

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

Mayor productividad de los empleados

Posibilidad de trabajar con más flexibilidad

Uso del dispositivo en cualquier momento y lugar

Permite a los empleados dar mejor servicio al cliente

DESVENTAJAS

Riesgo en la seguridad y la privacidad de la información corporativa

Requiere nuevas políticas de control de accesos

Precisa recursos de red suficientes para soportar la llegada de los dispositivos

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://oceanobiblioteca.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

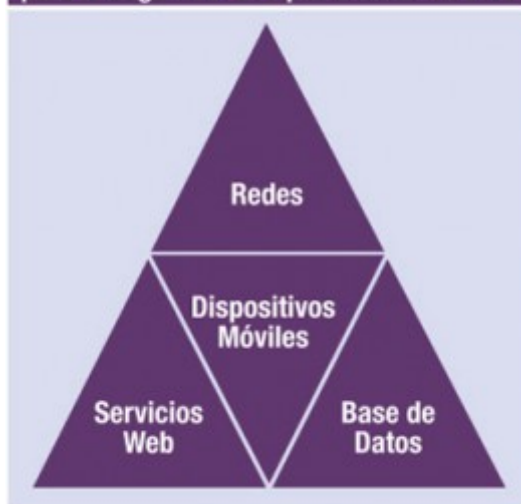
[2] Ashwin Chaudhary, « Privacy Assurance for BYOD », ISACA Journal, volume 5 (2014): 31 – 34. <https://www.isaca.org/Journal/archives/2014/Volume-5/Documents/Journal-vol-5-2014.pdf>

[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.

Figura 1—Cuatro Segmentos de Riesgo para la Seguridad de Aplicaciones Móviles



Source: Mohammed Khan. Reprinted with permission.

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: <ul style="list-style-type: none"> • 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) 	
Redes	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
	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
Servicios Web	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
	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

	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.	
Base de Datos	Inyección SQL	El acceso a la BD del Backend 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.	Acceso no autorizado y fraude
	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 reforzada 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:

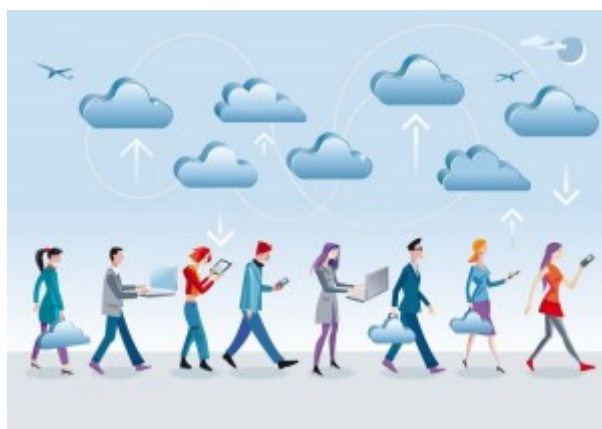
[1] Mohammed J. Khan, « Mobile App Security Audit Framework », ISACA Journal, volume 4 (2016): 1 – 4.
https://www.isaca.org/Journal/archives/2016/volume-4/Documents/Mobile-App-Security-Audit-Framework_joa_Eng_0716.pdf .

[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 tratarían 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

Relevancia en la industria y herramientas de Seguridad Móvil

El trabajo a distancia, es decir el teletrabajo, tiene muchas ventajas, tanto para la empresa como para los empleados. Por ello, las empresas son conscientes de sus beneficios y en algunos países, como Reino Unido, se ha convertido en un derecho de los empleados el solicitar el trabajo móvil [1]. Esto les hace sentir una mayor flexibilidad, libertad y autogestión, lo cual facilita a aquellos que necesitan cuidar de sus hijos o tienen un largo tiempo de desplazamiento para llegar a su lugar de trabajo. Por ejemplo, los empleados remotos no quieren que su gerencia piense que, si no están entregando en los tiempos esperados, es porque el trabajar remotamente los está retrasando. Por lo tanto, trabajarán más que las horas contractuales para alcanzar los objetivos. Además, ayuda a las empresas a reducir costos, especialmente en renta y gastos de consumo (electricidad, agua, servicios de basura, etc.), y encontrar empleados cualificados, independientemente de su ubicación. Con el progreso de la tecnología, la fuerza de trabajo móvil es una tendencia que no va a detenerse. Se prevé que para 2020, el 72,3 por ciento de la mano de obra estadounidense será remota [2].

