LOS DIEZ MANDAMIENTOS DE LOS DISPOSITIVOS PERSONALES BYOD

MaaS360
by Fiberlink

MaaS360® by Fiberlink, an IBM company

Permitirá el registro de dispositivos personales

A muchos directores de departamentos de informática les da la impresión de que la rápida proliferación de los dispositivos móviles que entran en el lugar de trabajo es obra divina. Es como si una voz que surgiera de los cielos pidiera que todos los empleados a los que presta soporte trajeran la mayor cantidad posible de dispositivos y que los conectaran a los servicios corporativos en masa. En cuanto nació la idea de traer al trabajo los dispositivos personales propios (BYOD), los empleados la siguieron con fervor.

No tiene sentido fingir que no ocurre, ni decir que no permite a sus empleados hacerlo. La verdad es que ya lo están haciendo y seguirán introduciendo dispositivos incompatibles en la red con y sin su permiso. Un estudio de Forrester realizado con trabajadores del conocimiento de EE. UU. reveló que el 37 % utiliza la tecnología antes de que se establezcan permisos formales o políticas.[1] Es más, una encuesta de Gartner CIO determinó que el 80 % de los empleados tendría autorización para usar sus propios equipos con los datos de empleados de la empresa en 2016.[2]

Este hecho plantea una pregunta inevitable: ¿cómo dará respuesta al deseo de la plantilla de trabajadores de usar aplicaciones y dispositivos personales al tiempo que consigue que sigan siendo productivos en un entorno seguro, donde se protegen los datos corporativos? Los diez mandamientos de los dispositivos personales (BYOD) indican cómo crear un entorno móvil tranquilo, seguro y productivo.

Los diez mandamientos de los dispositivos personales (BYOD)

1. Creará la política antes de facilitar la tecnología
2. Buscará los dispositivos del personal
3. Simplificará el registro
4. Configurará los dispositivos de forma inalámbrica
5. Dará autoservicio a los usuarios
6. Considerará sagrada la información personal
7. Separará las aguas entre los datos corporativos y los personales
8. Vigilará a la plantilla de forma automática
9. Gestionará y controlará el uso de los datos
10. Beberá de la fuente del rendimiento de las inversiones

[1] Benjamin Gray y Christian Kane, "Fifteen Mobile Policy Best Practices", investigación de Forrester, enero de 2011.

[2] Ken Dulaney y Paul DeBeasi, "Managing Employee-Owned Technology in the Enterprise", Gartner Group, octubre de 2011.

MaaS360® by Fiberlink, an IBM company

1. Creará la política antes de facilitar la tecnología

Como en cualquier otro proyecto informático, la política debe preceder a la tecnología; incluso en la nube. A fin de aprovechar eficazmente la tecnología de administración de dispositivos móviles (MDM) para los dispositivos de los empleados, tendrá que seguir tomando decisiones sobre las políticas. Estas políticas afectan a más ámbitos que el informático; tienen implicaciones para los equipos de recursos humanos, jurídicos y de seguridad, es decir, cualquier sección de la empresa que use dispositivos móviles en nombre de la productividad.

Dado que todas las líneas de negocio se ven afectadas por la política de uso de dispositivos personales BYOD, no se puede diseñar esta misma en un vacío informático. Puesto que los usuarios tienen diferentes necesidades, los responsables del departamento de informática deben garantizar que todas ellas forman parte de la creación de la política.

No hay una única política de dispositivos personales correcta, pero sí hay algunas cuestiones que debe sopesar:

- **Dispositivos**: ¿Qué dispositivos móviles se admitirán? ¿Solo determinados dispositivos o todos los que el empleado quiera?

Según Forrester, el 70 % de los teléfonos inteligentes pertenecen a los usuarios, el 12 % se elige de una lista de dispositivos autorizados y el 16 % los facilita la empresa. Alrededor del 65 % de las tabletas pertenecen a los usuarios, el 15 % se elige de una lista y el 16 % las facilita la empresa. Es decir, en la mayoría de los casos, los usuarios traen sus propios dispositivos.

