BYOD: ¿Es posible controlar algo que no es tuyo?

En el anterior post redacté algunos de los riesgos que nos podemos encontrar al utilizar las tendencias BYOD y COPE que estoy tratando en esta serie de entradas. En aquel momento finalicé diciendo que la próxima vez iba a hablar única y exclusivamente de los controles que se les podían aplicar a esos problemas y, como no puede ser de otra manera, así va a ser. Os preguntaréis, ¿Es realmente necesario aplicar controles?, pues sí. Una sociedad que se toma a la ligera lo que ocurra sin tener en cuenta si existen problemas, tarde o temprano terminará en desastre. Y esto se puede aplicar a todos los ámbitos de la vida, eso sí, sin llegar a tener que vivir, como decía uno de mis compañeros en uno de sus posts, vigilados por el "gran hermano".

Lo primero de todo será identificar la persona encargada de hacer estos controles. En este punto es donde entra en juego la figura del Auditor, que en este caso tendrá el rol de hacer que se cumplan las políticas adoptadas para la empresa, identificar los controles internos y deficiencias que puedan afectar a la organización y detectar cualquier problema de seguridad de la información que esté relacionado con la poca seguridad de los dispositivos móviles. Recientemente, desde ISACA ha sido lanzado un programa para la auditoría de BYOD [1]. Este, se centra en los dispositivos BYOD que se conectan a la red de la organización o contienen su información, incluyendo todas las variedades de Smartphone, Tablet, Ordenadores portátiles y todos sus sistemas operativos. Además, los propios auditores tendrán que adaptar esta guía para sus organizaciones, ya que, se plantea como un punto de partida para la realización de su trabajo.

Una de las prácticas más recomendables para una empresa o incluso nosotros mismos, es la de crear una política de uso de

los dispositivos. Para ello, podemos tener en cuenta el estándar ISO 27001 [2], el cual se refiere a la seguridad de la información. Sin embargo, aunque parezca increíble en la sociedad en la vivimos, en ningún momento se nombra la palabra BYOD en el estándar, pero sí que existen numerosos controles [3] de esta que son imprescindibles en cualquier compañía moderna y que los podríamos adoptar para este caso.

El primero de ellos, **la política de dispositivos móviles** (6.2.1), que requiere el desarrollo de una política de uso de dispositivos móviles para reducir los riesgos. El segundo, el correspondiente al **teletrabajo** (6.2.2), ya que los dispositivos son usados no solo en las oficinas. Este, está formado por controles para el acceso, procesamiento y almacenamiento de información. El tercero, **las políticas y procedimientos de intercambio de información** (13.2.1), se centra en la protección de la información que se transfiere mediante cualquier modo de comunicación, incluyendo en este caso los dispositivos móviles. Finalmente, el último control que se podría incorporar, el de **mensajería electrónica** (13.2.3) que recogerá la forma en la que los mensajes electrónicos serán protegidos. Pero no nos podemos limitar solo a estos, otros como **el uso aceptable de los activos** (8.2.3) y **el control de acceso a redes y servicios asociados** (9.1.2) serían igual de relevantes para una compañía que utilice el *BYOD* en su día a día.

Además de los controles relacionados con los estándares ISO, también pueden ser planteados otros muchos en relación a los riesgos que pueden surgir en las tendencias BYOD y COPE. Teniendo en cuenta los mencionados en la anterior entrada, voy a comentar algunos controles que se pueden aplicar.

Comenzando por la seguridad [4], para la pérdida de información sensible habría que implementar políticas y procedimientos que comunicasen los límites para el uso de los dispositivos y que ocurrirá si eso es ignorado. Para prevenir las vulnerabilidades, es recomendable el uso de una VPN y así

verificar que la información que se transmite se encuentra encriptada y es la correcta, por parte del administrador, la existencia de perfiles únicos de seguridad permitiría adaptar la infraestructura a cada usuario. Así mismo, para evitar que se mezcle la información personal con la de negocio, se puede invertir en software EMM o *Enterprise Mobility Management* que monitoriza y detecta los riesgos antes de que estos ocurran. Otro de los riesgos comentados se refería a la pérdida de los dispositivos, para esto, una política de seguridad aplicada mediante una solución MDM o *Mobile Device Management* sería la ideal al permitir al administrador bloquearlo remotamente. Finalmente, para poder combatir las infraestructuras no preparadas para BYOD, se debería hacer una auditoría de todo el entorno TI de la empresa para revisar si puede ser usada con dispositivos móviles y documentar los usos de la red permitidos para evitar el exceso en su uso (descargas, etc…).

Además de todo esto, se debe controlar que los propios dispositivos tienen la seguridad adecuada como, por ejemplo, no permitir dispositivos con 'jailbreak' [5], y asegurarse de que los empleados conocen la política de empresa para este uso de los dispositivos, así como, que están concienciados de los riesgos que puede haber en ella. El auditor debería asegurarse de que esto se está realizando por medio de la firma de un contrato confirmando que conocen sus libertades y limitaciones. Otro de los problemas es la posible pérdida de las contraseñas de la empresa [6], por lo que debe existir una política de guardado de las mismas y asegurarse que se encuentran encriptadas.

Todos estaremos de acuerdo en que muchas veces a pesar de tener estos controles no se les hace demasiado caso. En numerosas ocasiones, son hojas y hojas incomprensibles que pasan desapercibidas. Por ello, nuestro objetivo no tiene que ser el de rellenar documentos, esos carecen de importancia y cuanto más cortos y simples sean mejor será (Adoptando el ya conocido principio KISS "*keep it simple stupid*"). Lo

importante siempre deben ser las personas, por lo que lo más relevante debe ser cambiar su comportamiento y hacer que trabajen de una forma segura sin cambiar ninguna de las libertades de las que disponían hasta ahora.

[1] BYOD Audit/Assurance Program, ISACA, http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/byod-audit-assurance-program.aspx, Visitado el 21 de noviembre de 2016

[2] How to write an easy-to-use BYOD policy compliant with ISO 27001, Advisera, http://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-iso-27001/ , Visitado el 21 de noviembre de 2016

[3] Controles ISO 27002-2013, iso27000, http://www.iso27000.es/download/ControlesISO27002-2013.pdf, Visitado el 21 de noviembre de 2016

[4] 5 BYOD security implications and how to overcome them, Edel Creely, Trilogy Technologies, http://trilogytechnologies.com/5-byod-security-implications/, Visitado el 21 de noviembre de 2016

[5] BYOD: How your business can address the 5 biggest vulnerabilities, Scott Anderson, Ccb Technology, http://ccbtechnology.com/byod-5-biggest-security-risks/, Visitado el 22 de noviembre de 2016

[6] 10 worst-case BYOD scenarios (and how to prevent them), Jack Wallen, Techrepublic, http://www.techrepublic.com/blog/10-things/10-worst-case-byod-scenarios-and-how-to-prevent-them/, Visitado el 22 de noviembre de 2016