BYOD: Trae tu propio dispositivo… ¡Y tus propios riesgos!

Ahora que ya conocéis en profundidad las tendencias BYOD y COPE y hemos visto que son realmente importantes en la actualidad creo que ha llegado el duro momento de conocer otra de las realidades de estas políticas, sus riesgos. El riesgo es algo inherente en todo lo que hacemos en la vida, en mayor o menos medida, por ello, seguramente ninguno de vosotros pensaba que todo era tan perfecto como lo podía parecer hasta el momento. Además, el hecho de que tanta gente lo aplique no es motivo para pensar que no va a ocurrir nada al hacer uso de ello. Dicho esto, voy a dedicar esta entrada a detallar los problemas que pueden surgir con el uso de estas tendencias.

Estos riesgos se podrían diferenciar en 3 grandes grupos [1] que voy a analizar a continuación desgranando los que se pueden incluir en cada uno de ellos. El primero de ellos, incluye los relacionados con la **seguridad** [2]. Aquí se pueden encontrar el riesgo a ataques dirigidos contra los sistemas de la empresa, posibilidad de fuga o robo de información sensible (sobre todo en móviles y tablets) y riesgo a vulnerabilidades como, por ejemplo, la conexión a puntos de acceso Wi-Fi sin protección. También existe el riesgo de mezclar los datos personales y de negocio al instalar el usuario aplicaciones no seguras, riesgo de pérdida de dispositivos y, por tanto, todos los datos almacenados en él, el riesgo a que la infraestructura no esté lo suficientemente protegida para el uso de estos dispositivos y, por último, el riesgo a que los empleados comentan fallos debido a la no comprensión de la política BYOD de la empresa.

En el segundo de los grupos, se incluyen los riesgos relacionados con la **privacidad** que probablemente muchos de ellos también se podrían incluir en el grupo anterior. En este existe el riesgo de que el usuario por desconocimiento ponga en compromiso sus datos pulsando en lugares inadecuados y el riesgo de compartir dispositivos con otros miembros de tu familia o amigos y poner en compromiso tu trabajo. Además, sobre todo en las políticas COPE, el usuario puede ser sometido a un borrado remoto de sus datos (sin distinciones) corriendo el riesgo de perder todo lo que tenía [3]. Esto ocurre debido a las políticas *ActiveSync* que están adoptando muchas empresas como primera línea de defensa. Otro de los riesgos que pueden ocurrir es el de tener que ceder tu dispositivo para su examinación en caso de ocurrir algún problema, perdiendo toda la privacidad de tus datos. En este último punto se incluyen tus páginas web visitadas, tus contactos, tus emails, las películas que te has descargado, etc… En definitiva, una pérdida total de tu privacidad que deberías estar dispuesto a tener si usas esta política.

Finalmente, el grupo de **vulneración de los derechos fundamentales** está especialmente orientado a la tendencia COPE, ya que existe el riesgo de que la propia empresa ejerza un control sobre los trabajadores y el uso que les dan a los dispositivos. Aquí se incluyen hechos como el seguimiento de la localización del dispositivo (para comprobar si lo has perdido) o de cualquier actividad que se haga con él. Esto no ocurrirá en el BYOD al

pertenecer los dispositivos al propio usuario, pero si en la otra tendencia ya que los dispositivos son adquiridos por la propia empresa. La verdad, me ha sorprendido saber que el artículo 20 del Estatuto de los Trabajadores permita que el empresario realice este control, aún así, si no se hace adecuadamente se vulnerarán los derechos de la persona, por lo que siempre se debe tener extrema precaución. Fuera de estas tres categorías, también existen riesgos como el de que los costes indirectos de la política BYOD se nos vuelvan en nuestra contra (al tener que hacer inversiones extra) o el riesgo de que los usuarios hagan compras dentro de las aplicaciones y eso suponga un aumento de coste para la empresa.

Y ahora os preguntaréis, ¿esto ocurre siempre? Pues no, ni es algo que exista en todas las empresas, ni es algo al azar lo que provoca que ocurra, sino que hay varias condiciones que lo provocan [4]. Primero de todo, cuando permitimos que los datos de la empresa y personales coexistan en un mismo dispositivo, ya estamos aumentando muchísimo las posibilidades de tener problemas de seguridad en la empresa o de privacidad a nivel personal. Además, que muchos dispositivos se encuentren casi las 24 horas del día encendidos también incrementa este número teniendo más posibilidades de recibir un ataque. A parte de estos dos factores, también nos podemos encontrar la dificultad que tienen los departamentos de TI para soportar todos los sistemas operativos que se utilizan para acceder. Dependiendo del empeño por asegurar el sistema que tengan en la empresa, serán vulnerables en mayor o en menor medida.

Una vez que conocemos los riesgos de esta tendencia, que como os he mostrado son de lo más variado, y un breve razonamiento de por qué ocurren, el próximo paso será descubrir cómo controlar esos riesgos. Esto vendrá en mi próxima entrada de este blog, pero hasta entonces, os quiero dejar algunas preguntas que te ayudarán, si utilizas esta política, a saber si puedes estar en riesgo [5]:

- ¿Tiene la organización la autoridad para investigar el dispositivo?
- ¿Conoces las aplicaciones que se encuentran instaladas en el dispositivo del usuario? ¿Son seguras?
- ¿Las aplicaciones acceden a la información del usuario?
- ¿Están los usuarios autorizados a usar soluciones en la nube?
- ¿Cuál es la forma de acceso a la compañía? (Escritorio remoto, etc.)
- ¿Se pueden borrar los dispositivos remotamente?

Estas, entre otras muchas, nos ayudarán a saber si nuestra compañía está teniendo en cuenta los riesgos del BYOD o, en cambio, está cayendo en sus problemas, pero recuerda, cada compañía debe tener su propia política. Incluso, las personas deberían plantearse crear sus propias normas para sus dispositivos personales. ¿Alguna vez te lo has planteado?

[1] BYOD imparable ¿riesgo controlable?, Abogacia.es, http://www.abogacia.es/2016/03/28/byod-imparable-riesgo-controlable/,

Visitado el 07 de noviembre de 2016

[2] 5 BYOD security implications and how to overcome them, Edel Creely, TrylogyTechnologies, http://trilogytechnologies.com/5-byod-security-implications/, Visitado el 07 de noviembre de 2016

[3] The Dark Side of BYOD – Privacy, Personal Data Loss and Device Seizure, Trend Micro, http://blog.trendmicro.com/consumerization-byod-privacy-personal-data-loss-and-device-seizure/, Visitado el 07 de noviembre de 2016

[4] Bring You Own Device, An overview of risk assessment, Robert Ogie, IEEE, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7353260&tag=1, Visitado el 08 de noviembre de 2016

[5] Devices are mobile – Is your security policy on board?, Scott Laliberte, KnowledgeLeader, https://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/HIDevicesAreMobileIsYourSecurityPolicyonBoard!OpenDocument, Visitado el 06 de noviembre de 2016