Los empleados están haciendo negocio desde cualquier dispositivo, haciendo uso de aplicaciones como el correo electrónico o el calendario durante el día e incluso la noche, desde cualquier lugar. Los dispositivos móviles evolucionan convenientemente a una necesidad y pasan a ser de un lujo a un componente necesario, pero crítico para el entorno empresarial. El aumento de las aplicaciones que residen en esos dispositivos conlleva un aumento de

retos de seguridad y aseguramiento de los que nunca se había enfrentado la empresa. Es cierto que tanto las organizaciones como los auditores IT se están volviendo más sofisticados en sus enfoques y, por lo tanto, cada vez son más capaces de anticiparse y responder a los retos.

Debido a esto, los expertos profesionales se mantienen de forma constante en una búsqueda de herramientas y técnicas, que pueden aplicar y adaptarse para ayudar a las organizaciones a garantizar que los dispositivos están protegidos adecuadamente. A continuación, os expondré herramientas de 4 categorías que están disponibles de forma gratuita, open source, etc. Debo destacar que las siguientes herramientas pueden ayudar a resolver problemas específicos de seguridad y seguridad en relación con el entorno móvil. [3]

- Herramientas de prueba de aplicaciones móvil

Las herramientas de proxy web, como [Burp Suite](#) y [ZAP de Open Web Application Security Project](#) (OWASP) son excelentes opciones. Permiten a los usuarios analizar el tráfico entre cualquier dispositivo y las aplicaciones web con las que interactúan. Un proxy de prueba web intercepta los mensajes intercambiados por el dispositivo y la aplicación y permite la manipulación de algunos parámetros, por ejemplo las cabeceras HTTP.

- Herramientas de prueba de dispositivo móvil

Las pruebas específicas de los propios dispositivos móviles incluyen las aplicaciones maliciosas y el comportamiento del usuario ante una situación como phishing. Para ello, se puede hacer uso de la herramienta [Dagah de Shevirah](#).

- Herramientas forenses móvil

La técnica de forense consiste en investigar un dispositivo y determinar si éste ha sido atacado o evaluar de otra manera un incidente potencial que pueda afectarle. La distribución de [Santoku Linux](#) se centra en el examen forense de dispositivos móviles. Otras plataformas de pruebas y respuesta a incidentes son [Kali](#) y [CAINE](#) que contienen herramientas de análisis móviles.

- Herramientas de gestión Sistemas Operativos

Desde el punto de vista de la administración de dispositivos, también hay algunas opciones que se adaptan a cada sistema operativo. Los sistemas operativos iOS y Android tienen incorporados los suyos propios, que les permite realizar tareas como borrado remoto en caso de un dispositivo borrado o perdido.

- [Configurador de Apple](#)

- [Administrados de dispositivos Android](#)

Existen otras herramientas que proporcionan herramientas de privacidad ([The Guardian Project](#)) y configuraciones de sistemas operativos reforzados ([CopperheadOS](#)).

Referencias:

[1] GOV.UK, «Flexible working», acceso 15 de noviembre de 2018, <https://www.gov.uk/flexible-working> .

[2] «Today's mobile workforce: any time, any place», The Telegraph, 5 de septiembre de 2016, acceso 15 de noviembre de 2018, <https://www.telegraph.co.uk/business/ready-and-enabled/todays-mobile-workforce-any-time-any-place/>

[3] Ed Moyle, «Tools: Mobile Security Tools on a Budget» ISACA Journal, volume 4 (2017): 52 – 53

¿Qué es la Gestión del Riesgo Empresarial en el Mundo Móvil?



