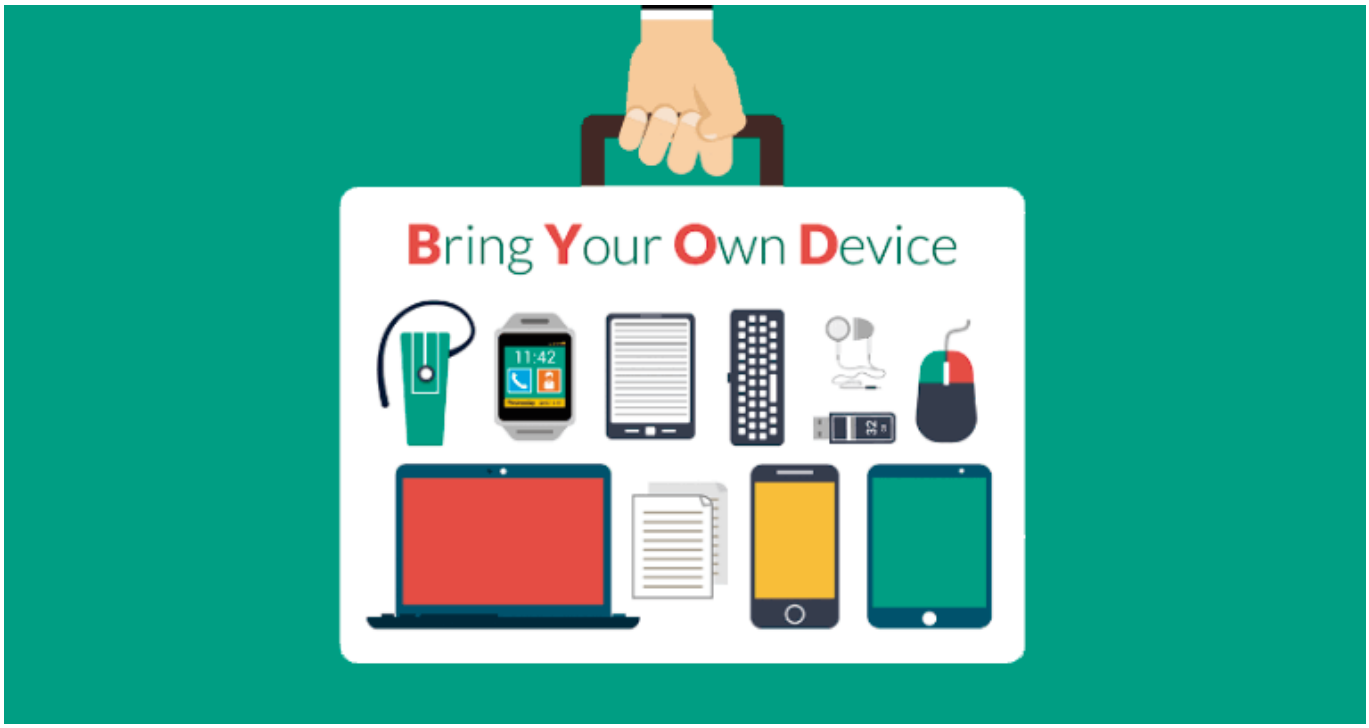
Qué es BYOD y su cercana relación con el Mundo Móvil

Buscando información sobre el mundo móvil, encontré una presentación de ISACA («La información se mueve») relacionada con los dispositivos móviles, en la que se muestra que existen varias posibles decisiones estratégicas que pueden tomar los directivos de una empresa:

- Solución de plataformas estandarizadas
- BYOD "Puro"
- Estrategia combinada

El punto que más me llamó la atención fue BYOD, ya que es un concepto cada vez con mayor tendencia, debido a que las nuevas tecnologías cada vez son más accesibles para todos los usuarios. Al igual que los anteriores posts, se centra directamente con los dispositivos móviles de la propia empresa, pero con un leve cambio de perspectiva que se puede intuir en el significado de sus siglas: Bring Your Own Device, cuya traducción es "trae tu propio dispositivo".

