



BYOD – CÓMO IMPACTA EN LAS NORMAS Y ESTÁNDARES APLICABLES DE SEGURIDAD

Luis Alonso

La tendencia byod (Bring Your Own Device "Tráete tu propio dispositivo") es una realidad dentro del ámbito empresarial que se está haciendo muy popular en México. Esta tendencia permite que los empleados lleven sus equipos a las empresas, ya sean laptops, smartphones o tablets para con ellos acceder a los recursos de la compañía.

La tónica habitual, hasta hace unos años, era que las tecnologías de punta estuvieran en el ámbito empresarial y no en el ámbito doméstico; sin embargo, hoy en día esta tendencia ha sufrido un vuelco radical. Los avances tecnológicos han propiciado que los usuarios tengan a su alcance dispositivos con mejor rendimiento que los que manejan sus propias empresas.

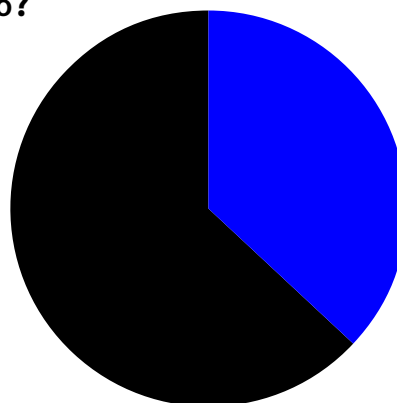
Es cierto que BYOD presenta grandes ventajas, pero muy pocas organizaciones adaptan sus procesos de seguridad y sus métodos de trabajo para incorporar esta nueva realidad a su empresa de forma segura. Una de las grandes desventajas que BYOD acarrea es que, en caso de una implementación no controlada, se pueden producir grandes brechas de seguridad en la organización. La pregunta que debemos hacernos es ¿qué alcance tendrá el BYOD?

Si nos enfocamos datos duros, según una encuesta de [Asus](#)¹, el 63.1% de los empleados mexicanos aseguran que llevan su propio equipo al trabajo; de ellos, el 51.3% lleva su propia notebook; 32.1%, su smartphone, y el 16.5%, su tablet.

GRÁFICA 1. CANTIDAD DE PERSONAS QUE LLEVAN SU EQUIPO AL TRABAJO

¿LLEVA SU PROPIO EQUIPO AL TRABAJO?

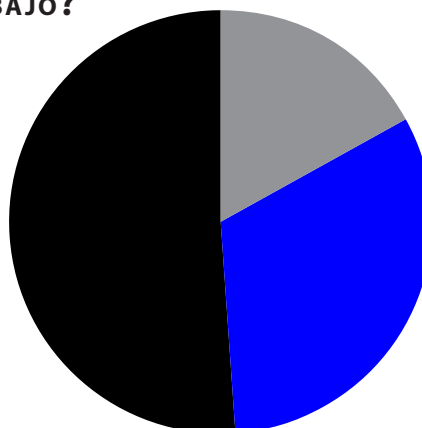
NO, 37%
SÍ, 63%



GRÁFICA 2. TIPO DE EQUIPO QUE LLEVAN SU EQUIPO AL TRABAJO

¿QUÉ EQUIPO ES EL QUE LLEVA AL TRABAJO?

TABLET, 17%
SMARTPHONE, 32%
NOTEBOOK, 51%





Es cierto que no parecen unos porcentajes abrumadores, pero si de acuerdo a la encuesta de [TYNTEC](#)² tomamos como referente a Europa, y más concretamente a España, observaremos un dato muy revelador: el 79% de los profesionales españoles afirma que utiliza sus dispositivos personales para cuestiones laborales. Esto significa algo más de quince puntos porcentuales arriba de los datos registrados en México.

Bajo esta premisa, podemos afirmar que la adopción de la tendencia [BYOD](#) en México se incrementará de manera significativa en los próximos años, pero ¿cómo impactará esta situación a las normas de seguridad aplicables?

Si nos centramos en la norma [iso 27.001](#), estándar para la seguridad de la información, nos encontraremos con algunos puntos singulares que debemos definir cuidadosamente si queremos permitir que dispositivos externos accedan a nuestra red:

- En el apéndice normativo [A](#), control 6.2.1, se menciona que se debe adoptar una política y medidas de seguridad para gestionar los riesgos introducidos por el uso de equipos móviles. Esto quiere decir que [TODOS](#) los equipos móviles (ya sean de organizaciones o propiedad de los empleados) se sometan a los lineamientos que esta política menciona.