- **Planes de datos:** ¿La organización se encargará de pagar el plan de datos? ¿Destinará un extra o serán los empleados quienes envíen los informes de gastos?

¿Quién paga estos dispositivos? En el caso de los teléfonos inteligentes, el 70 % paga la factura completa, el 12 % obtiene un descuento, el 3 % paga parte de la factura y, en el 15 % de los casos, la empresa asume el pago de la totalidad de la factura. Para las tabletas, el 58 % llevaba la suya propia, el 17 % obtenía un descuento de la empresa, el 7 % compartía los costes y, al 18 %, sus empresas les daban las tabletas y les pagaban las facturas. (Fuente: Forrester, 2011)

- **Conformidad:** ¿Qué normativa regula los datos que su organización tiene que proteger? Por ejemplo, la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) requiere la aplicación de un cifrado nativo en todos los dispositivos que contengan datos que se acojan a dicha ley.
- **Seguridad:** ¿Qué medidas de seguridad se necesitan (protección por código de acceso, dispositivos liberados o rooteados, aplicaciones contra malware, cifrado, restricciones para los dispositivos, copia de seguridad de iCloud, etc.)?
- **Aplicaciones:** ¿Qué aplicaciones están prohibidas? ¿Escaneo de IP, uso compartido de datos, Dropbox?
- **Acuerdos:** ¿Hay acuerdos de uso aceptable (AUA) para aquellos dispositivos de los empleados que contengan datos corporativos?
- **Servicios:** ¿A qué tipos de recursos pueden acceder los empleados? ¿El correo electrónico? ¿Determinadas redes inalámbricas o VPN? ¿CRM quizás?
- **Privacidad:** ¿Qué datos se recogen de los dispositivos de los empleados? ¿Qué datos personales no se recopilan nunca?

Ninguna pregunta está fuera de lugar si hablamos de que los empleados se traigan al trabajo sus dispositivos personales (BYOD). Debe producirse un diálogo franco y sincero sobre cómo se utilizarán los dispositivos y de qué forma puede satisfacer el departamento de informática las necesidades de forma realista.

MaaS360® by Fiberlink, an IBM company

2. Buscará los dispositivos del personal

Imagínese: Empieza a emplear una solución MDM, suponiendo que su empresa admita 100 dispositivos aproximadamente. Conserva una lista meticulosa de los tipos de dispositivos y los usuarios, por lo que no debería haber sorpresas. Sin embargo, cuando va a comprobar por primera vez el informe aparecen más de 200 dispositivos. Esta situación es real, no ficticia. Sucede con más frecuencia de lo que imagina.

No sirve de nada negar la realidad. No vale eso de "ojos que no ven, corazón que no siente". Entienda la situación real de su población de dispositivos móviles antes de grabar su estrategia en las tablas de la ley. Para ello, necesitará una herramienta que pueda comunicarse en tiempo real con el entorno de correo electrónico y detectar todos los dispositivos conectados a la red de la empresa. Recuerde que tras activar ActiveSync en una bandeja de correo electrónico, normalmente no hay límite para sincronizar varios dispositivos sin que el equipo informático lo sepa.

Todos los dispositivos móviles tienen que incorporarse a la iniciativa móvil y sus propietarios tienen que recibir la notificación de que se están estableciendo nuevas políticas de seguridad.

3. Simplificará el registro

Nada hay que engendre casos de incumplimiento más rápidamente que la complejidad. Una vez identificados los dispositivos que hay que registrar, su programa de dispositivos personales debe aprovechar la tecnología que permite que los usuarios se registren de forma sencilla. El proceso debe ser sencillo y seguro y, además, debe configurar el dispositivo al mismo tiempo.

En una situación ideal, los usuarios podrán hacer clic en un enlace de correo electrónico o un texto que les lleve a un perfil de MDM creado en su dispositivo, incluida la aceptación del siempre importante AUA.

