Hay que tener aplicaciones MDM para gestionar y securizar el nuevo modelo de trabajo

La gestión con sistemas MDM y los entornos BYOD serán muy populares en los próximos años

En el encuentro que Computing ha organizado en colaboración con Orange para tratar el fenómeno del BYOD (Bring Your Own Device) y los retos que está planteando en las organizaciones de todos los sectores de actividad, ha quedado de manifiesto que para securizar y gestionar el nuevo entorno de trabajo generado por la movilidad es preciso utilizar una capa de soluciones de gestión de dispositivos móviles (MDM). Una tecnología que cada vez va teniendo más adeptos en las empresas.

El fenómeno Bring Your Own Device (BYOD), que está dando paso a nuevas tecnologías como las soluciones MDM (Mobile Devices Management, por sus siglas en inglés), es uno de los temas que han ocupado en los últimos meses la primera línea de actualidad para las organizaciones en el ámbito de las TI, por las oportunidades de ahorro, flexibilidad de despliegue y mejoras de productividad que plantean. En un entorno cada vez más complejo donde conviven múltiples dispositivos smartphone & tablet, diferentes sistemas operativos, terminales de empresa y del propio empleado, cada vez más potentes y útiles para desempeñar el trabajo en cualquier lugar, muchas organizaciones se están planteando el reto de cómo manejar con seguridad ese entorno, donde los empleados muchas veces llevan sus propios dispositivos personales al ámbito empresarial.

Para intercambiar ideas y enriquecer la visión sobre esta tendencia, Computing ha organizado, en colaboración con Orange, una Tertulia en la que se ha puesto de manifiesto cómo las soluciones MDM están ayudando a garantizar la seguridad de los sistemas de información corporativos. Dando inicio a la charla, así lo confirmaba Gabriel Cerrada, director de Grandes Empresas en Orange, quien aseguraba que, "desde el punto de vista de los clientes, hay una demanda cada vez mayor de este tipo de soluciones por la heterogeneidad de los dispositivos, y porque hoy en día el usuario manda. En el mundo del PC mantener una disciplina homogénea es muy fácil, pero no así en el entorno de las tablet y smartphones donde la gestión es más complicada. Por dicho motivo, desde Orange ofrecemos una propuesta de valor de comunicaciones fijas y móviles que incluye una capa de servicios para ayudar a los clientes a gestionar los dispositivos móviles de los empleados. Hay estudios que aseguran que en menos de dos años, habrá más de tres dispositivos móviles por usuario, lo que implica un reto de gestión enorme. En este sentido, no es algo que vaya a venir, sino que ya está aquí. Es más, ya hay clientes que usan nuestras soluciones MDM, y no en modo piloto, sino de utilización real. Lo cierto es que hay ventajas de ahorro para las compañías, pero son más importantes los beneficios en flexibilidad y productividad.

Nuestro papel como operadora es facilitar este servicio de gestión, asegurando que el terminal del empleado cumple con los parámetros definidos por la organización; aunque aquí el tema legal es clave porque dependerá de hasta dónde permitirá el usuario que se introduzca la empresa en su dispositivo".

Precisamente los aspectos de seguridad son uno de los mayores quebraderos de cabeza para los CIO, que tienen que garantizar el control y el acceso a las redes y aplicaciones corporativas de la organización. Aunque hay determinados sectores más concienciados con este tema, -principalmente los que tratan con datos confidenciales-, no todos los empleados cumplen con las políticas de seguridad cuando se trata de sus propios dispositivos personales. Emilio López Álvarez, director de Red Corporativa de Indra, señalaba que esto se debe a un problema cultural. "Es una gran idea dar la oportunidad al usuario de elegir el dispositivo para trabajar, pero tiene que cumplir las reglas del juego. En España tenemos una cultura que va en contra de eso. Muchos de nosotros nos traemos nuestro terminal al trabajo pero no acatamos las normas de protección, y eso nos obliga a las compañías a gastar mucho dinero en seguridad. BYOD es un concepto nuevo por lo que hay pocas soluciones en el mercado y además son caras. Hay que esperar a que se popularicen, como las soluciones MDM, por ejemplo. No obstante, en Indra estamos notando que los profesionales que se incorporan ahora al mercado de trabajo están más concienciados de la seguridad que los perfiles más altos de las compañías. Tenemos que asumir que el futuro pasa porque la gente traiga sus dispositivos", advertía.