Aquí ya nos encontramos contra uno de los grandes paradigmas del [BYOD](#). ¿Debo controlar los equipos, propiedad de mis empleados, que son utilizados para fines laborales?

- En el mismo apéndice normativo [A](#), control 8.1, se hace mención de la necesidad de identificar los activos de la organización y definir las responsabilidades de protección adecuadas. Dentro de este inventario deben incluirse todos los elementos que procesen información, y por extensión deben contemplarse los equipos que los trabajadores incorporen a su rutina de trabajo, aunque sean de su propiedad.

Aquí nos encontramos con un segundo paradigma. ¿Debo inventariar los equipos que no son técnicamente propiedad de la organización pero acceden a recursos corporativos?

Existen otros ámbitos relacionados con la seguridad que deben tenerse en cuenta a la hora de incorporar la tendencia [BYOD](#) dentro de nuestra organización. Sin ir más lejos, la propia Ley Federal de Protección de Datos

Personales en Posesión de Particulares ([LFPDPPP](#)) marca límites legales que deben cumplirse en el acceso, control y divulgación de cierta información sensible, aun cuando los empleados utilicen sus propios dispositivos. Aquí nos encontramos con el tercer paradigma: que un empleado utilice su celular para consultar el correo corporativo ¿es una brecha de seguridad?

La respuesta a los tres paradigmas presentados es muy simple: [sí](#):

- [sí](#), es necesario controlar los equipos de los empleados que accedan a recursos de la organización.
- [sí](#), deben auditarse los equipos de los empleados que accedan a recursos de la organización.
- [sí](#), el acceso a correos corporativos desde equipos personales es una de las mayores brechas de seguridad que se puede plantear.

Es por eso que a la hora de implementar un acercamiento a BYOD en una organización es importante garantizar que se cubran dos aspectos fundamentales:

- Que los equipos de los usuarios se inventarién y se controlen con software que, por ejemplo, impida que la información se almacene de forma local en los equipos, e incluso se cuente con mecanismos que permitan bo-



rrarlos de manera remota en caso de necesidad.

- Robustecer los procesos de auditoría sobre los accesos a los recursos de información. Conocer quién, qué, cómo y cuándo accede a los recursos de la organización es fundamental para garantizar la seguridad.

adopción de esta tendencia, deben tenerse presentes los parámetros ya mencionados. Tomar en consideración dichas limitantes, así como su debido control, será esencial para garantizar una implementación segura y satisfactoria.

Como hemos visto, el control de los dispositivos que los empleados utilizan dentro de la organización es una obligación de cualquier empresa que tenga el compromiso de preservar la seguridad de la información. Para ello contamos en el mercado con una gran variedad de *software* **MDM** (*Mobile Device Management*) que facilita el trabajo en este aspecto. Es obvio que las organizaciones van a requerir cambios e inversiones para dotarse de la infraestructura física y lógica que les permita soportar tendencias como **BYOD**. También supone que los usuarios cedan gran parte de control sobre sus propios activos. Esto implica que deben ser conscientes de que renunciarán al libre uso de sus equipos, por ejemplo, no podrán instalar ciertas aplicaciones, y la organización puede requerir instalar herramientas de control que permitan garantizar que se cumplan los lineamientos en cuanto a seguridad de la información.

Como podemos observar, el **BYOD** no es tan sencillo como “me llevo mi equipo y me conecto a la red de la empresa”. Para una correcta

¹ ASUS. “ASUS MOBILITY REPORT” [en línea], In Slideshare, México, 2015, [fecha de consulta: octubre 2016], disponible en: <<http://www.slideshare.net/dmedina83/asus-mobility-report-2014-hbitos-de-movilidad-de-los-usuarios-en-mxico>>.

² TYNTEC. “TYNTEC BYOD USER SURVEY” [en línea], Tyn-tec.com, Inglaterra, 2015, [fecha de consulta: octubre 2016], disponible en: <<http://tyntec.com/sites/default/files/uploads/tyntec-byod-summary-20150709.pdf>>.