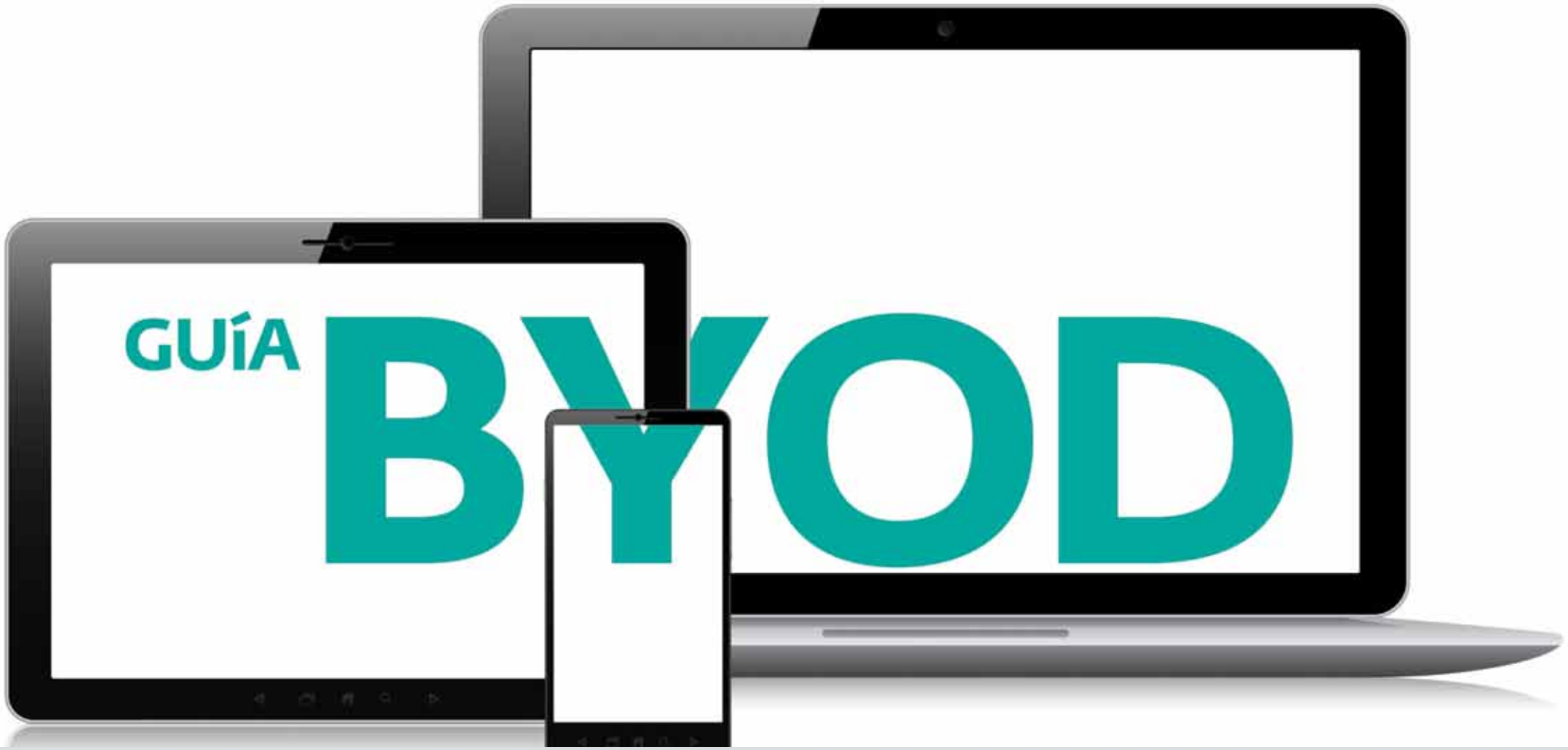
