IBM Security
Folleto acerca del Liderazgo Intelectual

Transformación de la Productividad

Asegure el contenido que se comparte en el camino

IBM

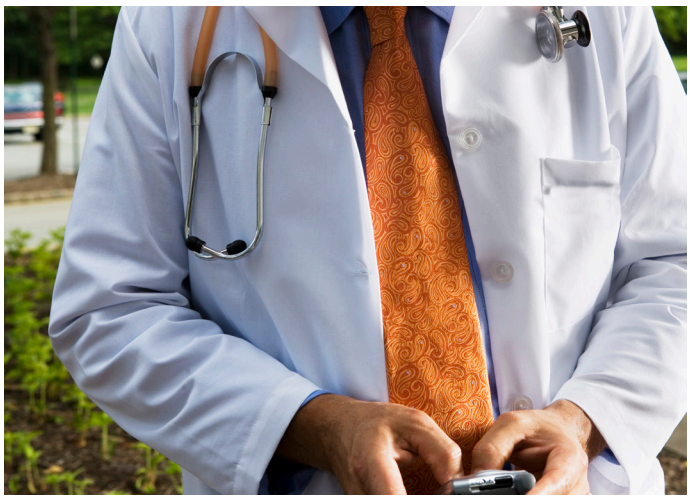
Introducción

Este folleto presentará la rápida transformación de la productividad de los lugares de trabajo gracias al aseguramiento del contenido empresarial, que permite a los empleados utilizar sus smartphones y tablets para realizar actividades empresariales desde la palma de su mano.

A medida que más personas utilizan dispositivos móviles para trabajar, ¿cuáles son los elementos clave de una solución de gestión de movilidad empresarial (EMM) que permiten satisfactoriamente crear, editar, compartir, sincronizar e insertar contenido en los dispositivos móviles? Este folleto le dará la respuesta con casos específicos de industria y consejos para ayudarlo a satisfacer las exigencias de productividad de los altos ejecutivos y los requerimientos de uso y de seguridad de TI.

A medida que los dispositivos reducen su tamaño, aumentan sus capacidades para soportar los cambios abruptos de productividad provenientes de poder acceder a contenido desde dispositivos sin pérdida de funcionalidad o apariencia del producto final.

Transformación de la productividad



Un médico de Chicago quiere traer un especialista para un caso complicado. El médico utiliza su smartphone para enviar historiales médicos e imágenes de rayos X por correo electrónico a un cirujano consultor en Baltimore, con quien intercambia información y exámenes a través de archivos adjuntos en correos electrónicos.

La presentación de un importante accionista requiere una actualización de último minuto sobre información financiera de diferentes fuentes de información. Desde la pista de aterrizaje, la CEO usa su tablet, el tiempo del CFO y una aplicación para consumidores para compartir y sincronizar archivos.

Estos son casos de la vida real, pero no se ajustan a las buenas prácticas. De hecho, ni siquiera son prácticas de bajo riesgo en la colaboración segura de contenido, sino que son extremadamente peligrosas, posibles pesadillas normativas.

Contenido móvil

En la transformación de la productividad móvil, que compite con la introducción de portátiles en la empresa, los empleados llevan consigo contenido confidencial y clave en sus dispositivos mientras trabajan de manera móvil.

Crean, abren, actualizan, analizan, editan y comparten documentos fuera de la oficina, desde aeropuertos, estaciones de tren, cafeterías y salas de conferencia. La eficiencia obtenida gracias a la colaboración con colegas y clientes ya no se debe limitar a dispositivos fijos.

Sin embargo, este contenido se almacena en redes corporativas que deben verificar que las transacciones sean seguras, como Windows File Share, SharePoint, intranets y aplicaciones web. Actualmente, la información esencial para la colaboración entre colegas, socios y clientes está atrapada en unidades internas y wikis, bases de datos, ERP, SCM, HRM, CRM y otros sistemas de gestión.

A medida que los dispositivos reducen su tamaño, aumentan sus capacidades para respaldar los cambios abruptos provenientes de poder acceder a contenido desde dispositivos sin pérdida de funcionalidad ni apariencia de los productos finales.

