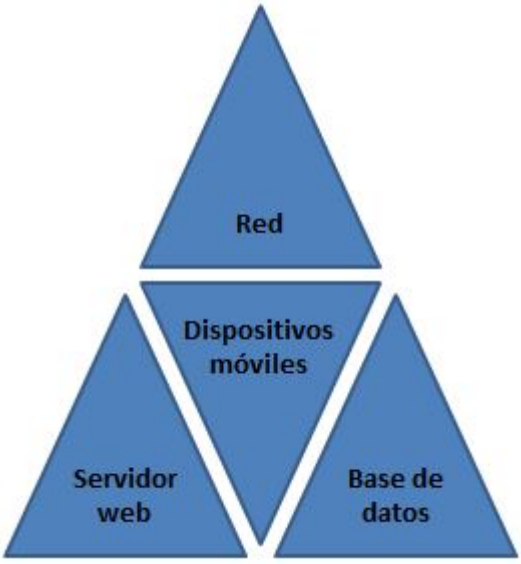
Factores de riesgo en las aplicaciones móviles y algunos controles básicos con los que abordarlos

Con la continua evolución tecnológica, especialmente en el ámbito empresarial, la auditoría del TI y los profesionales de seguridad deben adaptarse al escenario de las amenazas cambiante creado por las aplicaciones móviles adelantándose al riesgo. Para ello deben poner controles apropiados y probar las aplicaciones móviles desde su concepción hasta su lanzamiento. Es por ello que he seguido leyendo sobre la **Gestión del Riesgo Institucional en el Mundo Móvil**, y esta vez he investigado acerca de los **factores de riesgo** en las aplicaciones móviles y algunos **controles básicos** con los que abordarlos. En este Post he utilizado como fuente un artículo de una revista llamada **"ISACA Journal: mobile apps"**.

Los riesgos en las aplicaciones móviles se pueden dividir en cuatro categorías:



Riesgos y controles en la categoría de Dispositivos móviles:

1. **Almacenamiento de datos:**
    - **Riesgo:** Pérdida y divulgación de datos.
    - **Control:** El cifrado de los datos en reposo en el dispositivo móvil se establece en el Estándar de Cifrado Avanzado (Advanced Encryption Standard: AES) de 128, 192 o 256. Mediante este control los datos se almacenan de forma segura para evitar la extracción maliciosa de la aplicación cuando los datos están en reposo.
2. **Transmisión de datos:**
    - **Riesgo:** Pérdida y divulgación de datos.
    - **Control:** El cifrado de datos se aplica para los datos en

transmisión a través de la Capa de Puertos Seguros (Secure Sockets Layer: SSL) y fuertes protocolos de seguridad tales como:
    - Acceso Web – HTTPS vs. HTTP
    - Transferencia de archivos – FTPS, SFTP, SCP, WebDAV sobre HTTPS vs. FTP, RCP
    - Protocolos de seguridad – Seguridad en la Capa de Transporte (Transport Layer Security: TLS)

  Mediante este control la transmisión datos de la aplicación móvil está cifrada cuando no se dispone de datos en reposo.

IMPORTANTE: Estos dos primeros riesgos tratan sobre la pérdida y la divulgación de datos, tema que hace referencia a la **DLP** y a la gestión de contenido móvil (**MCM**).

3. **Aplicación de gestión de acceso y seguridad:**
    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** La gestión de aplicaciones móviles (**MAM**) se utiliza para gestionar el acceso y el despliegue de la aplicación. Además, se mantienen unas adecuadas listas blancas y listas negras. Mediante este control la aplicación está configurada para limitar el acceso y configurada adecuadamente para uso autorizado limitado.
4. **Llevar dispositivos móviles fuera del perímetro empresarial:**
    - **Riesgo:** Pérdida o robo del dispositivo móvil, haciendo posible el acceso no autorizado a las aplicaciones móviles del dispositivo y al fraude de los datos de éstas.
    - **Control:** (**MAM**) *Leer el control 3.2 de esta categoría.

Riesgos y controles en la categoría de Red:

1. **Conectividad inalámbrica:**
    - **Riesgo:** Pérdida y divulgación de datos (**DLP & MCM**).
    - **Control:** La transmisión de datos utiliza, como mínimo, SSL o TLS. Ambos protocolos criptográficos para la transmisión segura de datos. Mediante este control el cifrado se aplica cuando se activa la conexión Wi-Fi.
2. **Secuestro de sesión (Session hijacking):**
    - **Riesgo:** Pérdida y divulgación de datos y acceso no autorizado (**DLP & MCM**).
    - **Control:** Los protocolos de conexión para el Localizador Uniforme de Recursos (Uniform Resource Locator: URL) a través de TLS son a través de HTTPS en lugar de HTTP para conectarse de forma segura a una URL. Mediante este control se evita el secuestro de una sesión debido a un protocolo de conexión inseguro.