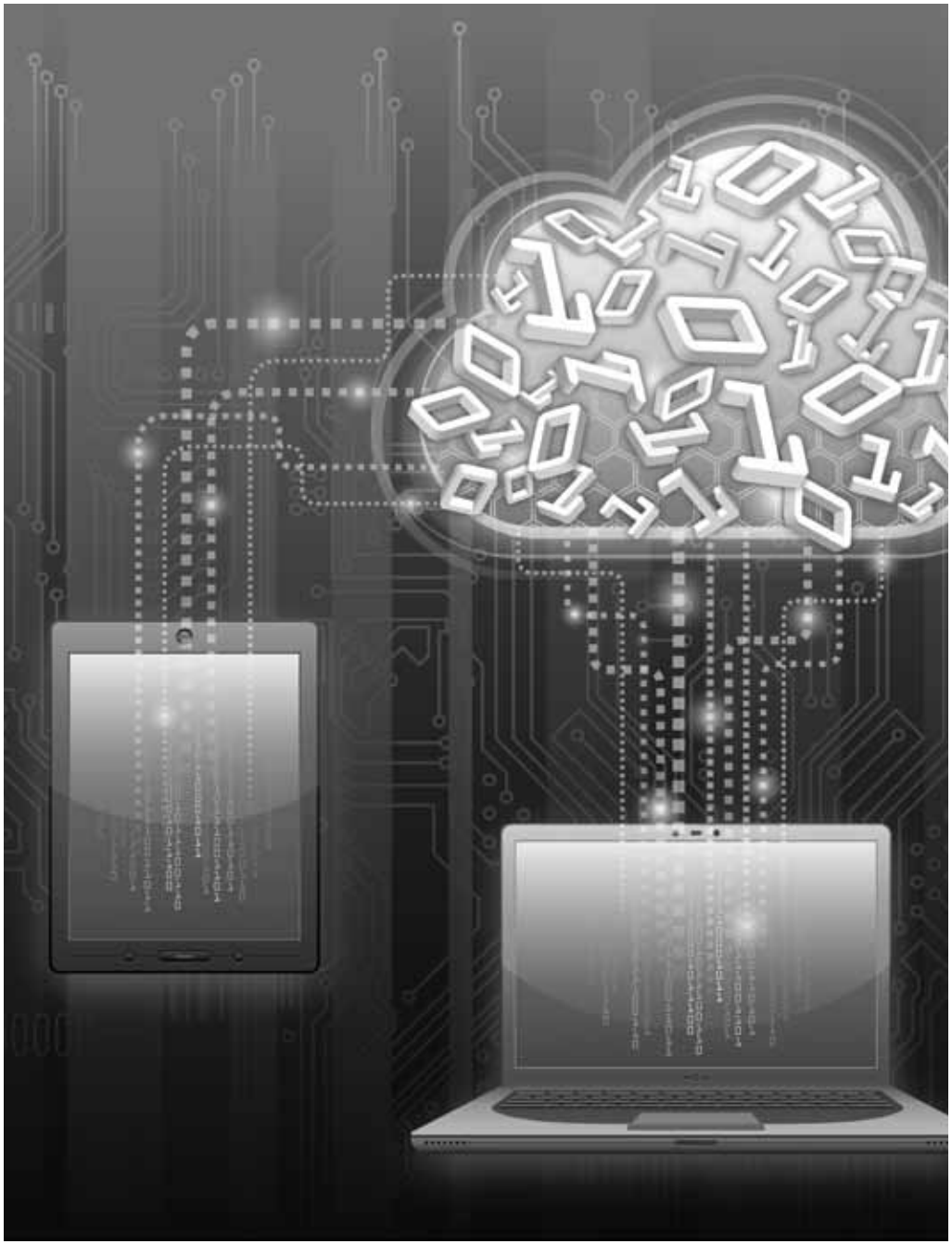


