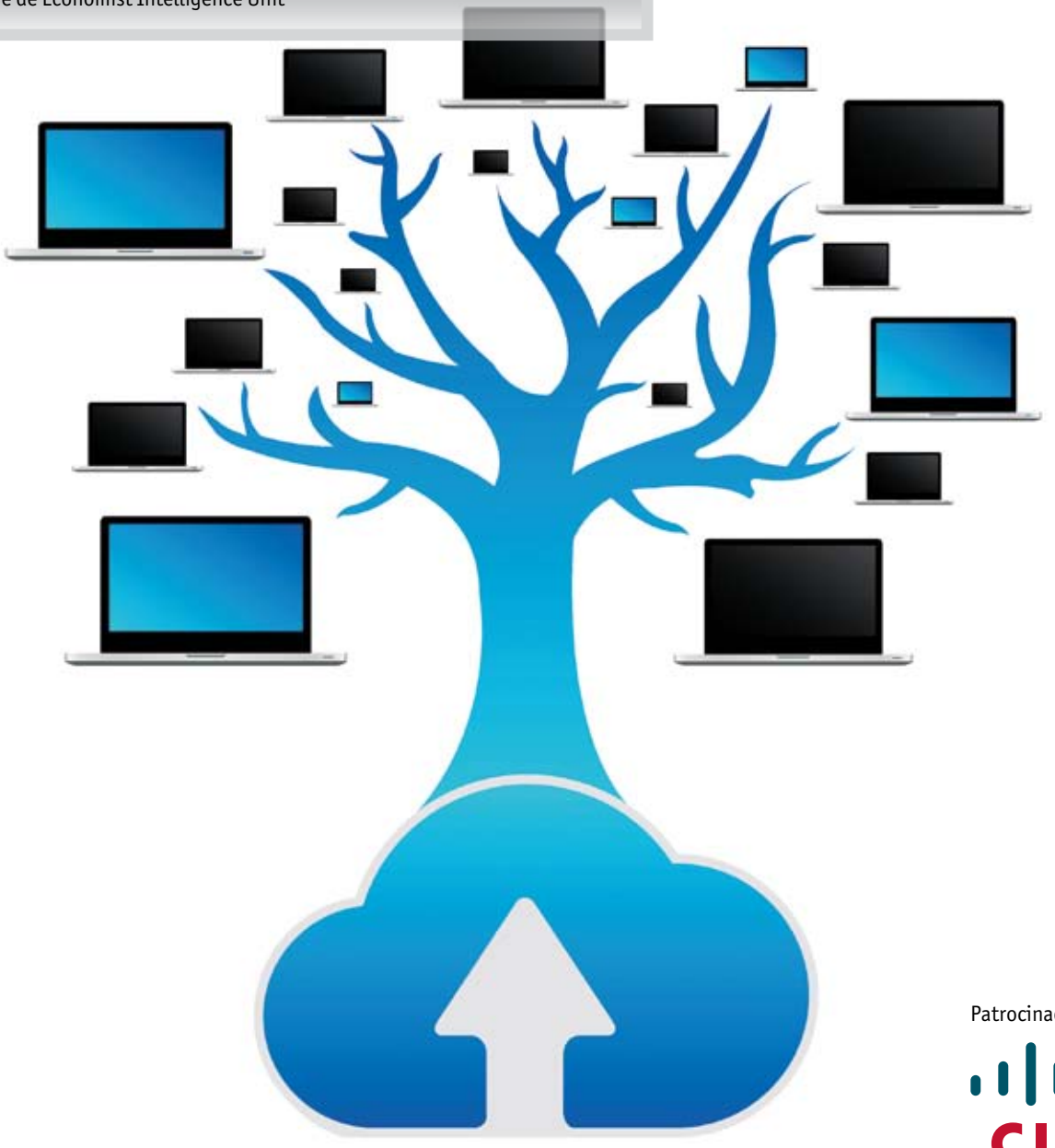
Economist Intelligence Unit

The Economist

Acceso seguro a los datos en un universo móvil

Un informe de Economist Intelligence Unit



Patrocinado por

CISCO

Índice

Prólogo

Las empresas deben reaccionar ante el uso cada vez más frecuente de dispositivos personales en el lugar de trabajo y la necesidad de maximizar la productividad de los ejecutivos y empleados con movilidad. El artículo *Acceso seguro a los datos en un universo móvil* analiza cómo las compañías pueden adaptarse a las crecientes demandas de acceso móvil a la información empresarial a la vez que se minimizan los riesgos para la seguridad de los datos. Como base para el estudio, el Economist Intelligence Unit realizó una encuesta global a 578 ejecutivos sénior en junio de 2012. La encuesta profundiza en el modo en el que las organizaciones están (o deberían estar) respondiendo ante los retos actuales y emergentes que surgen de una imparable tendencia hacia la iniciativa "trae tu propio dispositivo" (BYOD), así como el aumento generalizado de la movilidad de los trabajadores. También se realizó una serie de entrevistas en profundidad. Los resultados y opiniones que se incluyen en este informe no son necesariamente un reflejo del punto de vista del patrocinador. El autor es Lynn Greiner. Michael Singer y Justine Thody son los editores, y Mike Kenny se encargó de la maquetación. Queremos mostrar nuestro agradecimiento a todos los ejecutivos que participaron en la encuesta y las entrevistas, incluidos aquellos que nos proporcionaron la información de forma anónima, por prestarnos su valioso tiempo y su orientación.

Entrevistados

Lucy Burrow, Directora de administración de TI, King's College London

Mike Cordy, Director de tecnología global, OnX Enterprise Solutions

Steve Ellis, Vicepresidente ejecutivo, Wells Fargo

Jay Leek, Responsable de seguridad de la información, Blackstone Group

Arturo Medina, Director de tecnología de la información, Ipsos México

Bill Murphy, Director de tecnología, Blackstone Group

Al Raymond, Vicepresidente, Aramark

Ashwani Tikoo, Director de informática, CSC India

Resumen ejecutivo

A finales de la década de 1990, surgieron los primeros portátiles y dispositivos móviles que permitieron a los ejecutivos seguir siendo productivos fuera de sus oficinas. Dispositivos como el ThinkPad de IBM y la BlackBerry de RIM marcaron una nueva era de equipos móviles multifunción que en seguida captaron la atención de los ejecutivos de nivel jerárquico. Actualmente, el número de trabajadores móviles ha aumentado considerablemente y se espera que alcance los 1300 millones, o casi el 38% de la fuerza total de trabajo, para el año 2015, según un informe de la firma de investigación tecnológica IDC. Según algunas estimaciones, el 76% de las compañías ha implementado alguna política sobre la iniciativa "trae tu propio dispositivo" (BYOD), lo que les obliga a aplicar medidas de seguridad en dispositivos que no son de su propiedad. La mayoría de estas firmas asegura permitir a sus empleados el uso de sus dispositivos personales con el fin de tomar decisiones más eficaces, evitar la pérdida de oportunidades y trabajar de un modo más eficiente con partners y clientes; precisamente las mismas razones que impulsan a las compañías a permitir el acceso móvil a los datos con los dispositivos corporativos.

En junio de 2012, el Economist Intelligence Unit realizó una encuesta global, patrocinada por Cisco, entre 578 ejecutivos sénior con el fin de conocer su punto de vista con respecto a la seguridad del acceso a los datos con dispositivos móviles. A continuación mostramos los principales resultados:

¿Quién realizó la encuesta?

Respondieron a la encuesta 578 ejecutivos sénior de todo el mundo. Los encuestados se encontraban principalmente en las regiones de América del Norte (29%), Europa Occidental (25%) y Asia-Pacífico (27%), y el resto se repartía entre Oriente Medio y África, y Europa del Este. Del número total de encuestados, el 23% procede de EE. UU., el 10% de la India, el 7% de Canadá y el 6% del Reino Unido. En cuanto a los cargos, el 27% tiene nivel de CEO, el 17% nivel de vicepresidente sénior y el 15% nivel de gerente. Por lo que respecta al tamaño de las organizaciones, el 55% pertenece a compañías con ingresos anuales superiores a los 500 millones de dólares y el 22% a empresas con ingresos por encima de los 10 000 millones de dólares. Los participantes en la encuesta representan una amplia variedad de sectores, especialmente los de TI y tecnología (13%), servicios financieros (11%), servicios profesionales (11%) y energía y recursos naturales (9%). Desde el punto de vista de sus funciones, los encuestados identificaron sus roles principales como dirección general, desarrollo empresarial, finanzas, y ventas y marketing. ■

- **La mayoría de los ejecutivos muestra preocupación por las políticas de acceso móvil a los datos de su compañía.** A pesar de que el 42% de los encuestados manifestó que los ejecutivos de nivel C necesitan un acceso seguro y a su debido tiempo a los datos de planificación estratégica para aumentar su productividad, solo el 28% considera que es adecuado que los datos sean accesibles a través de dispositivos móviles. Cerca de la mitad de los encuestados (49%) coincide al señalar que la complejidad que supone proteger varias fuentes de datos y la falta de conocimientos sobre la seguridad y los riesgos del acceso móvil (48%) son los principales retos que afronta su compañía.

- **Las compañías de mayor tamaño están más abiertas a permitir el acceso móvil a los datos críticos, pero también aplican reglas más estrictas.** Más del 90% de las compañías con ingresos por encima de los 1000 millones de dólares anuales permite el acceso a los datos a través de dispositivos personales o corporativos. No obstante, más de la mitad de las organizaciones con ingresos superiores a 5000 millones de dólares solo permite el acceso con dispositivos de la compañía, mientras que una tercera parte permite el uso de dispositivos personales para el mismo fin. Por el contrario, solo el 37% de las compañías con ingresos por debajo de los 500 millones de dólares insiste en utilizar exclusivamente dispositivos corporativos, mientras que el 47% permite el acceso a los datos también con dispositivos personales. Los usuarios móviles pertenecientes a las compañías de mayor tamaño, sin embargo, deben limitarse al uso de los dispositivos aprobados y firmar varias políticas.

- **Las políticas sobre acceso móvil no pueden dejar de lado las redes sociales.** Mientras que el 56% de los participantes en la encuesta cuenta con políticas para el uso aceptable de las redes sociales con dispositivos móviles, el 33% de los ejecutivos encuestados no está autorizado a hablar sobre su trabajo en las plataformas de redes sociales. La aplicación de políticas que regulen el uso de las redes sociales puede facilitar la eficiencia en las interacciones a la vez que se protegen los datos corporativos y se evitan responsabilidades.

- **La infraestructura existente es el factor que más influye en las políticas corporativas que regulan el acceso móvil.** Aunque el 44% de los encuestados indica que las presiones de los ejecutivos son una de las mayores influencias en la aplicación de políticas, no es nada comparado con el 60% que menciona los requisitos de la infraestructura de TI. Estos resultados muestran que existe una buena oportunidad para las compañías que ofrecen servicios para la seguridad y la administración del acceso móvil.

¿Es la tendencia del acceso móvil a los datos imparable? La respuesta es sí; la aparición de dispositivos más sofisticados que ofrecen una mejor experiencia al usuario acelera aún más la tendencia. Por consiguiente, el uso de políticas no es una opción, sino una obligación. Según la opinión de los ejecutivos entrevistados en este estudio, si se involucra a los empleados en la creación de las políticas, aumentan las posibilidades de que las cumplan. ■

Introducción

La adopción de las políticas adecuadas para el acceso móvil a los datos se está convirtiendo en una creciente preocupación para muchas compañías. Tanto los empleados veteranos como los más jóvenes demandan acceso a los datos corporativos desde cualquier lugar, en cualquier momento y a través de dispositivos fijos o móviles. Muchas compañías se están dando cuenta de que la aplicación de políticas sobre el uso de dispositivos móviles puede reportarles beneficios en forma de un mayor compromiso y un aumento de la productividad, incluida una mayor predisposición a responder fuera del horario de trabajo. Los lugares de trabajo que adoptan iniciativas BYOD son más propensos a atraer trabajadores duchos en tecnología, lo que suele estimular la innovación.

