |
| | Implementar cifrado del dispositivo o contenedor. |
| | Implementar mecanismos de borrado remoto del contenedor de datos. |
| | Implementar mecanismos autenticación de dispositivo. |
| | Entrega de contenido por múltiples canales de comunicación. |
| | Implementar mecanismos de control de acceso granular. |

*Tabla 4. Vulnerabilidades y Controles – Datos. Elaboración propia.*

# CAPÍTULO 4 : HERRAMIENTAS

Este capítulo está enfocado en dar a conocer las herramientas que las organizaciones pueden utilizar para cumplir con los requerimientos y controles mencionados en el capítulo anterior.

En cada categoría se encuentran soluciones específicas además de algunos ejemplos de dichas herramientas en el mercado.

## 4.1 Dispositivos y Aplicaciones

### 4.1.1 *Mobile Device Management* (MDM)

Como nos explican Wang y Koh [5], [30], las soluciones MDM brindan capacidades de control sobre las configuraciones de los dispositivos móviles. Permiten forzar el cumplimiento de políticas de seguridad en todos los dispositivos registrados.

En entornos BYOD, MDM tiene la capacidad de crear listas blancas y listas negras de aplicaciones, pero no permite monitorear ni controlar el acceso a las mismas.

Otra de las limitaciones, es la carencia de una funcionalidad de separar el espacio personal del espacio corporativo en los dispositivos, lo cual conlleva a que el usuario pierda la flexibilidad del dispositivo. Rhee[31] propone una lista de requerimientos que estas soluciones deben de cumplir:

- Autenticación del usuario del dispositivo antes de acceder al mismo y a sus funcionalidades.
- Prevenir la modificación o eliminación de los datos de configuración y auditoría.
- Proveer control del hardware del dispositivo.
- Proteger los datos confidenciales.
- Imponer el uso de cifrado.
- Controlar la instalación, eliminación, ejecución de aplicaciones.
- Detener y prevenir la modificación de los sistemas operativos.
- Geolocalización de los dispositivos.

### 4.1.2 *Mobile Application Management* (MAM)

Según Eslahi et al.[22], [32] las soluciones MAM, brindan un control menos invasivo que MDM. Son utilizadas para manejar el ciclo de vida entero de las aplicaciones corporativas lo que permite: instalar, actualizar, remover, auditar, monitorear remotamente las aplicaciones corporativas instaladas y provee un contenedor que aísla el espacio corporativo en el dispositivo.

A diferencia de MDM que controla el hardware, MAM monitorea y controla ciertas aplicaciones contra las políticas y requerimientos de la organización, ignorando las demás aplicaciones y datos en el dispositivo, permitiendo al usuario flexibilidad y privacidad.

De forma general un MAM[22] debe realizar las siguientes funciones:

- Aislamiento de espacio corporativo y personal en dispositivos.
- Gestión en tiempo real de las aplicaciones.
- Catálogo de aplicaciones empresariales.
- Monitoreo y seguimiento de aplicaciones.
- Listas Blancas y negras de aplicaciones.
- Ciclo de vida de aplicaciones.
- Actualización, Backups y eliminación de aplicaciones.

En la actualidad las soluciones de MDM y MAM han sido integradas en una sola consola de gestión, pero su funcionalidad depende de la licencia adquirida.

## 4.2 Infraestructura

Muchas empresas e investigadores[3][23]–[25][30] han desarrollado diferentes tecnologías y herramientas que proveen mecanismos de autenticación y acceso que permite tener una mejor visibilidad y control sobre las redes de la organización en general.

Para el caso de *BYOD* analizamos dos tecnologías diferentes para asegurar la comunicación de los dispositivos personales. *Virtual Private Networks* para las comunicaciones remotas y *Network Access Control* para el control de las redes internas.

### 4.2.1 *Virtual Private Networks* (VPNs)

En entornos *BYOD*, según Wang[5], las VPNs proveen una comunicación segura a los dispositivos personales que desean acceder a las redes corporativas desde internet.

Cabe mencionar que las VPNs, no proveen mayor seguridad dentro de las redes corporativas. En entornos *BYOD* son una solución necesaria, pero no suficiente.

Dentro de las funcionalidades que tienen las VPNs[33] tenemos:

- Autenticación de usuarios.
- Autenticación de datos e integridad.
- Cifrado de datos en tráfico.

### 4.2.2 *Network Access Control* (NAC)

Como describe Koh[30], los NAC son utilizados en conjunto con las soluciones MDM (aun cuando algunas funcionalidades se vean traslapadas).

Esta tecnología inspecciona los dispositivos, determina si estos se encuentran en cumplimiento con las políticas de seguridad y brinda acceso a una red determinada.

Dentro de las funcionalidades que proveen los NAC[23], [25], [26] tenemos:

- Implementar políticas de control de acceso.
- Inspeccionar la configuración de los dispositivos antes de brindar acceso a la red.
- Descubrimiento de dispositivos, incluyendo dispositivos no tradicionales conectados a la red.
- Identificación de los tipos, ubicaciones y atributos de los dispositivos.
- Reportar y poner en cuarentena a los clientes que fallen en cumplir los estándares de seguridad.
- Proveer acceso de control granular.
- Identificar dispositivos no autorizados (conectados a WAPs por ejemplo).

- Imponer políticas de seguridad personalizadas para dispositivos BYOD.

Debido a que el objetivo de los NAC es autenticación de usuario y control de acceso, carece de funciones para detectar comportamiento anormal de usuarios y dispositivos; esto da una pauta para decir que las soluciones NAC por si solas, no son suficientes para manejar la seguridad en entornos BYOD.

## 4.3 Datos

Debido a la tendencia de trabajo actual de sincronización y colaboración de documentos o datos. Es necesario, contar con una capa de seguridad que permita controlar la interacción que los usuarios tienen con la información a través de sus dispositivos personales o de la organización como BYOD.

Para resolver esta situación en todos los entornos móviles, se han desarrollado herramientas que toman el nombre de *Enterprise File Sync and Sharing (EFSS).*

Estas herramientas, deben ser utilizadas junto con otras mencionadas en los enfoques anteriores, ya que, al tratar específicamente la seguridad de la información, carece de controles sobre dispositivos e infraestructura.

### 4.3.1 *Enterprise File Sync and Sharing* (EFSS)

Gartner define estas herramientas como “soluciones de oferta *on-premise* o *cloud* que permite a individuos a sincronizar y compartir archivos entre dispositivos móviles y PCs”[34].

Según Thru[35], estas herramientas permiten mejorar la productividad de los usuarios limitando los riesgos de seguridad y cumplimiento existentes.

Al mismo tiempo Thru menciona que funcionalidades de seguridad deben contar estas soluciones:

- Control granular mediante identificación de características únicas de dispositivos (ej: *MAC Address*).

- Limitar el acceso de archivos fuera de la aplicación *EFSS* utilizada.
- Auditoría de eventos de acceso, almacenamiento y modificación de información.

## 4.4 Infraestructuras comerciales más importantes

Existen diferentes infraestructuras enfocadas a la gestión de dispositivos móviles. El cuadrante mágico de Gartner de *Enterprise Mobility Management*[36] nos muestra que los lideres actuales son *Airwatch, Citrix, MobileIron y Blackberry.*

Todas estas soluciones están mayormente cumplir funciones de herramientas de MDM, MAM y EFSS.

A continuación, se describen brevemente las ventajas y desventajas de cada solución.

