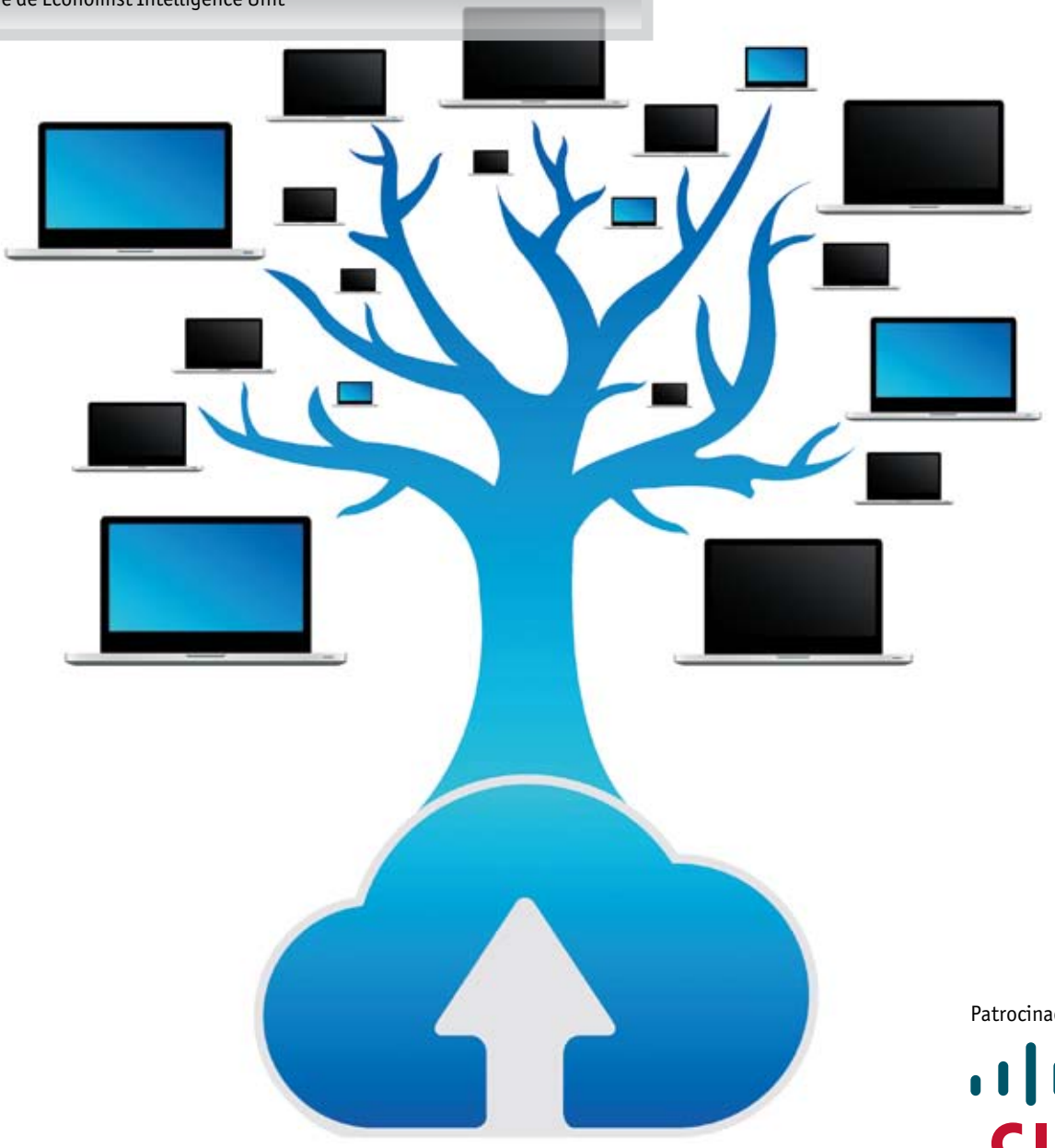
Economist Intelligence Unit

The Economist

Acceso seguro a datos en un universo móvil

Un informe de Economist Intelligence Unit



Patrocinado por

CISCO

Contenido

Prefacio

El uso cada vez mayor de dispositivos de comunicación de los consumidores en el lugar de trabajo y la necesidad de maximizar la productividad de ejecutivos y trabajadores que están en movimiento exigen que las empresas respondan. *Este informe* analiza el modo en que las empresas pueden conciliar las exigencias que surgen a partir del acceso móvil a información comercial y al mismo tiempo minimizar los riesgos de seguridad de datos de propiedad exclusiva. Como base para esta investigación, Economist Intelligence Unit realizó una encuesta a nivel mundial a 578 ejecutivos sénior en junio de 2012. La encuesta analiza de qué modo las organizaciones están, o deberían estar, respondiendo a los desafíos emergentes actuales que surgen de la tendencia imparable de "traiga su propio dispositivo" (BYOD, bring your own device), así como también del aumento de la movilidad de los trabajadores de forma más general. También realizamos una serie de entrevistas exhaustivas. Los hallazgos y las opiniones que se expresan en este informe no necesariamente reflejan la visión del patrocinador. Lynn Greiner es el autor. Michael Singer y Justine Thody editaron el informe y Mike Kenny es responsable de la diagramación. Queremos agradecer a todos los ejecutivos que participaron en la encuesta y entrevistas, incluyendo a quienes brindaron su conocimiento pero prefirieron no ser identificados, por su valioso tiempo y orientación.

Entrevistados

Lucy Burrow, Directora de gestión de TI, King's College, Londres

Mike Cordy, Director general de tecnología mundial OnX Enterprise Solutions

Steve Ellis, Vicepresidente ejecutivo, Wells Fargo

Jay Leek, Director general de seguridad informática, Blackstone Group

Arturo Medina, Director de tecnología informática, Ipsos, México

Bill Murphy, Director general de tecnología, Blackstone Group

Al Raymond, Vicepresidente, Aramark

Ashwani Tikoo, Director general de informática, CSC, India

Resumen ejecutivo

A fines de los 90, surgieron computadoras portátiles y dispositivos móviles que le permitieron a los ejecutivos ser productivos mientras se encontraban lejos de la oficina. Dispositivos como IBM ThinkPad y RIM BlackBerry dieron lugar a la era de equipos móviles multifunción que se volvió irresistible para el personal jerárquico. Actualmente, la población mundial de trabajadores móviles se amplió mucho más allá de quienes ocupan las oficinas principales y se espera que llegue en 2015 a 1300 millones de personas o aproximadamente el 38% de la fuerza laboral total, según la empresa de investigaciones tecnológicas IDC. Según algunos cálculos, un 76% de empresas actualmente tiene una política de "traiga su propio dispositivo" (BYOD, bring your own device), obligándolas a tener que asegurar el acceso a datos desde dispositivos que no son de su propiedad. La mayoría de estas empresas sostienen que permiten que los empleados utilicen dispositivos personales para tomar decisiones más eficientes, evitar la pérdida de oportunidades y trabajar en forma más eficaz con partners y clientes, es decir, por los mismos motivos que impulsan a las empresas a habilitar el acceso móvil a datos en dispositivos de propiedad de la empresa.

En junio de 2012 el Economist Intelligence Unit realizó una encuesta mundial, patrocinada por Cisco, en la que entrevistó a 578 ejecutivos sénior para analizar sus perspectivas acerca de cómo asegurar datos en dispositivos móviles. Los principales hallazgos de la investigación son los siguientes:

¿Quiénes respondieron a la encuesta?

Respondieron la encuesta 578 ejecutivos sénior de todo el mundo. La mayoría de los encuestados basados en América del Norte (29%), en Europa Occidental (25%) y en la región del Pacífico Asiático (27%), mientras que el resto pertenecen a Medio Oriente y África, América Latina y Europa del Este. De la cantidad total de encuestados, el 23% eran de los Estados Unidos, el 10% de India, el 7% de Canadá y el 6% del Reino Unido. En términos de jerarquía el 27% eran directores ejecutivos, el 17% eran vicepresidentes sénior y el 15% eran gerentes. Con respecto al tamaño de las organizaciones, el 55% de los encuestados pertenecían a empresas con ingresos anuales de USD 500 millones o más, entre ellos el 22% pertenecían a empresas con ingresos anuales de USD 10 mil millones o más. Los encuestados representaban una amplia variedad de sectores, en particular TI y tecnología (13%), servicios financieros (11%), servicios profesionales (11%) y energía y recursos naturales (9%). En cuanto a las funciones, los encuestados identificaron sus funciones primarias como tareas de administración general, desarrollo comercial, finanzas, ventas y marketing.

- **La mayoría de los ejecutivos no se sienten cómodos con las políticas de acceso móvil a datos de sus empresas.** A pesar de que el 42% de los encuestados dijeron que los altos cargos necesitan un acceso seguro y oportuno a los datos de planificación estratégica para ser más productivos, solamente el 28% cree adecuado que se pueda acceder a estos datos desde dispositivos móviles. Casi la mitad de los encuestados (49%) sostiene que los desafíos principales para sus empresas son la complejidad de asegurar muchas fuentes de datos y la falta de conocimiento sobre los riesgos y la seguridad del acceso móvil (48%).

- **Las empresas de mayor tamaño tienen mayor predisposición para permitir el acceso móvil a los datos importantes, pero también imponen reglas más estrictas.** Mas del 90% de empresas con ingresos de más de USD mil millones permiten el acceso a datos a través de dispositivos personales o pertenecientes a la empresa. Sin embargo, más de la mitad de las organizaciones con ingresos de más de USD 5 mil millones permiten el acceso solo a través de dispositivos pertenecientes a la empresa, mientras que un tercio permite también el acceso con dispositivos personales. Por el contrario, solo el 37% de empresas con ingresos por debajo de USD 500 millones insisten en el uso de dispositivos pertenecientes a la empresa, mientras que el 47% permite también el acceso con dispositivos personales. Los usuarios móviles de empresas grandes deben, no obstante, permanecer dentro de la línea de dispositivos aprobados que exigen la aprobación de muchas políticas.

- **Las políticas de movilidad no deben descuidar el uso de redes sociales.** Mientras que el 56% de los encuestados cuentan con políticas que tratan el uso aceptable de redes sociales a través de dispositivos móviles, el 33% de los ejecutivos encuestados tienen prohibido discutir su trabajo en plataformas de redes sociales. Prestar mucha atención a las políticas de uso de redes sociales puede permitir una interacción más eficaz y al mismo tiempo proteger los recursos de datos empresariales y evitar la responsabilidad legal.

- **La disponibilidad de infraestructura ejerce una influencia clave en las políticas empresariales sobre acceso móvil.** Mientras que el 44% de los encuestados sostienen que la presión de los ejecutivos es una de las influencias más importantes de la política, esa cifra se ve disminuida ante el 60% que citan los requisitos de infraestructura de TI. Esto indica que existe una oportunidad para las empresas que ofrecen servicios para asegurar y administrar el acceso móvil.

¿Es la tendencia de acceso móvil a datos imparable? La respuesta corta es sí; los dispositivos más sofisticados que brindan una mejor experiencia al usuario solo sirven para acelerar la tendencia. Esto significa que las políticas son obligatorias y no opcionales. Según los ejecutivos entrevistados para esta investigación, involucrar a los empleados en el diseño de estas políticas aumenta la probabilidad de cumplimiento. ■

Introducción

La adopción de las políticas correctas con respecto al acceso móvil a datos se está convirtiendo en una creciente preocupación para muchas empresas. Tanto los empleados sénior como los recién contratados están exigiendo el acceso a datos empresariales desde cualquier lugar y en cualquier momento, ya sea en dispositivos móviles o fijos. Y muchas empresas están tomando conciencia de que las políticas de soporte a los dispositivos móviles pueden generar dividendos en forma de mayor participación y productividad, incluida una mayor disposición a responder fuera del horario de trabajo. Además, los lugares de trabajo que aceptan BYOD resultan más atractivos para los empleados con conocimientos técnicos, lo que generalmente ayuda a estimular la innovación.