BYOD - Retos de seguridad

ÍNDICE

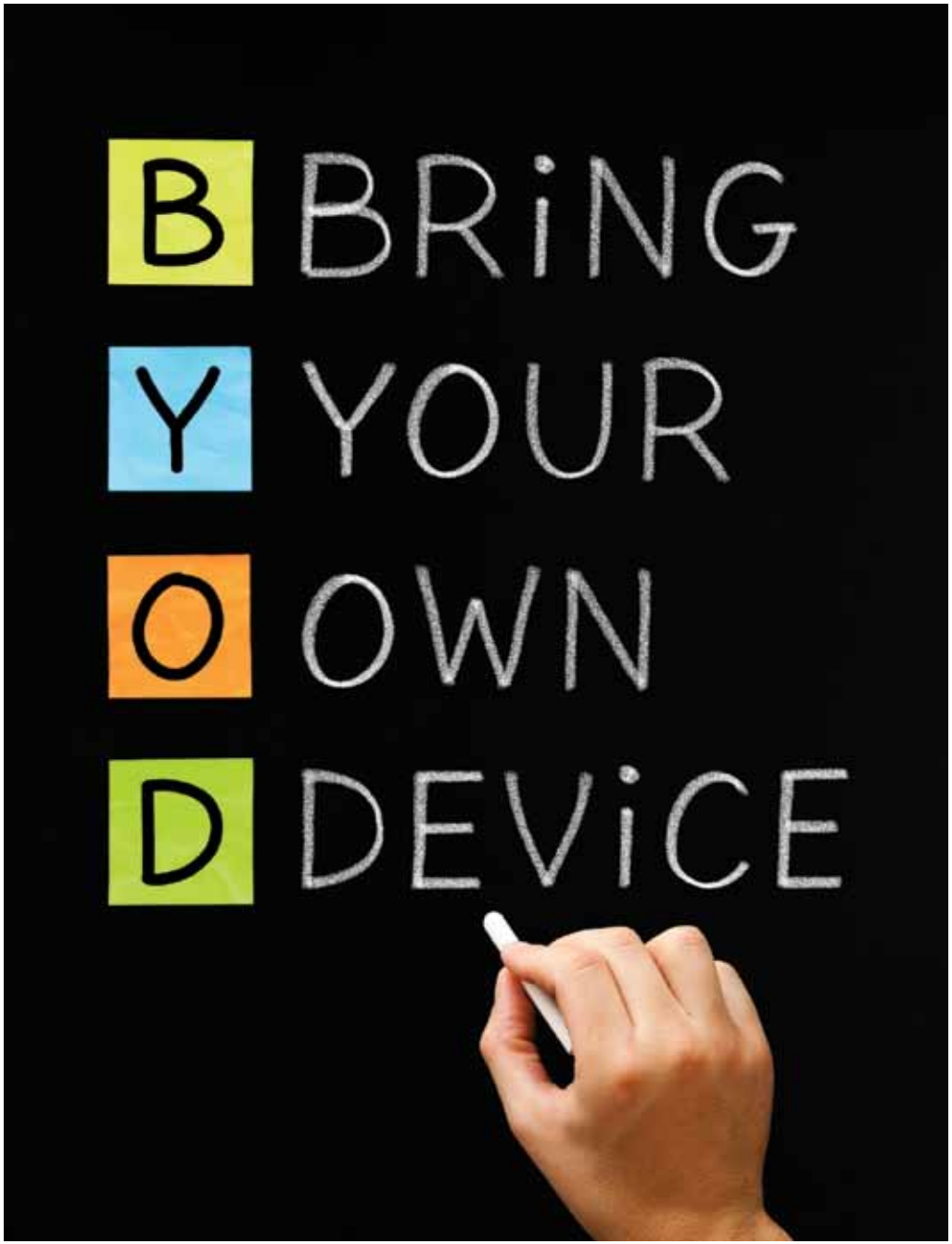
Haga clic en cada uno de los items del indice para acceder directamente a la pagina correspondiente.



INTRODUCCIÓN

A raíz del gran crecimiento que experimentaron los dispositivos móviles, se pudo observar cómo los usuarios aprovechan características como su portabilidad y las facilidades de conexión para utilizarlos como una herramienta de trabajo. Esto se debe principalmente al crecimiento y las innovaciones que brindan las redes sociales y las tecnologías de conectividad.