### 4.4.1 *VMware AirWatch*

Según Gartner, Airwatch presenta una de las consolas de administración más fáciles de utilizar. Además, cuenta con mucha documentación lo que permite un aprendizaje rápido para nuevos administradores.

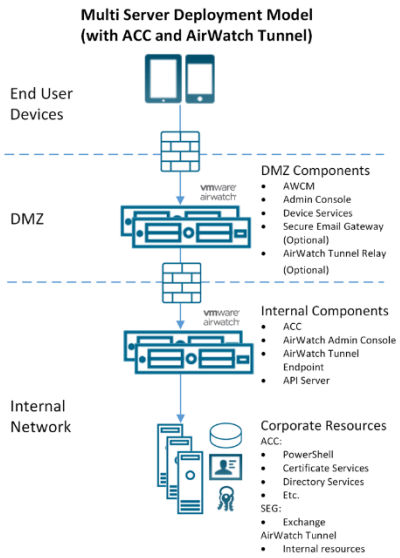



*Gráfico 2. Arquitectura de VMware AirWatch.[37]*

**VMware Airwatch**

| Ventajas | Desventajas |
|---|---|

| | |
|---|---|
| • Posibilidad de implementación de tipo *SaaS* u *on-premise*<br>• Solución modular que puede adaptarse a los casos de uso requeridos por las organizaciones.<br>• Integración profunda con otras soluciones de Vmware.<br>• Separación de entornos utilizando controles nativos del sistema operativo. | • Solución mayormente enfocada al control de los dispositivos.<br>• Implementación *on-premise* tiene altos requerimientos de hardware.<br>• Licenciamiento por dispositivo.<br>• Funcionalidades como navegación segura requiere un licenciamiento superior.<br>• Se requiere apertura de multiples puertos para servicios.<br>• No cuenta con una solución *EFSS.*<br>• Soporte limitado para ciertas aplicaciones de Android. |

*Tabla 5.Ventajas y Desventajas de soluciones VMware Airwatch. Elaboración Propia basada en bibliografía[37]–[40]*

### 4.4.2 Citrix *XenMobile*

Solución recomendada para entornos con otras soluciones Citrix debido al nivel de integración entre todas las soluciones. Citrix ofrece una de las soluciones *EFSS* más completas del mercado.

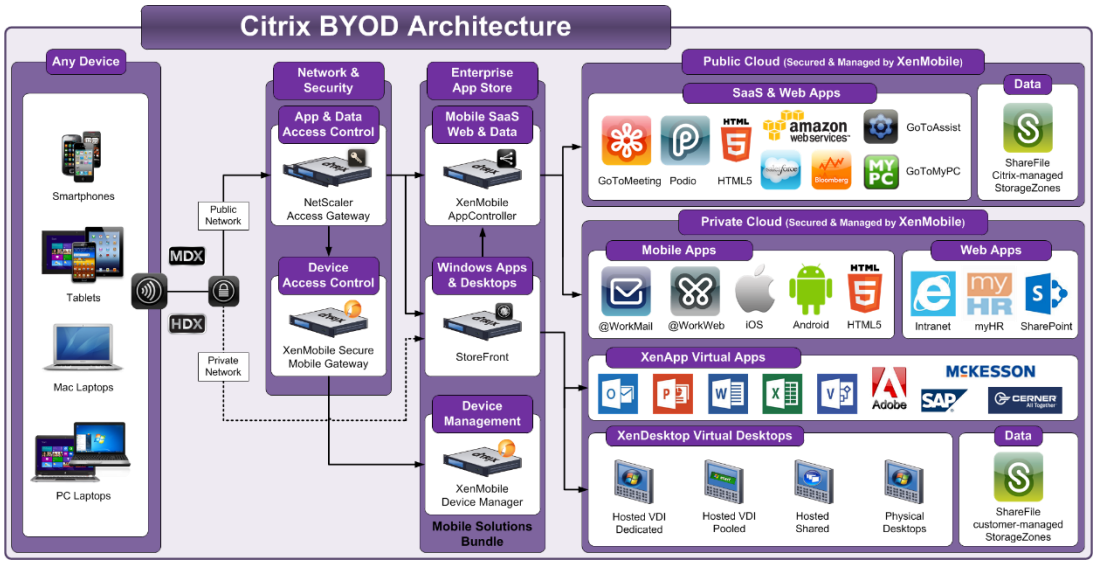



*Gráfico 3. Arquitectura XenMobile para entornos BYOD.[41]*

**Citrix *XenMobile***

| Ventajas | Desventajas |
|---|---|
| • Solución abarca un amplio espectro de dispositivos.<br>• Permite aplicar control de acceso basado en ubicación.<br>• Tecnología *Micro-VPN* para un control más granular de cada aplicación corporativa en los dispositivos.<br>• Integración completa con otras soluciones citrix.<br>• Solución *EFSS* es una de las más maduras del mercado. | • Implementación *on-premise* requiere multiples servidores para contar.<br>• Requerimientos de hardware altos debido a que la solución está enfocada a la virtualización de entornos.<br>• Alta complejidad de implementación. |

*Tabla 6. Ventajas y desventajas de Citrix Xenmobile. Elaboración propia basada en [36], [41], [42]*

### 4.4.3 *MobileIron EMM*

MobileIron es una solución rica en funciones, estable y escalable en cuanto a seguridad móvil y cuenta con un gran ecosistema de aplicaciones aseguradas.

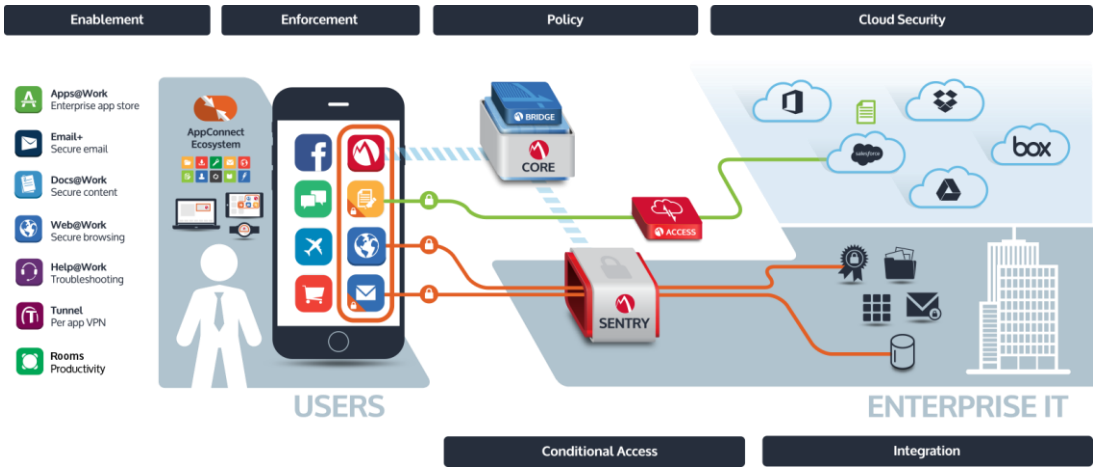



*Gráfico 4.Arquitectura de MobileIron.[43]*

**MobileIron Mobility Enterprise Management**

| Ventajas | Desventajas |
|---|---|
| • Implementación on-premise simple y de bajo costo.<br>• Permite licenciamiento por usuario (3 dispositivos por usuario) o dispositivo único.<br>• Amplio ecosistema de aplicaciones.<br>• Integración con soluciones SIEM. | • Requiere tener implementado cliente MDM para separación de entornos.<br>• Para unificar gestión de dispositivos de escritorio, requiere de otra del mismo proveedor.<br>• No cuenta con una solución EFSS. |

*Tabla 7. Ventajas y desventajas de MobileIron EMM. Elaboración propia basada en [36], [43]*

### 4.4.4 *Blackberry Unified Endpoint Management*

Gartner cataloga la solución de blackberry ofrece la protección más fuerte del mercado. Tiene la capacidad de aplicar funciones de MDM, MAM, EFSS de manera individual. Además, cuenta con un ecosistema de más de 2000+ aplicaciones aseguradas.