A medida que aumenta el número de dispositivos y la línea entre la TI de consumo y empresarial sigue difuminándose, surgirán nuevos retos a los que deben enfrentarse las compañías con el fin de adaptarse a este cambio cultural.

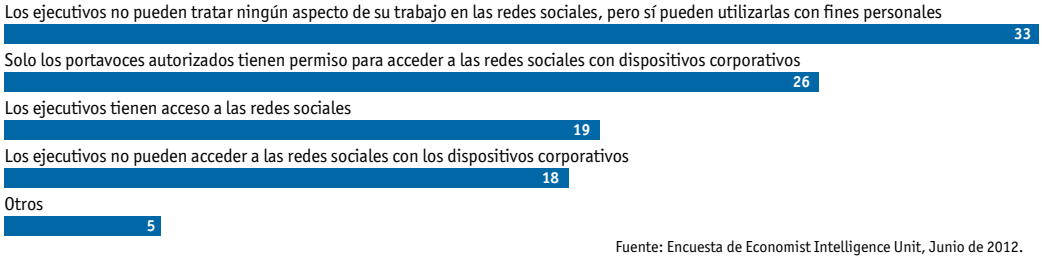
La ampliación del ámbito de acceso a los datos empresariales presenta riesgos evidentes para la empresa, además de nuevos desafíos tecnológicos. Los dispositivos portátiles pueden perderse o ser robados. Es posible que los usuarios compartan sus dispositivos con familiares y amigos, lo que aumenta el riesgo de pérdida de datos confidenciales. A menudo, aplicaciones de software no autorizadas por la compañía tienen acceso a estos datos. Sin embargo los esfuerzos de los departamentos de TI por controlar los dispositivos que los empleados traen al lugar de trabajo o el modo en el que utilizan los dispositivos fuera de la oficina resultan cada vez más inútiles. Deben responder a una mayor vulnerabilidad de las redes de datos corporativos aplicando mecanismos de seguridad eficaces, tanto para proteger los datos empresariales críticos como para cumplir con la normativa aplicable en cada región donde opera la compañía. ■

1 Movilidad actual: ¿en qué punto nos encontramos?

Se vendieron cerca de mil millones de dispositivos inteligentes conectados en todo el mundo en 2011 y se prevé que esa cifra se duplique para el año 2016, según un informe de la firma de investigación tecnológica IDC. Estos dispositivos incluyen productos basados en PC, como portátiles y netbooks, teléfonos móviles y tablets. La encuesta de Economist Intelligence Unit demostró que muchas personas utilizan varios dispositivos, que en la mayoría de los casos es una combinación de portátil y smartphone, aunque el uso de tablets está creciendo a un ritmo vertiginoso. Las ventas de tablets en todo el mundo crecieron en un 33,6% en el segundo trimestre de 2012 con respecto al primer trimestre del mismo año y en un 66,2% en comparación con el mismo trimestre de 2011, según las estimaciones de IDC. Se prevé un importante crecimiento en el uso de tablets tras el lanzamiento de los sistemas operativos de software de próxima generación. Las funciones de colaboración y comunicación que se incluirán en los nuevos tablets resultarán muy atractivas para los ejecutivos, que dispondrán así de una gama más amplia de opciones de acceso que con los smartphones.

La posibilidad de que los ejecutivos accedan a la información desde sus dispositivos móviles cuando no están en la oficina los ayuda a tomar decisiones fundamentadas con rapidez, especialmente en momentos clave, como negociaciones, según palabras de Ashwani Tikoo, Director de informática de CSC India, empresa proveedora de servicios de TI. En el segundo mayor centro de operaciones de CSC, Ashwani Tikoo es responsable de las políticas de seguridad para la protección de los datos empresariales en dispositivos móviles. La disponibilidad instantánea de los datos permite al personal de ventas tomar las decisiones correctas de inmediato, sin hacer esperar a los clientes, afirma. Para evitar la pérdida de datos, las políticas de seguridad de CSC requieren el cifrado de los datos en todos los dispositivos móviles, incluidos

Políticas sobre el uso móvil de redes sociales para ejecutivos
¿Qué políticas sobre el uso de redes sociales con dispositivos corporativos aplica su empresa? (Porcentaje de encuestados)



Fuente: Encuesta de Economist Intelligence Unit, Junio de 2012.

CASO PRÁCTICO Ipsos, un enfoque híbrido

En regiones como América Latina, donde se prefiere el cara a cara en las actividades de estudio de mercado, smartphones y tablets están sustituyendo al lápiz y el papel como las herramientas preferidas para realizar encuestas. Ipsos, firma internacional de estudios de mercado, ha adoptado esta tendencia hacia el uso de dispositivos móviles en sus operaciones en México y el resto de países donde desarrolla su actividad. La compañía opera actualmente en 84 países y cuenta con 16 000 empleados a tiempo completo. Sus estudios emplean diversas metodologías, tanto actividades online como en persona, y alcanzan más de 70 millones de encuestados al año en todo el mundo.

Actualmente, Ipsos proporciona a sus encuestados dispositivos portátiles de la compañía, pero está estudiando un nuevo enfoque, comenta Arturo Medina, Director de TI de Ipsos México. "Dado que el coste de los dispositivos móviles personalizados es bastante alto, estamos adoptando un modelo híbrido de políticas 'trae tu propio dispositivo'", añade.

En el modelo híbrido que están desarrollando, se pide a los encuestados que elijan entre tres modelos de smartphone en los que Ipsos sabe que se puede ejecutar su software de entrevistas. Los empleados pagan sus dispositivos mediante deducciones incrementales del sueldo. Según Arturo Medina, en circunstancias normales los empleados pagan el dispositivo en 2 o 3 semanas.

Ipsos proporciona una conexión VPN a los datos corporativos y el empleado debe pagar por el resto de funciones del smartphone. La administración de los dispositivos es responsabilidad de Ipsos, de modo que puede eliminar la información empresarial de forma remota si lo cree necesario. Los datos a los que se accede con el smartphone están cifrados, evitando así las pérdidas. Los entrevistados deben además adherirse a las políticas corporativas de uso. Los participantes en las entrevistas tienen la flexibilidad de utilizar un dispositivo en cualquier lugar, menciona Arturo Medina, pero la compañía cuenta con control suficiente para proteger el acceso a sus datos. ■

los dispositivos personales cubiertos por la política BYOD.

Otra estrategia consiste en evitar que los datos se almacenen en un dispositivo móvil. Al Raymond, Vicepresidente responsable de la privacidad y la administración de registros de Aramark, proveedor de servicios de alimentación estadounidense, explica que los usuarios autorizados que necesitan acceder a la información corporativa de forma remota lo hacen a través de una red privada virtual (VPN) segura desde sus portátiles o dispositivos móviles. Ningún dato, salvo el correo electrónico, se almacena en el dispositivo, de modo que resulta muy sencillo proteger los datos corporativos en caso de que el empleado deje la empresa o pierda el dispositivo.

Similares son los desafíos que surgen alrededor del acceso a las redes sociales con dispositivos móviles fuera de la oficina, aunque a menudo las políticas de las compañías restringen la participación en estas redes de los ejecutivos. El 33% de los ejecutivos que participaron en la encuesta de EIU manifestó que no se le permitía hablar sobre ningún aspecto de su trabajo en las redes sociales, y otro cuarto indicó que solo los portavoces autorizados tenían permiso para acceder a las redes sociales con los dispositivos de la compañía. Nuestro estudio puso de manifiesto que el uso de las redes sociales por parte de los ejecutivos seguirá estando restringido, ya sea por políticas o acuerdos no escritos, con el fin de proteger la información corporativa y limitar las responsabilidades.

Por supuesto, los diferentes rangos profesionales requieren acceso a diferentes tipos de datos y nuestra encuesta descubrió alguna sorpresa en este sentido. Para los ejecutivos de alto rango, la información financiera (60%) y la

planificación estratégica (42%) son importantes impulsores de la productividad. Los gerentes se inclinan por los datos operativos (44%) y los datos sobre ventas y marketing (43%), mientras que el personal de menor rango por lo general necesita acceder a información de clientes (42%) y datos operativos (42%). La toma de decisiones eficaces (52%) y evitar la pérdida de oportunidades (42%) son las dos principales razones por las que los ejecutivos sénior utilizan el acceso móvil a los datos críticos de la compañía, según la encuesta. Las relaciones con terceros, como partners, aparecen en un lugar destacado en la lista de las compañías de menor tamaño; el 42% de los encuestados pertenecientes a firmas con ingresos por debajo de los 500 millones de dólares incluyeron este aspecto entres los tres principales, en comparación con el 37% de todas las firmas en general. La necesidad de permanecer conectado ayudó a transformar el correo electrónico en una aplicación imprescindible en los dispositivos móviles y sigue siendo la herramienta más utilizada por los ejecutivos que participaron en nuestro estudio para acceder de forma remota a los datos corporativos (81%). ■

2 Pérdida, robo y malas costumbres: ¿qué están haciendo las firmas para superar los retos?

La implementación de sistemas que garanticen la seguridad de los datos corporativos a los que se accede a través de diversas plataformas cuesta dinero. Por ello, no es de extrañar que solo los encuestados pertenecientes a las empresas de mayor tamaño muestren plena confianza en las directrices de seguridad de los datos que aplican sus organizaciones. Mientras que el 45% de los encuestados de firmas con ingresos anuales por encima de los 10 000 millones de dólares afirma que sus compañías aplican las más avanzadas medidas de seguridad de la información, la cifra cae al 10% de los pertenecientes a empresas pequeñas (500 millones de dólares). Es más, incluso en el caso de las firmas con ingresos comprendidos entre 500 y 5000 millones de dólares, una tercera parte de encuestados considera que las políticas de sus compañías son inadecuadas o totalmente inadecuadas.

En general, los ejecutivos encuestados aceptan que las inversiones son necesarias y un 69% considera que la inversión en servicios de seguridad es una las principales prioridades. No obstante, nuestro estudio indica que aún queda mucho por hacer para concienciar a los ejecutivos sobre los riesgos para la seguridad. Algunas compañías creen aplicar fuertes medidas de seguridad; sin embargo permiten prácticas de riesgo. Por ejemplo, entre los ejecutivos que manifiestan que sus empresas aplican las lmedidas de seguridad líderes del sector (20%), el 13% afirmó que no existen restricciones en cuanto al uso de redes sociales. Esta práctica presenta sin duda riesgos de exposición accidental de la información confidencial de la compañía. Nuestro estudio pone de manifiesto que la aplicación de políticas sobre el uso de las redes sociales puede posibilitar una interacción eficaz y, al mismo tiempo, ayudar a proteger los datos corporativos y evitar responsabilidades.

Al contar con menos recursos que sus competidores de mayor tamaño, las pequeñas empresas se enfrentan a difíciles retos en el ámbito de la seguridad de los datos móviles. Cerca del 40% de los encuestados pertenecientes a compañías con ingresos anuales inferiores a los 500 millones de dólares describió las políticas de seguridad del acceso móvil a los datos de sus empresas como inadecuadas o totalmente inadecuadas. Al igual que ocurre con las grandes organizaciones, las empresas pequeñas que aplican políticas por escrito pueden lograr grandes resultados en seguridad de los datos corporativos con un coste relativamente bajo. Los dispositivos vendidos en los últimos años ya incluyen funciones de cifrado, solo es necesario activarlas. Sin embargo, a menudo es necesario el uso de herramientas de administración adicionales para automatizar los procesos de seguridad, por lo que las empresas de menor tamaño deben compensar el gasto de la adquisición de tecnologías de protección con enfoques de menor coste, como el seguimiento de políticas de seguridad por parte de los empleados.

