Texto R. Contreras
Fotografía Santiago Ojeda
Vídeo Rubén Pagán

EL EQUILIBRIO ENTRE PRODUCTIVIDAD Y SEGURIDAD, LA CLAVE

En busca de una estrategia para la movilidad corporativa

"Hay tecnología que permite la gestión del dato inteligente y aportar valor al mismo"

La movilidad genera un efecto multiplicador para la agilidad de las empresas y, a su vez, complica la gestión y protección de los datos en entornos de usuario. Los nuevos canales internos y con clientes hacen que no se conciba un modelo de negocio sin utilizar smartphones, tabletas u ordenadores portátiles con un carácter colaborativo. Todo ello es un cóctel al que hay que añadir problemas potenciales como el ransomware, los derivados del Bring Your Own Device y del cumplimiento legal. Pese a esta tendencia creciente, apenas la mitad de las empresas cuenta con una estrategia de protección del dato móvil. También se percibe que la protección de las compañías va centrada al dispositivo con herramientas de MDM (Mobile Device Management), pero que no se cubren todos los entornos.

Estas son algunas de las conclusiones a las que se llegó en el encuentro organizado por Computing, en colaboración con Commvault, en torno a la problemática de los datos, en el que participó una decena de responsables de TI tanto del ámbito privado como de la Administración Pública.

Diferentes tipos de usuario

La estrategia de Repsol pasa por conjugar movilidad y colaboración. Así lo explica Ignacio Rodríguez, responsable de TI, Atención a Usuarios de Repsol: "Para todas las personas que tenemos catalogadas con perfiles de movilidad, que disponen de smartphone o tablet, con posibilidad de compartir datos, hemos creado nuestra propia nube Repsol". Para dar una pincelada más de colaboración, "estamos trabajando en un entorno de Office 365 y OneDrive con algún proyecto piloto concreto".

En el caso del Ministerio de Hacienda y Función Pública, la cosa se complica, como es natural en un contexto institucional. Según explica Pablo Jesús Escudero, Jefe de Área de Administración Electrónica adscrito a la Financiación Autonómica y Local, "las características de nuestro sistema es que tenemos unos usuarios internos de un volumen medio, pero nuestros principales usuarios están fuera de la organización, pues son los ayuntamientos y las comunidades autónomas. A los usuarios externos no les damos soporte de movilidad, sino que viene de sus respectivos órganos territoriales y con el personal interno tenemos una estrategia de movilidad corporativa para la directora del centro, la subdirectora general, los miembros del gabinete, subdirectores y subdirectores adjuntos". Para este grupo se suministra un PC portátil para teletrabajo, una tableta Surface y un móvil corporativo de diferente gama en función del perfil directivo. Para el móvil y la tableta utilizan un MDM Afaria y de cara a la estrategia Byod, el directivo se inclina por un dispositivo del Ministerio y que se pueda disponer de él tanto para uso profesional como uso personal; lo que se define como COPE (Corporate-Owned Personally-Enabled).

Entornos virtualizados

El punto de vista de Codeactivos es diametralmente opuesto como relata su IT Manager, Álvaro Valero: "Nosotros adoptamos dos fases en el tema de seguridad del puesto de trabajo. En 2013, subimos los puestos a entornos de VMware View, donde todos los equipos están virtualizados. Conseguimos que todo estuviera centralizado bajo el mismo paraguas de una única solución y aplicamos configuraciones de seguridad dentro de este entorno". En 2015, enfocado hacia la transformación digital, Codeactivos inició un ejercicio dentro de la empresa para ver qué rumbo seguir. La edad media de la compañía es de unos 25 años y el Byod o el teletrabajo suponían algún problema. "Pusimos todo en la coctelera e incorporamos el Byod dentro de Codeactivos, con la garantía de tener un MDM detrás. Transformamos el puesto de trabajo con un catálogo de aplicaciones para poder configurar el puesto en función de las necesidades del usuario". En cuanto a colaboración, han estado trabajando en Office 365 y con Google, y cuentan con un equipo de usuarios expertos para seguir de cerca las necesidades de los trabajadores.

José María Gallo,
AC Hoteles

Francisco Javier Serrano,
Agroseguro

Rafael Picazo,
CLH

Álvaro Valero,
Codeactivos

David Sanz | EMEA Endpoint & Mobile Competency Lead

"LA CLAVE ESTÁ EN LA VISIBILIDAD DE LOS DATOS"

"Aparte de sus grandes aportaciones, la movilidad tiene sus riesgos implícitos, de pérdida de información corporativa o de cumplimientos normativos. Al fin y al cabo, los dispositivos móviles son fáciles de perder e incluso de robar, y en estas situaciones lo que hay que garantizar es que la información corporativa no se vea comprometida". Este es el punto de partida de David Sanz en torno a la problemática de la gestión y protección de datos. Es el equilibrio entre productividad y seguridad lo que las organizaciones están buscando cuando se trata de movilidad, y "desde Commvault damos como respuesta la capacidad de gestionar los datos corporativos de forma global, estén donde estén, habilitándolos para su uso productivo de forma segura".