Con BYOD, los empleados utilizan sus propios dispositivos móviles personales, portátiles y tablets para acceder al correo electrónico corporativo, la documentación, aplicaciones, etc. Básicamente consiste en utilizar los dispositivos personales de los empleados en el ámbito corporativo para el desarrollo de sus actividades profesionales. De esta forma, las personas tienen un solo dispositivos para usar tanto para fines profesionales como personales. [1]



¿Qué ventajas y desventajas tiene BYOD?

VENTAJAS	DESVENTAJAS
Mayor productividad de los empleados	Riesgo en la seguridad y la privacidad de la información corporativa
Posibilidad de trabajar con más flexibilidad	Requiere nuevas políticas de control de accesos
Uso del dispositivo en cualquier momento y lugar	Precisa recursos de red suficientes para soportar la llegada de los dispositivos
Permite a los empleados dar mejor servicio al cliente	Necesidad de soporte TI para una diversidad de dispositivos, aplicaciones y software

Debido a las consecuencias de esta decisión estratégica, los propietarios de negocios dudan si seguir este camino debido a las preocupaciones que genera sobre la seguridad. Un temor que puede reducirse con una administración de riesgos adecuada. Los riesgos a los que se enfrentan los auditores IT son los siguientes [2]:

- Riesgo de privacidad del usuario
- Riesgo empresarial
- Asuntos legales
- Medidas proactivas para la privacidad del usuario

RIESGOS DE BYOD

- *Riesgo de privacidad del usuario*

Dado que en el propio dispositivo del empleado tendrá contenido tanto personal como profesional de la propia empresa, el usuario tiene una preocupación continua de qué pueda serle reclamado de su propio dispositivo los siguientes aspectos:

- Historial de navegación web
- Bloqueo, deshabilitación y borrado de datos
- Trabajo extra sin compensación
- Registros telefónicos o contactos
- Emails personales
- Nombres de usuario y contraseñas de redes sociales u otras cuentas
- Datos personales que se trasladan a la nube
- GPS e información de ubicación
- Datos financieros personales
- Historias de chat y mensajes
- Imágenes, video u otros medios
- etc.

Uno de los casos en los que estos datos pueden ser solicitados es si la empresa se ve involucrada en temas legales, ya que los dispositivos personales de los empleados pueden ser reclamados como prueba.

- *Riesgo empresarial*

El departamento de TI son los responsables de mantener el control sobre los datos de una organización, lo que da a la empresa libertad para ver el dispositivo y cómo se está utilizando. Esto se debe a que la empresa se preocupa principalmente por la confidencialidad de sus datos. Por ello, aunque el dispositivo personal sea del usuario, la organización deberá asegurarse de la eliminación de dichos datos o de no perder información en caso de pérdida del dispositivo. Para ello hacen uso de herramientas de administración de dispositivos móviles (Mobile Device Management:MDM).

- *Asuntos legales*

En el área de la privacidad, muchos países han creado leyes relacionadas con el BYOD para protegerse como Personal Information Protection and Electronic Documents Act (PIPEDA) en Canadá. Las organizaciones están sujetas a obligaciones legales, contractuales relacionadas con la recopilación de datos, la retención, la destrucción segura de datos y los términos de los acuerdos/obligaciones de confidencialidad también pueden tener problemas de privacidad.

- *Medidas proactivas para la privacidad del usuario*

Los empleados deben leer detenidamente las políticas BYOD establecidas por la empresa, a pesar de que pueden ser difíciles de comprender debido a su jerga legal y técnica.