Incluso los dispositivos más pequeños son cada vez más potentes, lo que aumenta el riesgo de pérdida de datos por razones no necesariamente

Control de BYOD

Puesto que el modelo "trae tu propio dispositivo" es relativamente nuevo, existen aún pocos estándares del sector probados para las políticas BYOD. Normalmente, si un empleado deja la compañía, ya sea voluntariamente o de otro modo, los datos empresariales deben eliminarse rápidamente del dispositivo, preferiblemente sin interferir con la información personal del empleado. Las políticas de uso aceptable para BYOD suelen incluir una cláusula que lo permite. Las compañías también pueden protegerse a sí mismas dentro de la legalidad modificando sus políticas móviles existentes, según se recomienda en un informe publicado en junio de 2012 por National Law Review. Las políticas sobre acoso, discriminación e igualdad de oportunidades en el trabajo; las políticas sobre confidencialidad y protección de secretos comerciales y las políticas sobre cumplimiento y ética podrían actualizarse para proteger a las compañías del uso abusivo de los dispositivos móviles por parte de los empleados.

Como salvaguarda frente a las prácticas de ejecutivos arriesgadas, muchas compañías instalan software en los dispositivos de los empleados para bloquear su software, cifrar los datos y realizar otras funciones administrativas, como la actualización de calendarios o la aplicación de actualizaciones de seguridad. Estas medidas pueden parecer intrusivas a los empleados, pero la mayoría de las políticas sobre el uso de dispositivos móviles requiere algún tipo de control de acceso administrativo remoto. Algunas compañías que han adoptado políticas sobre BYOD esperan que tanto ejecutivos como empleados se aseguren de que sus dispositivos incluyen el software necesario, que deben adquirir por su cuenta. Otras organizaciones rembolsan el coste total o parcial de los programas necesarios específicamente para tareas profesionales. Las prácticas sobre el buen uso y la configuración correcta deben supervisarse y aplicarse de forma centralizada, comenta el Al Raymond, de Aramark, quien añade que impartir regularmente formación para la concienciación sobre seguridad consigue que los empleados tengan siempre presente la importancia de la seguridad en el acceso a los datos.

Raymond manifiesta que su compañía ha adoptado un enfoque alternativo hacia la administración centralizada de la seguridad de los dispositivos móviles. Los empleados utilizan los dispositivos móviles únicamente para visualizar la información. Los datos de la compañía permanecen en los 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 aplicados en este proceso, entre los que se incluye el uso de la tecnología de escritorios virtuales y el acceso a los datos a través de servicios basados en Web, como Salesforce.com, se están extendiendo rápidamente gracias a que el acceso móvil a redes seguras permite a la compañía controlar las actividades de cifrado, autenticación y administración.

Arturo Medina, de Ipsos, compañía que aplica similares controles basados en la red, recomienda que se establezca un diálogo constante con los empleados para garantizar el cumplimiento y evitar descargas no autorizadas de los datos corporativos. "Los límites de la información confidencial y la información de los usuarios deben estar claros, y es importante saber de qué datos se realiza una copia de seguridad como información corporativa y qué se considera información personal", aconseja Arturo Medina. ■

relacionadas con la tecnología. Kensington, empresa estadounidense dedicada a la fabricación de periféricos, afirma que se pierden más de 70 millones de smartphones cada año, de los que únicamente el 7% se recuperan. Los portátiles tampoco son inmunes. El estudio de Kensington cifra en un 10% los portátiles perdidos o robados a lo largo del ciclo de vida útil de un PC. Tres cuartas partes de las pérdidas se producen durante desplazamientos o mientras los empleados trabajan en ubicaciones remotas. Un alto porcentaje de los equipos perdidos contiene algún tipo de datos empresariales.

El coste medio de un incidente de infracción de datos corporativos alcanzó los 7,2 millones de dólares en 2010, según datos de la consultora Ponemon Institute. Esto supone más del doble del coste medio en 2005. Al Raymond, de Aramark, considera que estas cifras se ajustan bastante a la realidad, dado el número y los tipos de infracciones, y añade que hay cientos de pequeños incidentes cada año y algunos otros de mayor envergadura que pueden alcanzar entre 25 y 500 millones de dólares.

Este hecho es de especial relevancia para aquellas compañías que deseen evitar las infracciones de datos causadas por empleados, pues muchas de las pérdidas de datos móviles son resultado directo de la negligencia de los usuarios. El estudio de Ponemon *2011 Cost of Data Breach* (Coste de la infracción de los datos en 2011) puso de manifiesto que entre el 30 y el 40% de las infracciones se debieron a la negligencia, seguidas por aquellas ocasionadas por ataques maliciosos (43%). El informe muestra que el 50% de las infracciones sufridas por compañías italianas fueron consecuencia de la pérdida o robo de un dispositivo móvil. Solo Alemania (42%), Francia (43%) y Australia (36%) sufrieron más pérdidas debido a ataques maliciosos que por negligencia. India fue el único país en el que los fallos del sistema superaron a las negligencias y a los ataques maliciosos como causas de las infracciones.

Algunas pérdidas de datos móviles notables ilustran la facilidad con la que puede producirse una infracción. La clínica oncológica Cancer Care Group de Indianápolis perdió los datos de más de 55 000 pacientes y de todos sus empleados en julio de 2012 debido al robo del portátil de un empleado que contenía archivos de copia de seguridad del servidor cuando se encontraba dentro de un vehículo cerrado. Los datos no estaban cifrados, a pesar de que su código de buenas prácticas así lo recomendaba. La clínica MD Anderson Cancer Center de Texas sufrió dos infracciones entre junio y julio de 2012. Mientras uno de los incidentes se debió a la pérdida de una unidad USB portátil no cifrada, la otra se produjo por el robo de un portátil, también sin cifrar, de la casa de un miembro del cuerpo docente. La información de más de 30 000 pacientes se vio comprometida en ambas infracciones. Tras la segunda infracción, la clínica comenzó a proteger sus datos mediante el cifrado.

Las compañías pueden evitar muchas de las infracciones de la información añadiendo protección mediante contraseña a los dispositivos móviles, ya se trate de portátiles, smartphones o dispositivos de almacenamiento de datos portátiles, y mediante el cifrado completo del disco o unidad USB.

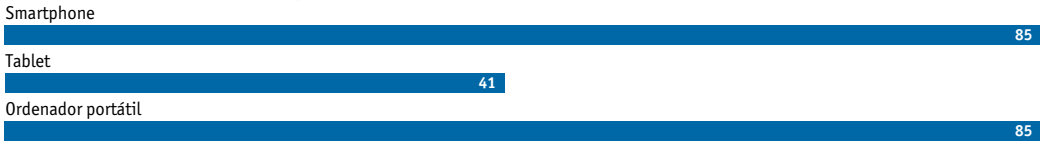
Estos dispositivos deberían además protegerse físicamente. Por ejemplo, no deberán dejarse nunca en vehículos sin supervisión, incluso si están cerrados con llave. Los teléfonos móviles y algunos ordenadores (aquellos equipados con la tecnología VPro de Intel) pueden desactivarse de forma remota y es posible además borrar sus datos en caso de pérdida. Cuanto mayor sea el grado de confidencialidad de los datos que almacenan, mayor importancia tiene que se aplique este mecanismo, ya que el cifrado no es infalible y puede descifrarse. ■

3 Cada vez más datos móviles: las tendencias emergentes

Casi el 90% de las organizaciones de todo el mundo permiten el acceso móvil a datos críticos, según la agencia de las Naciones Unidas International Telecommunication Union (ITU). De las organizaciones identificadas en la encuesta de EIU que no aplican políticas formales sobre la iniciativa BYOD, el 25% afirma tener planes de implementar un programa en los próximos 12-18 meses. Son conscientes de que este tipo de programas fomentan la motivación de los empleados, observación confirmada por estudios independientes. Según el estudio realizado en agosto de 2012 por iPass, compañía de software móvil estadounidense, muchos empleados trabajan hasta 20 horas adicionales no pagadas a la semana si cuentan con conectividad permanente. Casi el 90% de los encuestados por iPass manifestó que la conectividad inalámbrica es una parte de sus vidas tan importante como el agua corriente o la electricidad.

Aunque cada vez es mayor el número de empleados que trabaja fuera de la oficina, establecer un programa de acceso móvil, incluida la iniciativa BYOD, sigue sin ser una opción para algunas firmas. Las compañías bancarias y financieras, que están muy reguladas, aplican estrictas políticas que prohíben que los ejecutivos accedan a los datos de la compañía desde sus dispositivos personales. Steve Ellis, Vicepresidente ejecutivo de Wells Fargo, confiesa que su compañía está adoptando la iniciativa BYOD con precaución y actualmente está valorando las diversas opciones. Quizá pase otro año hasta que tengamos un plan formal, añade Ellis. Otras compañías que no cuentan con una política formal de BYOD admiten ser conscientes del aumento del uso de dispositivos personales en la empresa. Antes de la introducción hace diez meses de la política formal sobre acceso móvil de Aramark, no existían reglas definidas que indicaran a los empleados qué dispositivos y sistemas operativos podían conectarse a la red de la empresa. Gracias a la nueva política, que permite el acceso en función del cargo y mediante dispositivos y configuraciones aprobados, la

Q Dispositivos para el acceso de ejecutivos
¿Qué dispositivos proporciona su organización a los ejecutivos para que accedan a los datos críticos?
Seleccione las opciones aplicables.
(Porcentaje de encuestados)



Fuente: Encuesta de Economist Intelligence Unit, Junio de 2012.

Caso práctico La EEOC pone en marcha un programa piloto de movilidad

El presupuesto para el ejercicio de 2012 de la Comisión para la Igualdad de Oportunidades en el Empleo (EEOC) de EE. UU. se recortó casi en un 15%, de 17,6 a 15 millones de dólares. Debido a la necesidad de reducir costes operativos, su Directora de informática, Kimberly Hancher, redujo a la mitad el presupuesto de la agencia destinado a dispositivos móviles. Con el fin de cubrir el vacío creado, la agencia implementó un proyecto piloto de BYOD. El proyecto se centró en permitir a los empleados el acceso al correo electrónico, los calendarios, los contactos y las tareas de la agencia. Además, a algunos ejecutivos sénior se les concedió acceso "privilegiado" a los sistemas internos de la agencia como parte del proyecto.

En la fase de prueba inicial, 40 voluntarios entregaron sus dispositivos BlackBerry propiedad del gobierno y utilizaron en su lugar sus smartphones personales. El personal encargado de la seguridad de la información, el departamento legal y el sindicato de empleados crearon reglas que equilibraban la privacidad de los empleados (políticas sobre redes sociales o políticas de monitorización) con la seguridad gubernamental, como la normativa SP 800-53 del Instituto Nacional de Normas y Tecnología (NIST) de EE. UU. (también conocida como "Controles de seguridad recomendados para organizaciones y sistemas de información federales"). La segunda fase del programa se puso en marcha en junio de 2012. La EEOC trabajó junto a sus contratistas en la configuración del acceso al correo electrónico de la agencia de los empleados participantes en las pruebas secundarias. A los 468 empleados restantes de la agencia que utilizaban dispositivos BlackBerry propiedad de EEOC se les ofrecieron tres opciones:

1. Devolver voluntariamente los dispositivos BlackBerry y traer al trabajo un smartphone BlackBerry, Apple o Android o una tablet personal.