TI: El epicentro de la productividad y la seguridad

Los grupos de Tecnologías de la Información están haciendo todo lo posible para que se forme una legión de trabajadores en constante crecimiento y movimiento con sus dispositivos móviles y grandes expectativas acerca de contenidos que aumentan su tamaño. El simple hecho de que la tendencia "Traiga su Propio Dispositivo (Bring Your Own Device – BYOD) haya cambiado el paradigma de adquisición de dispositivos no significa que las responsabilidades en cuanto a la seguridad de los datos y las entregas sin restricciones hayan sido desplazadas.

Una solución de gestión de movilidad empresarial (EMM) permite realizar colaboraciones de contenido seguro y, simultáneamente, satisfacer las exigencias de rentabilidad de los altos ejecutivos junto con las de productividad de la línea de negocios. Este folleto analiza el cambio de gestión de dispositivos móviles a protección proactiva de EMM de contenido y datos en dispositivos móviles.

Creación de un programa de contenido seguro y exitoso

Sí, seguramente es fácil y práctico para los médicos consultores compartir historiales de clientes por e-mail, lo han hecho durante años. Pero el hecho de que lo hagan no quiere decir que deban.

Sincronizar y compartir archivos en la pista de aterrizaje con soluciones para consumidores es útil para el CEO que está a punto de partir. Para el equipo de TI en tierra, es una pesadilla de seguridad que está a punto de hacerse realidad.

Los smartphones, las tablets y los dispositivos transportables hacen que sea posible la colaboración continua, pero una solución de EMM puede hacer que sea segura. El hecho de que los archivos salgan de la oficina o ER no quiere decir que se deban ignorar las recomendaciones de TI para el transporte.

El correo electrónico y compartir/sincronizar archivos son soluciones comunes y acciones erróneas

En la actualidad, existen millones de maneras de compartir datos, desde e-mails probados y confiables hasta colaboración en la nube a nivel de consumidores, pero estos métodos no se destacan precisamente como buenas prácticas. Dejan el contenido expuesto a vulnerabilidades que atentan contra la productividad de los empleados y comparten información confidencial con personas que podrían aprovecharse de ella.

Has recibido un correo electrónico... y un espacio abierto para todo lo que se comparte

El e-mail, método más utilizado durante mucho tiempo para compartir documentos, generalmente no es un repositorio de contenido seguro, productivo o eficiente. Además de que existe la posibilidad de enviar o compartir los archivos por error, el tamaño de los archivos adjuntos creció demasiado para las cargas de tráfico de los servidores de e-mail tradicionales. Normalmente, el e-mail tampoco es compatible con filtros, ediciones o sincronización en tiempo real. Finalmente, el e-mail no solo es inseguro, sino que puede dificultar la productividad y la colaboración.

Pero las personas continúan usándolo. Compartir archivos a través del e-mail continúa siendo una práctica común. Una encuesta global realizada reciente de Ovum[1] de más de 5100 empleados mostró que el 44 % de ellos continúa utilizando el e-mail y tarjetas de memoria para compartir documentos.

El 46 % de los profesionales de TI encuestados están de acuerdo en que "los datos de las compañías se filtran debido al uso no gestionado de productos destinados a compartir archivos"[2]

Aplicaciones para compartir/sincronizar para consumidores: riesgosas e inseguras

El mercado para consumidores está lleno de aplicaciones para compartir y sincronizar archivos: Dropbox, Google Drive, Evernote y iCloud, son solo algunas de ellas. Los métodos desarrollados

en las empresas (internamente) están en estadios incipientes y muchas veces presentan más frustraciones que productividad. Por ese motivo, no sorprende que los empleados opten por utilizar el mismo Dropbox que usan para las fotos familiares para almacenar presentaciones de gran tamaño para trabajar durante el fin de semana. Según el estudio de Ovum, el 89 % de los empleados utiliza sistemas para consumidores porque no les agrada el enfoque restrictivo de la empresa.[3]

Si bien son accesibles y prácticas para los empleados, generalmente las aplicaciones para compartir y sincronizar archivos para consumidores no cumplen los requisitos de seguridad en cuanto a visibilidad, o la aplicación de normas centralizadas de contenido. Cuando no están protegidas, estas soluciones representan un riesgo potencial para las empresas, que pueden sufrir filtraciones de datos, ataques de seguridad y violaciones de cumplimiento normativo.

Pero los empleados insisten en utilizarlas, inclusive cuando, según un estudio de Interlink[4] el 46 % de los profesionales de TI encuestados están de acuerdo en que "los datos se filtran de las compañías debido al uso no gestionado de productos destinados a compartir archivos", y el 84 % cree que el uso por parte de los empleados de productos gratuitos para compartir y sincronizar archivos crea un posible problema de seguridad.