Para organismos como la Fabrica Nacional de Moneda y Timbre (FNMT), la seguridad es crucial pues se dedica a temas de certificación, entre otras cosas. Además, como vaticina Diego Hernández, director de Ceres, "el mundo de la movilidad está funcionando porque hay muchas aplicaciones móviles, y en un futuro muy corto, será un boom y podremos transaccionar con cualquier cosa. Pero será clave la certificación, y en unos meses tendremos en los navegadores y en multitud de diferentes dispositivos este tipo de soluciones de certificación". Por otro lado, convenía con el directivo de Indra en que el tema del BYOD es una cuestión cultural. "A las personas mayores no les gusta utilizar sus propios dispositivos personales, sino trabajar con los entregados por la empresa. En cambio, esto no sucede con los más jóvenes", apuntaba.

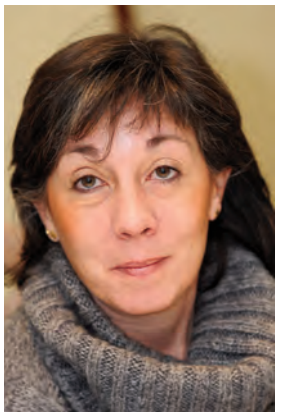
Medtronic Ibérica es otra de las firmas que por su actividad maneja datos de carácter personal al operar en el sector sanitario. Por dicho motivo, emplea tecnología MDM, que se aplica a los tablets y smartphones, y soluciones eWatch, que monitorizan los requisitos de los terminales antes de permitir su conexión a las redes corporativas. "En Estados Unidos dejan libertad para que el empleado se compre el terminal que quiera, pero también imponen pautas como el sistema operativo que debe llevar. Yo creo que a España llegará también esta tendencia. Es cierto que se está dejando libertad pero con ciertos límites. Aquí tenemos una cultura más personalizada donde la gestión es parte de la empresa. Aunque, en realidad, el BYOD es una simplificación para nuestro trabajo como responsables del área de TI", explicaba Felix Ríos, IT Manager de Medtronic.

No todos los empleados cumplen con las políticas de seguridad cuando se trata de sus dispositivos personales

"Efectivamente, los CIO ya no gestionan tecnologías, sino que ahora somos proveedores de servicios. En Hedonai, todo es web y se puede entrar desde cualquier dispositivo, algo que a mí me simplifica el trabajo, aunque obliga a llevar la seguridad a otro punto como las certificaciones, soluciones UTM… en servidores, aplicaciones y redes", coincidía Óscar Serrano, CIO de Hedonai. "Hemos intentado no depender de ninguna plataforma móvil, por eso nosotros no entregamos al usuario el terminal, pero sí la capacidad de elegirlo. En ese sentido, damos bastante libertad a nuestros empleados, es un problema de hardware menos, y no entramos en la guerra de desarrollar aplicaciones para diferentes dispositivos", continuó.

"Queremos que la seguridad siga estando en el CPD, y tener control y flexibilidad securizando la conectividad del terminal con la nube"

José María Gallo, IT Manager de AC Hoteles.



"Hay que buscar el equilibrio de lo que más valor aporta a mi negocio, más allá de elegir la plataforma porque mañana serán otras"

Isabel Tarodo, directora general de Álava Ingenieros Telecom.