Se trata de extender de la manera más natural posible a los dispositivos móviles aquellas políticas que se emplean en el centro de datos. "Debemos dar a los usuarios herramientas de colaboración para que sean productivos, pero dichas herramientas tienen que caer dentro del ámbito de la gestión de TI corporativa. Un ejemplo claro son las herramientas de compartición de archivos: muchos usuarios tienen la necesidad de colaborar con compañeros o clientes y, si desde la organización no se les da una opción sencilla para ello, serán los propios usuarios los que la busquen empleando soluciones gratuitas en la nube sin ningún control, lo que supone un gran riesgo".

En una palabra: la clave es visibilidad. Las organizaciones necesitan tener visibilidad en todo momento de la información accedida, almacenada o compartida en el entorno móvil, y así analizar riesgos ante posibles pérdidas o normativas legales.

Javier Menéndez,
Correos

David Peña,
Grupo TBWA

Pablo Jesús Escudero,
Ministerio de Hacienda

Manuel Alonso Redondo,
IGAE

Javier Menéndez, Subdirector de Explotación de Correos, explica que su organización aborda tres ecosistemas de dispositivos: "Por un lado, los 20.000 PC portátiles de los usuarios que están evolucionando, por mor de la seguridad, hacia puesto virtual (RDS para oficina). En segundo lugar, están los equipos VDI de los administrativos, en cuyo caso hacemos que los datos estén en el servidor. También contamos con herramientas de Office 365 para evitar que la gente use servicios del estilo de Dropbox". En tercer lugar, se encuentran los PDA que utilizan los carteros en un entorno controlado y totalmente securizado por una herramienta de MDM. "Los mayores problemas los tenemos en los 1.500 dispositivos móviles, tablets y smartphones, que tenemos repartidos y no hay una solución MDM definitiva para gestionarlos. Estamos en licitación de las comunicaciones y nuestro plan es montar una herramienta de gestión completa".

La protección de datos no es algo de ahora, se viene desarrollando desde siempre, y así lo constata José María Gallo, Director of Information Systems & Innovation de AC Hoteles, "lo que sucede es que con la movilidad todo se ha descontrolado". En el caso de AC Hoteles hay dos vertientes, la gente del hotel que no se mueve de su puesto de trabajo y los comerciales. Para los primeros, cuentan con un entorno centralizado, con todo el control de aplicaciones virtuales, bajo una nube privada solamente accesible para el personal de los hoteles. Lo que han hecho es separar por completo el tema de la movilidad. Algún problema de legislación o de tarjetas se resuelve a través del PCI. "En cuanto a la movilidad, estuvimos hablando de instalar un MDM, pero valorando la criticidad de la información y vimos que se trataba de un pequeño porcentaje. Nosotros generamos información de cliente que pierde su validez el día que abandona el hotel. En cuanto a temas de virus, casi es más importante montar una política de backup consecuente con la situación actual. Y un punto final clave es el de la formación de los usuarios".

Formar y concienciar es el caballo de batalla

Precisamente es la educación en el punto que incide Rafael Picazo, Subdirector de Aplicaciones de CLH. "La formación es lo más importante; estamos haciendo campaña en la empresa advirtiendo sobre los riesgos de la nube. Los usuarios consideran la movilidad una herramienta estupenda que te permite hacer de todo en cualquier sitio pero tienen que ser conscientes con quién comparten, con el hecho de que hacer copias en el mundo digital es muy fácil". Al igual que Repsol, esta empresa de transporte de combustible está planeando desplegar una oficina colaborativa, haciendo hincapié en formar al usuario que siempre va a pensar que es más sencillo utilizar Dropbox que cualquier otra herramienta. "No quiero contar cuando hablé de pasar de 8 a diez caracteres en la password, las quejas que surgieron". Y recalca, "formar y concienciar es el caballo de batalla".

Francisco Javier Serrano, Responsable de Explotación de Agroseguro, confirma esta idea, los peligros vienen más de dentro que de fuera y este problema "lo tenemos resuelto desde hace hace tiempo. Contamos con terminales thin client en toda la organización, incluso en las delegaciones". No hay datos fuera de la empresa, lo cual, en su opinión, resuelve gran parte de la problemática. "Se habla de la nube y de la movilidad, pero dentro no hay que relajarse. Los thin client no exigen un periodo corto de renovación ni procesadores, sino conectividad y estructura de servidores". Como otros contertulios aborda el tema cloud y afirma que "tenemos cierto temor a la nube, porque ¿quién te garantiza la localización geográfica de tus datos y dónde está la seguridad?". Por tanto, Agroseguro se apoya en servidores de datos, con todo securizado; y lo que se refiere a portátiles y móviles se resuelve a través de redes privadas virtuales (VPN). "Nuestros usuarios tienen más difícil la entrada y salida del dato, con la imposibilidad física de insertar una llave USB".