> Considere el estándar BYOD y que los empleados aporten sus propios dispositivos personales como un matrimonio; así verá el AUA como una especie de acuerdo prematrimonial, que garantiza la armonía de la unión.

Las instrucciones deben ayudar a los usuarios existentes a registrarse en el programa de dispositivos personales. Recomendamos que los usuarios existentes borren sus propias cuentas de ActiveSync, para que pueda aislar y administrar los datos corporativos en el dispositivo. Los nuevos dispositivos deben iniciarse con un perfil nuevo.

Desde el punto de vista de la informática, sería conveniente contar con la capacidad de registrar los dispositivos existentes en grupo o de que los usuarios registren sus propios dispositivos. También tiene que autenticar a los empleados con un proceso de autenticación básico, como un código de acceso que solo se introduce una vez o el uso de los directorios corporativos existentes, como Active Directory/LDAP. Todos los nuevos dispositivos que intenten acceder a los recursos corporativos deben ponerse en cuarentena y se debe informar de ello al departamento de informática. Así, los responsables de la informática tendrán flexibilidad para bloquear o iniciar un flujo de registros adecuado si se aprueban, garantizando de este modo el cumplimiento de las políticas de la empresa.

MaaS360® by Fiberlink, an IBM company

4. Configurará los dispositivos de forma inalámbrica

Si hay algo que su política de dispositivos personales BYOD aportados por los empleados y su solución MDM tienen que evitar, es atraer a más usuarios al servicio de asistencia. Todos los dispositivos deben configurarse de forma inalámbrica, a fin de maximizar la eficacia, tanto del departamento de informática como de los usuarios corporativos.

Después de que los usuarios acepten el AUA, su plataforma debe ofrecer todos los perfiles, las credenciales y las configuraciones a los que el empleado tiene que acceder, incluidos los siguientes elementos:

- Correo electrónico, contactos y calendario
- VPN
- Contenido y documentos corporativos
- Aplicaciones internas y públicas

Llegados a este punto, también creará políticas para restringir el acceso a determinadas aplicaciones y generará advertencias cuando un usuario exceda su consumo de datos o el límite de gasto mensual.

5. Dará autoservicio a los usuarios

Y se congratulará por ello. Los usuarios quieren un dispositivo que funcione y usted, optimizar el tiempo del servicio de asistencia. Una plataforma de autoservicio sólida permite que los usuarios se encarguen directamente de cosas como:

- Restablecer las contraseñas y los códigos PIN en caso de que el empleado los olvide
- Efectuar la localización geográfica de un dispositivo perdido desde un portal web, usando la integración de mapas
- Borrar el contenido de un dispositivo de forma remota, eliminando toda la información corporativa sensible

Garantizar la seguridad, la protección de los datos corporativos y el cumplimiento son responsabilidades compartidas. Puede resultar duro para los empleados, pero no se pueden mitigar los riesgos sin su colaboración. Un portal de autoservicio puede ayudar a que los empleados comprendan por qué podrían estar incumpliendo la normativa.

MaaS360® by Fiberlink, an IBM company

6. Considerará sagrada la información personal

Desde luego, la política de dispositivos personales aportados por los propios empleados (BYOD) no puede ceñirse solamente a proteger los datos corporativos. Un buen programa de dispositivos personales considera sagrados los datos de los empleados y como tales los protege. La información identificable personalmente (PII) se puede usar para identificar, localizar o ponerse en contacto con una persona. Algunas normativas sobre privacidad impiden que las empresas puedan siquiera ver estos datos. Dé a conocer la política de privacidad a los empleados y deje claro qué datos no puede recopilar usted de sus dispositivos móviles. Por ejemplo, una solución MDM debe ser capaz de analizar a qué información puede acceder y a cuál no; a saber:

- Correo electrónico, contactos y calendario personales
- Datos de aplicaciones y mensajes de texto
- Historial de llamadas y mensajes de voz

Por otro lado, permita que los usuarios sepan qué información recoge, cómo se va a utilizar y por qué les beneficia.