"Debemos desarrollar aplicaciones para los distintos sistemas operativos, aunque hay mayor tendencia hacia Android y Apple"

Álvaro Valeros, IT Manager de Codeactivos.

"La movilidad está funcionando porque hay muchas aplicaciones móviles, y a corto plazo, podremos transaccionar con cualquier cosa"

Diego Hernández, director de Ceres (FNMT).

"Con el BYOD, tenemos un problema de hardware menos, y no entramos en la guerra de desarrollar aplicaciones para diferentes dispositivos"

Óscar Serrano, CIO de Hedonai.

"Muchos empleados se traen el terminal al trabajo, pero no acatan las normas de protección, y eso obliga a invertir en seguridad"

Emilio López, director de Red Corporativa de Indra.

"No nos importa que un empleado use su propio dispositivo porque para nosotros es crucial la flexibilidad"

Raúl Medrano, IT Manager de Inspectorate Española.

"El Bring Your Own Device es una simplificación para nuestro trabajo como responsables del área de TI"

Félix Ríos, IT Manager de Medtronic Ibérica.

Securizar el BYOD

Una de las problemáticas que plantea la gestión del BYOD es el soporte de los terminales personales de los empleados, pues muchos operadores no se responsabilizan de este servicio. Pero, como apuntó Juan Guirado, gerente de Marketing de Empresas de Orange, "con las soluciones MDM ya nos metemos en la gestión diaria del administrador de sistemas, un hecho que agradecen muchísimo porque antes, para gestionar el entorno móvil, tenían herramientas más limitadas. Además, nosotros sí gestionamos la parte física del dispositivo, mientras que la parte de software se gestiona con MDM, que en los próximos años evolucionará bastante".

Wolters Kluwer, por ejemplo, es una organización que

"La cuestión legal es clave porque dependerá de hasta dónde permita el usuario que se introduzca la empresa en su propio terminal"

Gabriel Cerrada, director de Grandes Empresas de Orange.

"Con las soluciones MDM nos metemos en la gestión diaria del administrador de sistemas, un hecho que agradecen muchísimo"

Juan Guirado, gerente de Marketing de Empresas de Orange.

"Ya no se trata de preguntarse qué vamos a hacer con el BYOD, sino qué hacer con este fenómeno que ya tenemos dentro de casa"

Luis Pezzi, director de Operaciones Infraestructuras Globales de Wolters Kluwer.

ya está haciendo uso de este tipo de soluciones. Luis Pezzi, director de Operaciones de Infraestructuras Globales de la firma, planteaba que "ya no se trata de preguntarse qué vas a hacer con el tema BYOD, sino qué vas a hacer con este fenómeno que ya tienes dentro de casa. Nosotros estamos proyectando un piloto para MDM que facilite la convergencia de los dispositivos del usuario con este tipo de soluciones de gestión, pero estamos dando los primeros pasos. Somos una subsidiara de una multinacional norteamericana, y en EE.UU. los requerimientos de seguridad para las aplicaciones de Wolters son my altas, por tanto el BYOD nos plantea un problema muy serio".

Medtronic Ibérica e Indra también están empleando soluciones MDM para cubrir los aspectos de seguridad de la integración de los dispositivos móviles en las redes corporativas. Sin embargo, hace falta una capa de seguridad más, tal y como subrayaron los asistentes a la Tertulia.

Codeativos, por ejemplo, recurre a la virtualización de los puestos de trabajo con tecnología de VMware. Álvaro Valeros, IT Manager de esta compañía, declaraba que "con toda esta revolución de smartphones y tablets hemos probado un MDM, y nos va muy bien. Es cierto que hay que desarrollar aplicaciones para los distintos sistemas operativos aunque hay mayor tendencia hacia Android y Apple. Como no podemos trabajar con todos en todo, hemos recurrido al escritorio remoto con VMware. Una vez abierto el escritorio, se aplica toda la seguridad al dispositivo, así limitamos todo al cerebro de VMware, y no tenemos que migrar todas las aplicaciones a la web".