La invasión de los dispositivos móviles en nuestras vidas cada vez es más

evidente y notable, solamente tienes que pararte a pensar cuántos móviles, portátiles, tablets, etc. tienes a tu alrededor. La próxima vez que salgas de paseo por tu ciudad te invito a fijarte cuántas personas a tu alrededor tienen un dispositivo móvil con el cual hablan, chatean o capturan momentos, te darás cuenta de que no importa la edad y cualquiera dispone de un aparato electrónico. De hecho, una encuesta realizada por la empresa Deloitte, Global Mobile Consumer, encontró que el 85% de las personas de 16 a 75 años posee o tiene acceso a un teléfono inteligente, destacando que las personas entre 55 y 75 años son el grupo de edad de crecimiento más rápido en los últimos cinco años, alcanzando dos tercios con acceso a un teléfono inteligente.[1]

Hace diez años, la mayoría de las organizaciones no abordaban los medios móviles, la nube y las redes sociales. Debido a la explosión experimentada en los últimos diez años en estas plataformas, parece que casi todo el mundo tiene al menos una cuenta de redes sociales y un teléfono en el bolsillo, lo cual ha obligado a las empresas a actuar de la misma forma para no quedarse atrás en este momento de cambios, esto supone un nuevo impacto, la seguridad de la fuerza de trabajo móvil (workforce).

Para muchas personas, la tecnología de la información ha cambiado el significado del trabajo. El lugar de trabajo clásico es la oficina, un lugar donde los empleados se reúnen para realizar una variedad de tareas con un propósito común. En cambio, ahora muchas personas ya no tienen la necesidad de ir a trabajar, ya que disponen de portátiles, smartphones, impresora y conectividad a Internet en sus propios hogares [2]. Su "oficina" es donde viven. Estos nuevos perfiles de trabajo yo los denomino "trabajadores móviles", capaces de realizar su trabajo desde cualquier lugar, siempre y cuando tengan las herramientas técnicas necesarias para ello.

Sin embargo, en este post y en los siguientes no nos centraremos en la gestión de los "trabajadores móviles", sino en la **Gestión del Riesgo Empresarial en el Mundo Móvil**, es decir de las tecnologías de la información de la propia empresa que hacen uso en el exterior.

Si los trabajadores ya no tienen la necesidad de ir a la empresa, ésta no tendrá la necesidad de guardar un escritorio para cada empleado, dado que al tener su propio material será tan sencillo como llegar y sentarse donde ellos gusten. El teletrabajo es un concepto que están intentando implementar varias empresas en España con gran dificultad, ya que si analizamos los datos proporcionados a lo largo de 10 años por el INE (Instituto Nacional de Estadística) apenas alcanza una variación del 3%. En 2017, un 95,4% de los asalariados aseguró no trabajar "ningún día" desde casa, tal y como se muestra en la siguiente gráfica. [3]



Figura 1: Porcentaje de asalariados que trabajan desde su domicilio particular, desde 2007

Esto conlleva a reflexionar en un riesgo añadido, si ellos traen y llevan sus propios dispositivos tecnológicos, toda la información de la empresa reside en dichos dispositivos y estos a su vez se conectan en diferentes redes de internet que pueden resultar inseguras, por ejemplo. Esto puede suponer que su información caiga en manos no deseadas.

¿Qué impacto produce el Mundo Móvil en la Auditoría Interna?

Las tecnologías evolucionan de forma más rápida y constante lo que obliga a los auditores internos a mantenerse al día de las nuevas tecnologías móviles que usan las organizaciones y analizar los riesgos a los que están expuestos en todo momento, los cuales se analizarán en uno de los próximos posts relacionados con la Gestión del Riesgo Empresarial en el Mundo Móvil. [4]

Según el análisis de Deloitte de "2018 Hot topics for IT Internal Audit in Financial Services", donde se muestran los cambios que ha sufrido dicho ranking desde 2012, se aprecia como hasta el año 2014 apenas se valoraba este aspecto en las empresas, ya que se presenta por primera vez en el ranking sin perder presencia desde dicho año. Actualmente, en el año 2018, ha descendido del séptimo puesto al noveno.[5]

Referencias:

[1] Deloitte, «Global Mobile Consumer Survey 2018: The UK Cut», acceso 10 de noviembre de 2018, <http://www.deloitte.co.uk/mobileUK/>.