Algunas recomendaciones de medidas proactivas para reducir el riesgo de privacidad son:

- Aclara tus preocupaciones con el departamento RRHH. y TI y considera si vale la pena asumir dicho compromiso de privacidad para usar tu dispositivo personal en el trabajo
- Considera la opción de no participar en BYOD, ya que es la mejor opción para mantener privada la información personal del dispositivo.
- Ten en cuenta que tus dispositivos deberán tener una configuración de privacidad a la cual el usuario deberá de adaptarse.
- No olvides realizar una copia de seguridad de los datos personales, ya que la empresa tiene la capacidad de borrar de forma remota los datos del dispositivo. A través de esto al menos mantendrás el concepto de disponibilidad, pero no de privacidad.

- **Programas de aseguramiento para la empresa.**

El punto que más destaca en BYOD es la privacidad de los usuarios, por ello los programas de auditoria y garantía de privacidad pueden ayudar a las organizaciones a mitigar el riesgo. Además, dichos programas también deben incluir aspectos relacionados con la seguridad de la empresa. Los programas de auditoria dirigido a BYOD son los siguientes:

- ISACA’s BYOD Audit/Assurance Program es una herramienta que los auditores de TI podrán usar para completar el proceso de aseguramiento. Se centra en la gestión de riesgos, la gestión de la configuración y la

seguridad de los dispositivos, los recursos humanos y la capacitación de los usuarios.
- Service Organization Control (SOC) 2 y 3 es un informe que se centra en la privacidad desarrollado por el Instituto Americano de Contadores Públicos Certificados (AICPA).

Referencias:

[1] Deusto Océano, «BYOD», Marzo 2016, acceso 29 de diciembre de 2018, https://oceano.biblioteca.deusto.es/primo-explore/fulldisplay?docid=TN_proquest1779441059&context=PC&vid=deusto&lang=es_ES&search_scope=default_scope&adaptor=primo_central_multiple_fe&tab=default_tab&query=any,contains,byod&offset=0

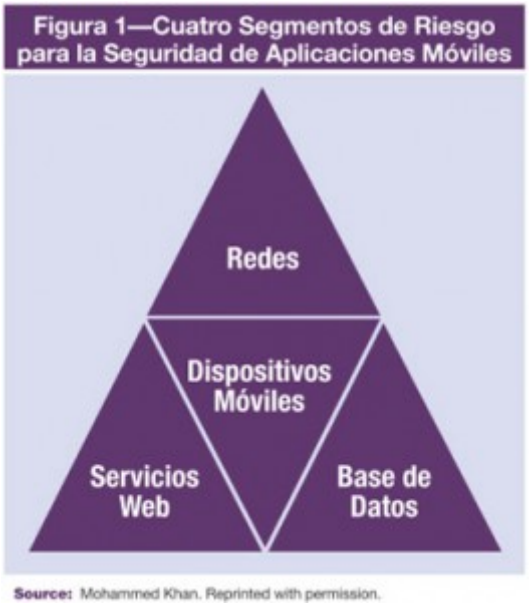
[2] Ashwin Chaudhary, « Privacy Assurance for BYOD », ISACA Journal, volume 5 (2014): 31 – 34. https://www.isaca.org/Journal/archives/2014/Volume-5/Documents/Journal-vol-5-2014.pdf

---

Controles para la Gestión del Riesgo Empresarial en el Mundo Móvil

Con los cambios continuos en el ámbito tecnológico y empresarial, surgen nuevas amenazas creadas por las nuevas aplicaciones móviles, por ello los auditores de TI y los profesionales de la seguridad deben adaptarse a estos cambios y anticiparse a los riesgos aplicar controles apropiados.

Para seleccionar dichos controles, primero se deben de localizar las capas de riesgo, los cuales hemos desarrollado en el anterior post "Gestión del Riesgo Empresarial en el Mundo Móvil". En este post se explicaban las principales áreas de riesgo relacionadas con Mobile Workforce, pero si nos paramos a analizarlos la mayoría tienen un factor de riesgo común que afecta directamente a la organización: la información del dispositivo. Alrededor de este factor podemos segmentarlo en cuatro categorías principales de seguridad de aplicaciones móviles como se muestra en la figura 1.