En contraste, Telefónica aboga por la nube con fe declarada. Leonardo Amor, Head of Security de la operadora, así lo declara: "Creemos en nuestras nubes y en las de terceros". Todo lo han migrado a Office 365 y bloquean Dropbox o Wetransfer desde sus redes internas. "El problema es el perfil y el dato que se quiere guardar y no encriptar todo. Estamos trabajando en temas de cifrado pero no hemos implantado nada porque hasta hace seis meses las soluciones de nube no las recomendaba el fabricante y lo dejaban a tu criterio".

Para Amor, "nadie puede decir que no tenga nada en la nube. Un buen ejemplo es cómo Salesforce empezó en Telefónica, a través de una unidad en Latinoamérica mediante Shadow IT. Hace veinte años, las empresas dotaban de tecnología a los usuarios, y ahora ese proceso se ha invertido, son ellos los que traen la tecnología a las empresas; es el caso de Yammer o Linkedin, que las terminó adquiriendo Microsoft por su aceptación popular". El experto de Telefónica llama la atención sobre el caso del 'phising del CEO' que afecta a Linkedin y que

su compañía pudo neutralizar. "La incorporación de Chema Alonso como CDO de la compañía nos ha hecho más transparentes", asegura Leonardo Amor. Telefónica es consciente de que no puede prohibir el uso de dispositivos particulares y la única manera de acceder a la red internacional es a través de VDI. En lo que se refiere a móviles, están utilizando varias soluciones MDM en el grupo y en la esfera de los top directivos donde extreman precauciones controlando sus perfiles de redes sociales y el de sus familiares más cercanos. El resto de los usuarios utiliza Office 365 y Onedrive.

Las soluciones de la Intervención General de la Administración del Estado tienden a un entorno controlado, como comenta Manuel Alonso, Subdirector General Adjunto de Explotación. "Lo primero que intentamos fue convertir el puesto de trabajo en puesto de movilidad. Tenemos una solución de puesto remoto, basada en Terminal Server de Microsoft. Una solución desplegada por nosotros que no nos cuesta dinero", explica Alonso. La decisión de ir a cliente ligero resulta caro, comenta, y "nosotros tenemos ordenadores de hace diez años sin coste; el éxito fue reconvertir el PC en puesto de trabajo". De los 5.000 usuarios con los que cuenta la IGAE, 3.000 son clientes ligeros, y el resto son movilidad con un peso importante del tablet, pero han descartado el mundo Apple iOS porque no tiene "mucho encaje con los sistemas de la Administración". Como institución pública, está condicionada por ciertos requisitos que limitan la movilidad, si bien no tiene grandes necesidades porque las tareas son fundamentalmente internas y todo se resuelve con VPN. "En cuanto al acceso por movilidad, no nos preocupa demasiado porque a lo único que puede acceder un dispositivo que no está gestionado con MDM es al correo electrónico". Por otro lado, la IGAE cuenta con un centro de datos distribuido activo (de tal manera que es posible cerrar un centro y trabajar con uno solo) y todo es transparente para los usuarios.

David Peña, Director de Tecnología de TBWA, expone un punto de vista diferente: "Hasta ahora todos habláis de seguridad fija y móvil. Metemos en el mismo saco de movilidad a los dispositivos, pero pienso que es un enfoque erróneo". A su parecer, es la información la que es fija o es móvil. "Yo no distingo entre ordenador de sobremesa o móvil. La información que tengo que securizar está en cualquier sitio". Antes del ataque hay que tener en cuenta la prevención y aquí, siguiendo la corriente general, pone el acento en la educación: "El usuario es el punto débil y ahora corremos graves riesgos con el ransomware. El correo electrónico se ha convertido en un repositorio de información importante para la empresa. Hay que proteger el end point, y las estrategias de backup tradicionales ya no sirven", concluye Peña.

Gabriel Martín, director general de Commvault España, está convencido de que tiene que evolucionar la forma en que las empresas gestionan los datos. "Se securiza más la infraestructura que el dato, porque las políticas de seguridad están más centradas en los dispositivos. Tampoco se puede guardar toda la información que se genera para siempre, existen sistemas que permiten discriminar datos que no son útiles. La deduplicación está muy bien para ahorrar, pero el que más y el que menos tiene las mismas políticas de backup de hace veinte años. Ahora existe mucha tecnología que permite la gestión del dato inteligente y aportar valor en la gestión del mismo". ■

Ignacio Rodríguez,
Repsol YPF

Leonardo Amor,
Telefónica

Gabriel Martín,
Commvault

"Hay que proteger el endpoint. Las estrategias tradicionales de backup ya no sirven"