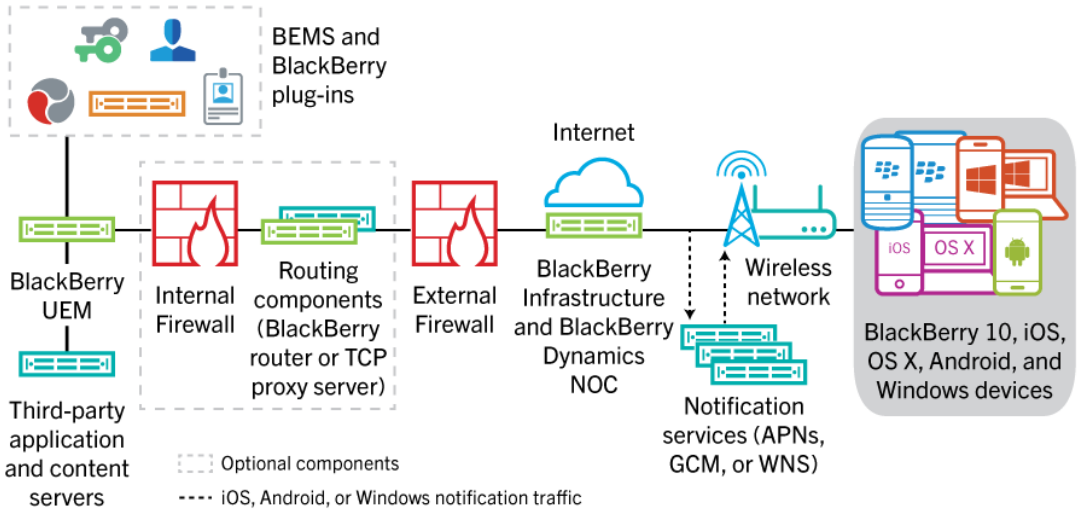



*Gráfico 5. Arquitectura de Blackberry UEM.[18]*

**Blackberry Unified Enterprise Management**

| Ventajas | Desventajas |
|---|---|
| • Implementación on-premise o cloud.<br>• Licenciamiento por usuario (10 dispositivos por usuario).<br>• Amplio ecosistema de aplicaciones.<br>• Despliegue de MDM o MAM independiente desde la misma consola.<br>• Utilización de infraestructura propia de blackberry para brindar un mayor nivel de seguridad en las comunicaciones.<br>• Amplio ecosistema de aplicaciones.<br>• Soporta sistemas operativos iOS, Android, Windows y Blackberry. | • *EFSS* disponible solamente para licenciamiento superior.<br>• Servidor de solución requiere muchos recursos. |

*Tabla 8. Ventajas y desventajas de Blackberry UEM. Elaboración propia basada en [1], [18], [36], [44]*

# CAPÍTULO 5 RECOMENDACIONES

Para culminar este trabajo y según la investigación realizada, se presentan lineamientos básicos recomendados para implementar estrategias BYOD de manera más segura.

## 5.1 Recomendaciones Generales

- Definir o contar con una estrategia de movilidad empresarial.
- Definir los objetivos de las políticas de BYOD.
- Identificar los riesgos asociados al uso de dispositivos personales.
- Definir los servicios disponibles para estos dispositivos.
- Definir los perfiles de usuarios y servicios autorizados.
- Anexar estos perfiles a la política de control de acceso existente en la organización.
- Definir las responsabilidades y deberes de los usuarios de dichos dispositivos.
- Seleccionar las herramientas que más se adecuen al entorno de la organización.
- Definir el nivel de cumplimiento de los dispositivos.
- Generar una política de uso aceptable.
- Generar una política de BYOD que englobe toda esta información.
- Realizar campañas de concientización a los usuarios.

## 5.2 Recomendaciones Dispositivos y Aplicaciones

A nivel de dispositivos y aplicaciones se recomienda tener en cuentas los siguientes puntos:

- Implementar una solución de MDM o MAM.
- Activar desbloqueo mediante huella dactilar o contraseña para un nivel más robusto de autenticación.
- Forzar bloqueo de inactividad entre 30 segundos a 1 minuto.
- Forzar lista negra de aplicaciones no permitidas.
- Forzar borrado de dispositivo o área corporativa luego de los 10 intentos fallidos.
- Forzar activación remota de GPS, bloqueo y borrado remoto.
- Hacer a los usuarios lean y acepten las políticas de acuerdo de uso y uso aceptable definidas por la organización.

## 5.3 Recomendaciones Infraestructura

En base al tamaño de las organizaciones, se recomienda implementar las herramientas descritas en este trabajo de la siguiente manera:

| | Tamaño Organización | | |
|---|---|---|---|
| Herramientas | Pequeña | Mediana | Grande |
| MDM | ✓ | ✓ | ✓ |
| MAM | | ✓ | ✓ |
| VPNs | ✓ | ✓ | ✓ |
| NAC | | | ✓ |
| EFSS | | | ✓ |

*Tabla 9. Herramientas por tamaño de organización. Elaboración propia*

Se recomienda tener en cuenta los siguientes puntos:

- Definir los controles a implementar (Ver tablas 2, 3 y 4 del capítulo 3).
- Al evaluar las soluciones, verificar que cumplan con las funcionalidades descritas en el capítulo 3.
- Evaluar la infraestructura y arquitectura de red actual para detectar puntos de mejora.
- Definir puntos de acceso para dispositivos personales aislados de las redes productivas.
- Elegir las soluciones que más se adecuen a la infraestructura actual en base a compatibilidad e integración.

## 5.4 Recomendaciones Datos

Para asegurar los datos utilizados por los dispositivos personales se recomienda seguir los siguientes puntos:

- Aplicar mecanismos de aislamiento local del espacio corporativo y personal.
- Forzar el uso de cifrado de almacenamiento local en caso de no tener asilamiento de espacio local.
- Forzar el borrado remoto de datos en los dispositivos móviles en caso de pérdida.
- Utilizar una herramienta *EFSS* para asegurar los archivos que deben ser compartidos sin perder el control de los mismos.

# CAPÍTULO 6 CONCLUSIONES

Las estrategias de BYOD son muy útiles para conservar la cultura organizacional y brindar mayor movilidad y flexibilidad a los usuarios, lo que aumenta su productividad.

En el ámbito de seguridad, estos entornos conllevan muchos desafíos que deben ser tomados en cuenta para no perder el control ni la visibilidad de nuestros datos, infraestructura y comunicaciones.

En este trabajo se logró separar los componentes involucrados en estas estrategias en las capas de dispositivos y aplicaciones, Infraestructura y datos.

Estas estrategias sufren de vulnerabilidades como el acceso físico al dispositivo debido a su naturaleza móvil, la falta de implementación de medidas de seguridad no ser propiedad de la organización y el almacenamiento de información local, lo que puede conllevar a pérdida de información corporativa.