Para afrontar el reto los auditores de TI hacen uso de los siguientes puntos mostrados en la siguiente tabla, de esta forma resulta más sencillo detectar la amenaza debido a la clasificación de los riesgos en dichas categorías [1].

MARCO DE PRUEBAS DE AUDITORÍA PARA APLICACIONES MÓVILES

ÁREA DE AMENAZA	TEMA DEL CONTROL	CONTROL A VERIFICAR	PRUEBA DE CONTROL	RIESGO MITIGADO
Dispositivos móviles	Almacenamiento de datos	Los datos se almacenan de forma segura para evitar las extracciones maliciosas cuando los datos están en reposo.	El cifrado de los datos en reposo en el dispositivo móvil se establece en el Estándar de cifrado Avanzado (Advanced Encryption Standard:AES) 128, 192 o 256.	Pérdida y divulgación de datos
	Transmisión de datos	Los datos transferidos de la aplicación móvil están encriptados.	El cifrado de datos se aplica a los datos en transmisión a través de la Capa de Puertos Seguros (Secure Sockets Layer: SSL) y protocolos de seguridad 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)	
	Gestión de acceso a aplicaciones y seguridad	La aplicación está configurada para limitar el acceso y configurada de forma adecuada para el uso autorizado limitado.	La gestión de aplicaciones móviles (MAM) se utiliza para gestionar el acceso y el despliegue de la aplicación. Además, las listas blancas y listas negras se mantienen.	Acceso no autorizado y fraude
Redes	Conectividad inalámbrica	El cifrado se aplica cuando se activa la conexión Wi-Fi.	Para garantizar la seguridad de los datos, la transmisión de datos utiliza, al menos, los protocolos SSL o TLS.	Pérdida y divulgación de datos
	Secuestro de sesión (Session hijacking)	Evitar conexiones inseguras para prevenir el secuestro de una sesión.	Los protocolos de conexión para el Localizador Uniforme de Recursos (URL) a través de TLS son a través de HTTPS en lugar de HTTP para garantizar la seguridad a una URL.	Pérdida y divulgación de datos, acceso no autorizado
Servicios Web	Gestión de acceso	Roles y responsabilidades para la propiedad han sido establecidos, documentados y comunicados.	Todos los servidores web aplicables se asignan a propietarios de sistemas técnicos y negocios. Los roles y las responsabilidades definidas son adecuadas, especialmente para el personal interno y de terceros.	
	Ataque de fuerza bruta	La estrategia de gestión de Denegación de Servicio (DoS) incluye programas adecuados para bloquear protocolos no autorizados.	Los protocolos de bloqueo están habilitados para cuentas con varios intentos de contraseña incorrecta. Se recomienda el uso de CAPTCHA (programa que distingue entre humanos y ordenadores) para evitar DoS.	Acceso no autorizado y fraude, disponibilidad de la aplicación

Base de Datos	Acceso privilegiado	El acceso elevado a las bases de datos se asegura adecuadamente utilizando las mejores prácticas.	El acceso a la BD está limitado a las personas adecuadas, y las revisiones de acceso apropiadas y las cuentas documentadas del sistema se mantienen archivadas. Todas las cuentas y contraseñas predeterminadas se deshabilitan aplicando estrictos controles de contraseña.	Acceso no autorizado y fraude
	Inyección SQL	El acceso a la BD del Back-end está protegido apropiadamente contra vulnerabilidades utilizando técnicas de validación de entrada adecuadas.	Existe una técnica de validación de entrada; Existen reglas específicamente definidas para el tipo y la sintaxis de las reglas clave del negocio.	
	Validación de la entrada de la aplicación (cliente)	Los datos procedentes de las aplicaciones móviles deben examinarse antes de extraerlos o enviarlos a la capa de BD.	La limpieza de los datos del usuario de la aplicación móvil se protege adecuadamente mediante comprobaciones lógicas integradas dentro de la aplicación. La correcta implementación de las comprobaciones lógicas está en el lado del servidor.	
	Servicios de BD de aplicaciones	El software de la BD del servidor se actualiza a las versiones seguras más actuales.	El servidor de la BD está probada adecuadamente y reforzado contra ataques maliciosos. Los formularios de inicio de sesión requieren HTTPS. Las conexiones SSL son obligatorias	

