Qué es BYOD y su cercana relación con el Mundo Móvil

Author : M.B.

Categories : Auditoría, Certificación y Calidad de Sistemas Informáticos

Date : 1 diciembre, 2018

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