Mientras proliferan los dispositivos y continúan siendo borrosos los límites entre la tecnología informática empresarial y de los consumidores, aumentarán los desafíos que deben afrontar las empresas para adaptarse a este cambio cultural. Ampliar el alcance de los datos empresariales presenta riesgos comerciales obvios, además de desafíos tecnológicos. Los dispositivos portátiles se pueden perder o pueden ser robados. Es posible que algunas personas compartan sus dispositivos con familiares o amigos, actitud que aumenta el riesgo de filtración de datos confidenciales. Con frecuencia se accede a estos datos desde aplicaciones de software que no están sancionadas por la empresa. Pero resulta cada vez más en vano que el departamento de TI intente controlar los dispositivos que la gente lleva al trabajo o el modo en que utilizan sus dispositivos fuera de la oficina. Deben responder a la mayor vulnerabilidad de las redes de datos empresariales aplicando protecciones eficientes para proteger los datos empresariales más importantes y para cumplir con los entornos reglamentarios de cada región en la que opera la empresa. ■

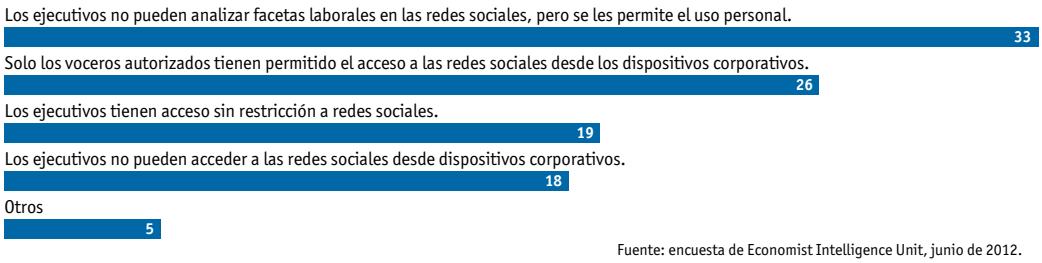
1 Movilidad moderna: ¿dónde estamos en este momento?

Casi mil millones de dispositivos inteligentes conectados se vendieron mundialmente en 2011 y se espera que esta cantidad se duplique en 2016, según la empresa de investigaciones tecnológicas IDC. Estos dispositivos incluyen productos de acuerdo con las PC como computadoras portátiles, netbooks, teléfonos móviles y tablets. La encuesta del Economist Intelligence Unit mostró que muchas personas usan varios dispositivos, generalmente una combinación de computadora portátil y smartphone, aunque está aumentando la penetración de tablets. En el segundo trimestre de 2012 la venta de tablets en el mundo creció en un 33,6% con respecto al primer trimestre del mismo año y un 66,2% con respecto al mismo trimestre de 2011, según los cálculos de IDC. Esperamos ver un crecimiento significativo en el uso de tablets después del lanzamiento de los sistemas operativos de software de próxima generación. Las funciones de colaboración y comunicación incluidas en tablets más nuevas serán atractivas para los ejecutivos ya que tienen opciones de acceso a datos más amplias que las de los smartphones.

Respaldar a los ejecutivos que están en movimiento con información proporcionada a sus dispositivos móviles les permite tomar decisiones rápidas e informadas, especialmente en momentos críticos como en negociaciones comerciales, observa Ashwani Tikoo, director general de tecnología de CSC India, un proveedor de servicios de TI. En el segundo centro de operaciones de mayor tamaño de CSC global, el Sr. Tikoo es el responsable de las políticas de seguridad que protegen los datos empresariales en dispositivos móviles. La disponibilidad instantánea de datos le permite al personal de ventas tomar las decisiones correctas en el momento, en lugar de hacer esperar al cliente, sostiene. Para evitar la pérdida de datos, las políticas de seguridad de CSC requieren el cifrado de datos en todos los dispositivos móviles, incluidos los dispositivos personales cubiertos por la política BYOD.

Otra estrategia es evitar el almacenamiento de datos en dispositivos móviles. Al Raymond, Vicepresidente de administración de registros y privacidad de Aramark, un proveedor de servicios gastronómicos de los Estados Unidos, sostiene que los usuarios autorizados que necesitan acceso remoto a la información de la empresa lo hacen a través de una red privada virtual segura (VPN)

Políticas móviles sociales para ejecutivos
¿Qué políticas enfrenta su organización sobre el uso de redes sociales en dispositivos corporativos?
(% de encuestados)



Fuente: encuesta de Economist Intelligence Unit, junio de 2012.

Estudio de caso Ipsos, un enfoque híbrido

En regiones como América Latina donde es preferible el contacto cara a cara para la investigación de mercado, los smartphones y tablets están reemplazando al lápiz y papel como herramientas de preferencia para realizar encuestas. Ipsos, una empresa de investigaciones de mercado a nivel mundial, adoptó el cambio hacia el uso de dispositivos en sus operaciones en México y en otros lugares. La empresa opera actualmente en 84 países y tiene16 000 empleados de tiempo completo. Sus investigaciones abarcan diversas tecnologías, desde investigaciones por Internet hasta en persona, con una producción de más de 70 millones de entrevistas por año en el mundo.

Actualmente, Ipsos proporciona a sus entrevistadores dispositivos manuales pertenecientes a la empresa, pero están trabajando en un nuevo enfoque, afirma Arturo Medina, Director de TI de Ipsos México. "Debido a que el costo de los dispositivos móviles personalizados es muy alto, estamos adoptando un modelo híbrido de políticas BYOD", dice Medina.

En el modelo híbrido en desarrollo, los entrevistadores pueden elegir uno de tres modelos de smartphones que pueden ejecutar el software de entrevistas de Ipsos. Los empleados pagan sus dispositivos mediante deducciones incrementales de su sueldos. En circunstancias normales, el Sr. Medina sostiene que los empleados tendrían la posesión del dispositivo directamente en 2 o 3 semanas.

Ipsos brinda una conexión VPN a los datos empresariales, mientras que el empleado paga las demás funciones del smartphone. Ipsos administra los dispositivos de modo tal que puede eliminar información comercial en forma remota, si fuera necesario. Los datos a los que se accede a través de los smartphones están cifrados para evitar algunas pérdidas. Los entrevistadores también deben cumplir con las políticas de uso corporativo. Los entrevistadores cuentan con la flexibilidad para utilizar un dispositivo en cualquier parte, sin embargo la empresa tiene control suficiente para proteger los recursos de datos, afirma Medina. ■

desde sus computadoras portátiles o dispositivos móviles. En el dispositivo no se almacenan datos excepto correos electrónicos, lo que hace relativamente fácil la tarea de proteger los recursos de datos empresariales en caso de que el empleado se vaya o pierda el dispositivo.

Existen desafíos similares alrededor del uso de redes sociales en dispositivos móviles fuera de la oficina, aunque las políticas de las empresas generalmente prohíben la participación de los ejecutivos. El 33% de los ejecutivos que respondieron a la encuesta EIU dijeron que no se les permitía analizar facetas laborales en las redes sociales y otro 25% sostuvo que solo los voceros autorizados tenían permitido el acceso a las redes sociales desde los dispositivos de la empresa. Según nuestras investigaciones, el uso de redes sociales por parte de los ejecutivos continuará prohibido, ya sea por políticas o acuerdos no escritos, para proteger la información de la empresa y limitar la responsabilidad legal.

Por supuesto que distintas jerarquías de empleo requieren acceso a distintos tipos de datos y la encuesta demostró pocas sorpresas en este tema. Entre los ejecutivos de nivel corporativo, la información financiera (60%) y la planificación estratégica (42%) fueron importantes factores de impulso de productividad. Los gerentes buscan datos operativos (44%) y datos de ventas y marketing (43%), mientras que el personal de menor rango necesita en general acceso a datos de clientes (42%) y datos operativos (42%). Según nuestra encuesta, los principales motivos de los ejecutivos sénior para solicitar el acceso móvil a los datos empresariales importantes son tomar decisiones más eficientes (52%) y evitar la pérdida de oportunidades (42%). La coordinación con terceras partes, como proveedores, tiene un puesto particularmente alto en la lista de las empresas más pequeñas; el 42% de los encuestados pertenecientes a empresas con ingresos por debajo de los USD 500 millones colocan este motivo entre los tres principales, comparado con el 37% de la totalidad de empresas. Esta necesidad de permanecer conectados ha transformado al correo electrónico en una aplicación imprescindible en los dispositivos móviles y sigue siendo la herramienta principal para el acceso remoto a datos empresariales según los ejecutivos entrevistados (81%). ■

2 Pérdidas, robos y malos hábitos: ¿qué están haciendo las empresas para enfrentar los desafíos?

La implementación de sistemas para asegurar los datos empresariales a los que se accede a través de una variedad de plataformas diferentes resulta costosa. Por lo tanto, no es sorprendente que únicamente los encuestados que trabajan en las empresas más grandes se sientan seguros con respecto a las disposiciones de seguridad de los datos de su empresa. Mientras que el 45% de los encuestados pertenecientes a empresas con ingresos anuales que alcanzan o superan los USD 10 mil millones sostienen que sus empresas cuentan con medidas de seguridad de datos de última generación, el porcentaje cae al 10% en el caso de los encuestados de empresas más pequeñas (USD 500 millones). Además, incluso entre las empresas con ingresos anuales que van desde 500 millones hasta 5 mil millones de dólares, un tercio de los encuestados describen las políticas de sus empresas como inadecuadas o completamente inadecuadas.

En general, los encuestados ejecutivos aceptan la necesidad de inversiones, con un 69% de encuestados que evalúan como prioritarias las inversiones en servicios de seguridad. Pero nuestras investigaciones indican que es necesario informar a los ejecutivos con respecto a los riesgos de seguridad. Algunas empresas creen tener una seguridad sólida, pero permiten prácticas riesgosas. Por ejemplo, entre los ejecutivos que sostienen que sus empresas cuentan con prácticas de seguridad líderes en el sector (20%), el 13% afirmó que no tiene restricciones en las actividades de redes sociales. Por supuesto que esta práctica implica el riesgo de exposición accidental de la información confidencial de la empresa. Nuestras investigaciones descubrieron que establecer políticas de uso de redes sociales puede por un lado permitir una interacción eficaz y, por el otro, ayudar a proteger los recursos de datos empresariales y evitar la responsabilidad legal.

Con menos recursos que las empresas grandes, las empresas más pequeñas enfrentan desafíos más difíciles en la seguridad de datos móviles. Casi el 40% de los encuestados pertenecientes a empresas con ingresos anuales de 500 millones de dólares o menos describen las políticas de seguridad de datos móviles de sus empresas como inadecuadas o completamente inadecuadas. Como con las organizaciones de mayor tamaño, las empresas más pequeñas que aplican políticas que tienen por escrito contribuyen en gran medida a asegurar datos empresariales a costos relativamente bajos. Los dispositivos vendidos en los últimos años cuentan con un cifrado incorporado que solamente hay que activar. Sin embargo, generalmente hacen falta herramientas adicionales de administración para automatizar los procesos de seguridad, y se obliga a las empresas más pequeñas a equilibrar entre la compra de tecnologías de protección con enfoques de menor costo, como imponer a los empleados políticas de seguridad.

En la medida en que la potencia incluso de los dispositivos más pequeños continúa aumentando, también aumenta el riesgo de perder datos por motivos menos tecnológicos. Kensington, fabricante de accesorios para computadoras de los Estados Unidos, sostiene que se pierden anualmente más de 70 millones de smartphones y solo se recuperan el 7%. Las computadoras portátiles tampoco son inmunes. Las investigaciones de Kensington muestran que el 10% se perderán o serán robadas durante el período de vida útil. Tres cuartas partes de las pérdidas se producen en tránsito o cuando el empleado está trabajando desde una ubicación remota. Un gran porcentaje de las máquinas perdidas contienen algún tipo de datos empresariales.