Riesgos y controles en la categoría de Servidor web:

1. **Gestión de acceso:**
    - **Riesgo:** Pérdida y divulgación de datos y acceso no autorizado (**DLP & MCM**).

    - **Control:** Todos los servidores web aplicables se asignan a los propietarios de sistemas técnicos y empresariales. Los roles y responsabilidades definidos son adecuados, especialmente para el personal interno y de terceros. Mediante este control los roles y responsabilidades de la propiedad son establecidos, documentados y comunicados.
2. **Ataque de fuerza bruta:**
    - **Riesgo:** Acceso no autorizado y fraude, disponibilidad de la aplicación.
    - **Control:** Los protocolos de bloqueo están habilitados para cuentas con varios intentos de contraseña incorrectos. Se recomienda la utilización de CAPTCHA (programa que distingue entre seres humanos y ordenadores) para evitar DoS (Denegación de Servicio). Mediante este control la gestión de la estrategia de DoS abarca programas adecuados para bloquear los protocolos no autorizados.

Riesgos y controles en la categoría de Base de datos:

1. **Acceso privilegiado:**
    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** El acceso a la BD está limitado a las personas apropiadas, y las revisiones de acceso adecuadas y las cuentas del sistema documentadas se mantienen archivadas. Todas las cuentas y contraseñas predeterminadas se deshabilitan al aplicar controles de contraseña estrictos. Mediante este control el acceso elevado a las BBDD se asegura adecuadamente utilizando las mejores prácticas.
2. **Inyección SQL (SQL injection):**
    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** Se da lugar a la técnica de validación de entrada; existen reglas específicamente definidas para el tipo y la sintaxis contra las reglas clave de negocio. Mediante este control el acceso a la BD del Back-end está protegido adecuadamente de vulnerabilidades utilizando técnicas de validación de entrada apropiadas.
3. **Validación de la entrada de la aplicación (cliente):**
    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** La limpieza de los datos de usuario de la aplicación procedentes de la aplicación móvil se protege adecuadamente mediante comprobaciones de lógica incorporada dentro de la aplicación. La correcta implementación de las comprobaciones lógicas está habilitada en el lado del servidor. Mediante este control los datos procedentes de aplicaciones móviles son examinados antes de confiar en ellos para extraerlos o enviarlos a la capa de BD.
4. **Servicios de BD de aplicaciones.**
    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** El servidor de BD se prueba adecuadamente y se protege contra ataques maliciosos. Los formularios de inicio de sesión requieren HTTPS. Las conexiones SSL son obligatorias.

¿Y el último post?:

No se han tratado amenazas como el **Phishing**. Puesto que considero que es fundamental tener ciernas nociones de esta amenaza, mi último post, tratará sobre ésta.