2. Devolver el smartphone BlackBerry y recibir un teléfono móvil propiedad del gobierno únicamente con funciones de voz.

3. Conservar el smartphone BlackBerry aceptando que la EEOC no ofrece dispositivos de repuesto.

Hasta el momento, los gerentes de la EEOC han informado de resultados muy positivos. Los empleados pagan por su propio uso de voz y datos y la agencia cubre las licencias del software de administración. Kimberly Hancher, de la EEOC, observó que, para algunos empleados, el coste puede ser un problema y surge la duda de si la agencia podrá proporcionar algún tipo de rembolso parcial de las tarifas de datos y voz. Hancher añade que el éxito se debe a la colaboración de empleados, sindicatos y el departamento legal desde el principio del proceso. ■

compañía puede saber con exactitud quién tiene acceso y a qué datos. "Ya no se hace nada en la sombra", comenta Al Raymond. Cuanto más visible es el programa, más probable es su cumplimiento.

Dejando las políticas a un lado, el tipo de los dispositivos también ha cambiado. Actualmente, algo más de una cuarta parte (27%) del acceso a los datos críticos se produce a través de smartphones, según datos de nuestra encuesta. Los encuestados esperan que la cifra aumente por encima de un tercio (35%) en los próximos 12-18 meses, con otro 30% de los datos críticos accesibles mediante otros dispositivos móviles, que actualmente suponen solo una quinta parte. Con la aparición de nuevo software y los dispositivos asociados, las tablets se encuentran en una posición ventajosa para convertirse en un escaparate de datos corporativos para los ejecutivos cada vez más utilizado, que podría incluso sustituir a los smartphones en el futuro, según se publica en un artículo de *The Economist* (octubre de 2011). Su pantalla de mayor tamaño aumenta el rango de datos que pueden visualizarse óptimamente y, si se complementan con teclados externos, facilitan la interacción con las aplicaciones.

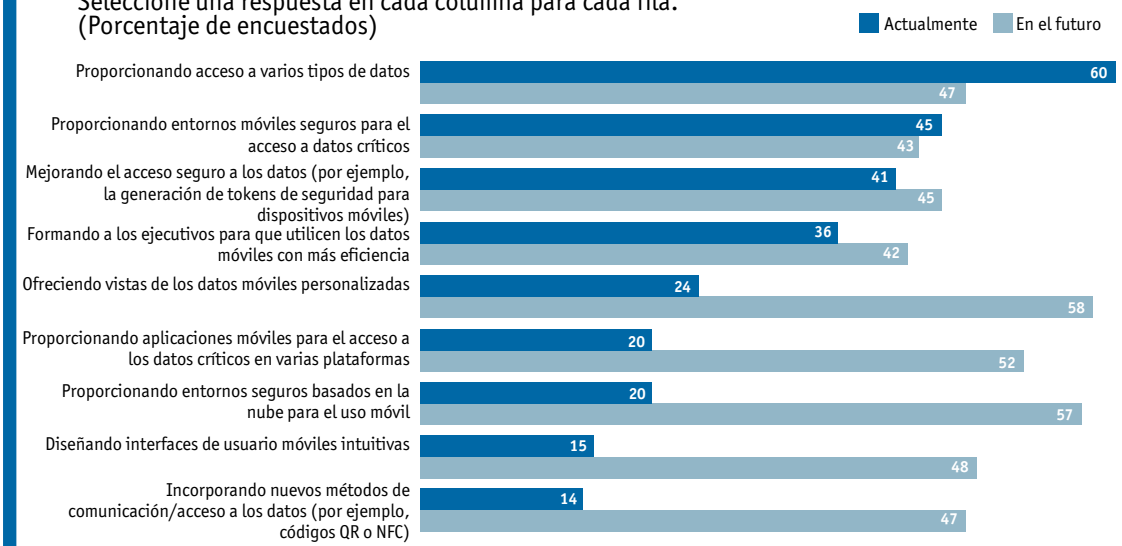
Resulta interesante comprobar que, a pesar de que el 42% de los encuestados manifestó que los ejecutivos de alto rango necesitan un acceso seguro y a su debido tiempo a los datos de planificación estratégica para aumentar su productividad, solo el 28% considera que es adecuado que los datos sean accesibles a través de dispositivos móviles. El principal reto, como era de esperar, es la preocupación por las potenciales amenazas para la seguridad y otros riesgos. No obstante, solo el 11% de nuestros encuestados afirma que su organización no permite el acceso a los datos críticos fuera de la oficina. ■

4 ¿Cómo pueden las compañías garantizar la aplicación de políticas móviles eficaces?

Los encuestados reconocen claramente las ventajas de permitir el acceso móvil a los datos y son conscientes de la necesidad de realizar inversiones. Algunas de las medidas que las compañías deben adoptar para garantizar el acceso seguro a los datos corporativos a través de dispositivos móviles pueden aplicarse de forma remota. Los responsables de TI pueden actualmente añadir funciones de seguridad a portátiles, smartphones y tablets, a menudo utilizando las herramientas de administración existentes. También pueden separar los datos corporativos de los datos personales y almacenar los datos empresariales en las redes corporativas. Los escritorios virtuales permiten el acceso móvil seguro a los datos en portátiles personales. Estos mecanismos de seguridad hacen posible que los trabajadores móviles puedan recuperar los datos de un dispositivo perdido o dañado con muy poco esfuerzo. Estas medidas permitirán que en el futuro más ejecutivos tengan acceso a los datos corporativos de forma segura desde cualquier equipo, según se desprende de las entrevistas a ejecutivos.

Para los ejecutivos de alto rango que se desplazan con frecuencia, la reducción del tiempo

Q Acceso móvil
¿Cómo permite su compañía el acceso a los datos críticos en la actualidad y cómo podría hacerlo en el futuro?
Seleccione una respuesta en cada columna para cada fila.
(Porcentaje de encuestados)



Fuente: Encuesta de Economist Intelligence Unit, Junio de 2012.

empleado en la actualización de los protocolos de seguridad se traduce en más tiempo productivo. En el futuro, la seguridad de los datos se reforzará con ayuda de las tecnologías incorporadas directamente en las aplicaciones que protegen los datos en sí, dificultando así la intercepción y el abuso de los datos, según afirma Ashwani Tikoo, de CSC. "Las aplicaciones deberían poder identificar que estoy trabajando en un iPad o con una pantalla de solo 5 pulgadas y adaptar a ello la visualización de los datos."

Al Raymond afirma que, a pesar de que su compañía no lo requiere, es importante contar con entornos diferentes para el uso personal y profesional. Sin embargo, si no se cumplen las políticas aplicables u otras medidas de seguridad, habrá consecuencias. El Sr. Raymond explica que siempre se sorprende al hablar con sus colegas y comprobar que la seguridad en las grandes organizaciones no es más que una "cortina de humo". Las palabras están ahí, pero no se cumplen.

Ipsos, una compañía de investigación global, requiere que cada empleado realice un curso de formación sobre seguridad que ofrece a través de su intranet; una forma rentable de llegar a todo su personal, repartido en 84 países. Su programa se desarrolló internamente, pero hay productos para la concienciación sobre la seguridad en las organizaciones como el Instituto Nacional de Seguridad (NSI) de EE. UU. que están disponibles comercialmente y que pueden adaptarse a las necesidades específicas. También se exige a los empleados que firmen la política de uso aceptable de dispositivos móviles, que cubre todos los aspectos, desde el tipo de datos a los que se puede acceder desde un dispositivo móvil hasta reglas relacionadas con la seguridad de las contraseñas.

Otros mecanismos de seguridad requieren acciones fiables por parte de los usuarios. A pesar de que los dispositivos móviles deberían tener contraseñas, Coalfire, firma de auditoría y cumplimiento, calcula que solo la mitad de los dispositivos personales cuenta con ellas. Los empleados que participen en un programa BYOD deberán aceptar que, en caso de pérdida o robo de sus dispositivos, es responsabilidad del departamento de TI borrar de forma remota toda la información contenida en dispositivos personales con el fin de proteger los datos de la compañía.

Queda claro 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 de datos de la compañía. La encuesta reveló que los ejecutivos fuera de Europa y América del Norte son más reticentes a la aplicación de políticas de seguridad de los datos en dispositivos personales. Sin embargo, en un entorno empresarial cada vez más conectado, las brechas de seguridad en una región pueden afectar a las compañías que sí cumplen las políticas (y a sus clientes) independientemente de su ubicación. ■

5 Conclusión

El acceso móvil a los datos no solo no dejará de crecer, sino que la tendencia es imparable. Los dispositivos no administrados y sin seguridad han logrado colarse en el entorno empresarial, poniendo en peligro los datos empresariales y abriendo una puerta a los ataques a través de los dispositivos vulnerables. Casi un tercio de nuestros encuestados admite que las políticas sobre dispositivos móviles de sus compañías son inadecuadas. El establecimiento de políticas razonables y factibles es el primer paso en la creación de un programa viable de acceso móvil a los datos.

Los ejecutivos que clasifican sus políticas sobre el uso de dispositivos como líderes del sector indican que utilizan los datos sobre la marcha para poder tomar decisiones más eficientes y en colaboración, evitar la pérdida de oportunidades y trabajar junto a partners y clientes con mayor eficiencia. Para garantizar que este acceso no ponga en peligro la seguridad de los datos empresariales, es posible que los ejecutivos quieran dar prioridad a los programas que mitiguen los riesgos y apoyen las inversiones en servicios de seguridad y datos.

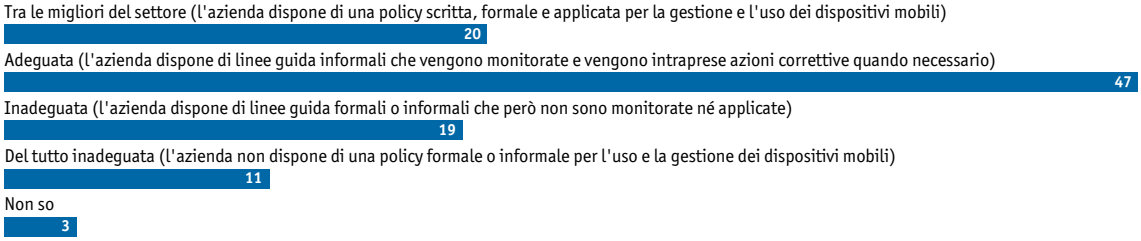
Los dispositivos conectados son cada vez más una parte integral de las empresas globales. El tipo de dispositivo en uso está evolucionando y las tablets son en la actualidad los dispositivos de mayor proyección. Cabe esperar un crecimiento considerable en el uso de tablets tras el lanzamiento de los sistemas operativos de próxima generación, que ofrecerán una más amplia gama de opciones de acceso a los datos con tablets que en el caso de los smartphones. Los analistas piensan que esto puede ser un arma de doble filo, pues las tablets serán dispositivos complementarios de los sistemas existentes, no los reemplazarán.