El costo promedio de un incidente de violación de datos empresariales alcanzó los USD 7,2

Cómo controlar BYOD

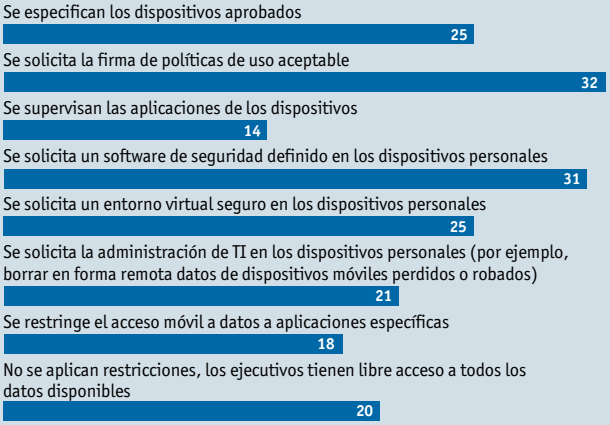
Debido a que el modelo "traiga su propio dispositivo" es comparativamente nuevo, existen algunas normas probadas del sector para políticas BYOD. Normalmente, si un empleado se va de la empresa, sea o no en forma voluntaria, se deben eliminar rápidamente los datos de la empresa, preferentemente sin interferir con la información personal del empleado. Las políticas de usos aceptables para BYOD generalmente incluyen una cláusula que lo permite. Un informe del Comité Legislativo Nacional de junio de 2012 recomienda que las empresas también pueden protegerse legalmente mediante una modificación de sus políticas móviles existentes. Todas las políticas centradas en acoso, discriminación e igualdad de oportunidades de empleo, las políticas de confidencialidad y protección de secretos comerciales y las políticas de ética y cumplimiento se pueden actualizar para proteger a las empresas contra el abuso de las políticas móviles por parte de los empleados.

Como protección contra las prácticas ejecutivas de riesgo, muchas empresas instalan software en los dispositivos de los empleados para bloquear software, cifrar datos y realizar otras funciones administrativas, como la actualización de calendarios o la aplicación de actualizaciones de seguridad. Aunque pueda parecer invasivo para el empleado, la mayoría de las políticas de dispositivos móviles requieren cierto tipo de controles de acceso administrativo remoto. Algunas empresas que cuentan con políticas BYOD esperan que los ejecutivos y los empleados se aseguren de tener el software necesario en sus dispositivos por propia cuenta y cargo. Otras empresas reembolsan la totalidad o parte del costo de los programas que se requieren específicamente para los negocios. La configuración correcta y las prácticas de buen uso deben estar controladas e implementadas en forma centralizada, sostiene el Sr. Raymond de Aramark, y agrega que la capacitación adecuada sobre la seguridad aplicada regularmente también mantiene fresca la noción del acceso seguro a datos en la mente de los empleados.

Raymond sostiene que su empresa utiliza un enfoque alternativo de la administración de seguridad móvil centrada en dispositivos. Los trabajadores utilizan el dispositivo móvil exclusivamente como visualizador, mientras que los datos empresariales no son almacenados en sus dispositivos sino en servidores corporativos a los que se accede de forma segura, y es en ellos donde se realizan las operaciones informáticas, no en el dispositivo en sí. Los métodos para hacer esto, que incluyen el uso de tecnologías de escritorios virtuales y el acceso a datos a través de servicios basados en la web como Salesforce.com, se están volviendo de uso más extendido ya que el acceso móvil a redes seguras permite el cifrado, la autenticación y la administración controlados por la empresa.

Arturo Medina de Ipsos, que impone controles similares de acuerdo con la red, recomienda mantener un diálogo continuo con los empleados para asegurar el cumplimiento y evitar descargas no autorizadas de datos empresariales. Medina aconseja aclarar los límites entre la información de carácter confidencial y la información del usuario y también establecer qué información obtiene copia de seguridad como información empresarial y qué información se considera de carácter personal.

Políticas BYOD
¿Cómo ha implementado BYOD su organización para acceder a datos críticos? Seleccione todo lo que corresponda.
(% de encuestados)



Fuente: encuesta de Economist Intelligence Unit, junio de 2012.

millones, en 2010 según la consultora Ponemon Institute. Esto es más del doble que el costo promedio del año 2005. El Sr. Raymond de Aramark piensa que estas cifras son ciertas dada la cantidad y el tipo de violaciones y agrega que hay cientos de pequeños incidentes por año y algunos incidentes mayores que pueden alcanzar desde USD 25 a USD 500 millones.

Muchas de las pérdidas de datos móviles son el resultado directo del descuido de los usuarios, lo cual es de particular preocupación para las empresas que buscan evitar violaciones provocadas por los empleados. El estudio *Costos de violaciones de datos de 2011* de Ponemon descubrió que entre el 30% y el 40% de las violaciones fueron causadas por negligencia, seguidas por las provocadas por ataques maliciosos (43%). El estudio descubrió que el 50% de las violaciones en empresas italianas fueron consecuencias de la pérdida o el robo de dispositivos móviles. Solamente en Alemania

(42%), Francia (43%) y Australia (36%) las violaciones causadas por ataques maliciosos superaron a las causadas por negligencia. India fue el único país en el cual las violaciones causadas por defectos de sistemas superaron a las causadas por negligencia o ataques maliciosos.

Algunas pérdidas destacadas de datos móviles muestran con qué facilidad se puede producir una violación. Cancer Care Group, una clínica contra el cáncer de Indianápolis, perdió en julio de 2012 los datos personales de más de 55 000 pacientes, así como también los datos de los empleados, cuando robaron de un vehículo cerrado la computadora portátil de un empleado que tenía los archivos de copias de seguridad del servidor. A diferencia de lo que se establece en el código de las mejores prácticas, los datos no estaban cifrados. El departamento médico de Anderson Cancer Center, una clínica médica de Texas, sufrió dos violaciones entre junio y julio de 2012. Mientras que un incidente fue causado por la pérdida de una llave USB no cifrada en un autobús, el otro se produjo cuando robaron una computadora portátil, que tampoco estaba cifrada, de la casa de un miembro del cuerpo docente. En las dos violaciones se puso en peligro la información de más de 30 000 pacientes. Después de la segunda violación en las instalaciones dieron comienzo a un proyecto para cifrar todos los datos.

La empresas pueden evitar muchas violaciones de datos al agregar una protección de contraseña a los dispositivos móviles, ya sean computadoras portátiles, smartphones o dispositivos portátiles de almacenamiento de datos y mediante el cifrado completo del disco o llave USB.

Estos dispositivos también deben asegurarse físicamente. Por ejemplo, no deben dejarse en vehículos sin atención, incluso aunque estén cerrados con llave. Los teléfonos móviles y algunas PC (aquellas equipadas con tecnología VPro de Intel) se pueden desactivar de manera remota y eliminar los datos que contienen en caso de desaparición. Mientras mayor sea el carácter de confidencialidad de los datos que contienen, mayor es la importancia de activar un mecanismo de este tipo, ya que el cifrado puede vulnerarse. ■

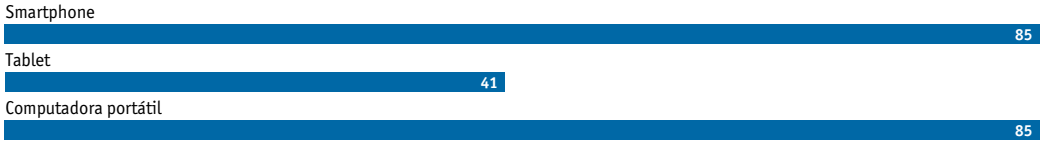
3 Más datos que nunca en marcha: las últimas tendencias

Casi el 90% de las organizaciones de todo el mundo permiten el acceso móvil a los datos más importantes, según la agencia Unión Internacional de Telecomunicaciones (ITU, International Telecommunication Union) perteneciente a Naciones Unidas. De las organizaciones identificadas en la encuesta EIU que no tienen políticas formales de BYOD, el 25% sostiene que planean implementar un programa en los próximos 12 a 18 meses. Ellos observan que este tipo de programas genera más empleados motivados, una observación confirmada por investigaciones independientes. Según investigaciones realizadas en agosto de 2012 por iPass, una empresa estadounidense de software para dispositivos móviles, muchos empleados trabajan hasta 20 horas adicionales semanales no remuneradas cuando están conectados permanentemente. Casi el 90% de los encuestados por iPass dijeron que la conectividad inalámbrica es un componente en sus vidas tan importante como la electricidad o el agua corriente.

A pesar de que más empleados están trabajando fuera de la oficina, establecer un programa de acceso móvil que incluya BYOD no es una opción para muchas empresas. Las empresas financieras y de operaciones bancarias altamente reglamentadas cuentan con políticas estrictas que prohíben a los ejecutivos acceder a los datos empresariales desde sus dispositivos personales. Steve Ellis, Vicepresidente ejecutivo de Wells Fargo, observa que su empresa se acercó a BYOD con precaución y actualmente están evaluando opciones. Podríamos tener un plan formal quizás dentro de un año, dice Ellis. Otra empresa sin política formal de BYOD informa haber visto pasar dispositivos personales en forma desapercibida. Antes de la introducción de la política formal móvil de Aramark hace diez meses, los empleados no contaban con reglas que establecieran los dispositivos y sistemas operativos calificados para conectarse a la red de la empresa. Con la nueva política, que implica acceso de acuerdo a los roles, los dispositivos y las configuraciones aprobados, la empresa sabe exactamente quién tiene acceso y a qué datos específicos. "Ya no se trata de darnos a entender" dice el Sr. Raymond. Mientras mayor sea la visibilidad del programa, mayor es la probabilidad de que se respete.

Políticas aparte, también ha cambiado la naturaleza de los dispositivos. Actualmente, un poco más de un cuarto (27%) del acceso a los datos más importantes se produce a través de smartphones, según nuestra encuesta. Los encuestados esperan que esto aumente a más de un tercio (35%) en los próximos 12 a 18 meses, con

Dispositivos de acceso ejecutivo
¿Qué dispositivos proporciona su organización a los ejecutivos para acceder a los datos críticos? Seleccione todo lo que corresponda.
(% de encuestados)



Fuente: encuesta de Economist Intelligence Unit, junio de 2012.

Caso de estudio La Comisión de igualdad de oportunidades en el empleo de los EE. UU. lanza plan piloto en movilidad

El presupuesto del año fiscal 2012 de la Comisión de igualdad de oportunidades en el empleo (EEOC, Equal Employment Opportunity Commission) de los Estados Unidos se recortó en casi un 15%, de USD 17,6 a USD 15 millones. Ante la necesidad de reducir los costos operativos, la Directora general de informática, Kimberly Hancher, redujo a la mitad el presupuesto de la agencia para dispositivos móviles. Para cubrir la brecha, la agencia lanzó un proyecto piloto BYOD móvil. El proyecto se centró en brindar a los empleados acceso al correo electrónico, calendarios, contactos y tareas de la agencia. Como parte del proyecto, algunos de los ejecutivos sénior obtuvieron acceso "privilegiado" a los sistemas internos de la agencia.