[2] Steven J.Ross, «I Left My Security in the Office», **ISACA Journal**, volume

4 (2018): 3 – 5.

[3] Laura Olías y Ana Ordaz, « El teletrabajo no acaba de despegar en las empresas españolas», eldiario.es, 8 de septiembre de 2018, acceso 10 de noviembre de 2018, https://www.eldiario.es/economia/teletrabajo-opcion-despegar-empresas-espanolas_0_811919417.html .

[4] Ed Page y Jason Goldberg, «Coping With the Pace of Change in Mobile Applications», *Top Priorities for Internal Audit in Financial Services Organizations*, nº 1 (2016), <https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/srfinancialservicesindustryresults2016> : 31-34.

[5] Deloitte, «2018 Hot topics for IT Internal Audit in Financial Services», acceso 12 de noviembre de 2018, <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-2018-hot-topics-for-it-internal-audit.pdf>.

¿Qué impacto produce el Mundo Móvil en la Auditoría Interna? ¿Qué hacemos? (BYOD)

He estado leyendo sobre la **Gestión del Riesgo Institucional en el Mundo Móvil**, ya que el uso de aplicaciones móviles es muy frecuente dentro de una empresa y en la actualidad existe una variedad inmensa de amenazas contra estos dispositivos. Aprovecho ahora para remarcar que el Mundo Móvil hace referencia a los dispositivos móviles, por lo que no está única y exclusivamente compuesto por teléfonos móviles o Smartphones, también están incluidas las Tablets y las PDAs, al igual que otros muchos dispositivos portátiles que puedan ser utilizados para desempeñar una función dentro de una empresa. Una vez asimilado esto, el siguiente paso es preguntarse:

¿Qué impacto produce el Mundo Móvil en la Auditoría Interna?:

Es un hecho que las aplicaciones móviles evolucionan rápida y constantemente, por lo que la auditoría interna debe asegurarse de que está al día con la tecnología móvil que está siendo utilizada por sus organizaciones y que estas están considerando todas las posibles exposiciones de riesgo en todo momento. Para entender mejor el impacto, he consultado el [Top 10 de Principales Prioridades de la Auditoría Interna en Organizaciones de Servicios Financieros](#) y he descubierto que las aplicaciones móviles se encuentran en este top, concretamente en el séptimo puesto. En la explicación

del top, justifican que las aplicaciones móviles tienen lugar en el top por los riesgos que suponen las aplicaciones móviles para las empresas, en especial en relación a la autenticación del usuario.

Entonces, una vez asumido que las aplicaciones móviles pueden suponer un problema en algunas organizaciones, queda preguntarse cuáles podrían ser unas buenas medidas a tomar dentro de las organizaciones para evitar los problemas. En algún post siguiente a este, trabajaré los riesgos más importantes, así como los controles a tomar para cada uno de ellos, pero de momento, en este post solo pondré, según la explicación del top, los puntos de acción que los auditores jefes ejecutivos y las funciones de auditoría interna necesitan considerar:

1. Garantizar que las **aplicaciones móviles** y la banca están completamente cubiertas en el universo de auditoría (todos los productos / servicios, plataformas, proveedores, etc.).
2. Asegurarse de que los terceros son tenidos en cuenta en las políticas y procedimientos de gestión de proveedores.
3. Considerar la posibilidad de riesgo de fraude en relación con las **transacciones móviles** dentro de los procesos de cara al cliente (orígenes y servicio).
4. Entender el enfoque de la seguridad por tener una **presencia móvil**.
5. Considerar el proceso de extremo a extremo de cara al servicio. Los **móviles** son la típica puerta de entrada a otros servicios y plataformas.
6. Entender los planes y controles de gestión del cambio de **aplicaciones móviles**.
7. Considerar todas las **plataformas móviles** compatibles aplicables (iOS, Android, Windows, etc.) en los planes de auditoría.
8. Si procede, tener en cuenta los controles necesarios para apoyar un modelo de entrega de software ágil.
9. Considerar la posibilidad de la gestión del servicio multiplataforma, incluyendo los componentes de otros fabricantes.
10. Tener en cuenta las responsabilidades de las empresas, las políticas y procedimientos en relación al aprovisionamiento de cuentas en los **dispositivos móviles**.