Componentes clave para asegurar el contenido empresarial de manera eficaz en dispositivos móviles

Para que los empleados ayuden a garantizar la productividad y a proteger la empresa, deben confiar en la gestión de movilidad empresarial, que debe ser segura, funcional y fácil de usar.

Una solución diseñada para satisfacer a todos debe incluir:

Herramientas accesibles e intuitivas: los usuarios necesitan herramientas que sean accesibles para crear, editar, sincronizar y compartir tipos de archivos comunes (Excel, Word, PowerPoint, PDF). El área de TI debe poder ver la manera en que se visualizan y comparten los documentos, e implementar de manera remota normas de seguridad en controles más profundos relacionados con la edición.

Seguridad y escalabilidad a través de la nube: las soluciones confiables de EMM se basan en un contenedor cifrado y seguro que protege datos confidenciales. También otorga al área de TI la posibilidad de definir, habilitar y hacer cumplir normas basadas en tiempo y ubicación, cumplimiento de contraseñas y flujos de trabajo de documentos basados en buenas prácticas. Con una solución basada en la nube, el área de TI puede brindar acceso basado en roles y gestión administrativa desde una consola centralizada. De esta manera, estará seguro de que los documentos no se podrán abrir excepto en el contenedor seguro, en el dispositivo del usuario.

Una solución global gestionada en la nube también puede ser la respuesta para una distribución escalable. Almacene documentos una única vez y distribúyalos con frecuencia, olvídese de la capacidad de almacenamiento y las restricciones de ancho de banda.

La rentabilidad y la facilidad de una implementación de EMM en la nube también benefician los objetivos de retorno de la inversión (ROI) en el mundo rápidamente cambiante de la movilidad. Pueden reducir de manera rotunda los costos de despliegue y mantenimiento, lo que permite disponer del tiempo y los recursos del área de TI para iniciativas empresariales de mayor valor, en vez de comprar y controlar otro servidor. Como los sistemas operativos móviles continúan respaldando las aplicaciones más nuevas, podría inutilizar toda la flota móvil si no realiza una actualización de un día de su software EMM.

Cumplimiento: las diferentes industrias están limitadas por requerimientos de cumplimiento y las soluciones de EMM se deben adaptar a dichas regulaciones.

Las compañías que cotizan en bolsa están sujetas a la legislación del Sarbanes-Oxley Act (SOX), que restringe la distribución de información financiera fuera de los períodos de presentación de informes financieros controlados, por ejemplo. En los servicios financieros, FINRA (Financial Industry Regulatory Authority) exige que los smartphones y las tablets cumplan con los requisitos de información confidencial más amplios de la firma para proteger la información de los consumidores.

El Health Insurance Portability and Accountability Act (HIPAA) establece restricciones similares en la industria médica, con reglas que prohíben el almacenamiento de información personal identificable sin cifrar e información de salud protegida. Para los vendedores minoristas, el Payment Card Industry Data Security Standard (PCI DSS) cuenta con guías estrictas para proteger los datos de los titulares de tarjetas, independientemente de la manera en que se use y dónde se almacene.

Promueva la Transformación

El paciente se cura y vuelve a su hogar. Duerme tranquilo sabiendo que su médico logró traer al mejor especialista para su caso. Su información médica permanece confidencial y segura en el e-mail contenido del dispositivo del médico.

El CEO realiza la presentación de una manera admirable, y sus accionistas y la junta están entusiasmados con las cifras actualizadas. Además, la información está protegida todo el tiempo en el espacio de trabajo seguro de la compañía.

Mucho tiempo después de que estos momentos móviles momentáneos se han acabado y los datos descansan en paz, las empresas están descubriendo los beneficios de contar con una solución de EMM que dé lugar a la productividad móvil al mismo tiempo que se garantiza la seguridad de datos en reposo, movimiento o uso.

Beneficios del Contenido Seguro

Desde la cama del paciente hasta la sala del aeropuerto y más allá, los beneficios de permitirles a las personas acceder, crear, editar, gestionar, compartir y sincronizar contenido son muchas, para el área de TI, los líderes de la línea de negocios, los empleados y la empresa en su conjunto.