Para contrarrestar todas las vulnerabilidades descritas en este trabajo, se determinaron controles estratégicos como la definición de una política de BYOD, una política de uso aceptable y acuerdo de usuario. Estas políticas deben de conocimiento interno y deben ser aceptadas por todos los partícipes.

Para obtener mayor control y visibilidad de estas estrategias, se investigaron herramientas como *Mobile Device Management, Mobile Application Management, Network Access Control y Entreprise File Sync and Sharing.* El uso conjunto de estas herramientas permite asegurar de manera sólida los entornos BYOD.

Para finalizar este trabajo, se brinda puntos a tener en cuenta al implementar estas estrategias y combinaciones de herramientas necesarias para asegurar mínimamente el entorno de las organizaciones en base a su tamaño.

# BIBLIOGRAFÍA

[1] "BlackBerry." [Online]. Available: http://el.blackberry.com/securityebook. [Accessed: 26-Feb-2017]

[2] FUJITSU Technology Solutions GmbH, "BYOD – It's About Infrastructure and Policies," 2013. [Online]. Available: http://sp.ts.fujitsu.com/dmsp/Publications/public/wp-byod.pdf. [Accessed: 06-Dec-2015]

[3] MeruNetworks, "BYOD Best Practices Requirements and Challenges." 2013 [Online]. Available: http://www.merunetworks.com/collateral/white-papers/wp-byod-implementation-whitepaper-for-wlan-security.pdf

[4] J. M. Stewart, M. Chapple, and D. Gibson, *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide*, 7 edition. Hoboken, NJ: Sybex, 2015.

[5] Y. Wang, J. Wei, and K. Vangury, "Bring your own device security issues and challenges," presented at the Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th, 2014, pp. 80–85 [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6866552. [Accessed: 06-Dec-2015]

[6] Hewlett-Packard Development Company, "Unleash the Full Potential of BYOD with Confidence," 2013. [Online]. Available: http://www.hp.com/hpinfo/newsroom/press_kits/2013/GPC2013/IMC_BYOD_Appliance_Whitepaper.pdf. [Accessed: 06-Dec-2015]

[7] PricewaterhouseCoopers, "PWC - Global Information Security Survey 2014," 2014. [Online]. Available: http://es.slideshare.net/GaldeMerkline/global-informationsecuritysurvey2014. [Accessed: 06-Dec-2015]

[8] TechTarget, "Mobile Device Security - The Eight areas of risks," 2007. [Online]. Available: http://www.meritalk.com/uploads_legacy/whitepapers/Nokia_eGuide_2.pdf. [Accessed: 06-Dec-2015]

[9] Ernst & Young, “Mobile device Security: Understanding vulnerabilities and managing risks,” 2012. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/EY_Mobile_security_devices/$FILE/EY_Mobile%20security%20devices.pdf. [Accessed: 05-Dec-2015]

[10] Ernst & Young, “Bring your own device - Security and risk considerations for your mobile device program,” 2014. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf. [Accessed: 06-Dec-2015]

[11] MTI Technology, “BYOD - The future of corporate computing?,” 2013. [Online]. Available: http://www.insightrain.com/byod-the-future-of-corporate-computing. [Accessed: 05-Dec-2015]

[12] Lacoon Mobile Security, “Practical Attacks against Mobile Device Management (MDM),” 2013. [Online]. Available: https://media.blackhat.com/eu-13/briefings/Brodie/bh-eu-13-lacoon-attacks-mdm-brodie-wp.pdf. [Accessed: 06-Dec-2015]

[13] M. M. Singh, S. S. Siang, O. Y. San, N. Hashimah, A. H. Malim, and A. R. M. Shariff, “Security Attacks Taxonomy on Bring Your Own Devices (BYOD) Model,” *Int. J. Mob. Netw. Commun. Telemat.*, vol. (1839-5678), no. 5, pp. 1–17, 2014 [Online]. Available: http://wireilla.com/papers/ijmnct/V4N5/4514ijmnct01.pdf

[14] C. Arthur, “Heartbleed makes 50m Android phones vulnerable, data shows,” *The Guardian*, 15-Apr-2014 [Online]. Available: http://www.theguardian.com/technology/2014/apr/15/heartbleed-android-phones-vulnerable-data-shows. [Accessed: 06-Dec-2015]

[15] “Stagefright (bug),” *Wikipedia*. 10-Jun-2017 [Online]. Available: https://en.wikipedia.org/w/index.php?title=Stagefright_(bug)&oldid=784959414

[16] “QuadRooter: New Android Vulnerabilities in Over 900 Million Devices,” *Check Point Blog*, 07-Aug-2016. [Online]. Available: http://blog.checkpoint.com/2016/08/07/quadrooter/. [Accessed: 11-Jun-2017]

[17] Ponemon Institute LLC, “The SQL Injection Threat Study,” 2014. [Online]. Available: http://www.dbnetworks.com/pdf/ponemon-the-SQL-injection-threat-study.pdf. [Accessed: 06-Dec-2015]

[18] “BlackBerry UEM Architecture and data flows.” [Online]. Available: http://help.blackberry.com/en/blackberry-uem/current/architecture/ake1452094272560.html. [Accessed: 10-Apr-2017]

[19] Dejan Kosutic, “ISO 27001 – How to create an easy-to-use BYOD Policy,” *27001Academy*, 07-Sep-2015. [Online]. Available: https://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-iso-27001/. [Accessed: 09-Apr-2017]

[20] “ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements.” [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed: 09-Apr-2017]

[21] IsecT Ltd, “ISO 27000 Model Policy on BYOD Security,” 2012. [Online]. Available: http://www.iso27001security.com/ISO27k_Model_policy_on_BYOD_security.pdf. [Accessed: 06-Dec-2015]

[22] davek, “The Security Pro’s Guide To MDM, MAM, MIM, and BYOD,” *TrustedSec - Information Security*. [Online]. Available: https://www.trustedsec.com/september-2012/the-security-pros-guide-to-mdm-mam-mim-and-byod/. [Accessed: 06-Dec-2015]

[23] Spire Security LLC, “NAC, 802.1X AND BYOD: Advantages, Constraints and Capabilities,” 2013. [Online]. Available: http://www.forescout.com/wp-content/media/Spire_Forescout_NAC_8021X_BYOD_Security.pdf. [Accessed: 06-Dec-2015]

[24] Cisco Networks Inc, “Cisco Enterprise Mobility Solution Device Freedom Without Compromising the IT Network,” 2014. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/solution_overview_c22-702775.pdf. [Accessed: 06-Dec-2015]

[25] Aerohive Networks Inc, “BYOD and Beyond: How To Turn BYOD into Productivity,” 2012. [Online]. Available: http://docs.aerohive.com/pdfs/Aerohive-Whitepaper-BYOD-and-Beyond.pdf. [Accessed: 06-Dec-2015]

[26] G. Mark Hardy, “SANS - The critical Security Controls: What NAC got to do with IT?,” 2013. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-what-039-s-nac-it-35115. [Accessed: 06-Dec-2015]

[27] AirWatch, “Mobile Content Management: Top 10 Considerations,” 2013. [Online]. Available: https://www.air-watch.com/downloads/resources/white-paper-mobile-content-management.pdf. [Accessed: 06-Dec-2015]

[28] Benjamin JH, “OWASP Bring Your Own Device - Could you, would you should you,” 2012. [Online]. Available: https://www.owasp.org/index.php/File:OWASP_Manchester_Bring_Your_Own_Device_v2.pptx. [Accessed: 06-Dec-2015]

[29] M. Brodin, “Combining ISMS with strategic management: the case of BYOD,” in *ResearchGate*, 2015 [Online]. Available: http://www.researchgate.net/publication/277007918_Combining_ISMS_with_strategic_management_the_case_of_BYOD. [Accessed: 05-Dec-2015]

[30] E. B. Koh, J. Oh, and C. Im, “A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment,” presented at the Proceedings of the International MultiConference of Engineers and Computer Scientists 2014, 2014, pp. 634–639 [Online]. Available: http://www.iaeng.org/publication/IMECS2014/IMECS2014_pp634-639.pdf. [Accessed: 06-Dec-2015]

[31] K. Rhee, H. Kim, and H. Y. Na, “Security test methodology for an agent of a mobile device management system,” *Intl J Secur. Its Appl.*, vol. 6, no. 2, 2012 [Online]. Available: http://www.sersc.org/journals/IJSIA/vol6_no2_2012/14.pdf

[32] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, and E. H. M. Saad, “BYOD: Current state and security challenges,” in *2014 IEEE Symposium on*

*Computer Applications and Industrial Electronics (ISCAIE)*, 2014, pp. 189–192.