En el futuro, la seguridad de los datos críticos podría significar la creación de requisitos de acceso aún más estrictos. El cambio hacia el uso de tablets para actividades empresariales fuera de la oficina, por ejemplo, generará nuevos retos, pues los ejecutivos querrán acceder a una mayor diversidad de datos. Muchas compañías tendrán que replantearse todos los aspectos, desde los dispositivos y sus puntos débiles a la infraestructura disponible o los usuarios mismos. ■

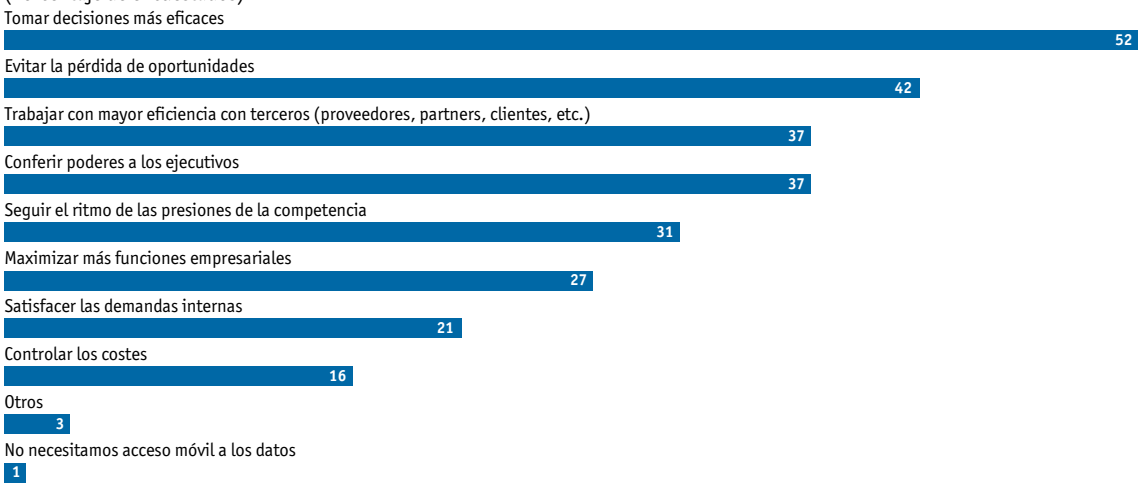
Apéndice: resultados de la encuesta

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

In base alle conoscenze in proprio possesso, come risulta la policy per i dispositivi mobili dell'azienda rispetto alla concorrenza del settore?
(percentuale di intervistati)

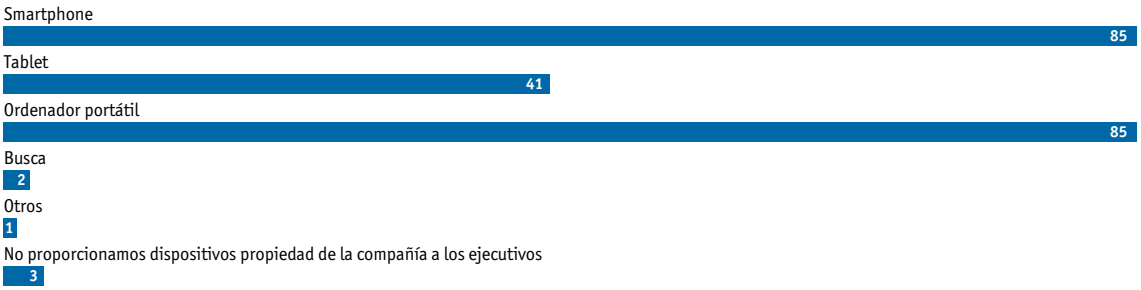


¿Cuáles son los principales factores empresariales que están generando la necesidad de acceder a los datos críticos desde dispositivos móviles?
Seleccione un máximo de tres.
(Porcentaje de encuestados)



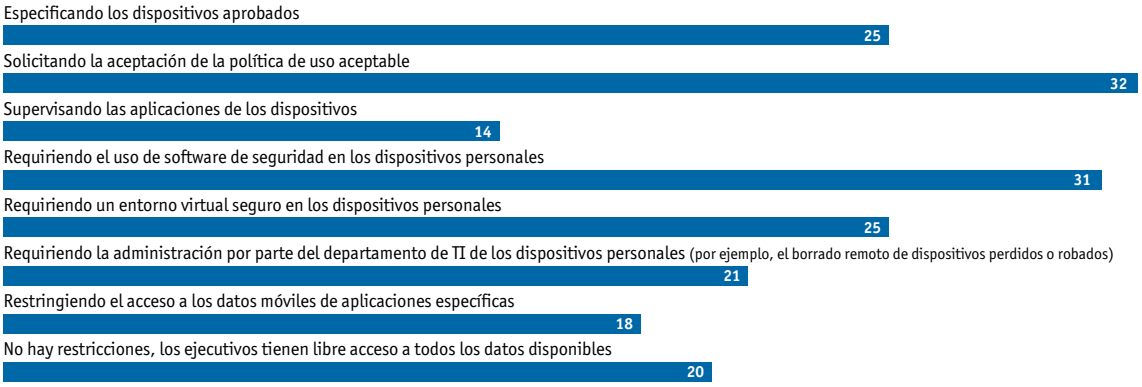
¿Permite su organización el acceso a los datos críticos fuera de la oficina?
(Porcentaje de encuestados)

¿Qué dispositivos proporciona su organización a los ejecutivos para que accedan a los datos críticos? Seleccione las opciones aplicables.
(Porcentaje de encuestados)

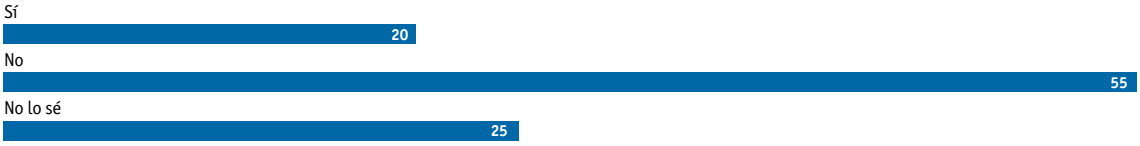


¿Permite su organización que los ejecutivos usen sus dispositivos personales (BYOD) en lugar de los dispositivos corporativos para acceder a datos críticos?
(Porcentaje de encuestados)

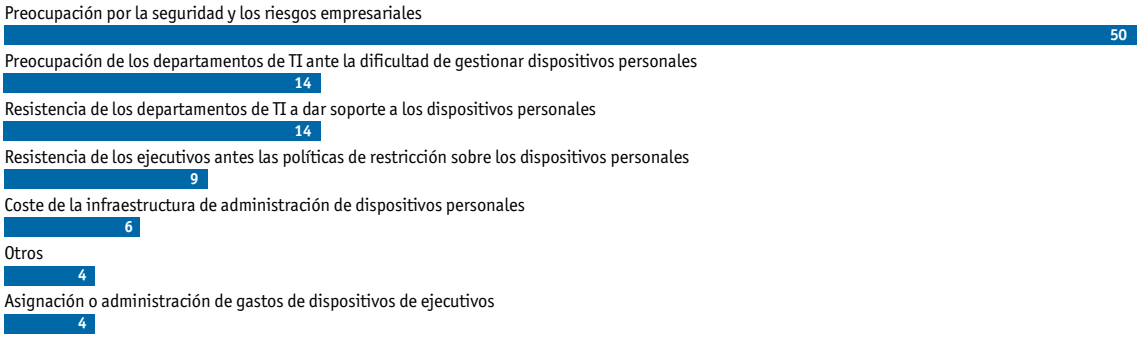
¿Cómo ha implementado su organización la iniciativa BYOD para el acceso a datos críticos?
Seleccione las opciones aplicables.
(Porcentaje de encuestados)



¿Está entre los planes de su organización implementar la iniciativa BYOD para el acceso a datos críticos?
(Porcentaje de encuestados)

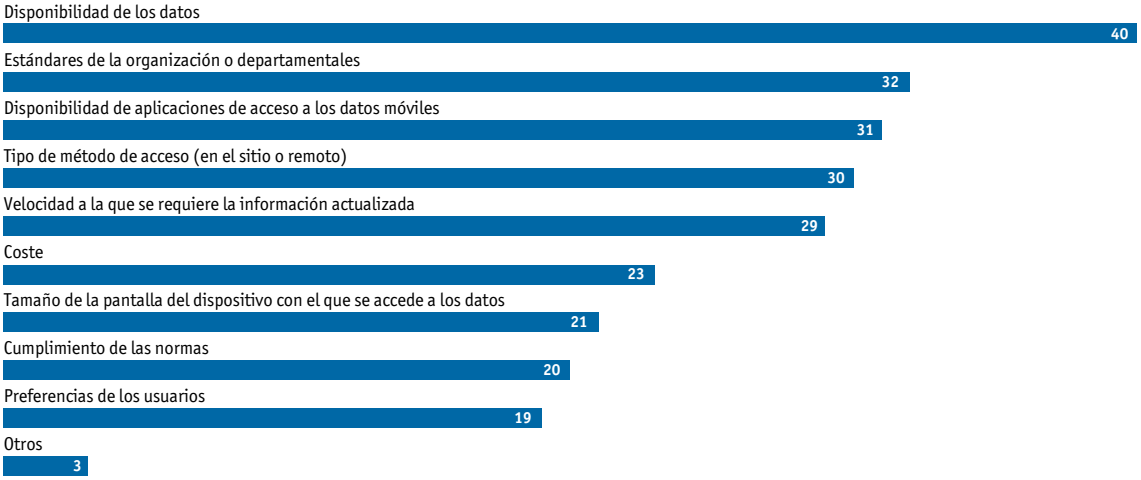


¿Cuál cree que es el mayor obstáculo en la implementación de la iniciativa BYOD para el acceso a los datos críticos?
(Porcentaje de encuestados)

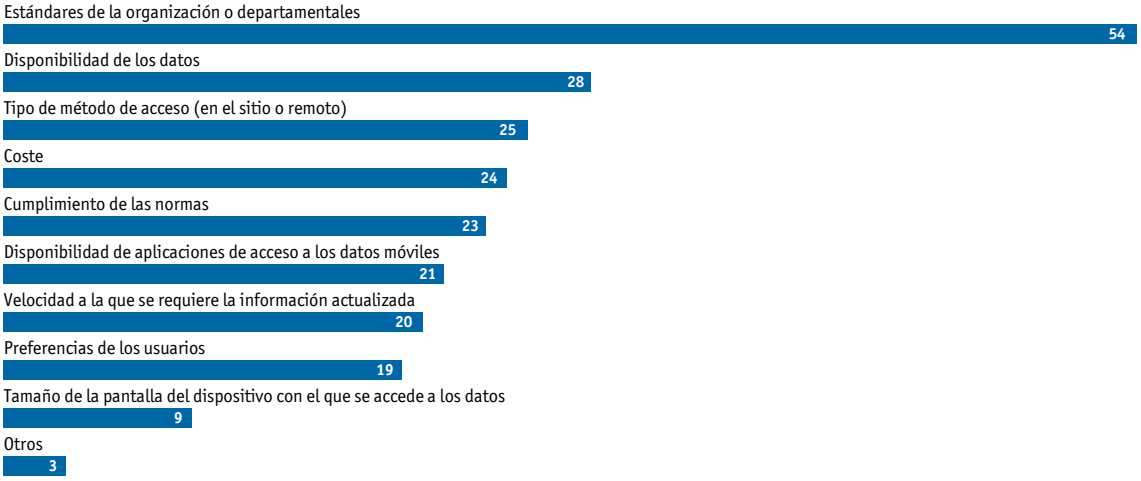


En su opinión, ¿cuáles son los principales retos a los que se enfrenta su compañía a la hora de garantizar el acceso seguro a los datos críticos con dispositivos móviles, tanto de la compañía como propiedad de los ejecutivos?
Seleccione un máximo de cuatro.
(Porcentaje de encuestados)

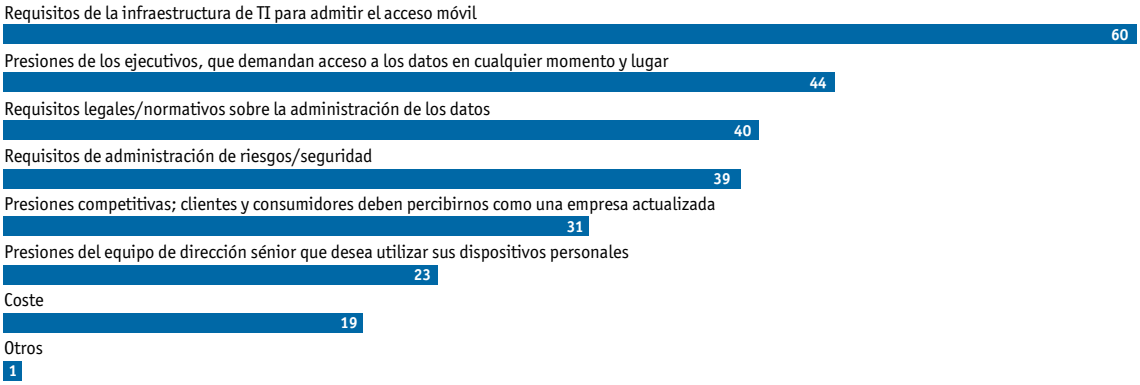
Además de su cargo, ¿qué determina el tipo de datos a los que puede o podrá acceder con un dispositivo móvil?
Seleccione un máximo de tres.
(Porcentaje de encuestados)