Cuando el mundo es el lugar de trabajo, **la empresa se transforma** en un lugar en el que las personas pueden trabajar de manera móvil, compartiendo contenido con otras personas de manera continua, inclusive si están en horarios diferentes.

Se observa un aumento de la productividad y la colaboración cuando los empleados logran trabajar de manera móvil sin tener que sortear obstáculos para acceder, editar, gestionar, compartir, sincronizar y colaborar en relación a documentos. El área de TI y los altos ejecutivos pueden contar con la tranquilidad de saber que el contenido y los datos confidenciales no son un riesgo de filtración ni uso incorrecto, ya sea que se encuentren en reposo o en movimiento.

En aquellos casos en los que los empleados pueden utilizar sus dispositivos para uso personal y privado sin poner en riesgo a la compañía, **el nivel de satisfacción del empleado** aumenta, lo que nos lleva a un círculo completo, ya que un empleado satisfecho es un empleado productivo.

Requisitos clave del contenido seguro

Para lograr que su contenido móvil esté seguro, necesita:

- **Un lugar de trabajo seguro e intuitivo** para almacenar, compartir y sincronizar archivos empresariales en plataformas móviles, totalmente separadas de los datos personales.
- **Controles administrativos centralizados** para que el área de TI pueda tener una visibilidad completa del acceso a los documentos y restricciones basadas en reglas.
- **Integración sin problemas** con sistemas de autenticación y autorización existentes.
- **La posibilidad de insertar documentos de manera remota y definir y reforzar flujos de trabajo** para distribución masiva o selectiva.
- **Garantizar el acceso a activos e inversiones existentes**, desde repositorios de datos a la medida hasta otros como IBM Connections, SharePoint y Google.
- **Poner en una lista negra determinadas aplicaciones para compartir y sincronizar archivos** en los dispositivos móviles para bloquear su uso a determinados usuarios, grupos o a todos.
- **E-mails y archivos adjuntos contenidos** para proteger los documentos que se comparten a través de e-mail.
- **Eliminación remota** para información desactualizada, dispositivos perdidos, salidas de empleados o dispositivos que no se ajustan a las normas que fueron "descodificados" o "descifrados".

IBM MaaS360

MaaS360 promueve la transformación al ayudar a las organizaciones a insertar, acceder, crear, editar, compartir y sincronizar contenido de manera segura en dispositivos móviles. Sus soluciones de EMM les otorgan a los empleados la posibilidad de trabajar de manera independiente y compartir documentos en esos dispositivos, al mismo tiempo que le brinda al área de TI la capacidad de administrar y controlar exhaustivamente en un contenedor cifrado y protegido.

Las soluciones de MaaS360 ofrecen:

- **Almacenamiento de contenido** con una interfaz fácil de usar para gestionar el contenido:
  - Varias opciones de repositorios de datos: nube, local o híbrida. Entre ellas: Box, Google Drive, Dropbox y MaaS360 basados en la nube; y locales, como IBM Connections, Windows File Share y SharePoint.
- **Contenedores en los dispositivos** para acceder a contenido para iOS, Android, Windows Phone y PC:
  - Transferencia de archivos protegida desde el dispositivo.
    - Acceso a varios tipos de repositorios de datos (nube y local).
    - Datos móviles protegidos del repositorio al dispositivo.
  - Integración de seguridad de dispositivos móviles: autenticación, protección de código de acceso y eliminación remota.
  - Integración en contenedor y prevención de pérdida de datos.
    - Cifre los datos en reposo en el contenedor.
    - Restrinja el acceso de otras aplicaciones a los datos, bloquee las opciones de cortar/copiar/pegar y evite las capturas de pantalla.
    - Habilite la eliminación selectiva de contenido.
    - Realice integraciones con otras aplicaciones móviles empresariales, como el e-mail.
- Sincronizar y compartir:
  - Sincronice contenido perteneciente al usuario entre varios tipos de dispositivos, cree contenido en un portátil y sincronícelo con smartphones/tablets e intégrelo al e-mail para facilitar el control y la seguridad de los datos adjuntos.
  - Comparta contenido con otras aplicaciones móviles y con usuarios externos e internos: colegas, socios o clientes. Refuerce las normas para compartir, como la autenticación y el vencimiento de recursos compartidos.
- Manipulación del contenido
  - Cree, edite y anote de manera más segura.