En la fase inicial de prueba, 40 voluntarios devolvieron los dispositivos BlackBerry otorgados por el gobierno y en su lugar utilizaron sus smartphones personales. El personal de seguridad informática, el personal legal y el sindicato de empleados generaron reglamentaciones que equilibraban la privacidad de los empleados (políticas de supervisión y de redes sociales) con la seguridad gubernamental, como la reglamentación SP 800-53 del Instituto Nacional de Estándares y Tecnología (NIST, National Institute of Standards and Technology), también conocida como "Controles de seguridad recomendados para organismos y sistemas informáticos generales". La segunda fase del programa se lanzó en junio de 2012. La EEOC trabajó junto con los contratistas para configurar el acceso al correo electrónico de la agencia para los empleados que participaban en la prueba secundaria. A los restantes 468 empleados de la agencia que utilizaban dispositivos BlackBerry otorgados por la comisión se les ofrecieron tres alternativas:

1. Devolver voluntariamente el dispositivo BlackBerry y llevar al trabajo un smartphone personal Android, Apple o BlackBerry o una tablet
2. Devolver el dispositivo BlackBerry y recibir un teléfono celular con funciones de voz únicamente, otorgado por el gobierno
3. Conservar el dispositivo BlackBerry bajo el acuerdo de que la Comisión no tiene dispositivos de reemplazo

Hasta el momento, los gerentes de la Comisión han informado resultados positivos del programa piloto. Los empleados pagan el uso de datos y voz y la agencia cubre las licencias del software de administración. La Sra. Hancher de la Comisión observó que, para algunos empleados, el costo puede ser un problema y existe la cuestión pendiente de que si la agencia podrá proporcionar algún tipo de reembolso para parte de los servicios de datos y voz. La Sra. Hancher destaca que el éxito se logró al involucrar a los empleados, al sindicato y a los departamentos legales en el proceso de manera anticipada. ■

otro 30% de acceso a datos críticos por medio de dispositivos móviles, incrementando la cifra actual del 20%. Con la llegada de software más novedoso y sus dispositivos relacionados, las tablets están listas para convertirse en una ventana móvil a los datos empresariales de mayor uso por parte de los ejecutivos, quizás incluso reemplazarán en el futuro a los smartphones, según un artículo de *The Economist* (octubre de 2011). El mayor tamaño de pantalla amplía el rango de datos que pueden verse de manera eficaz y, con la ayuda de teclados externos, permiten una interacción más fácil con las aplicaciones.

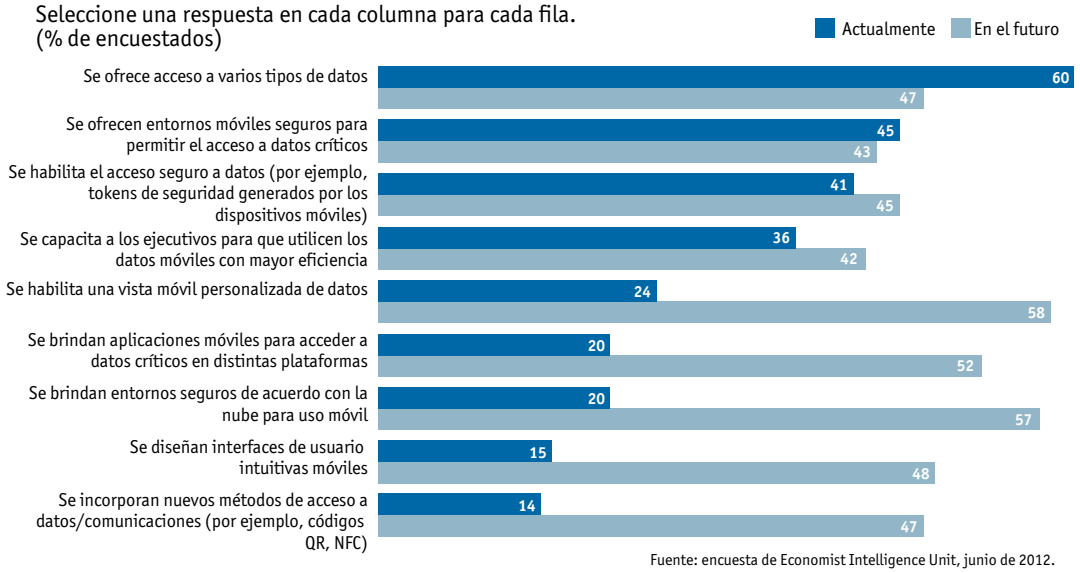
Curiosamente, a pesar de que el 42% de los encuestados dijeron que los altos cargos necesitan un acceso seguro y oportuno a los datos de planificación estratégica para ser más productivos, solamente el 28% cree adecuado que se pueda acceder a estos datos desde dispositivos móviles. Previsiblemente, el desafío principal es la preocupación con respecto a riesgos potenciales de seguridad y otros riesgos. No obstante, solamente el 11% de los encuestados sostienen que sus organizaciones no proporcionan acceso a datos críticos fuera de las oficinas. ■

4 ¿Cómo pueden las empresas asegurarse de tener políticas de movilidad eficaces?

Los encuestados reconocen claramente las ventajas de habilitar el acceso móvil a datos y son concientes de las inversiones que hacen falta. Algunas de las medidas que las empresas deben adoptar para asegurar el acceso a través de dispositivos móviles a los datos empresariales pueden implementarse a distancia. Actualmente, los gerentes de TI pueden agregar funciones de seguridad a computadoras portátiles, smartphones y tablets, generalmente por medio de las herramientas de administración existentes. También pueden separar los datos empresariales de los datos personales y duplicar y almacenar los datos comerciales en redes de la empresa. Los escritorios virtuales proporcionan acceso móvil seguro a los datos desde computadoras portátiles personales. Estas protecciones permiten a los trabajadores móviles recuperar fácilmente los datos de un dispositivo perdido o dañado. Según nuestros entrevistados ejecutivos, estas medidas permitirán en el futuro que una mayor cantidad de ejecutivos pueda acceder de manera segura a datos empresariales desde cualquier computadora.

Para los ejecutivos de nivel corporativo que viajan, dedicar menos tiempo a la actualización de protocolos de seguridad implica disponer de más tiempo para trabajar. En el futuro, la seguridad de los datos se verá reforzada con la ayuda de tecnologías de protección de datos incorporadas directamente en las aplicaciones, por lo que se

Atribuciones móviles
¿De qué maneras está habilitando actualmente su empresa el acceso a datos críticos y cómo puede cambiar esto en el futuro?
Seleccione una respuesta en cada columna para cada fila.
(% de encuestados)



Fuente: encuesta de Economist Intelligence Unit, junio de 2012.

dificultará la intercepción y el uso indebido de datos, sostuvo el Sr. Tikoo de CSC. “Las aplicaciones deberían ser capaces de reconocer si estoy trabajando en un iPad o en una pantalla pequeña de 5 pulgadas y mostrarme los datos en forma adecuada”.

El Sr.Raymond dice que aunque su empresa no lo requiere, es importante mantener entornos independientes de uso comercial y personal. Pero si no se aplican las políticas que los circundan ni otras medidas de seguridad, habrá consecuencias. El Sr. Raymond afirma que siempre se sorprende cuando habla con sus colegas acerca de hasta qué punto la seguridad de las grandes organizaciones es solo “trucos e ilusiones”. Las palabras están ahí, pero la aplicación no.

Ipsos, una empresa de investigaciones a nivel mundial, exige a los empleados hacer un curso de capacitación orientado a la seguridad que se imparte a través de la intranet de la empresa: un modo rentable de llegar al personal en 84 países. Mientras que el programa se desarrolló internamente, hay productos comerciales orientados a la seguridad que se pueden personalizar según las necesidades locales y que tienen disponibilidad inmediata a través de organismos como el Instituto de Seguridad Nacional (NSI, National Security Institute) de los Estados Unidos. También se exige a los empleados firmar una política de uso móvil aceptable que cubre todos los aspectos, desde el tipo de datos a los que pueden acceder desde un dispositivo móvil hasta reglas sobre el nivel de seguridad de las contraseñas.

Otras protecciones de seguridad requieren una actuación confiable de los usuarios. Mientras que los dispositivos móviles deben estar protegidos por contraseña, Coalfire, una empresa auditora y de cumplimiento, estima que actualmente solo la mitad de los dispositivos cumplen este requisito. Los empleados en un programa BYOD deben aceptar que si su dispositivo personal se pierde o es robado, la responsabilidad del departamento de TI incluye la eliminación remota de los datos almacenados en el dispositivo personal para proteger los datos empresariales.

Es evidente que hay mucho camino por recorrer en la mayoría de las organizaciones para educar al personal sobre los problemas de seguridad planteados por el acceso móvil a datos de la compañía. La encuesta indica que los ejecutivos fuera de Europa y América del Norte oponen más resistencia a las políticas de seguridad de datos en dispositivos personales . Sin embargo, en un mundo comercial cada vez más interconectado, las brechas de seguridad de una región pueden afectar a empresas que cumplen con las normas (y a sus clientes) en otros lugares. ■

5 Conclusión

No solamente se va a ampliar el acceso móvil a datos, sino que la tendencia es imparable. Ya se han introducido en el entorno comercial dispositivos que no están protegidos ni administrados, que ponen en peligro datos empresariales y abren la puerta a posibles ataques a través de dispositivos comprometidos. Casi un tercio de los encuestados informaron sobre políticas inadecuadas para dispositivos móviles en sus empresas. Establecer políticas factibles y razonables es el primer paso para lograr un programa viable de acceso móvil a datos.

Los ejecutivos que clasificaron como líderes del sector a sus políticas para dispositivos indican que ellos utilizan datos en movimiento para tomar decisiones más eficientes y conjuntas, evitar la pérdida de oportunidades y trabajar en forma más eficaz con partners y clientes. Para asegurar que este tipo de acceso no comprometa los datos comerciales, es posible que los ejecutivos deseen priorizar programas que mitigan riesgos y apoyar inversiones en servicios de seguridad y datos.

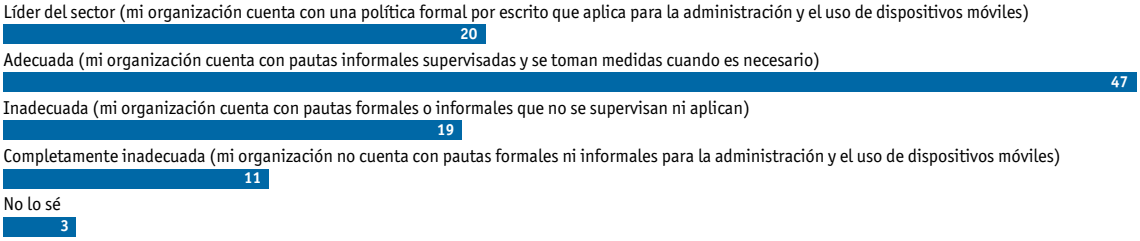
Los dispositivos conectados se están integrando cada vez más como parte de las empresas a nivel mundial. El tipo de dispositivos en uso está evolucionando, dentro de los cuales las tablets son los dispositivos modernos de preferencia. Podemos esperar un crecimiento significativo en el uso de tablets después del lanzamiento de los sistemas operativos de software de próxima generación, que permitirán a las tablets opciones de acceso a datos más amplias que las de los smartphones. Los analistas consideran que esto tendrá sus pros y sus contras ya que el uso de tablets será complementario de los sistemas existentes y no su reemplazo.

En el futuro, la seguridad de los datos de mayor importancia puede implicar la creación de requisitos de acceso aún más estrictos. El cambio hacia el uso de tablets para negocios fuera de la oficina, por ejemplo, abrirá todo un conjunto nuevo de desafíos porque alentará a los ejecutivos a buscar acceso móvil para un rango de datos más amplio. Esto requerirá que muchas empresas den una nueva mirada al asunto,desde los dispositivos y sus puntos débiles hasta la infraestructura disponible e inclusive los usuarios mismos. ■

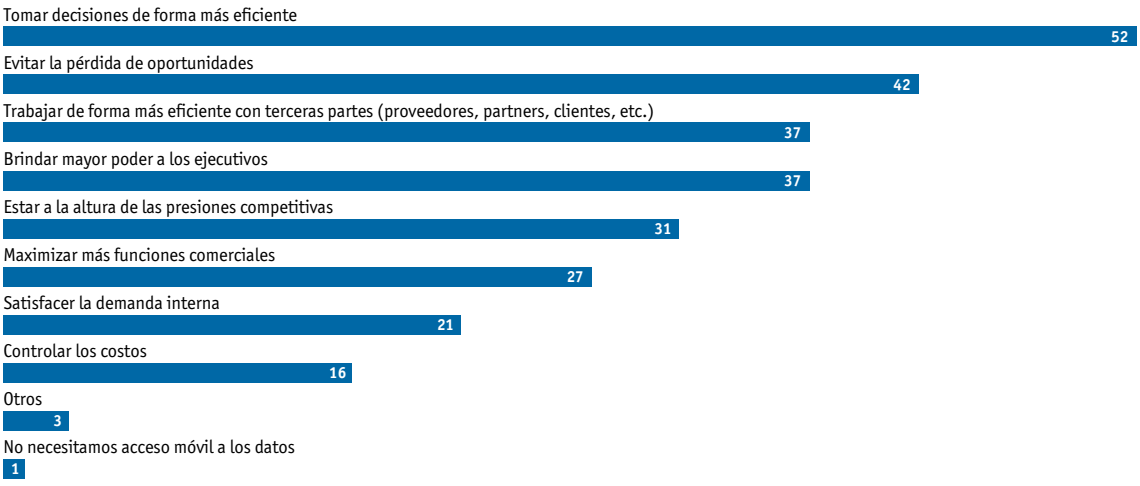
Apéndice: resultados de la encuesta

Es posible que los porcentajes no sumen 100% debido al redondeo o a la capacidad de los encuestados de elegir varias respuestas.