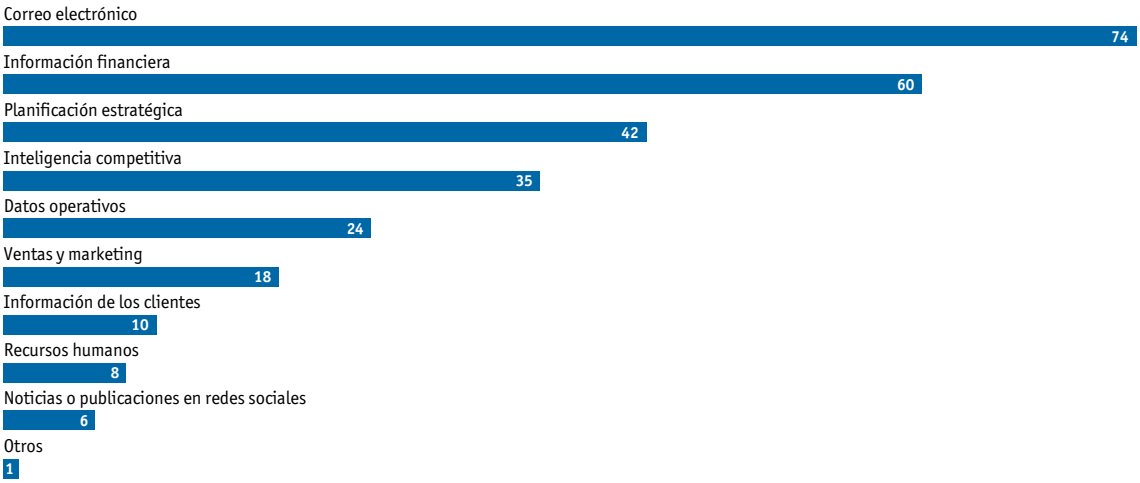
¿Qué determina los usuarios a quienes se permite o permitirá el acceso a los datos críticos con dispositivos móviles?
Seleccione un máximo de tres.
(Porcentaje de encuestados)



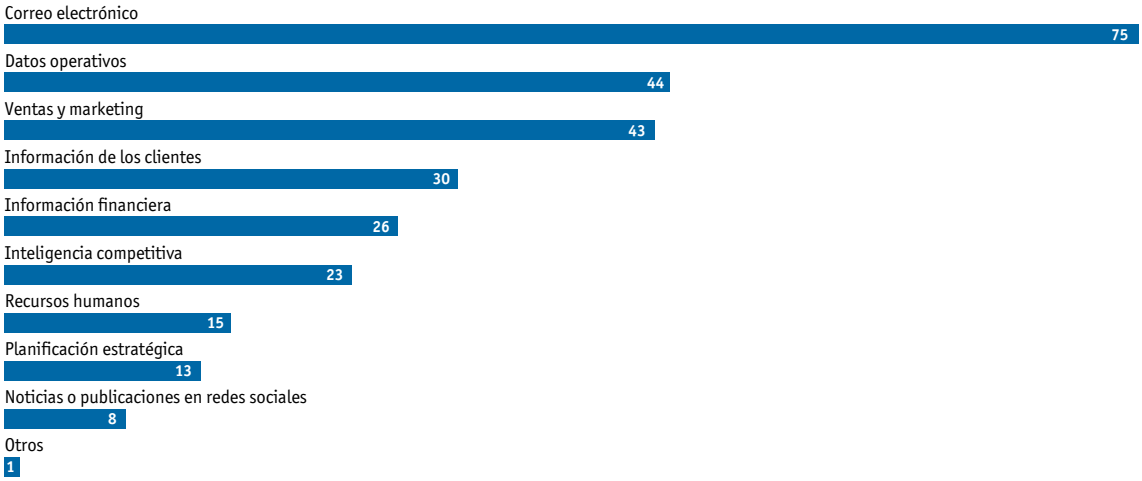
¿Cuáles son las principales influencias a la hora de crear políticas de la compañía y enfoques dirigidos a la creación de una estrategia de aplicaciones y dispositivos móviles?
Seleccione un máximo de tres.
(Porcentaje de encuestados)



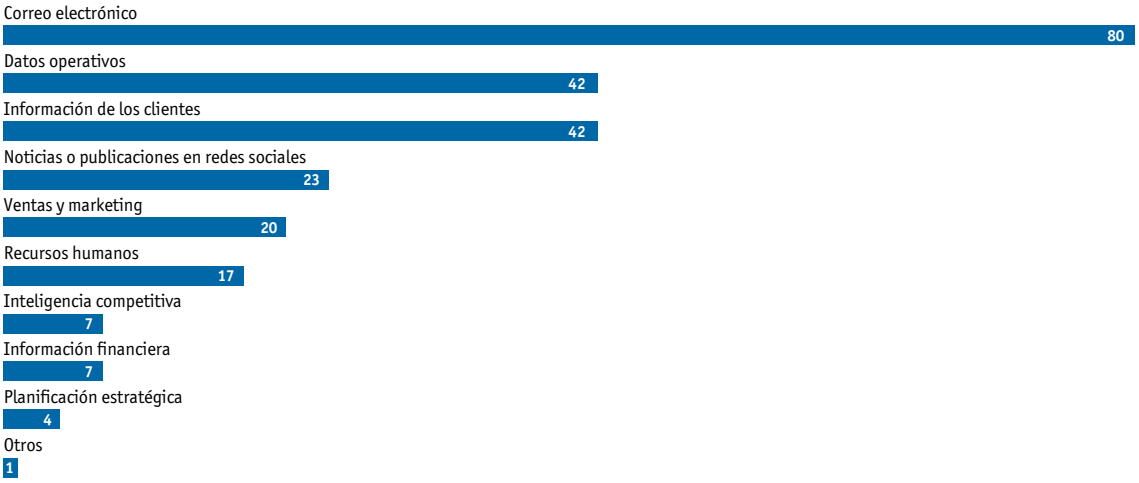
¿A cuáles de estos tipos de información debe permitirse el acceso de forma segura y oportuna a los siguientes cargos con el fin de aumentar su productividad? Ejecutivos de alto rango
Seleccione un máximo de tres para cada cargo.
(Porcentaje de encuestados)



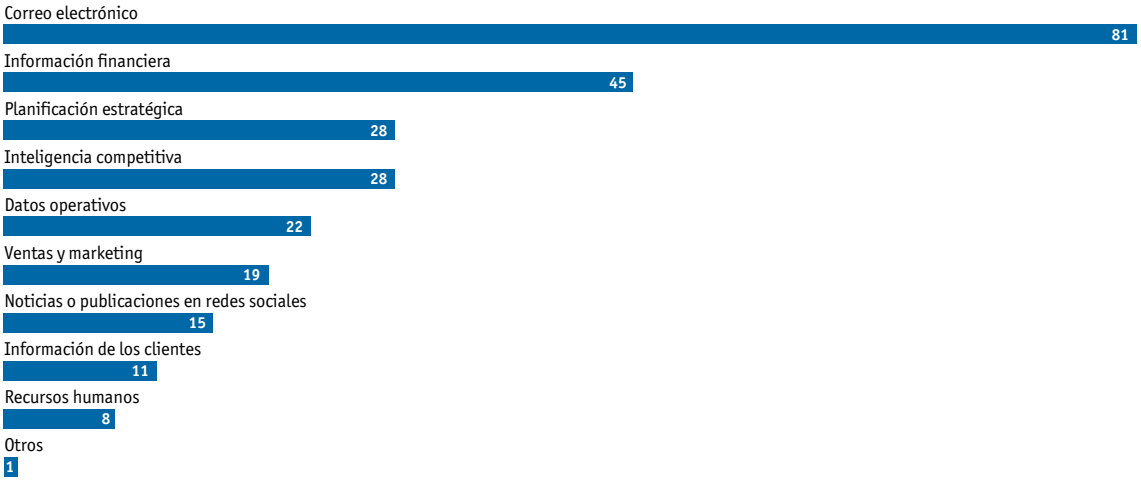
¿A cuáles de estos tipos de información debe permitirse el acceso de forma segura y oportuna a los siguientes cargos con el fin de aumentar su productividad? Directores comerciales
Seleccione un máximo de tres para cada cargo.
(Porcentaje de encuestados)



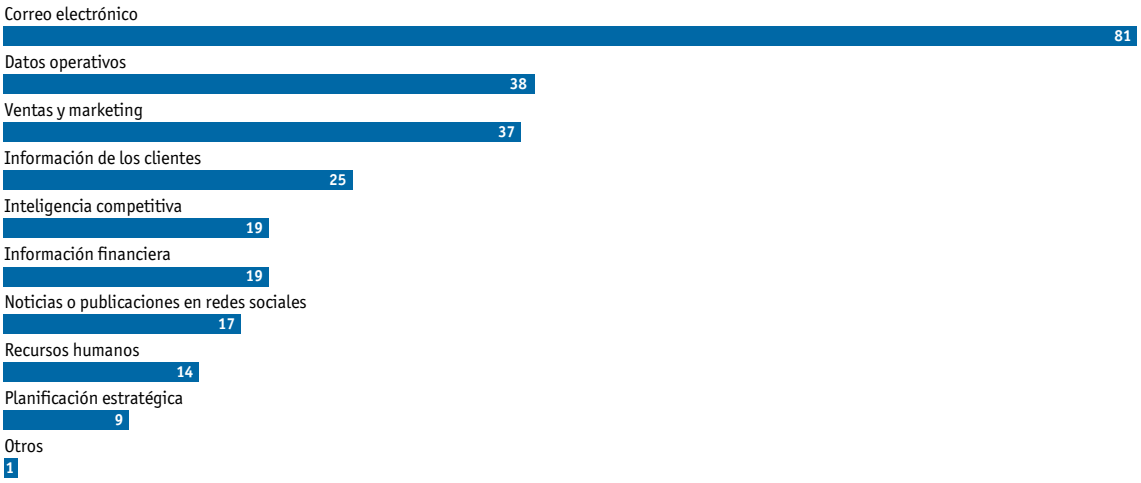
¿A cuáles de estos tipos de información debe permitirse el acceso de forma segura y oportuna a los siguientes cargos con el fin de aumentar su productividad? Empleados
Seleccione un máximo de tres para cada cargo.
(Porcentaje de encuestados)



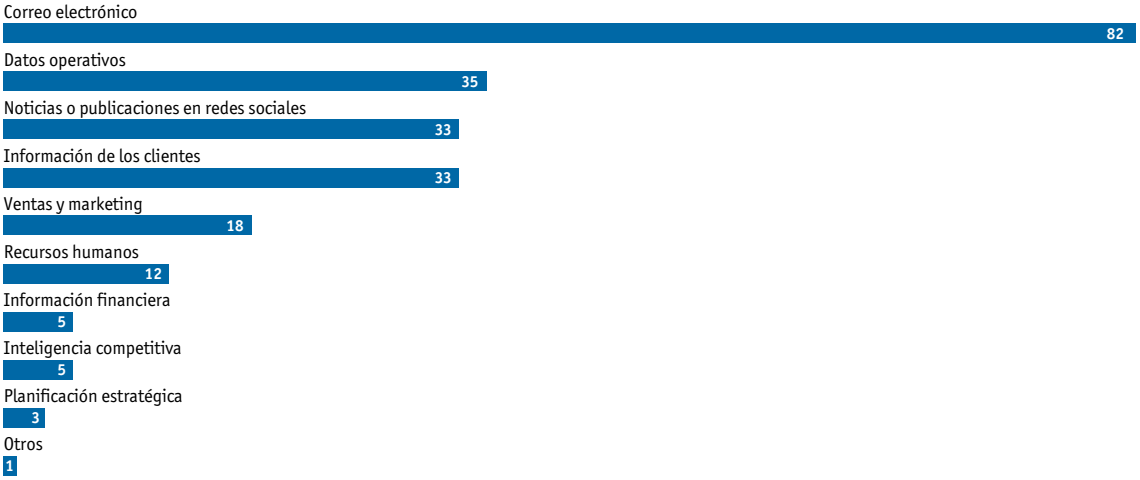
De estos tipos de información/medios, seleccione aquellos a los que sería adecuado poder acceder en dispositivos móviles.
Ejecutivos de alto rango
Seleccione un máximo de tres para cada cargo.
(Porcentaje de encuestados)