[33] "Properties of VPN Connections." [Online]. Available: https://technet.microsoft.com/en-us/library/cc958046.aspx. [Accessed: 12-Jun-2017]

[34] G. Inc, "Enterprise File Sync & Content Collaboration Software Reviews," *Gartner*. [Online]. Available: https://www.gartner.com/reviews/market/efss. [Accessed: 12-Jun-2017]

[35] "Thru for Enterprise File Sync and Sharing." [Online]. Available: http://www.infosecurityeurope.com/__novadocuments/51356?v=635328263496800000. [Accessed: 20-Jun-2017]

[36] "Gartner Reprint." [Online]. Available: https://www.gartner.com/doc/reprints?id=1-3BXR3BC&ct=160719&st=sb. [Accessed: 12-Jun-2017]

[37] AirWatch, "AirWatch On-Premises Deployment Model." [Online]. Available: https://my.air-watch.com/help/9.1/en/Content/Expert_Guides/Install_Arch/Recommended_Arch/C/On_Prem_Deployment_Model.htm. [Accessed: 15-Jul-2017]

[38] AirWatch, "Bring Your Own Device (BYOD) | AirWatch." [Online]. Available: https://www.air-watch.com/en/solutions/bring-your-own-device-byod/. [Accessed: 15-Jul-2017]

[39] AirWatch, "On-Premises Architecture Software Requirements." [Online]. Available: https://my.air-watch.com/help/9.1/en/Content/Expert_Guides/Install_Arch/Recommended_Arch/R/On_Prem_Software_Reqs.htm. [Accessed: 15-Jul-2017]

[40] "VMW-DS-Suite_Comparison-092016.pdf." [Online]. Available: https://www.air-watch.com/downloads/resources/VMW-DS-Suite_Comparison-092016.pdf. [Accessed: 15-Jul-2017]

[41] Citrix, "CitrixBYODArchitecture.png (2081×1059)." [Online]. Available: http://cdn.ws.citrix.com/wp-

content/uploads/2013/02/CitrixBYODArchitecture.png. [Accessed: 15-Jul-2017]

[42] “citrix-xenmobile-mobile-application-management-advantages.pdf.” [Online]. Available: https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/citrix-xenmobile-mobile-application-management-advantages.pdf. [Accessed: 15-Jul-2017]

[43] “MobileIron Product Overview | MobileIron.” [Online]. Available: https://www.mobileiron.com/en/products. [Accessed: 15-Jul-2017]

[44] “BYOD Guidance: BlackBerry Secure Work Space - GOV.UK.” [Online]. Available: https://www.gov.uk/government/publications/byod-guidance-blackberry-secure-work-space/byod-guidance-blackberry-secure-work-space. [Accessed: 20-Jun-2017]

# ANEXOS

## ANEXO 1: Guía de Instalación de Blackberry Unified Endpoint Management

Esta herramienta ha demostrado cumplir con todos los requerimientos para el manejo de dispositivos BYOD como solución MDM y MAM.

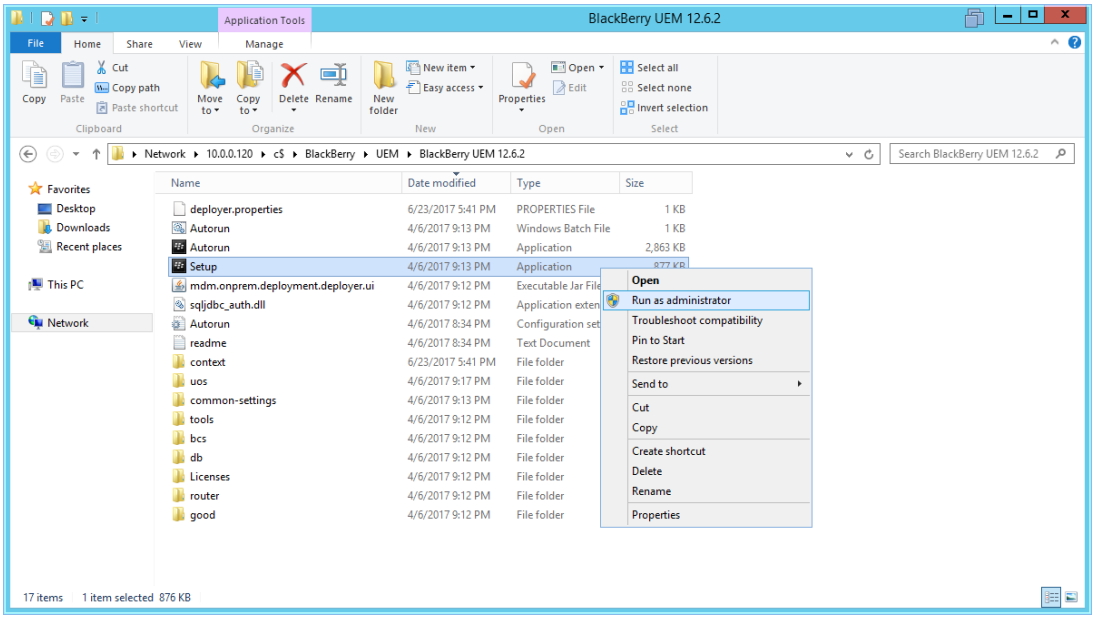
La plataforma puede descargada e instalada de manera gratuita. Para gestionar dispositivos es necesario contar con las licencias validas.