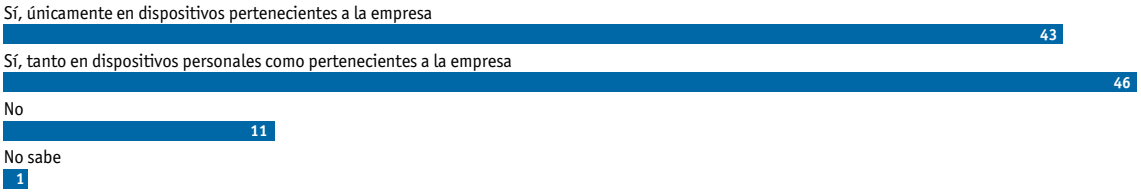
Según sus observaciones, ¿cómo se compara la política para dispositivos móviles de su organización con la de los competidores dentro de su sector?
(% de encuestados)



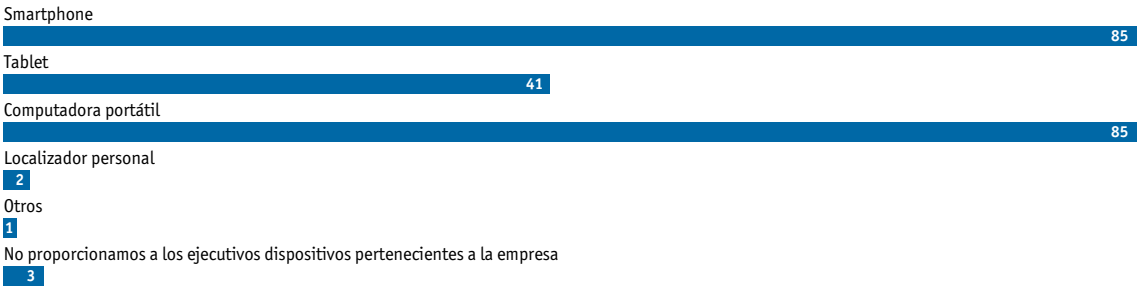
¿Qué factores comerciales principales están impulsando la necesidad de acceso a los datos críticos desde dispositivos móviles?
Seleccione hasta tres opciones.
(% de encuestados)



¿Su organización permite el acceso a datos importantes fuera de las oficinas?
(% de encuestados)

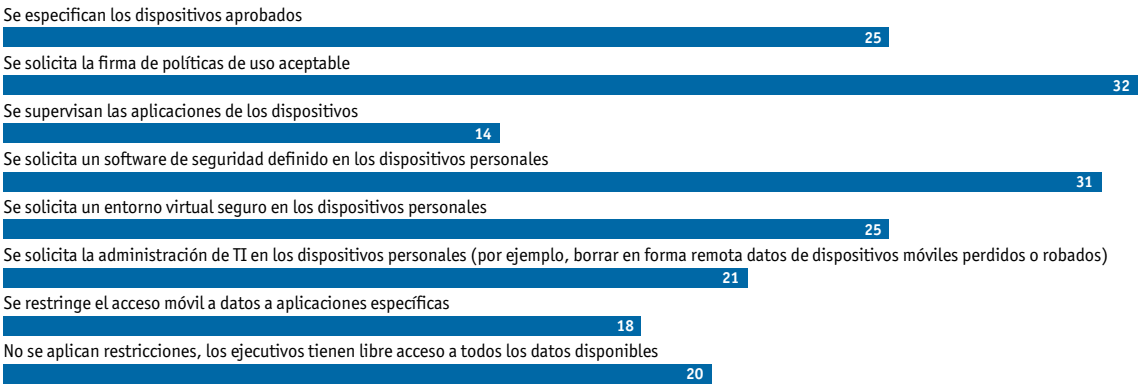


¿Qué dispositivos proporciona su organización a los ejecutivos para acceder a los datos críticos?
Seleccione todo lo que corresponda.
(% de encuestados)

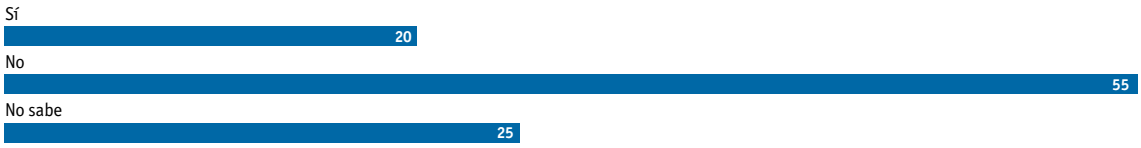


¿Su organización le permite a los ejecutivos traer su propio dispositivo (BYOD) y utilizarlos en lugar de usar dispositivos pertenecientes a la empresa para acceder a datos críticos?
(% de encuestados)

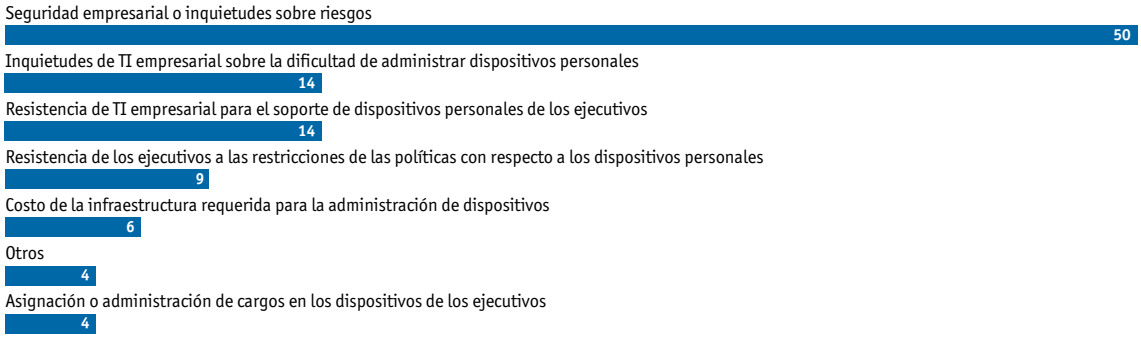
¿Cómo ha implementado BYOD su organización para acceder a los datos críticos?
Seleccione todo lo que corresponda.
(% de encuestados)



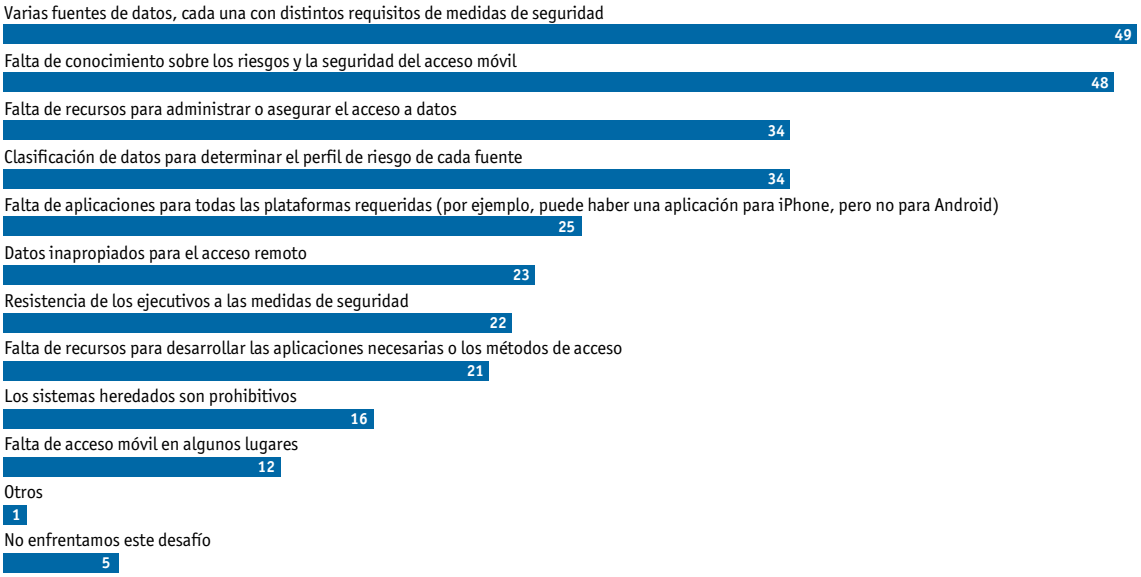
¿Su organización planea implementar BYOD para acceder a los datos críticos?
(% de encuestados)



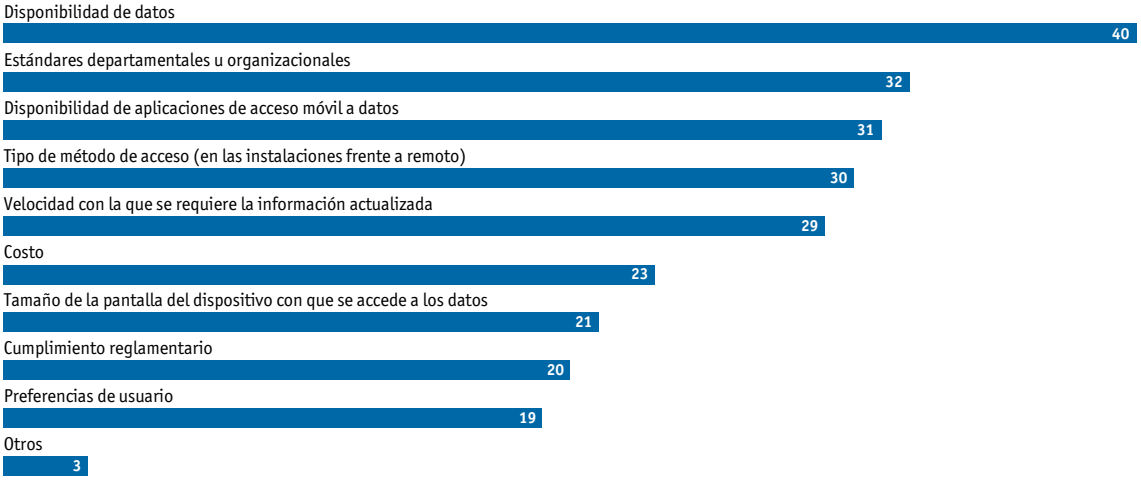
¿Cuál opción percibe como el mayor obstáculo para la implementación de BYOD para acceder a los datos críticos?
(% de encuestados)