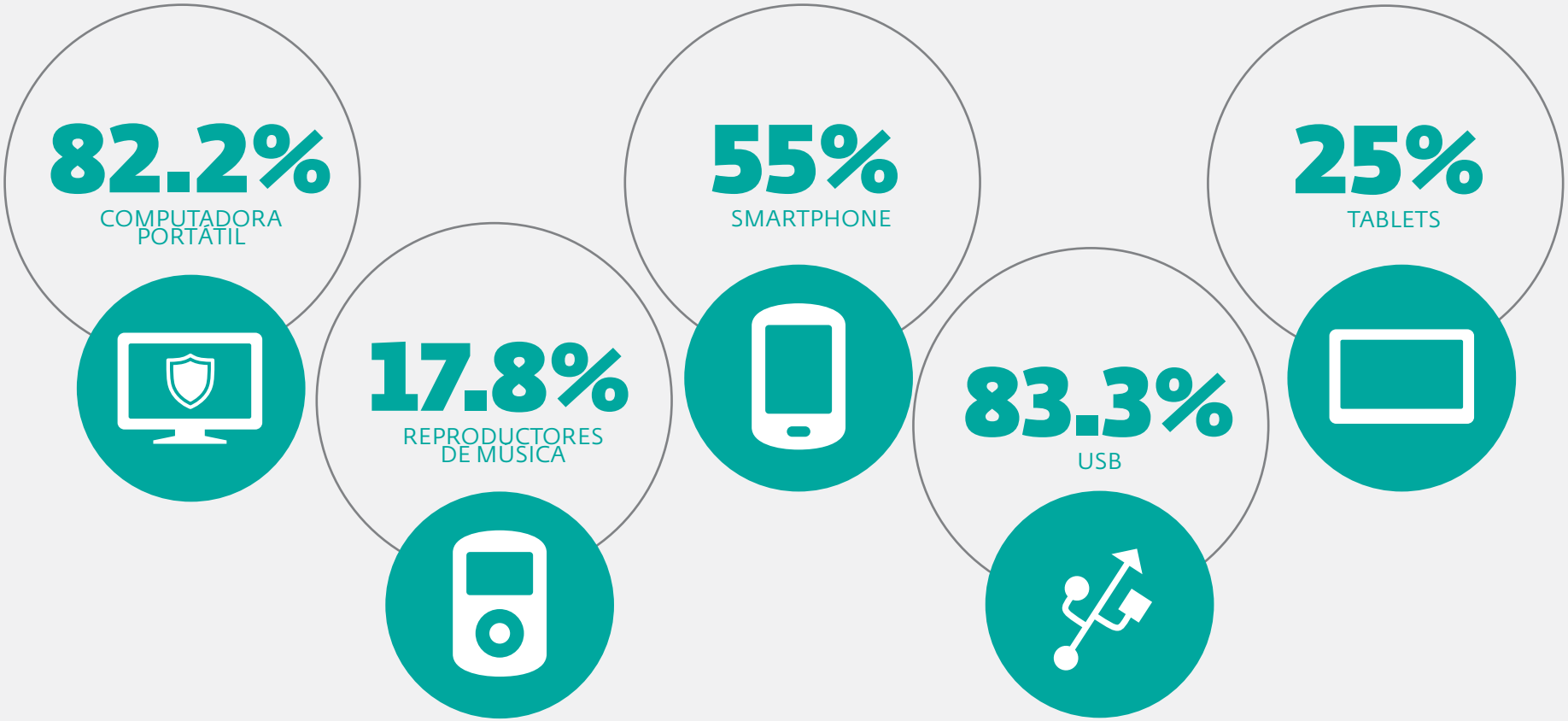
Esta nueva forma de trabajar, plantea una serie de oportunidades y riesgos para las empresas. Por lo tanto, es necesario aprovechar las ventajas y a su vez tomar todas las medidas preventivas necesarias para garantizar la protección de la información corporativa.



¿QUÉ ES BYOD?

La convergencia en el uso y aprovechamiento de todas estas características ha hecho que se consolide lo que se conoce como tendencia BYOD: Bring Your Own Device, que significa la incorporación de dispositivos tecnológicos de los empleados en el ámbito laboral para cumplir con las tareas profesionales.

DISPOSITIVOS MÁS UTILIZADOS[1]



Si bien no se suele incluir formalmente en esta tendencia a los dispositivos de almacenamiento USB, sí aparecen como los dispositivos personales predilectos para el intercambio y almacenamiento de información del trabajo.