Por otro lado, si analizamos la ISO/IEC 27002 (código de práctica para los controles de seguridad de la información) podremos destacar el punto 6.2 “Dispositivos para la movilidad y teletrabajo” el cual pertenece al punto 6 “Aspectos organizativos de la seguridad de la información” [2]. Este punto trata por un lado la política de uso de dispositivos para la movilidad y por otro el teletrabajo [3].

Con estos controles se demuestra que los auditores TI deben trabajar mano a mano con todos los equipos dentro de la organización responsable del desarrollo de aplicaciones móviles, (negocio, desarrollo TI, seguridad TI, legal y cumplimiento). Además, deben de facilitar el proceso que determine un mínimo de controles de seguridad que pueda aplicarse al vulnerable mundo móvil. No debemos olvidar que dichos controles deben realizarse según la aplicación móvil es actualizada y nuevas tecnologías se implementen para dar soporte a la aplicación. De esta forma, se reducirá el riesgo de vulnerabilidades internas y externas que pueden poner en un compromiso los datos.

Referencias:

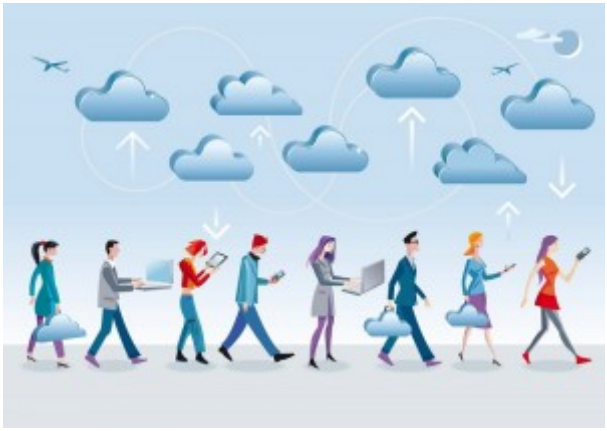
[1] Mohammed J. Khan, « Mobile App Security Audit Framework », ISACA Journal, volume 4 (2016): 1 – 4. https://www.isaca.org/Journal/archives/2016/volume-4/Documents/Mobile-App-Security-Audit-Framework_joa_Eng_0716.pdf .

[2] ISO 27002:2013, acceso 25 de noviembre de 2018, http://www.iso27000.es/download/ControlesISO27002-2013.pdf .

[3] ISO 27002:2013, acceso 25 de noviembre de 2018, Sección 6, http://www.iso27001security.com/html/27002.html#Section6 .

Gestión del Riesgo Empresarial en el Mundo Móvil

Como he comentado en anteriores posts, la fuerza de trabajo móvil (Mobile Workforce) permite que los empleados trabajen donde quieran. Pueden trabajar desde sus casas, que podría definirse como un lugar seguro, o en áreas públicas, como cafeterías o aeropuertos. En este último tipo de lugares es cuando el nivel de amenaza es mayor, ya que puede afectar a la integridad de los datos, pero también a la seguridad física de los empleados, lo que no ocurre en la propia oficina, puesto que se han implementado contramedidas durante décadas. A pesar de ello, no debemos olvidar que el descuido de un empleado remoto puede ser una fuente importante de riesgo que puede afectar a los activos de la empresa. A continuación, se describen las principales áreas de riesgo relacionadas con Mobile Workforce.



Riesgos

- **Activos de la empresa**

Existen dos tipos de activos: físicos (ordenadores portátiles, teléfonos móviles, tabletas) y lógicos (datos de los clientes, datos de los empleados, otra información crítica). Por lo tanto, si alguno de estos dos tipos de activos se pierde o dañan cuando están en posesión de un empleado remoto, suponen un gran riesgo para la empresa.