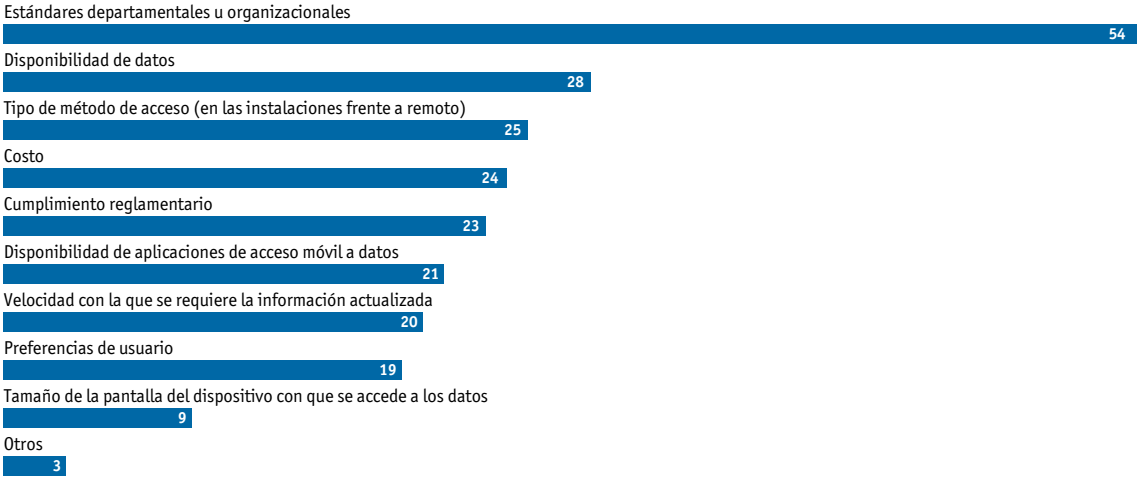
En su opinión, ¿cuáles son los mayores desafíos que enfrenta su empresa para asegurar el acceso a datos críticos desde dispositivos móviles, ya sean de propiedad de la empresa o de los ejecutivos?
Seleccione hasta cuatro opciones.
(% de encuestados)



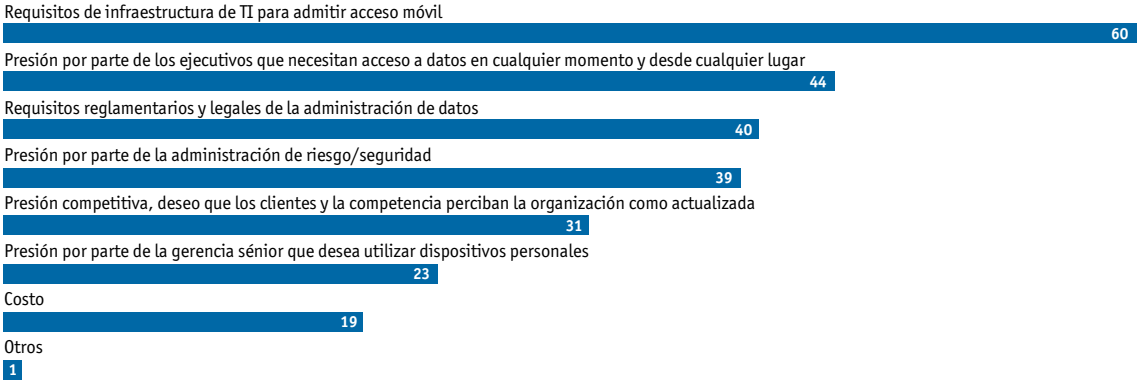
Además de su cargo, ¿qué factores determinan qué datos están o estarán disponibles para el acceso móvil?
Seleccione hasta tres opciones.
(% de encuestados)



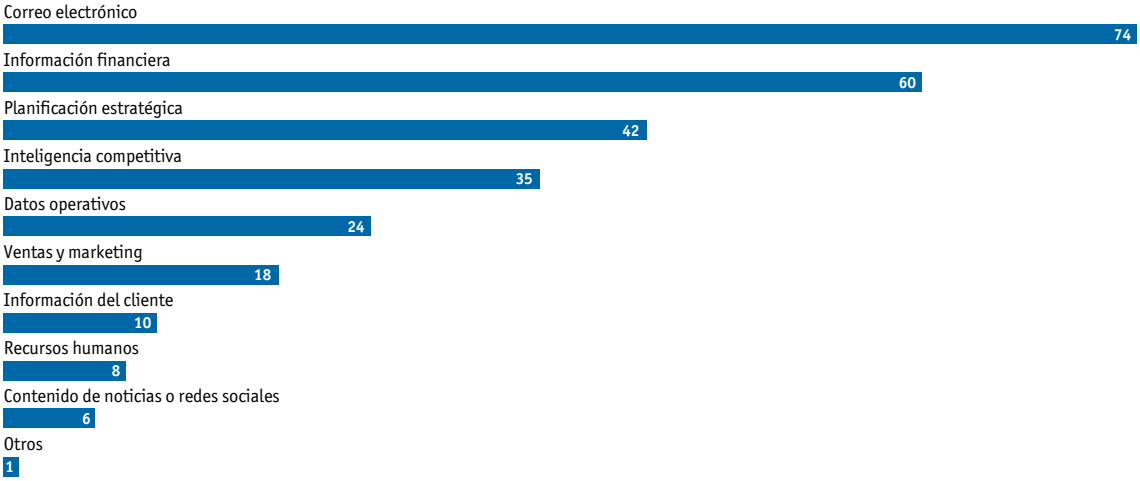
¿Qué factores determinan a qué usuarios se les permite o permitirá acceso a datos críticos en dispositivos móviles?
Seleccione hasta tres opciones.
(% de encuestados)



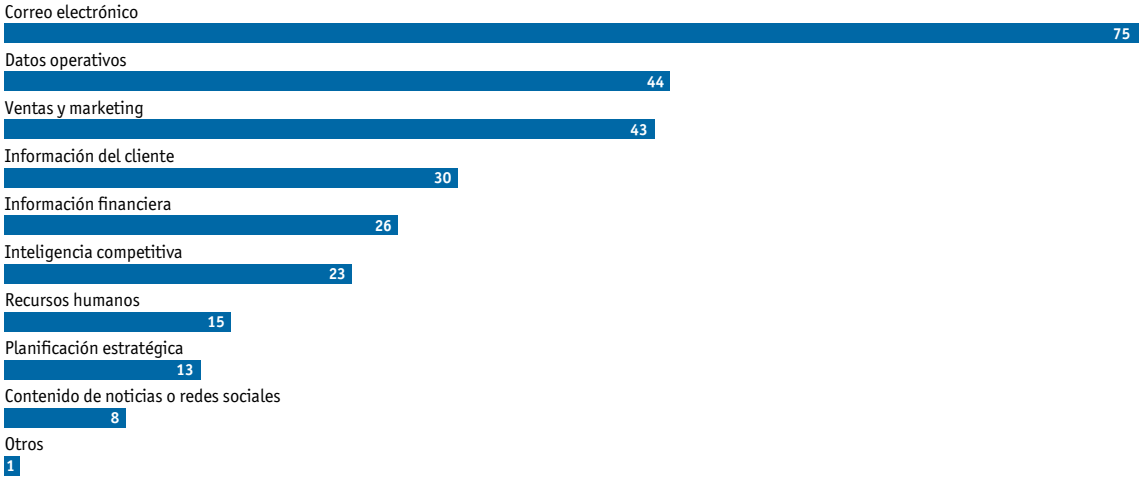
¿Cuáles son las influencias más importantes de los enfoques y políticas de la empresa para la creación de una estrategia para aplicaciones y dispositivos móviles?
Seleccione hasta tres opciones.
(% de encuestados)



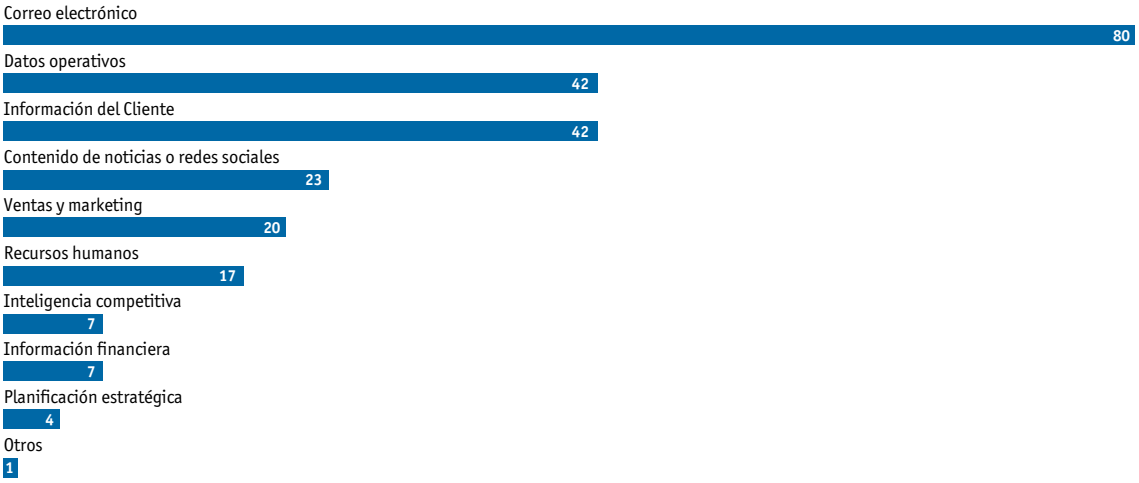
¿Cuál de los tipos de información que se enumeran debe distribuirse en forma segura y oportuna para que las siguientes funciones sean más productivas?
—Ejecutivos de nivel corporativo
Seleccione hasta tres para cada función.
(% de encuestados)



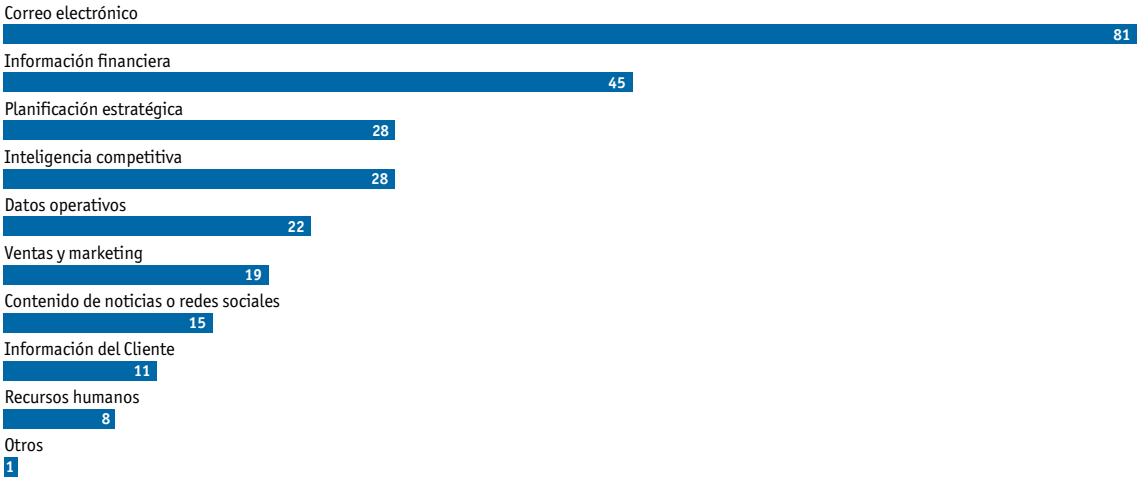
¿Cuál de los tipos de información que se enumeran debe distribuirse en forma segura y oportuna para que las siguientes funciones sean más productivas?
—Gerentes comerciales
Seleccione hasta tres para cada función.
(% de encuestados)



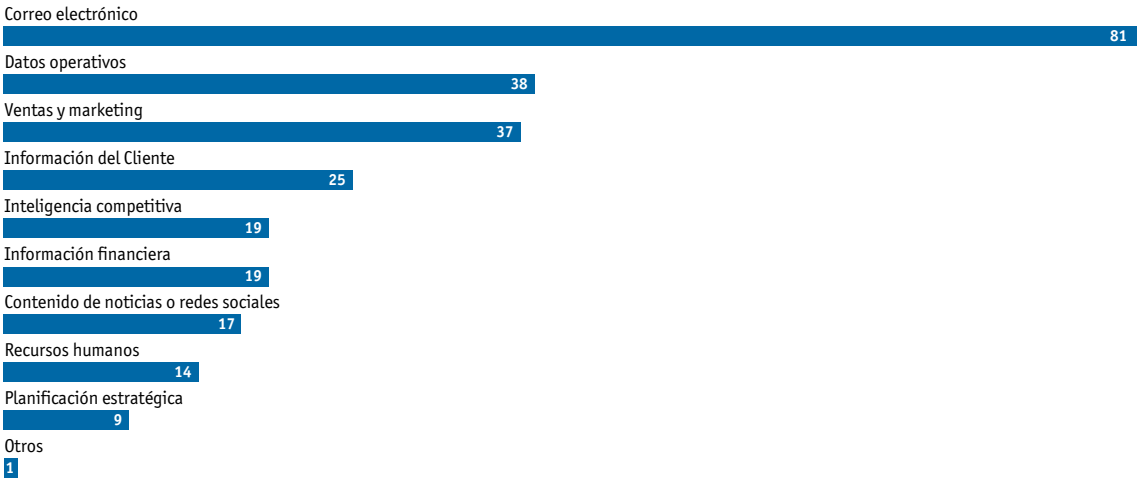
¿Cuál de los tipos de información que se enumeran debe distribuirse en forma segura y oportuna para que las siguientes funciones sean más productivas?
—Empleados
Seleccione hasta tres para cada función.
(% de encuestados)