El instalador puede conseguirse en la siguiente dirección:

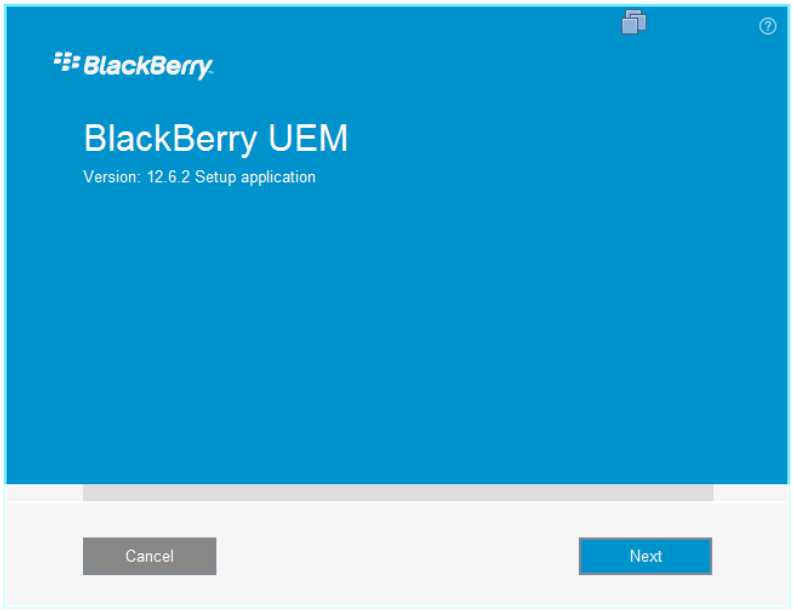
https://global.blackberry.com/en/support/business/blackberry-uem

Para Instalar esta solución es necesario realizar los siguientes pasos:

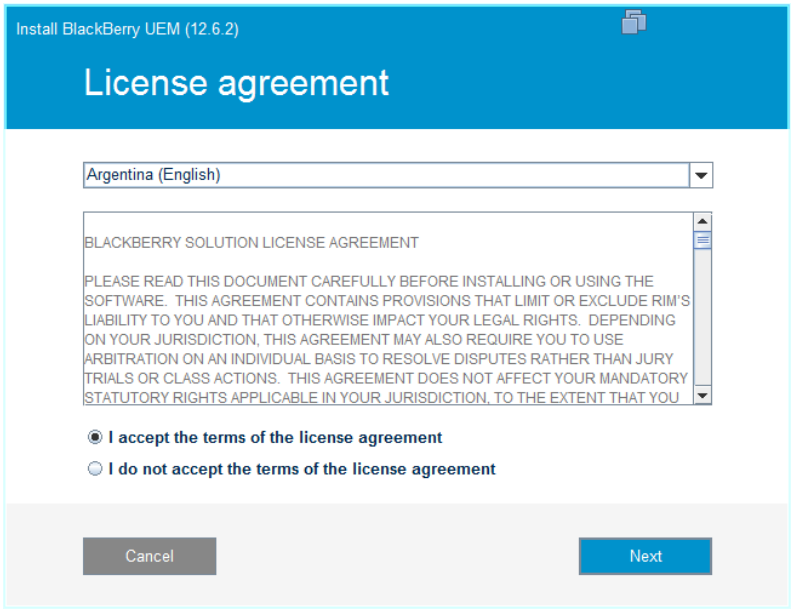
1. Hacer click en el instalador:



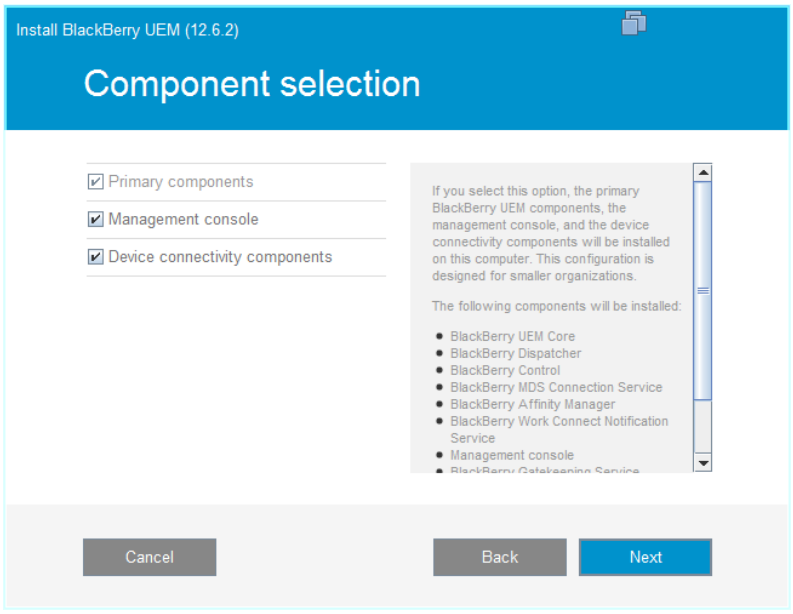
2. Hacer click en ***Next***:



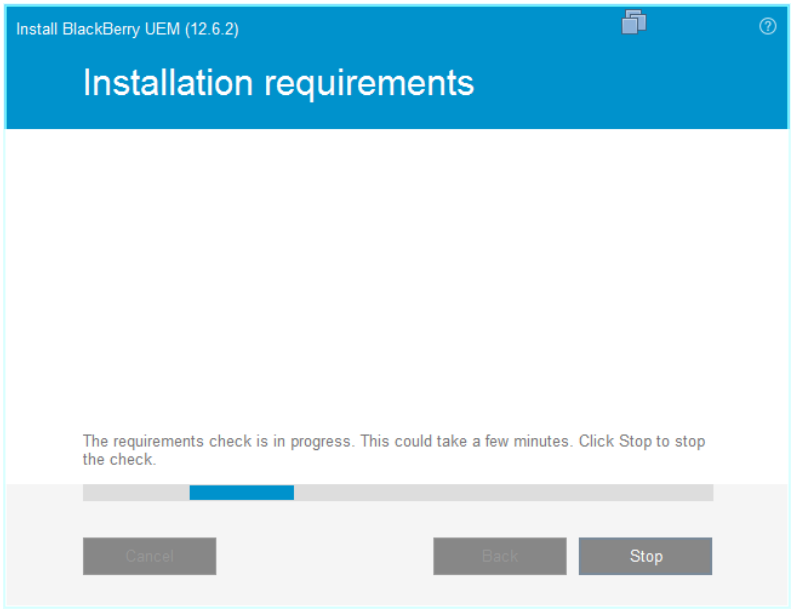

3. Seleccionar el país de instalación, leer los términos y condiciones, Seleccionar ***I Accept the terms of the license agreement*** en caso de estar de acuerdo y hacer click en ***Next***.



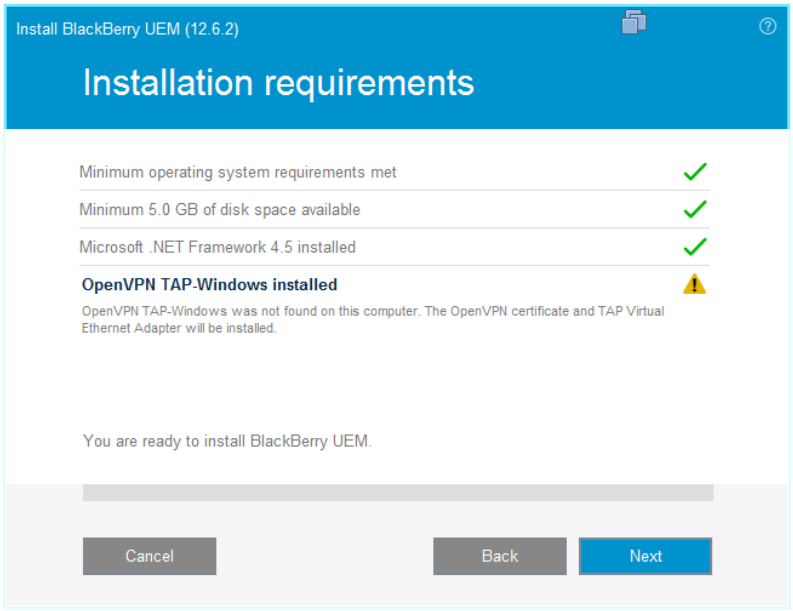
4. Seleccionar los todos componentes para instalar la plataforma completa y hacer click en ***Next***.