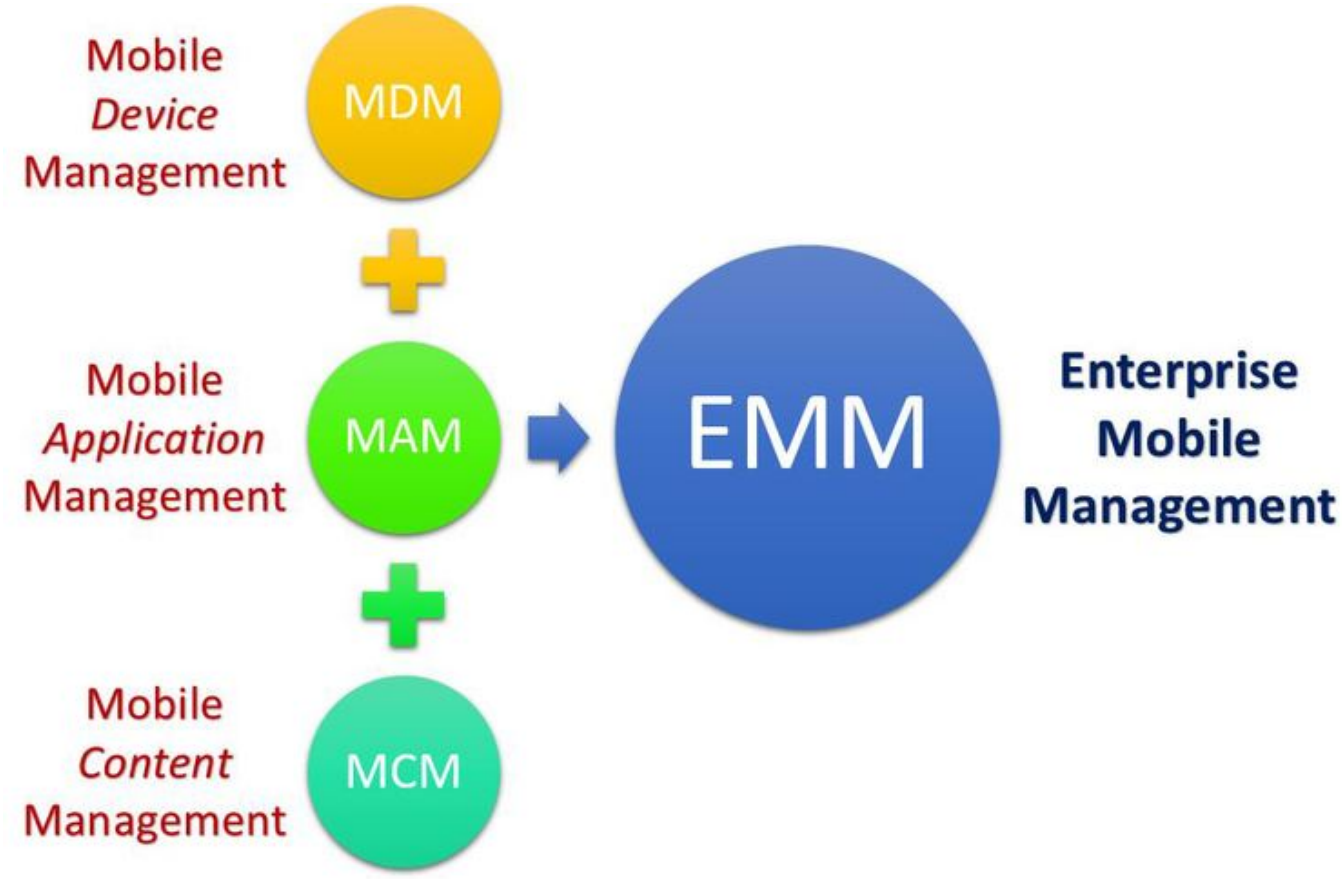
Referencia:

Revista de ISACA:

J. Khan, Mohammed «Mobile App Security Audit Framework», *ISACA Journal: mobile apps,* nº 4 (2016): 14-17.

Gestión de aplicaciones móviles

He seguido leyendo sobre la **Gestión del Riesgo Institucional en el Mundo Móvil**, y esta vez he investigado acerca de la gestión de aplicaciones móviles (**MAM**) y de una herramienta llamada **XenMobile**, la cual tiene como función proporcionar gestión de dispositivos móviles (**MDM**), gestión de aplicaciones móviles (**MAM**) y gestión de contenido móvil (**MCM**).



MAM, MDM y MCM son tres tipos de software, los cuales forman la **gestión**

de movilidad empresarial (EMM). Pero en vez de centrarme en **EMM** y tratar los tres tipos de software por igual, he preferido tratar solo **MAM**, puesto que es, con diferencia, la más importante y porque también permite tratar el conjunto software de **MDM** y de **MCM**.

¿Qué es MAM?:

Para saber que es **MAM** he consultado un documento de **IEEE Xplore** cuyo título es **"Power-Aware Mobile Application Management"** y según este documento la gestión de aplicaciones móviles (**MAM**) describe el software responsable de aprovisionar y controlar el acceso a aplicaciones móviles. Esta funcionalidad permite a los administradores de TI instalar remotamente, actualizar y eliminar aplicaciones móviles, las cuales podrían ser **MEAs** de la propia empresa. Además, con un software de **MAM**, los administradores pueden deshabilitar remotamente las aplicaciones móviles que se sabe que alojan software malicioso (malware).