1: Encuesta realizada por ESET Latinoamérica en agosto 2012; participaron 278 personas.

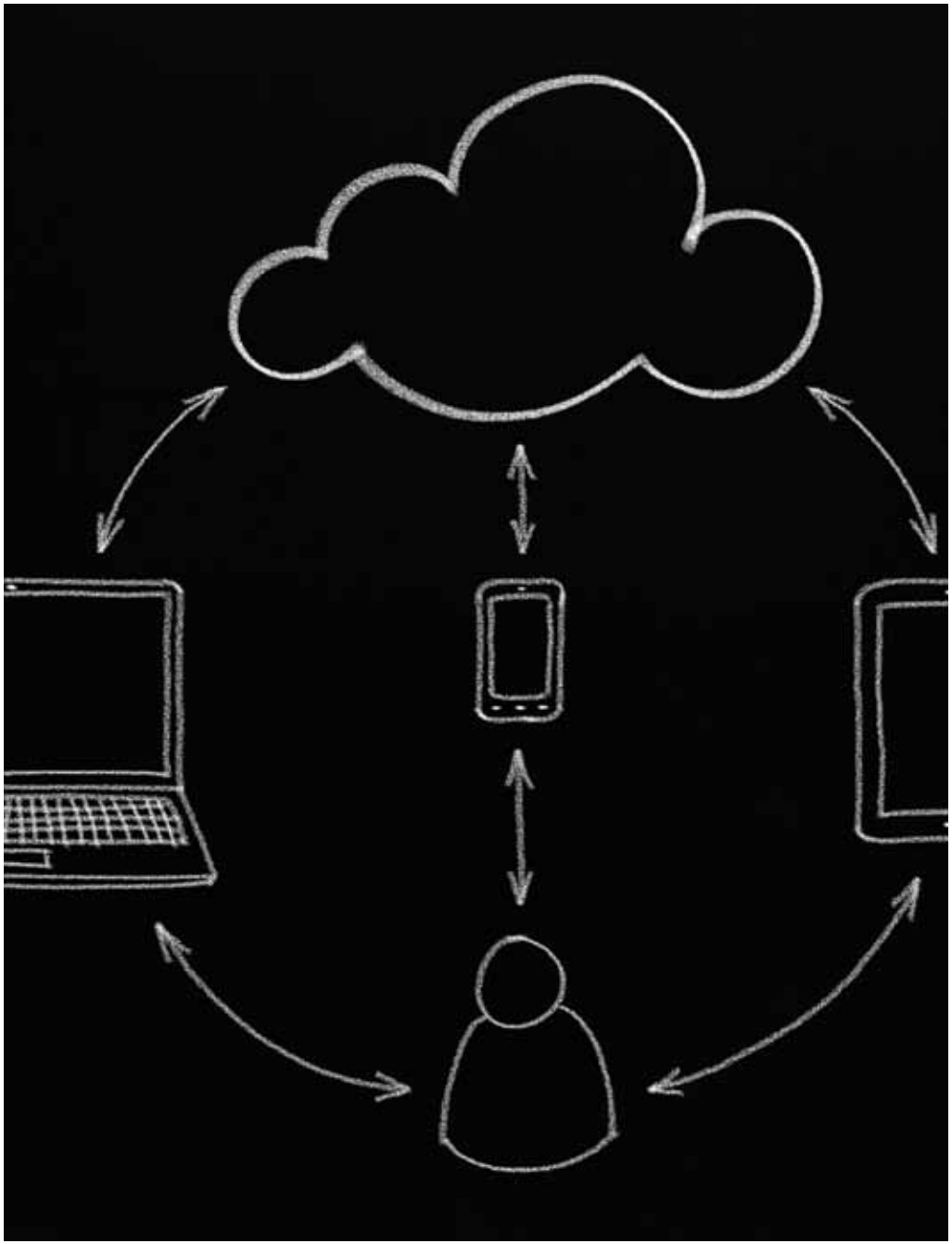
USOS DE LOS DISPOSITIVOS MÓVILES[2]

Dado que los empleados llevan sus dispositivos personales a la oficina, además de darles un uso personal, lo más usual es que los utilicen para la revisión del correo electrónico corporativo y como apoyo a las tareas del trabajo.