Inicie su Transformación

La transformación de la productividad ya comenzó. ¿Qué está haciendo para ponerla a disposición de los empleados de su empresa? Para respaldar la transformación en toda la empresa, comience respondiendo algunas preguntas clave:

- ¿Qué necesitan sus líneas de negocio para ser productivas?
- ¿Cuál es su desempeño actualmente?
- ¿Qué tipo de normas de seguridad o para compartir y sincronizar archivos brinda o hace cumplir actualmente?
- ¿Es posible escalar sus herramientas existentes?
- ¿Cuál es su plan para mejorar?

Estudios de Caso

Una compañía global de seguros aumenta la productividad, reduce los costos y ahorra tiempo gracias a MaaS360. “IBM MaaS360 Content Suite nos resultó extremadamente útil. Si un representante de ventas está en una reunión con un nuevo grupo que desea seguros, puede solicitar al área de suscripción de seguros los detalles de costos e inscripción y podemos enviarle los documentos necesarios mientras aún se encuentra sentado con los clientes. El cliente puede incluso completar el formulario de inscripción en ese momento y lugar, lo que nos ayuda a agilizar el proceso de cierre”.

– Network Support Specialist, una compañía global de seguros.

Cuando una firma especialista en pagos a hospitales y ventas minoristas reemplazó los dispositivos empresariales BlackBerry Bold por iPhones y iPads, necesitaba brindar el mismo nivel de seguridad y gestión que tenían con BlackBerry Enterprise Server. Lo descubrieron en MaaS360, que ayuda a los empleados de la organización a acceder a documentos empresariales de manera más fácil y eficiente. “MaaS360 claramente se destacó, ya que es mucho más fácil de utilizar en todos los aspectos. La interfaz es más simple e intuitiva. La creación de informes es simple e incluye seguimiento de uso para gestión de gastos. Además, IBM MaaS360 Secure Mobile Browser y la funcionalidad de contenedor reducen automáticamente la vulnerabilidad de nuestra red”.

– Technical Systems Officer, una firma especializada en pagos a hospitales y ventas minoristas.

Acerca de IBM MaaS360

IBM MaaS360 es la plataforma de gestión de movilidad empresarial que permite proteger datos y productividad para la manera en la que trabajan las personas. Miles de organizaciones confían en MaaS360 como la base de sus iniciativas de movilidad. MaaS360 ofrece gestión integral con controles sólidos de seguridad para usuarios, dispositivos, aplicaciones y contenido para respaldar cualquier despliegue móvil. Para obtener más información acerca de IBM MaaS360 y para empezar a usar una versión de evaluación sin costo de 30 días, visite **ibm.com**/maas360

Acerca de IBM Security

La plataforma de seguridad de IBM ofrece inteligencia en seguridad para ayudar a las organizaciones a proteger de manera integral a las personas, los datos, las aplicaciones y la infraestructura. IBM ofrece soluciones para gestión de acceso e identificación, gestión de eventos e información de seguridad, seguridad de base de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de punto terminal, protección contra intrusiones de última generación, y más. IBM opera una de las organizaciones de suministro, investigación y desarrollo de seguridad más grandes del mundo. Para obtener más información, visite **ibm.com**/security

IBM de Colombia S.A.
Cra 53 No. 100 – 25
Bogotá – Colombia

Puede encontrar la página de inicio de IBM en:
ibm.com

Considere el medio ambiente antes de imprimir

1 *Ovum Mobility Survey 2014* (Septiembre de 2014) http://www.ovum.com/research/employee-mobility-survey-2014-results-enterprise-multi-screening-and-application-usage-trends/

2 *Intralinks Survey Report, Safe Sharing: A Survey of Enterprise IT Decision Makers on Best Practices for Adopting File Sync and Share Applications* (Intralinks, junio de 2014) https://www.intralinks.com/sites/default/files/file_attach/via14_65324_email_harrispaper_v1.1.pdf

3 *Ovum Mobility Survey 2014* (Septiembre de 2014) http://www.ovum.com/research/employee-mobility-survey-2014-results-enterprise-multi-screening-and-application-usage-trends/

4 *Intralinks Survey Report, Safe Sharing: A Survey of Enterprise IT Decision Makers on Best Practices for Adopting File Sync and Share Applications* (Intralinks, junio de 2014) https://www.intralinks.com/sites/default/files/file_attach/via14_65324_email_harrispaper_v1.1.pdf

WGW03151-COES-00