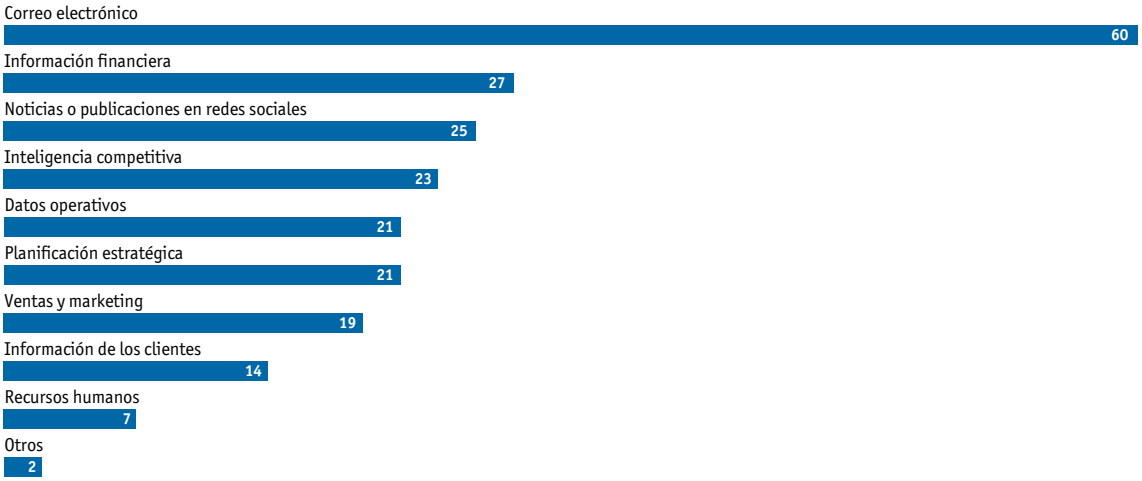
De estos tipos de información/medios, seleccione aquellos a los que sería adecuado poder acceder en dispositivos móviles.
Directores comerciales
Seleccione un máximo de tres para cada cargo.
(Porcentaje de encuestados)



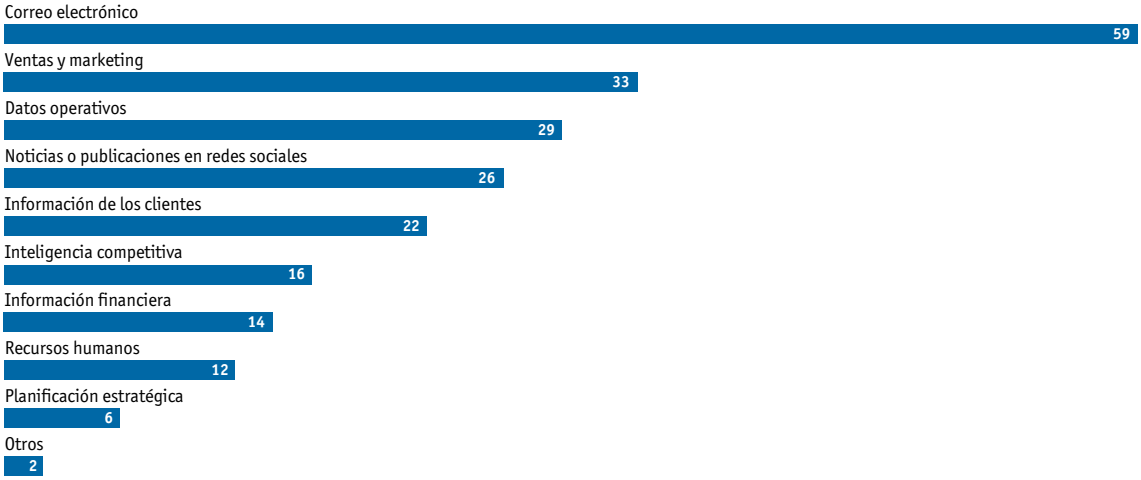
De estos tipos de información/medios, seleccione aquellos a los que sería adecuado poder acceder en dispositivos móviles. Empleados
Seleccione un máximo de tres para cada cargo.
(Porcentaje de encuestados)



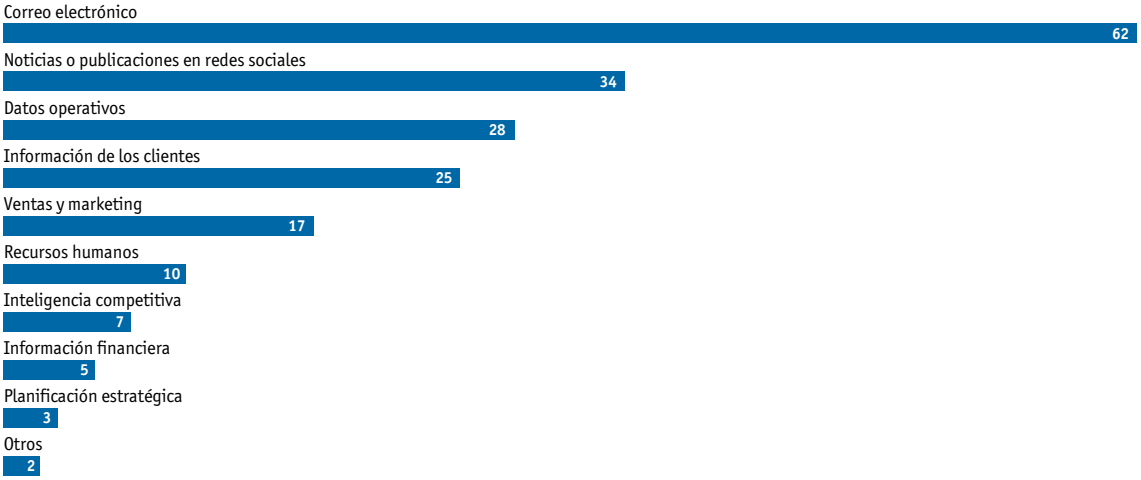
De estos tipos de información/medios, seleccione aquellos a los que sería adecuado poder acceder en dispositivos móviles desde almacenamiento basado en la nube. Ejecutivos de alto rango
Seleccione un máximo de tres para cada cargo.
(Porcentaje de encuestados)



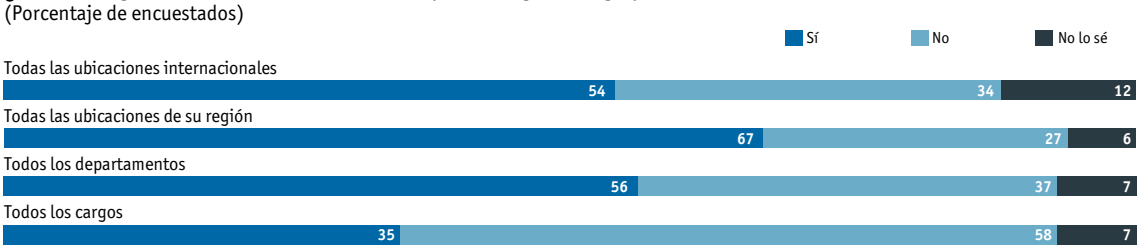
De estos tipos de información/medios, seleccione aquellos a los que sería adecuado poder acceder en dispositivos móviles desde almacenamiento basado en la nube.
Directores comerciales
Seleccione un máximo de tres para cada cargo.
(Porcentaje de encuestados)



De estos tipos de información/medios, seleccione aquellos a los que sería adecuado poder acceder en dispositivos móviles desde almacenamiento basado en la nube.
Empleados
Seleccione un máximo de tres para cada cargo.
(Porcentaje de encuestados)



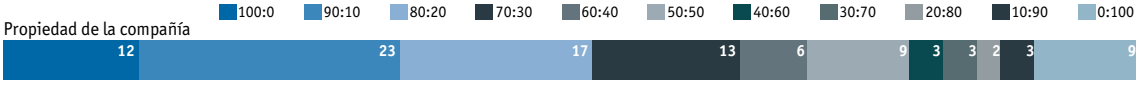
¿Ofrece su organización acceso móvil a los datos para los siguientes grupos?
(Porcentaje de encuestados)



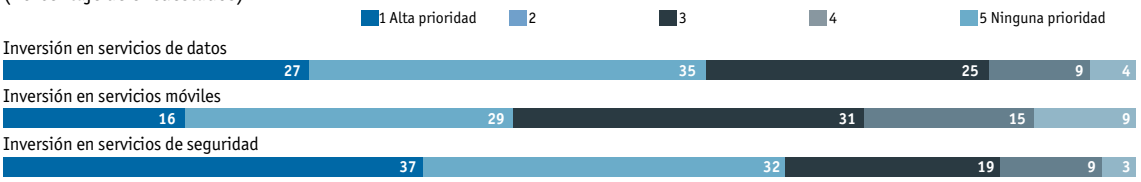
¿Cuenta su organización con políticas que regulen el uso aceptable de las redes sociales, como Facebook o Twitter, en los dispositivos corporativos?
(Porcentaje de encuestados)

¿Qué políticas sobre el uso de redes sociales con dispositivos corporativos aplica su empresa?
(Porcentaje de encuestados)

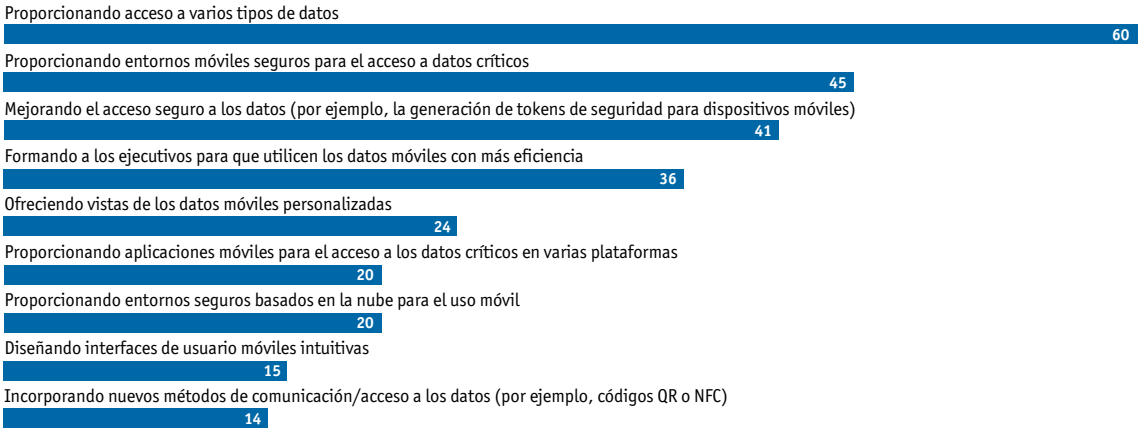
¿Qué proporción de tiempo utiliza dispositivos propiedad de la compañía frente a dispositivos personales para tareas profesionales?
Arrastre el botón deslizante para seleccionar los porcentajes que mejor reflejen la porción de tiempo dedicada a cada opción (por ejemplo, 60% a 40%).
(Porcentaje de encuestados)