La idea general es que utilizando **MAM**, una empresa puede bloquear, controlar y proteger todas sus **MEAs** de una forma más óptima y agradable, y en una organización de más de cien empleados la implementación de un software de **MAM** puede ser de gran importancia. Una vez que la empresa supera este tamaño, la administración de aplicaciones móviles puede convertirse en un trabajo de tiempo completo para los administradores de TI. Sin embargo, existen tres desafíos a los que el administrador de TI tendría que enfrentarse:

- Soporte de plataformas y dispositivos móviles. En la actualidad existen infinidad de plataformas móviles (por ejemplo, Android, iOS, BlackBerry, Mac OS, Symbian y Windows Phone), es por eso que los administradores de TI deben buscar una manera de hacer posible el uso de las aplicaciones móviles en cualquier plataforma móvil. Por otro lado, también existe una gran variedad de dispositivos móviles (por ejemplo, Tablets, netbooks, portátiles, teléfonos inteligentes y phablets), por lo que es fundamental que el administrador de TI proporcione un software que permita asegurar, monitorear y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios, también conocido como un software de gestión de dispositivos móviles (**MDM**).
- Impacto mínimo en la energía de la batería de los dispositivos móviles. La mayor queja cuando se trata de dispositivos móviles es que sus vidas de la batería han ido disminuyendo mucho en los últimos años. **MAM** reduce aún más la vida operacional de los dispositivos móviles porque los dispositivos agotan sus baterías cada vez que necesitan instalar, actualizar o eliminar aplicaciones móviles. Por lo tanto, los administradores de TI deben tratar de minimizar el impacto de **MAM** en la energía de la batería.
- Control del almacenamiento y transmisión de los datos. Es decir, que los datos estén seguros de extracciones maliciosas cuando estén almacenados y que estén encriptados cuando estén siendo transferidos. Este desafío se refiere a la **DLP** (Date Loss Prevention) y a la gestión de contenido móvil (**MCM**).

A medida que la tendencia **bring-your-own-device (BYOD)** sigue creciendo,

estos desafíos se vuelven aún más complicados debido a que los dispositivos móviles están proliferando en la empresa a un ritmo exponencial, y esto afecta muchísimo a la gestión de aplicaciones móviles (**MAM**), a la gestión de dispositivos móviles (**MDM**) y a la gestión de contenido móvil (**MCM**). Otra importante tendencia tecnológica que también afecta al software de **MDM** es el despliegue continuo en nubes de **Infraestructura como Servicio (IaaS)** para una gestión más rápida y rentable de dispositivos móviles.

Hasta aquí se puede apreciar que los software de **MAM** tienen gran importancia en el **Mundo Móvil**, a pesar de que existen tendencias que hacen que este tipo de software se vea afectado negativamente, puesto que este tipo de software ayuda a bloquear, controlar y proteger todas las **MEAs** de una organización.

¿Y qué herramientas existen para gestionar aplicaciones móviles? Existen aplicaciones como **Microsoft Intune, Appaloosa o Kaseya**, entre otras. Yo he investigado sobre **XenMobile**.

XenMobile:

En el año 2013, una empresa llamada **Citrix** lanzó la herramienta **XenMobile MDM**, que fue fruto de la compra de **Zenprise**. En el momento de su lanzamiento, **XenMobile MDM** solo era un software de gestión de dispositivos móviles (**MDM**) que otorgó a los usuarios la posibilidad de escoger el dispositivo que querían utilizar mientras que permitió a la empresa hacer frente a sus necesidades de gestión y cumplimiento.

Con el paso del tiempo **Citrix** fue incorporando software de gestión de aplicaciones móviles (**MAM**) y software de gestión de contenido móvil (**MCM**) a la herramienta, transformándola así en un software de **gestión de movilidad empresarial (EMM)**, con lo que **XenMobile MDM**, pasó a llamarse **XenMobile** a secas.

Para finalizar, facilito un vídeo que explica que es, en la actualidad,

XenMobile:

Referencias:

IEEE Xplore:

Arne Koschel, Carsten Kleiner e Irina Astrova, «Power-Aware Mobile Application Management», *Information Society (i-Society),* nº 1 (2014): 251-258.

Otros:

«UNDERSTANDING HOW YOUR EXISTING “MDM” SOLUTION CAN HELP YOU DISTRIBUTE, CONTROL AND SECURELY CONNECT YOUR MOBILE APPLICATIONS», MSC, acceso el 4 de noviembre de 2016, http://www.mscmobility.com.au/mobility-news/mobile-application-management.

«MDM, MAM und MCM – Was bedeuten diese Begriffe?», MOBILITYADMIN, acceso el 4 de noviembre de 2016, http://www.mobilityadmin.de/mobile-device-management/mdm-mam-und-mcm-was-bedeuten-diese-begriffe.

«Citrix lanza XenMobile, una solución MDM», ChannelBiz, acceso el 4 de noviembre de 2016, http://www.channelbiz.es/2013/02/21/citrix-lanza-xenmobile-una-solucion-mdm/.

«XenMobile», Citrix, acceso el 4 de noviembre de 2016, https://www.citrix.es/products/xenmobile/.