A esto se suma que para poder acceder a la información corporativa desde sus dispositivos personales, los empleados utilizan en su mayoría las redes WiFi que tiene la empresa. Además, el hecho de manipular este tipo de información permite que sea almacenada en los dispositivos personales, y en general no se tienen en cuenta las precauciones necesarias para eliminarla.

Finalmente, al ser un dispositivo personal no suele contar con controles como el cifrado de la información, una medida de seguridad que puede llegar a evitar que caiga en manos incorrectas si el dispositivo se extravía o es robado.

2: Encuesta realizada por ESET Latinoamérica en agosto 2012; participaron 278 personas



CAMBIOS EN LA GESTIÓN DE INFRAESTRUCTURA

A raíz de los nuevos usos para los dispositivos personales (vinculados con información corporativa), se plantean también nuevos retos para departamentos de TI en cuanto al manejo de sus recursos para garantizar la seguridad de los datos de la empresa.

Estas nuevas formas de manejar la información implican que las organizaciones deban prestar mucha más atención a la forma en que los usuarios se conectan a las redes de la empresa para manipular la información, y se preocupen cada vez menos por la infraestructura física.

No obstante, se generan nuevos riesgos que se deben gestionar adecuadamente para garantizar la seguridad de la información, con el objetivo de proveer mejores y más altos niveles de rendimiento y un control más preciso para los diferentes tipos de dispositivos que se podrían.

RETOS Y OPORTUNIDADES

Como se mencionó anteriormente, la adopción de BYOD implica un cambio en la forma de gestionar la seguridad de la información en una amplia variedad de dispositivos, aplicaciones y sistemas operativos. Este punto involucra una nueva forma de gestionar la seguridad, que puede representar incrementos en la productividad de los empleados de las compañías, con mayores cuidados en el acceso y manipulación de la información.

GESTIONAR LOS RIESGOS

Los análisis de riesgos deben partir de la clasificación de la información con el objetivo de establecer, por ejemplo, cuáles son los datos sensibles que requieren mayores niveles de protección; a qué información se puede acceder desde dispositivos personales; a cuál por fuera de la red de la empresa; y a cuál debe restringirse el acceso total.

Con estos datos se logrará establecer cuáles son las medidas de control más adecuadas para garantizar la seguridad de la información, ya sean de tipo tecnológico o a nivel de estructura y procedimientos.

Toda esta gestión de riesgos debe estar complementada con un adecuado plan de educación para que todos los empleados conozcan las implicaciones del uso de sus dispositivos personales, los riesgos a los que están expuestos y las medidas de seguridad que deben tener en cuenta.

TELETRABAJO

A raíz de la posibilidad de manejar información laboral en dispositivos personales, nacieron tendencias como el homeworking, es decir, la posibilidad de trabajar desde el hogar y a través de un equipo personal, tienen un impulso importante. Esta cuestión implica que las empresas contemplen diversos panoramas, como la manipulación de información laboral en dispositivos que pueden no están protegidos adecuadamente.

Si bien esta tendencia permite ahorrar costos operativos para las empresas y brindar un mejor ambiente a los empleados, es necesario que consideren opciones para que los usuarios tengan sus dispositivos protegidos con una solución de seguridad y con las aplicaciones actualizadas para prevenir infecciones.

MANEJO DE LA INFORMACIÓN

Si el empleado manipula información de la empresa en su dispositivo personal, debe estar claro qué pasará con ella una vez terminada la relación contractual, ya que es muy complicado tener la seguridad de que la información será eliminada.

Las acciones de control en estos casos pueden apoyarse en aspectos contractuales, como la firma de acuerdos de confidencialidad o medidas más estrictas en relación al tipo de información que se pueda descargar y almacenar en dispositivos personales.

GESTIÓN DE APLICACIONES Y DISPOSITIVOS

El reto para las organizaciones es garantizar que los dispositivos, a través de los cuales se accede a la información, cuenten con aplicaciones seguras que no pongan en peligro la integridad de la información.