Además, los hackers u otras personas u organizaciones pueden aprovecharse de los trabajadores remotos para robar datos de una empresa, sabiendo que es más probable que su ataque tenga éxito al atacar a un empleado aislado, que romper las capas de seguridad de toda una organización.

- **Seguridad personal**

La seguridad de los hogares de los empleados no es tan rigurosa como la del propio edificio de oficinas y los criminales son conscientes de ello. Dado

que los empleados tienen los activos en sus hogares, lo que significa que estos activos están expuestos al riesgo como un ladrón o un grupo criminal. Ambos pueden o no ser conscientes del valor de los contenidos y revenderlos.

- **Tecnologías de la nube**

Si una empresa externaliza parcialmente o totalmente sus sistemas e infraestructuras, el riesgo típico de TI relacionado con la confidencialidad, la integridad y la disponibilidad en torno a la administración y gestión de TI, el acceso a los programas y datos, la gestión del cambio y las operaciones aún se mantiene. Además, el uso de internet en las oficinas conlleva un aumento significativo del riesgo. De hecho, los proveedores de nube tienen muchos clientes de los cuales almacenan y administran un gran valor de datos, a los cuales trataran de obtener acceso los hackers a través de una brecha en el sistema de información. Incluso los propios empleados pueden aprovecharse de los datos de los clientes y robar dichos datos para diversos fines.

- **Regulación y Cumplimiento**

Las empresas son responsables de cumplir las regulaciones con las que deben atenerse todas las partes interesadas involucradas en el trabajo móvil. En general, las empresas son responsables de la seguridad de sus sistemas de información, incluso si están externalizados. Es responsabilidad de la compañía asegurar que los datos de los clientes permanecen confidenciales. Si el proveedor de servicios en la nube o un trabajador remoto se ubica en un país donde la protección de datos no es estricta, los datos podrían estar expuestos a un riesgo.

Las empresas están obligadas a cumplir diferentes leyes y reglamentos sobre sus sistemas de información. Este reglamento puede variar en cada país. En los EE.UU., la seguridad de los datos de atención de la salud se rige por el Seguro de Salud de EE.UU. (HIPAA), mientras que en Reino Unido existe la Ley del Servicio Nacional de Salud (NHS) de 2006, la Ley de Salud y Asistencia Social de 2012 y la Ley de Protección de Datos.

Recomendaciones

Para proteger los activos y los recursos, la empresa debería de tomar algunas medidas para reducir el riesgo:

- Identificar y documentar claramente todas las áreas potenciales de seguridad y privacidad relacionadas con el trabajo móvil.
- Realizar programas de capacitación y concienciación sobre los riesgos asociados a los sistemas de información utilizados por los empleados y sus consecuencias para el propio empleado, la empresa, sus clientes y el personal.
- Contraer una póliza de seguro contra pérdidas o daños de activos, de esta forma podrán protegerse contra tales costos. Debido al trabajo a distancia la prima del seguro puede aumentar debido al aumento del riesgo.
- Supervisar los proveedores de la nube. El proveedor debe generar un

informe de aseguramiento de terceros, firmado por un auditor externo, que muestre el estado de su control interno.

- Comunicaciones remotas seguras. La empresa debe informar con frecuencia para evitar el uso de áreas de conexión públicas, a no ser que se hayan implementado medidas de seguridad como conexión VPN.
- Dispositivos seguros y su contenido. Para evitar tragedias tras un robo de un dispositivo, los datos críticos deben ser cifrados y hacer uso de una contraseña fuerte. Además, debe de habilitarse el bloqueo de pantalla tras un periodo de inactividad. El antivirus debe de permanecer actualizado. Por otro lado, se debe administrar a los usuarios cerraduras de ordenadores para proteger el dispositivo físico.

Referencias:

[1] Guy Ngambeket, « Mobile Workforce Security Considerations and Privacy » ISACA Journal, volume 4 (2017): 18 – 19