Igualmente hace AC Hoteles, pero apoyándose en tecnología de Citrix. José María Gallo, IT Manager de la cadena hotelera, especificaba que "desde 2007 tenemos todo bajo la modalidad SaaS, y eso nos ha evitado tener problemas de dispositivos. Nosotros sí proveemos los terminales porque así lo demandan nuestros empleados, y quienes tienen mayor movilidad son la fuerza comercial y la de dirección. En nuestro caso, queremos que la seguridad siga estando en el CPD, y tener control y flexibilidad securizando la conectividad del dispositivo con la nube privada. De esta manera, los aplicativos son los mismos para todo tipo de terminal, y no tenemos que hacer ningún desarrollo personal para un determinado dispositivo".

BYOD ayuda a disminuir costes en terminales de las empresas, recursos que podrán dedicar a servicios de más valor

En Inspectorate Española también conceden libertad de uso de dispositivos a sus empleados, básicamente por el tipo de actividad que desempeña la firma. "Nosotros hacemos inspecciones en cargas de barco mayoritariamente, y siempre hemos estado muy enfocados a la flexibilidad en la utilización de cualquier dispositivo y hardware, pues estas inspecciones se hacen en cualquier momento y lugar. Debido a esta circunstancia nuestras aplicaciones son también web y están en la nube. Nuestros empleados van con su portátil y terminales móviles, y si tienen algún problema cogen otro terminal para que no se rompa la cadena de funcionamiento. Para el soporte y mantenimiento, tenemos un acuerdo con la operadora con la que trabajamos, y no nos importa que un empleado use su propio dispositivo porque para nosotros es crucial la flexibilidad. Y en seguridad, nunca ha habido un problema porque no son datos críticos, son públicos", aclaraba Raúl Medrano, IT Manager de Inspectorate.

La perspectiva de la dirección general

A esta Mesa Redonda también fue invitada la directora general de Álava Ingenieros Telecom, Isabel Tarodo, con objeto de conocer el punto de vista de la alta dirección en cuanto al fenómeno BYOD. Comentaba la directiva que hoy en día, en las empresas, la apuesta por la movilidad es clara; sin embargo, "hay que buscar el equilibrio sobre lo que me aporta más valor a mi negocio, más allá de elegir la plataforma, bien sea Android o Symbian, porque mañana serán otras. Mi core de negocio es vender así que el departamento de TI me tiene que dar soluciones para vender más y de forma rentable. Es cierto que los empleados se motivan más con sus terminales personalizados, pero hay unas normas. Es una herramienta de trabajo, y no puede ser un problema para la compañía. Al contrario, las claves son que tiene que aportar valor a la empresa, cuál va a ser el ROI, y qué voy a dejar de vender si no lo tengo. La tecnología mañana será diferente y los fabricantes de hardware nos pondrán en la mesa otra cosa diferente. Además, yo no veo que se puedan reducir los gastos, al revés, se incrementan".

Con esta declaración se cerraba el encuentro cuestionándose los presentes si realmente el BYOD lo necesita la empresa; un fenómeno, por cierto, muchas veces iniciado por la alta dirección, que empezó a traerse al trabajo los iPads y sus smartphones nuevos. Y coincidían en que esta tendencia acrecienta los costes de mantenimiento, terminal, soporte, seguridad… "Hay una necesidad para todos los entornos, ya sean cerrados o abiertos, de poner una capa de aplicaciones MDM para gestionarlos. Y esa es una necesidad. Lo que cambia el modelo de trabajo es el BYOD, porque una vez que tengo el sistema de gestión, ¿a qué modelo voy? Si el usuario se paga el dispositivo ¿es un ahorro? Estas cuestiones dependen de las líneas de actuación de cada compañía, pero, hay que tener un MDM para gestionar y securizar", concluía Gabriel Cerrada desde Orange.