Además, el área encargada de la seguridad de la de información dentro de la empresa debe tener políticas definidas que permitan especificar el uso que los empleados le pueden dar a los recursos de la empresa a través de sus dispositivos personales. De esta manera, se logra controlar y gestionar los recursos de red, pues estos se convierten en un punto de falla que podrían permitir la intrusión ilegal a los sistemas de la compañía.

ELEGIR EL CAMINO A SEGUIR

Más allá de si finalmente se adopte o no el BYOD en la organización, lo más coherente es que las organizaciones se preocupen por tomar una postura ya que este tema es una realidad tangible. Lo más peligroso y riesgoso es adoptar una posición indiferente.

Se debe definir explícitamente si se permitirá o no el uso de dispositivos personales con fines laborales.

Si se decide adoptar el BYOD, resulta necesaria una gestión adecuada de los equipos a fin de que se utilice la información de acuerdo a lo previsto en las políticas establecidas por la empresa.

En caso contrario, la empresa debe implementar los controles necesarios para que desde ningún dispositivo externo se pueda acceder a la información corporativa.

8 LINEAMIENTOS DE SEGURIDAD

ASEGURAR LAS REDES DE ACCESO

Analizar la capacidad y la cobertura que tienen las redes corporativas para permitir el acceso de dispositivos diferentes a los de la empresa, utilizando sistemas de autenticación que permitan identificar quién accede y qué tipo de información manipula.

GESTIONAR ROLES

El acceso a la información debe ser restringido de forma que se garantice que solo podrán acceder a la información aquellas personas que realmente estén habilitadas para ello.

ELEGIR DISPOSITIVOS

Teniendo en cuenta la amplia variedad de dispositivos en el mercado, es prudente hacer un análisis de para saber cuáles son los más adecuados para manejar la información de la empresa.

PROTEGER CONTRA CÓDIGOS MALICIOSOS

Para garantizar que ningún código malicioso afecte los datos, todos los dispositivos personales deberían contar con soluciones de seguridad que detecten proactivamente este tipo de amenazas.

PROTEGER LAS CONEXIONES WIFI

El acceso a través de conexiones WiFi debe ser correctamente configurado, por ejemplo con el uso de VPN, para garantizar la seguridad de la información.

MONITOREAR EL TRÁFICO BYOD

El tráfico de dispositivos BYOD debería ser claramente identificable y contar con un control estricto.

REDACTAR UNA POLÍTICA DE SEGURIDAD

A raíz de la diversidad de dispositivos y aplicaciones que se pueden manejar, es necesario redactar una política que aclare qué dispositivos pueden acceder a la información corporativa.

CONCIENTIZAR A LOS EMPLEADOS

La educación debe ser un pilar importante para que todos los usuarios sean conscientes de los riesgos a los cuales pueden verse expuestos y cuáles son los cuidados que deben tener al ingresar dispositivos ajenos a la compañía.

CONCLUSIÓN

Como hemos visto, cuando se habla de BYOD se hace referencia a una tendencia consolidada y ante la cual las empresas deben hacer un análisis de riesgos para tomar una posición al respecto. La adopción de esta tendencia puede traer grandes beneficios relacionados con la disminución de gastos en infraestructura, la comodidad de los empleados para el manejo de la información y por tanto el incremento de la productividad. No obstante, la empresa enfrenta nuevas amenazas que deben ser gestionadas, las principales y quizás las más preocupantes, son la fuga y el acceso no autorizado a la información.

Para enfrentar estos retos, las empresas deberían realizar una combinación entre políticas claras para el manejo de la información y el uso de herramientas adecuadas que permitan la gestión de la seguridad de la misma, sin dejar de lado la educación de los empleados para que conozcan los riesgos y sepan cómo enfrentarlos.

SI DESEAN CONOCER MÁS EN PROFUNDIDAD SOBRE ESTA TEMÁTICA, LOS INVITAMOS A QUE LEAN EL WHITEPAPER "SEGURIDAD EN BYOD" ESCRITA POR LOS ESPECIALISTAS EN SEGURIDAD DE ESET LATINOAMÉRICA