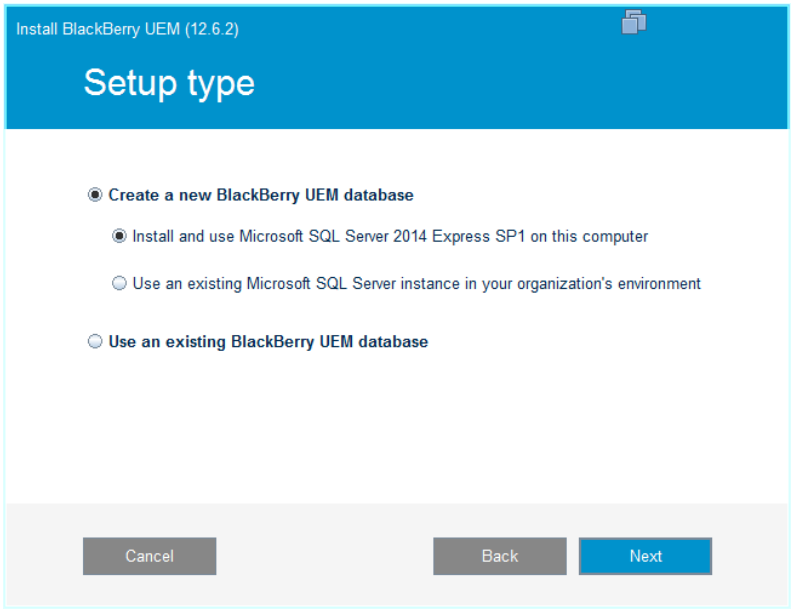

5. Esperar a que el instalador termine de revisar los requerimientos mínimos.



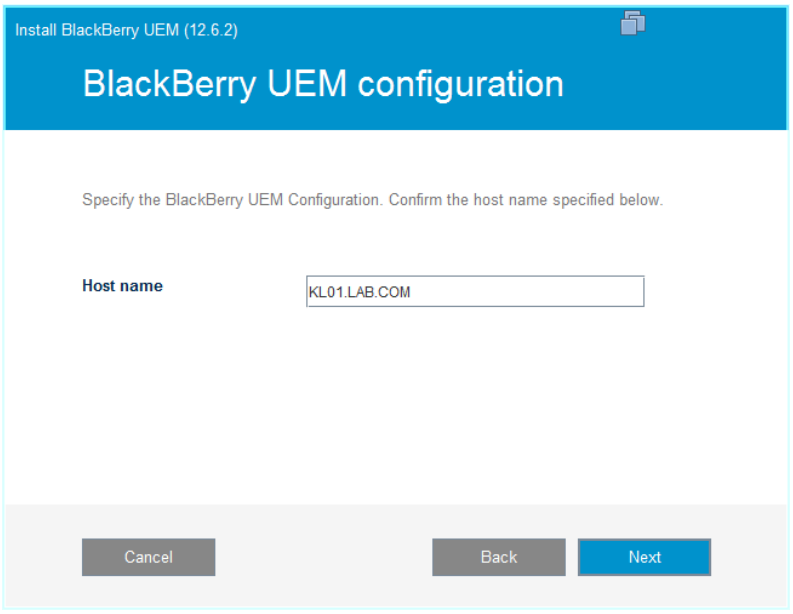
6. Una vez verificado, hacer click en ***Next***.



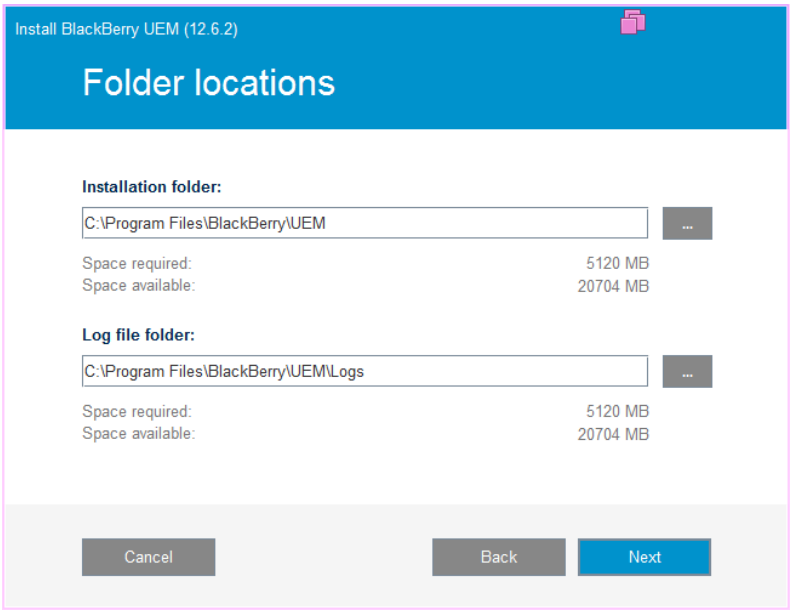

7. Seleccionar **Create a new BlackBerry UEM database** y seleccione:
   a. **Install and use Microsoft SQL Server 2014 Express SP1 on this computer** para instalar un nuevo motor local para la base de datos.
   b. **Use an Existing Microsoft SQL Server instance in your organization's environment** para elegir crear la base de datos en un motor pre existente.



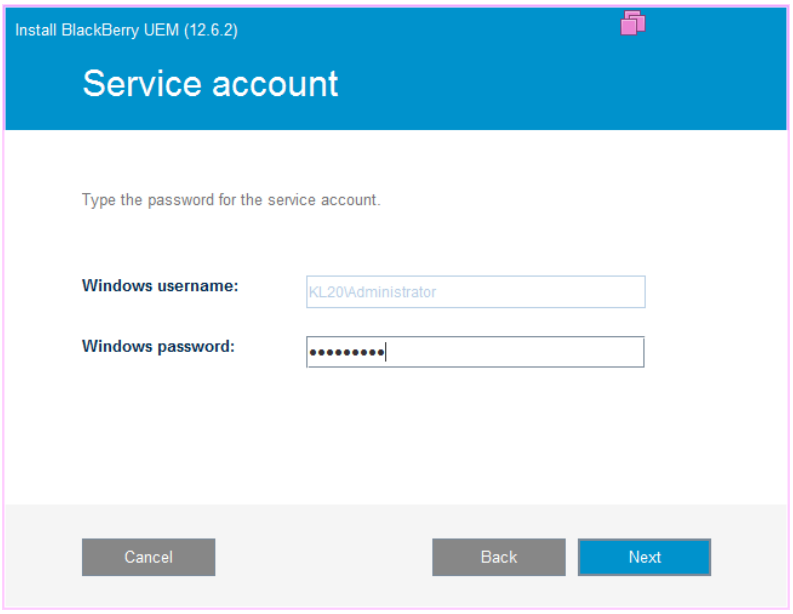
8. Especificar el **FQDN** del servidor donde se está realizando la instalación.