Una solución MDM avanzada puede convertir una política de privacidad en una configuración de privacidad para ocultar la información de la ubicación y el software de un dispositivo. Esto ayuda a las empresas a cumplir las normativas sobre PII y ofrece mayor comodidad a los empleados, impidiendo la visualización de información personal en teléfonos inteligentes y tabletas. Por ejemplo:

- Desactivar el informe de inventario de aplicaciones para restringir la visualización de las aplicaciones personales por parte de los administradores
- Desactivar los servicios de localización para impedir el acceso a los indicadores de ubicación como domicilios postales, coordenadas geográficas, direcciones IP y SSID de Wi-Fi

Transparencia y claridad son lemas importantes. Cuando todo el mundo conoce las reglas, la resistencia a las políticas sobre dispositivos personales es mucho menor.

7. Separará las aguas entre los datos corporativos y los personales

Para que la práctica de que los empleados traigan sus dispositivos personales (BYOD) se convierta en un acuerdo con el que el equipo del departamento de informática y los usuarios finales puedan convivir, la información personal, como las fotografías de las fiestas de cumpleaños o esa maravillosa novela que está escribiendo aquel empleado, deben quedar aislados de las aplicaciones de productividad.

En pocas palabras, el departamento de TI debe proteger las aplicaciones corporativas, los documentos y demás material si el empleado decide abandonar la organización, pero sin tocar el correo electrónico, las aplicaciones y las fotografías personales.

No solo lo usuarios valoran la libertad que da este enfoque, también lo hace el personal del departamento de informática, cuya labor será infinitamente más sencilla. Gracias a este enfoque, cuando un empleado deje de trabajar en la empresa, podrán borrar de forma selectiva los datos corporativos. Dependiendo de las circunstancias, si un empleado pierde el dispositivo, se puede borrar todo su contenido. Sin embargo, solo una verdadera solución MDM puede darle la opción.

Alrededor del 86 % de los borrados del contenido de los dispositivos es de tipo selectivo, es decir, solo se borran los datos corporativos.

MaaS360® by Fiberlink, an IBM company

8. Vigilará a la plantilla de forma automática

Una vez que se ha registrado el dispositivo, todo gira en torno al contexto. Los dispositivos deben vigilarse continuamente en ciertas situaciones y debe haber políticas automatizadas en vigor. ¿El usuario trata de desactivar las funciones de administración? ¿El dispositivo cumple con la política de seguridad? ¿Tiene que hacer modificaciones en función de los datos que ve? Desde este punto, puede empezar a comprender las políticas o las reglas adicionales que hay que crear. He aquí algunos problemas comunes:

- **Obtener la "raíz"o root de la liberación:** A veces, los empleados "liberan" o "rootean" un teléfono para conseguir aplicaciones de pago de forma gratuita, lo que abre la puerta al malware, que puede robar información. Si se libera el dispositivo, la solución MDM debe ser capaz de tomar medidas como el borrado selectivo de los datos corporativos inmediatamente.
- **Evite el borrado; envíe un SMS:** Si las aplicaciones que invitan a perder el tiempo, como Angry Birds, entran en conflicto con las políticas de la empresa, pero no las infringen, un borrado inmediato resulta excesivo. Una solución MDM puede aplicar políticas en función de la infracción. MDM puede enviar un mensaje al usuario, dándole tiempo para que elimine la aplicación antes de que el equipo del departamento de informática pulse el botón de borrar.
- **Nuevo sistema operativo disponible:** Para que el sistema BYOD siga siendo eficaz y los empleados empleen sin problemas sus dispositivos personales en el lugar de trabajo, los usuarios tienen que disponer de una forma sencilla de aviso cuando haya un nuevo SO listo para su instalación. Con la solución MDM adecuada, las actualizaciones de SO se convierten en una función de autoservicio. Restringir las versiones de SO obsoletas garantiza el cumplimiento y maximiza la operatividad del dispositivo.