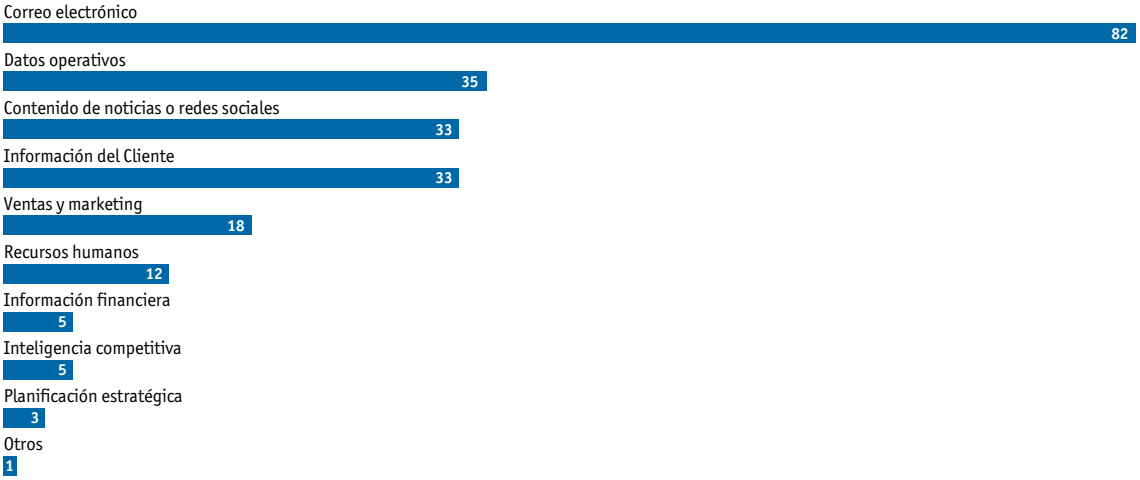
¿Cuáles de los siguientes tipos de información o medios son adecuados para el acceso en dispositivos móviles? —Ejecutivos de nivel corporativo
Seleccione hasta tres para cada función.
(% de encuestados)



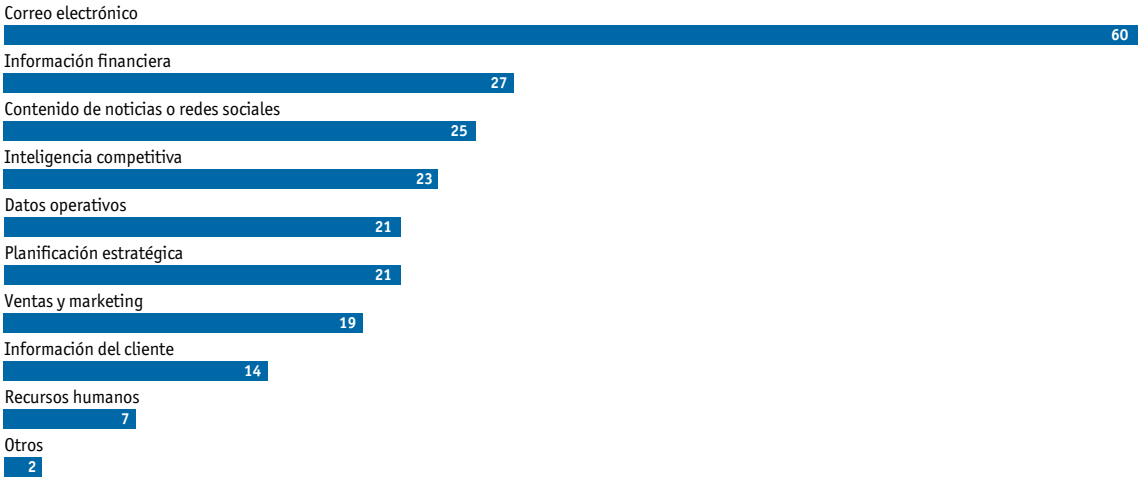
¿Cuáles de los siguientes tipos de información o medios son adecuados para el acceso en dispositivos móviles? —Gerentes comerciales
Seleccione hasta tres para cada función.
(% de encuestados)



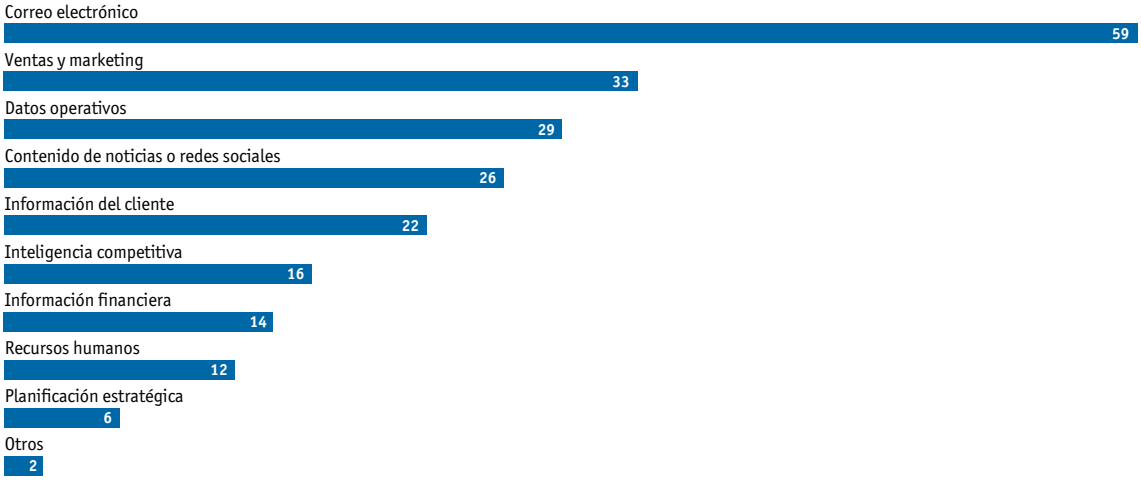
¿Cuáles de los siguientes tipos de información o medios son adecuados para el acceso en dispositivos móviles?
—Empleados
Seleccione hasta tres para cada función.
(% de encuestados)



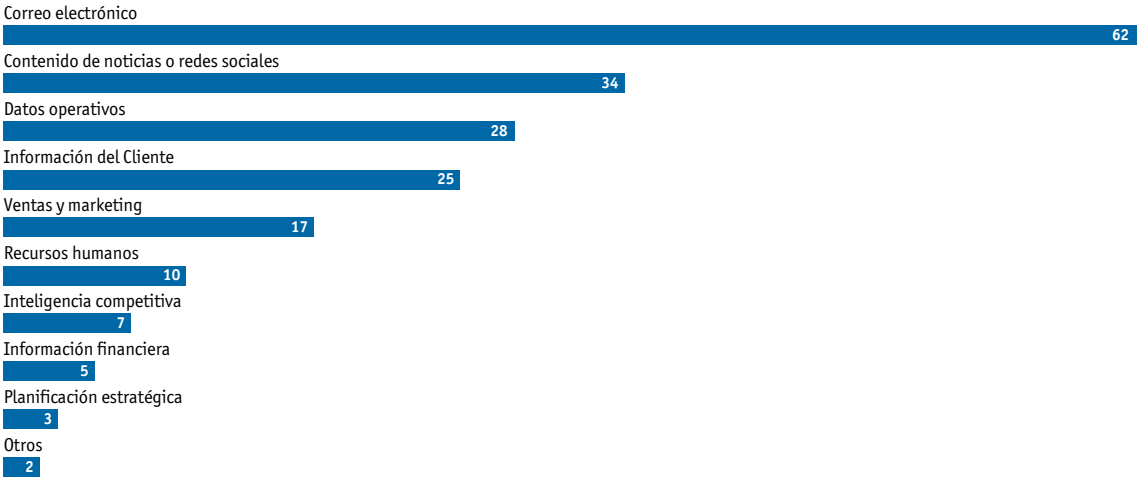
¿Cuáles de los siguientes tipos de información o medios son adecuados para el acceso en dispositivos móviles desde el almacenamiento en la nube?
—Ejecutivos de nivel corporativo
Seleccione hasta tres para cada función.
(% de encuestados)



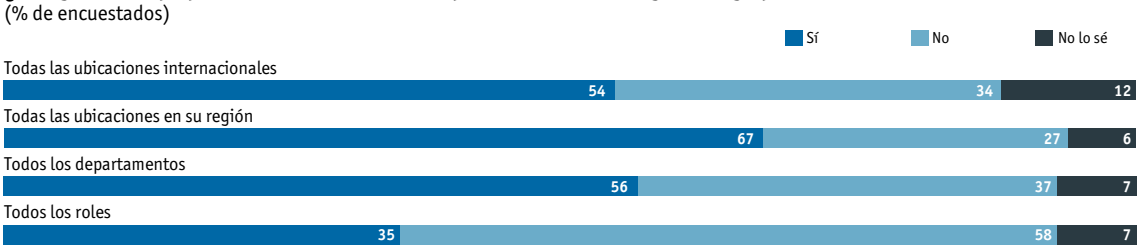
¿Cuáles de los siguientes tipos de información o medios son adecuados para el acceso en dispositivos móviles desde el almacenamiento en la nube?
—Gerentes comerciales
Seleccione hasta tres para cada función.
(% de encuestados)



¿Cuáles de los siguientes tipos de información o medios son adecuados para el acceso en dispositivos móviles desde el almacenamiento en la nube?
—Empleados
Seleccione hasta tres para cada función.
(% de encuestados)



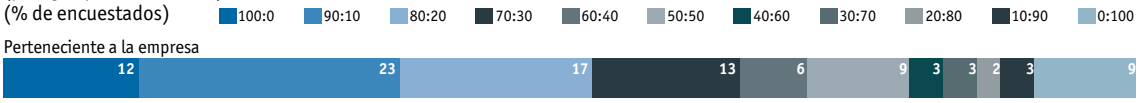
¿Su organización proporciona acceso móvil a datos para cada uno de los siguientes grupos?
(% de encuestados)



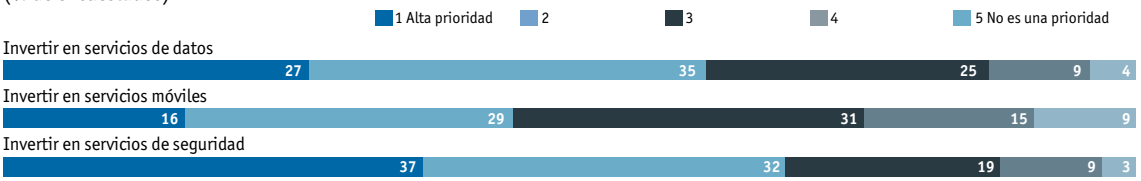
¿Su organización tiene políticas implementadas para el uso aceptable de redes sociales (por ejemplo, Facebook, Twitter) en dispositivos corporativos?
(% de encuestados)

¿Qué políticas enfrenta su organización sobre el uso de redes sociales en dispositivos corporativos?
(% de encuestados)