Y entonces, viendo los riesgos e impacto: ¿Todo está perdido? ¿Qué hacemos?

Llegados a este punto la solución es tomar una decisión estratégica. ¿Pero cuál?

¿Qué hacemos? (BYOD):

Según [un documento de ISACA](#) existen varias posibles decisiones estratégicas, cada una con sus respectivas ventajas y desventajas. A continuación, enumero algunas de las decisiones estratégicas que ISACA propone:

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

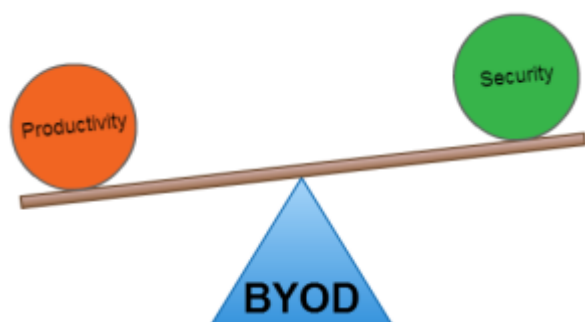
Aquí algo llamó mi atención. ¿BYOD? ¿Seguro? Para quienes no sepan muy bien que es esto del BYOD: BYOD significa Bring Your Own Device y es una estrategia que permite a los empleados, proveedores y otros usuarios el utilizar dispositivos seleccionados y comprados por ellos para ejecutar aplicaciones de la empresa (Típicamente Smartphones y Tablets, pero también se pueden usar en PCs).



BYOD, provocó la tendencia BY0x, o Bring Your Own "Everything":



Entonces, ¿qué implica ofrecer a todos los empleados la posibilidad de utilizar su propio material para trabajar? A priori, una gran comodidad para el empleado, lo que le mantiene motivado en su trabajo, con lo que aumenta considerablemente la productividad de la organización. ¿Pero a qué precio? ¿Dónde reside la seguridad en este caso? En el empleado, que no necesariamente va a controlar el uso que va a hacer de sus dispositivos. Esto es una fuente de incidencias de seguridad.



Y yo me pregunto, ¿dónde está el punto a favor de introducir BYOD en una empresa? Lo que en realidad se propone con el BYOD "Puro" es el cambio de migrar los datos a otro sitio y que no se almacenen en el dispositivo desde el que se accede a ellos. El objetivo es crear un sistema de acceso remoto a los recursos que los empleados necesitan para realizar su trabajo. De esta forma, se evita que un problema de seguridad en el equipo local se pueda transmitir a la red de la empresa. Aun así es necesario que las comunicaciones entre el equipo BYOD y los recursos se realicen de forma segura, sobre todo cuando el empleado no se encuentre dentro de las instalaciones de la empresa.

Por último y para concluir este post, el BYOD se vende como un ahorro y aunque ISACA propone el BYOD "Puro" como una decisión estratégica de cara a minimizar el riesgo, yo considero que el cambio de no tener BYOD a tenerlo se debe hacer si el objetivo es aumentar la productividad de la empresa, no la seguridad.

SYSADMINOTAUR



Referencias:

KnowledgeLeader:

Ed Page y Jason Goldberg, «Coping With the Pace of Change in Mobile Applications», *Top Priorities for Internal Audit in Financial Services Organizations*, nº 1 (2016): 31-34.

ISACA:

«La información se mueve, ¿tu seguridad también?», ISACA, acceso el 14 de octubre de 2016,
<http://www.isaca.org/chapters7/Monterrey/Events/Documents/20140409%20La%20Informacion%20se%20Mueve.pdf>.

Otros:

«El BYOD la pesadilla del responsable de seguridad», EOI, acceso el 14 de

octubre de 2016,

<http://www.eoi.es/blogs/ciberseguridad/2016/04/19/el-byod-la-pesadilla-del-responsable-de-seguridad/>.

«Cómo implementar una política segura de BYOD en la empresa», BBVA con tu empresa, acceso el 14 de octubre de 2016,

<http://www.bbvacontuempresa.es/como-implantar-una-politica-segura-de-byod-en-la-empresa>.