9. Gestionará y controlará el uso de los datos

Una política de dispositivos personales deja al equipo del departamento de informática en gran medida fuera del tema de las comunicaciones. Sin embargo, la mayoría de las empresas sigue teniendo que ayudar a sus empleados a gestionar el consumo de datos, para evitar que incurran en gastos excesivos.

Si es usted quien paga por el plan de datos, quizás quiera disponer de una forma de realizar el seguimiento del consumo. Si no, quizás le interese ayudar a los usuarios a que realicen el seguimiento de su propio consumo de datos. Debería ser capaz de supervisar el consumo de datos en la red y en itinerancia por parte de los dispositivos y generar alertas si un usuario rebasa el límite del consumo de datos.

Puede configurar los límites de megabits en itinerancia y en la red, así como personalizar la fecha de facturación a fin de crear notificaciones en función del porcentaje utilizado. Además, recomendamos informar a los usuarios de las ventajas de usar la conexión Wi-Fi siempre que esté disponible. La configuración de Wi-Fi automática ayuda a garantizar que los dispositivos se conecten automáticamente a la red Wi-Fi cuando se encuentran en las instalaciones de la empresa.

Si el pago solo cubre 50 dólares o 200 MB de datos al mes, los empleados sabrán valorar que una advertencia les indique que están a punto de rebasar el límite e incurrir en cargos adicionales.

MaaS360® by Fiberlink, an IBM company

10. Beberá de la fuente del rendimiento de las inversiones

Aunque la práctica de que los empleados aporten sus propios dispositivos personales (BYOD) deja la responsabilidad de comprar los dispositivos en manos de los usuarios, vale la pena tener en cuenta la perspectiva general y los costes a largo plazo para su organización.

Mientras redacte la política, tenga en cuenta de qué forma afectará dicha política al rendimiento de las inversiones. Ello incluye la comparación de los enfoques, como se indica en la tabla siguiente:

Modelo de propiedad de la empresa	**Uso de dispositivos personales (BYOD)**
Coste de adquirir cada dispositivo	Coste de un plan de datos parcialmente subvencionado
Coste de un plan de datos completamente subvencionado	Ausencia de costes por la compra de dispositivos
Coste del reciclaje de los dispositivos cada pocos años	Coste de una plataforma de administración móvil
Planes de garantía	
Tiempo y trabajo del departamento de informática para administrar el programa	

Las tallas únicas nunca se adaptan a todos, pero una política de dispositivos personales BYOD bien diseñada e implantada le permite tomar el rumbo necesario para administrar los dispositivos móviles de forma efectiva y eficaz.

Desde luego, el aumento de la productividad se nota a menudo cuando los empleados tienen movilidad y están permanentemente conectados. Que usen sus propios dispositivos personales para trabajar es una forma maravillosa de llevar este avance en la productividad a nuevos usuarios, quienes antes tal vez no tuviesen la oportunidad de contar con dispositivos corporativos.

Los empleados utilizan sus dispositivos personales para trabajar: la seguridad de la libertad

El estándar BYOD es una práctica recomendada en auge, que dota a los empleados de la libertad de trabajar en sus propios dispositivos y, además, libera al equipo del departamento de informática de significativas cargas económicas y administrativas. Sin embargo, los dispositivos personales no cumplirán las promesas de administración agilizada y ahorro de costes si no cuentan con una política bien redactada y una sólida plataforma de administración.

Si ha decidido que a su empresa le interesa que los empleados aporten y usen sus dispositivos personales, haga clic aquí para probar la versión gratuita de MaaS360 durante 30 días. Como MaaS360 es una solución basada en la nube, su entorno de prueba se hará inmediatamente productivo sin pérdida de datos.

Si se encuentra en las primera fases de la estrategia móvil, MaaS360 ofrece cantidad de recursos educativos, entre ellos los siguientes:

www.maas360.com
http://www.maas360.com/products/mobile-device-management/
MaaSters Center

Para obtener más información

Si desea obtener más información sobre nuestra tecnología y nuestros servicios, visite www.maaS360.com.

1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Teléfono 215.664.1600 | Fax 215.664.1601 | sales@fiberlink.com