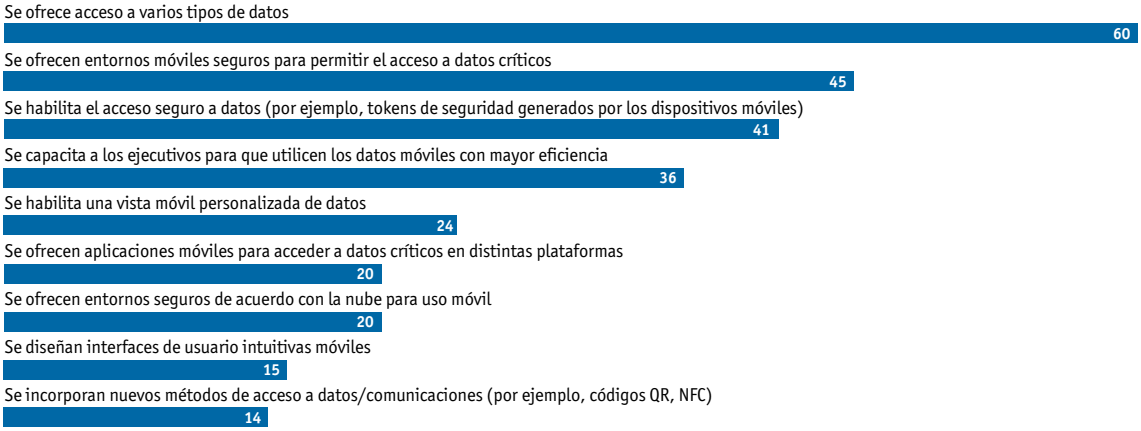
¿Cuál es la proporción de tiempo que dedica a su organización en dispositivos móviles pertenecientes a la empresa frente a dispositivos personales?
Arrastre el botón deslizante para seleccionar una división de porcentajes relevante que refleje cómo debe ponderarse cada opción (por ejemplo, 60% a 40%).
(% de encuestados)



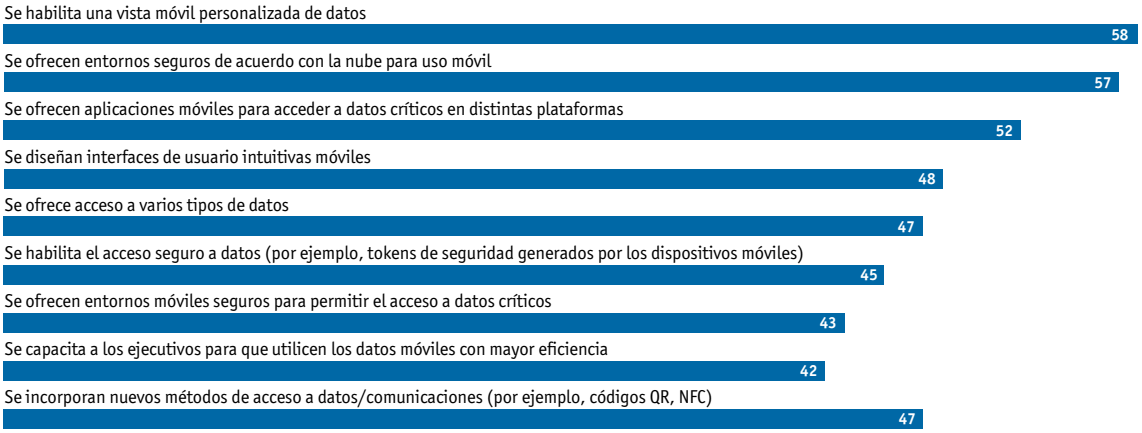
¿Qué tipo de prioridad otorga su organización a las siguientes estrategias?
Califique con una escala de 1 a 5, donde 1 significa alta prioridad y 5 no es una prioridad.
(% de encuestados)



¿De qué maneras está habilitando actualmente su empresa el acceso a datos críticos y cómo puede cambiar esto en el futuro? —Actualmente
Seleccione una respuesta en cada columna para cada fila.
(% de encuestados)



¿De qué maneras está habilitando actualmente su empresa el acceso a datos críticos y cómo puede cambiar esto en el futuro? —En el futuro
Seleccione una respuesta en cada columna para cada fila.
(% de encuestados)



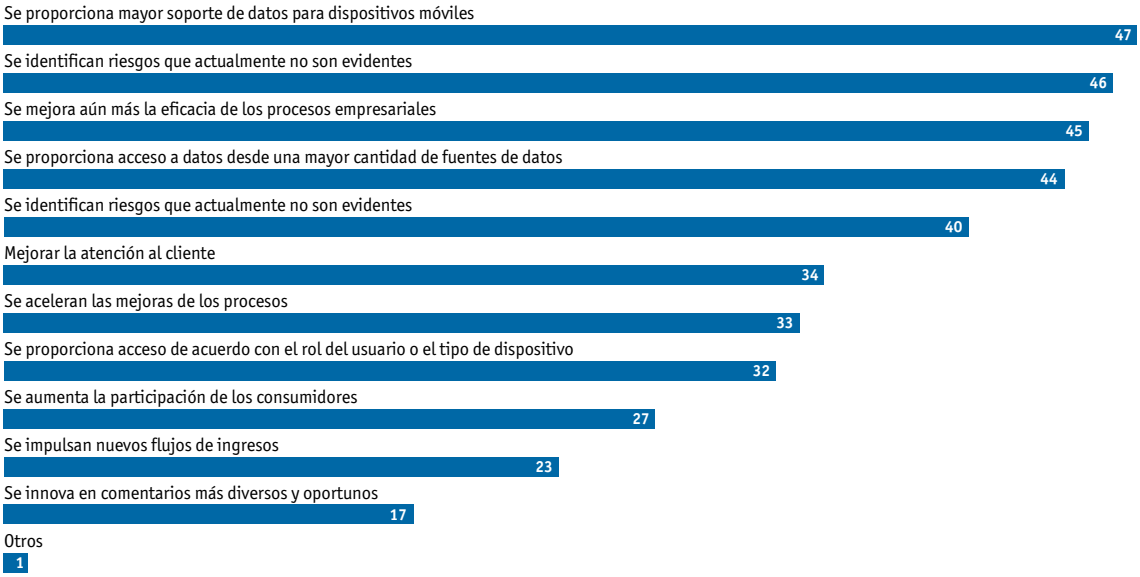
¿Cuál es la proporción de datos críticos a los que accede actualmente a través de canales móviles?
El total debe ser del 100%.

	Promedio
Acceso móvil a través de smartphone	26,9
Acceso móvil a través de otros dispositivos (por ej., tablet)	21,7
Acceso por medios no móviles	59,8

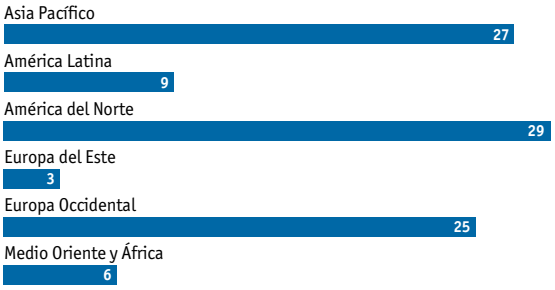
¿Cuál será la proporción de datos críticos a los que accederá a través de canales móviles dentro de 12 a 18 meses?
El total debe ser del 100%.

	Promedio
Acceso móvil a través de smartphone	34,5
Acceso móvil a través de otros dispositivos (por ej., tablet)	30,2
Acceso por medios no móviles	42,8

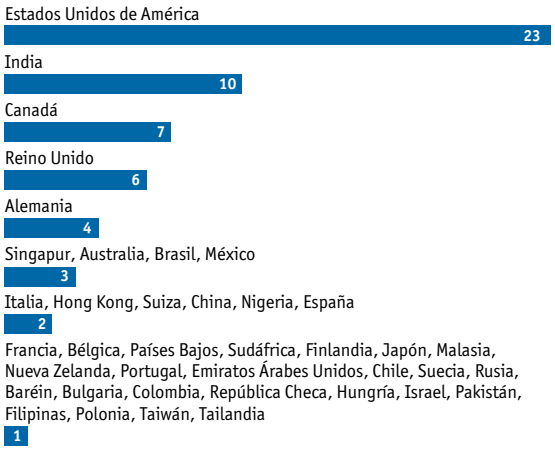
Qué espera hacer su organización en los próximos 12 a 18 meses con respecto al acceso a datos críticos que no pueda hacer actualmente?
Seleccione todo lo que corresponda.
(% de encuestados)



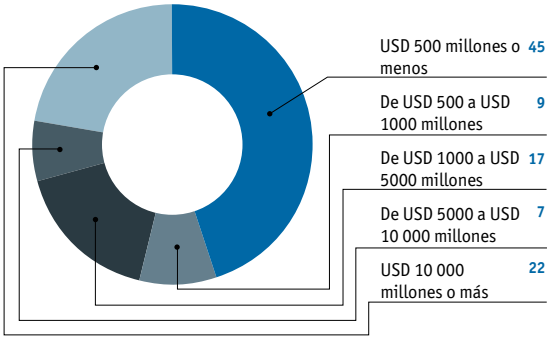
¿En qué región se encuentra?
(% de encuestados)



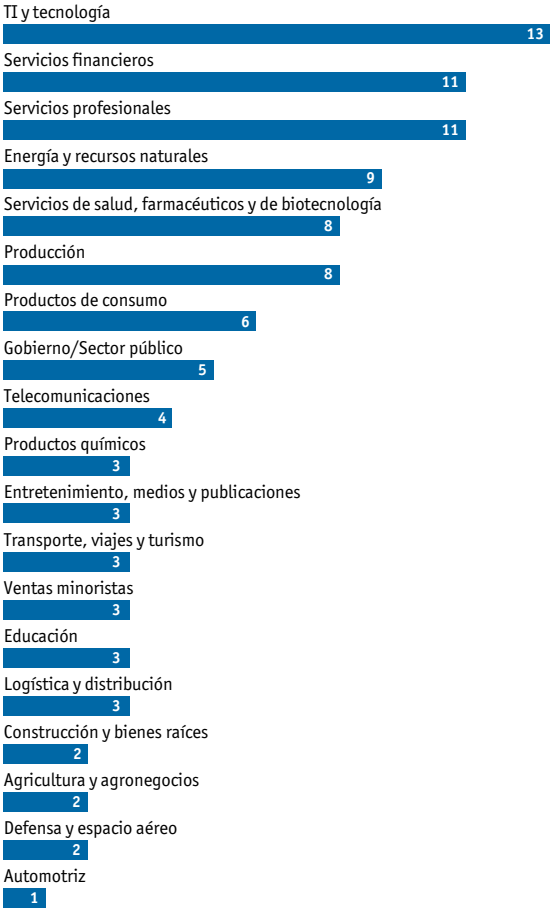
¿En qué país se encuentra?
(% de encuestados)



¿Cuál es el ingreso anual mundial de su organización en dólares estadounidenses?
(% de encuestados)



¿Cuál es su sector principal?
(% de encuestados)



¿Cuál de las siguientes opciones describe mejor su cargo?
(% de encuestados)

¿Cuál es su función principal?
(% de encuestados)

Se tomaron todas las medidas para verificar la precisión de esta información, sin embargo, ni The Economist Intelligence Unit Ltd. ni el patrocinador de este informe podrán aceptar responsabilidad legal por la información, opiniones o conclusiones establecidas en este informe técnico y su uso por parte de terceros.

Portada: Shutterstock

Londres
26 Red Lion Square
Londres
WC1R 4HQ
Reino Unido
Tel.: (44.20) 7576 8000
Fax: (44.20) 7576 8476
Correo electrónico:
london@eiu.com

Nueva York
750 Third Avenue
5th Floor
Nueva York, NY 10017
Estados Unidos
Tel.: (1.212) 554 0600
Fax: (1.212) 586 0248
Correo electrónico:
newyork@eiu.com

Hong Kong
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel.: (852) 2585 3888
Fax: (852) 2802 7638
Correo electrónico:
hongkong@eiu.com

Ginebra
Boulevard des
Tranchées 16
1206 Ginebra
Suiza
Tel.: (41) 22 566 2470
Fax: (41) 22 346 93 47
Correo electrónico:
geneva@eiu.com