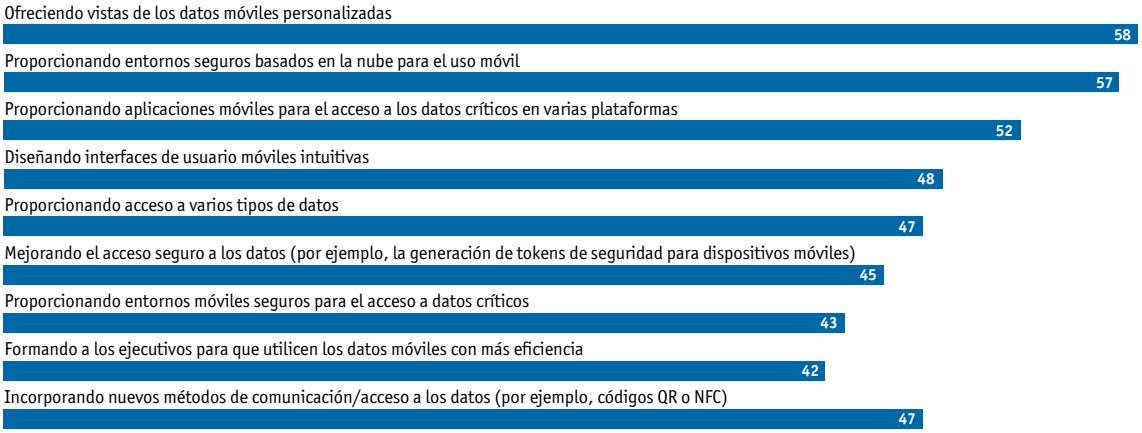
¿Qué prioridad confiere su organización a las siguientes estrategias?
Utilice una escala del 1 al 5, siendo 1 la más alta prioridad y 5 ninguna prioridad.
(Porcentaje de encuestados)



¿Cómo permite su compañía el acceso a los datos críticos en la actualidad y cómo podría hacerlo en el futuro?
Actualmente
Seleccione una respuesta en cada columna para cada fila.
(Porcentaje de encuestados)



¿Cómo permite su compañía el acceso a los datos críticos en la actualidad y cómo podría hacerlo en el futuro?
En el futuro
Seleccione una respuesta en cada columna para cada fila.
(Porcentaje de encuestados)



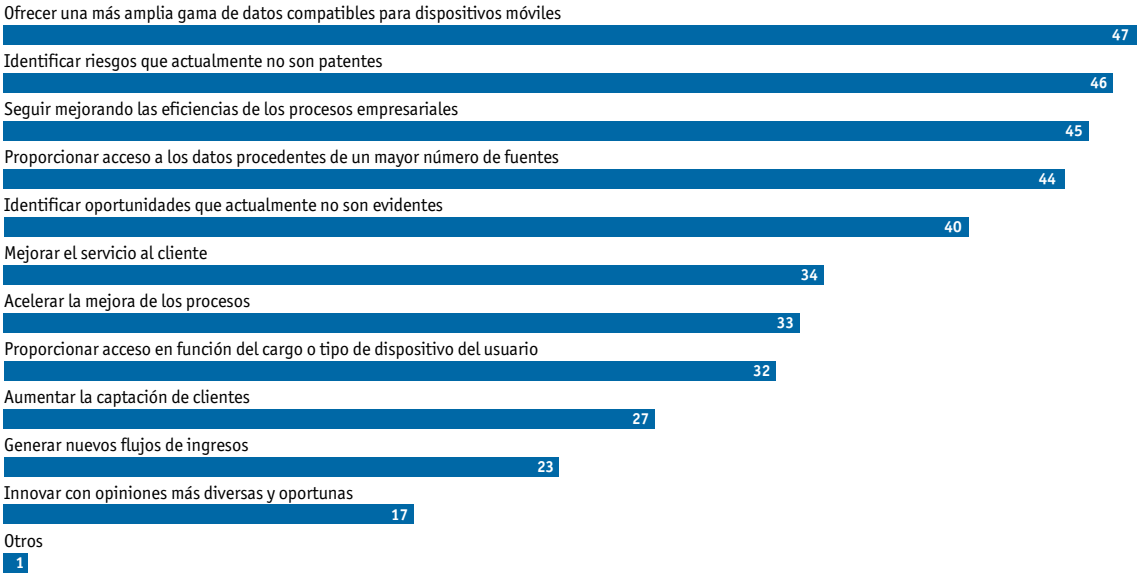
¿Cuál es la proporción de datos críticos a los que accede a través de canales móviles actualmente?
El total debería ser el 100%

	Media
Móvil a través de smartphone	26,9
Móvil en otros dispositivos (p. ej. tablet)	21,7
Acceso no móvil	59,8

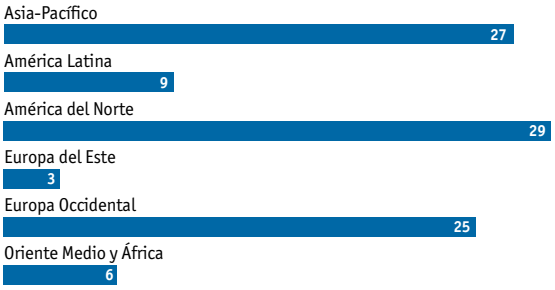
¿Cuál será la proporción de datos críticos a los que accederá a través de canales móviles en 12-18 meses?
El total debería ser el 100%

	Media
Móvil a través de smartphone	34,5
Móvil en otros dispositivos (p. ej. tablet)	30,2
Acceso no móvil	42,8

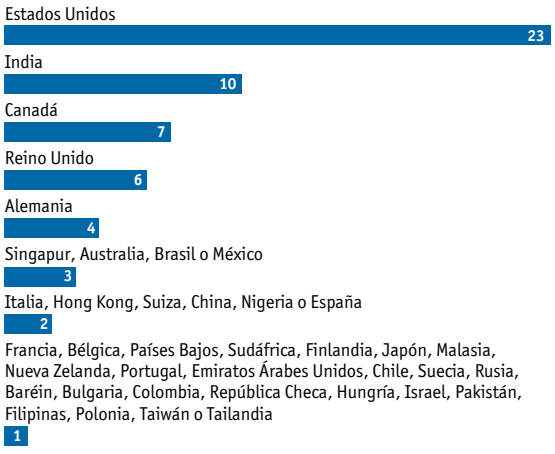
En los próximos 12–18 meses, ¿qué espera poder hacer su organización con respecto al acceso a los datos críticos que no puede hacer en la actualidad?
Seleccione las opciones aplicables.
(Porcentaje de encuestados)



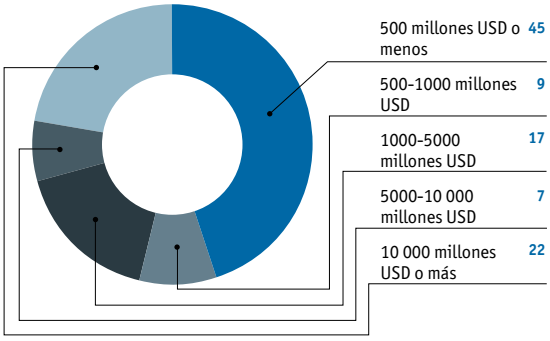
¿En qué región se encuentra?
(Porcentaje de encuestados)



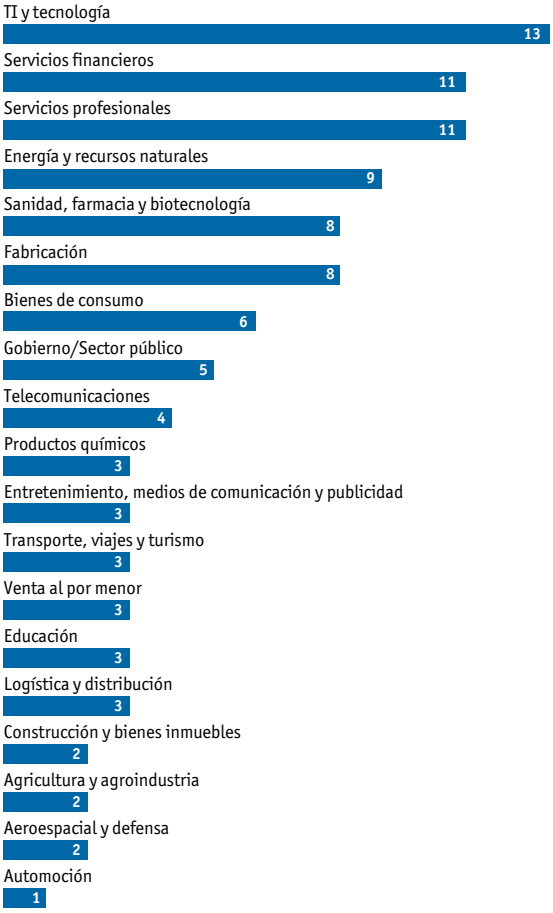
¿En qué país se encuentra?
(Porcentaje de encuestados)



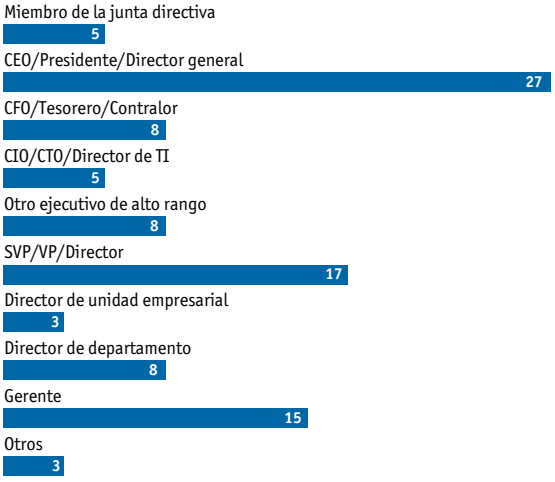
¿Cuáles son los ingresos totales anuales de su organización en dólares estadounidenses (USD)?
(Porcentaje de encuestados)



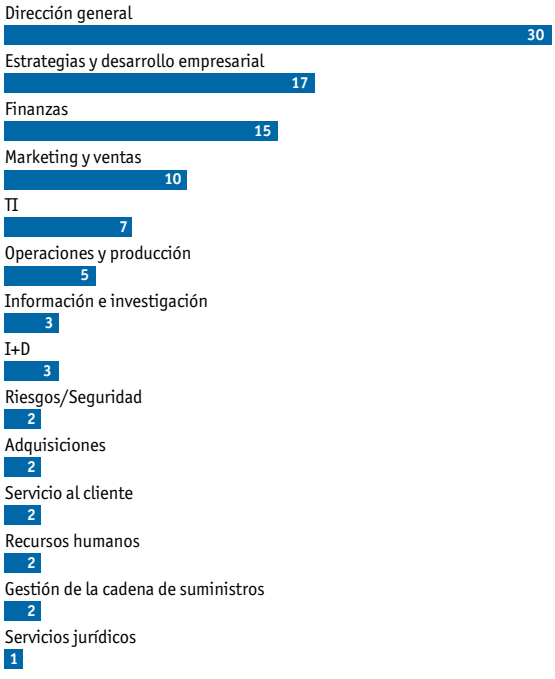
¿A qué sector pertenece principalmente su compañía?
(Porcentaje de encuestados)



¿Cuál de estas opciones describe mejor su cargo?
(Porcentaje de encuestados)



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



Aunque se han realizado todos los esfuerzos posibles para verificar la exactitud de esta información, ni el Economist Intelligence Unit Ltd. ni el patrocinador de este informe pueden aceptar responsabilidad alguna por la confianza que cualquier persona deposite en este informe técnico o en la información, opiniones o conclusiones que en él se incluyen.

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 9347
Correo electrónico:
geneva@eiu.com