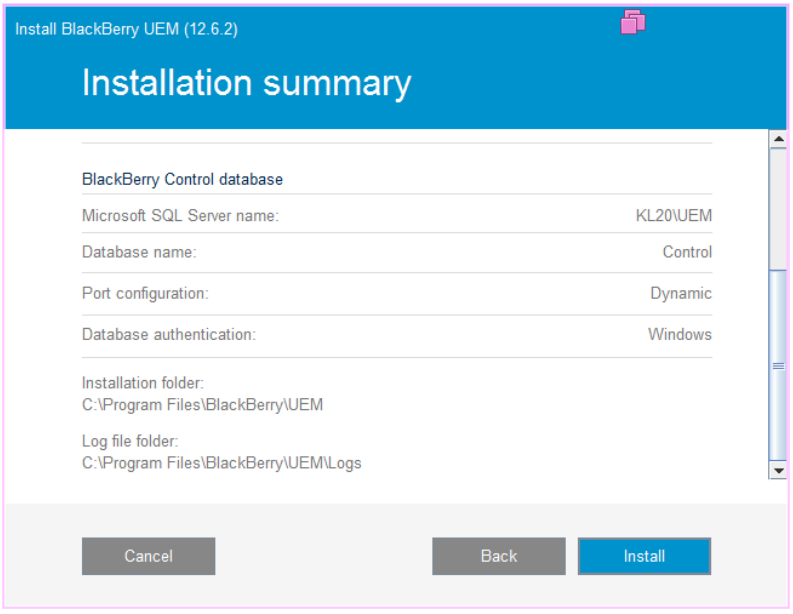

9. Seleccionar la ubicación de instalación de la consola y la ubicación de los *Logs* que generará la consola.



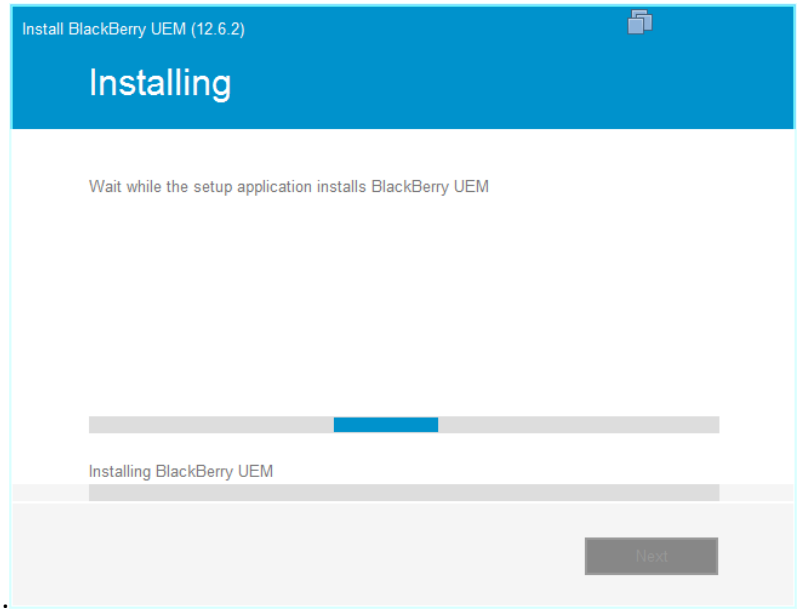
10. Definir las credenciales de la cuenta de servicio a utilizar (Administrador local).




11. Verificar los datos de la instalación y hacer click en ***Install*.**

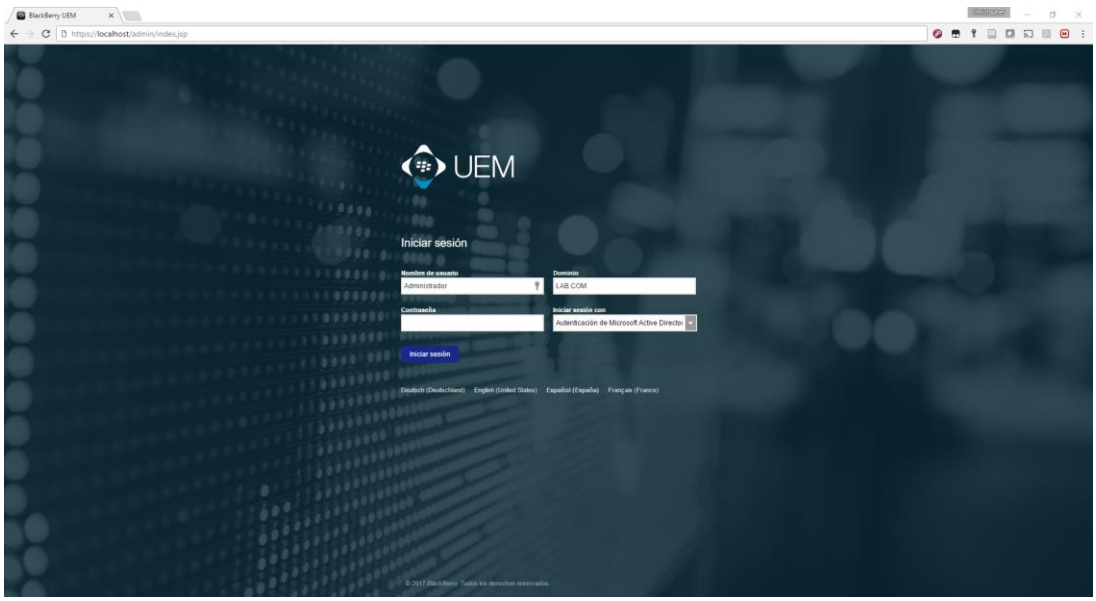


12. Esperar a que finalice el proceso de instalación.

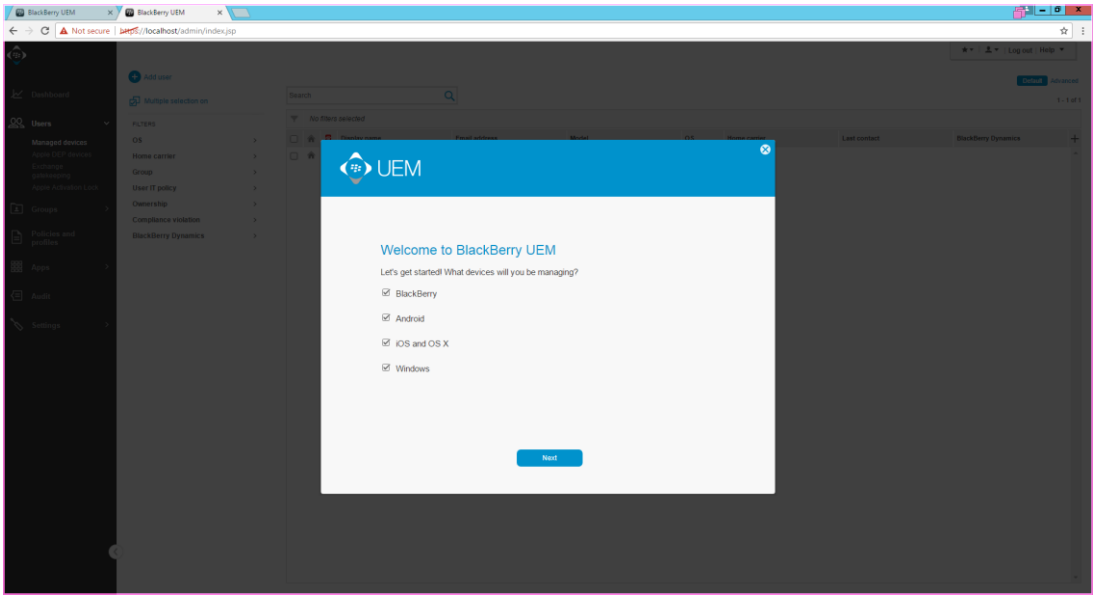



.

13. Una vez instalada la plataforma. Se puede ingresar a través del explorador de su preferencia por la dirección: https:/localhost/admin



14. Una vez ingresadas las credenciales, seleccionamos los dispositivos que serán administrados.




15. En este punto podemos comenzar a configurar la plataforma con la información suministrada en este trabajo.