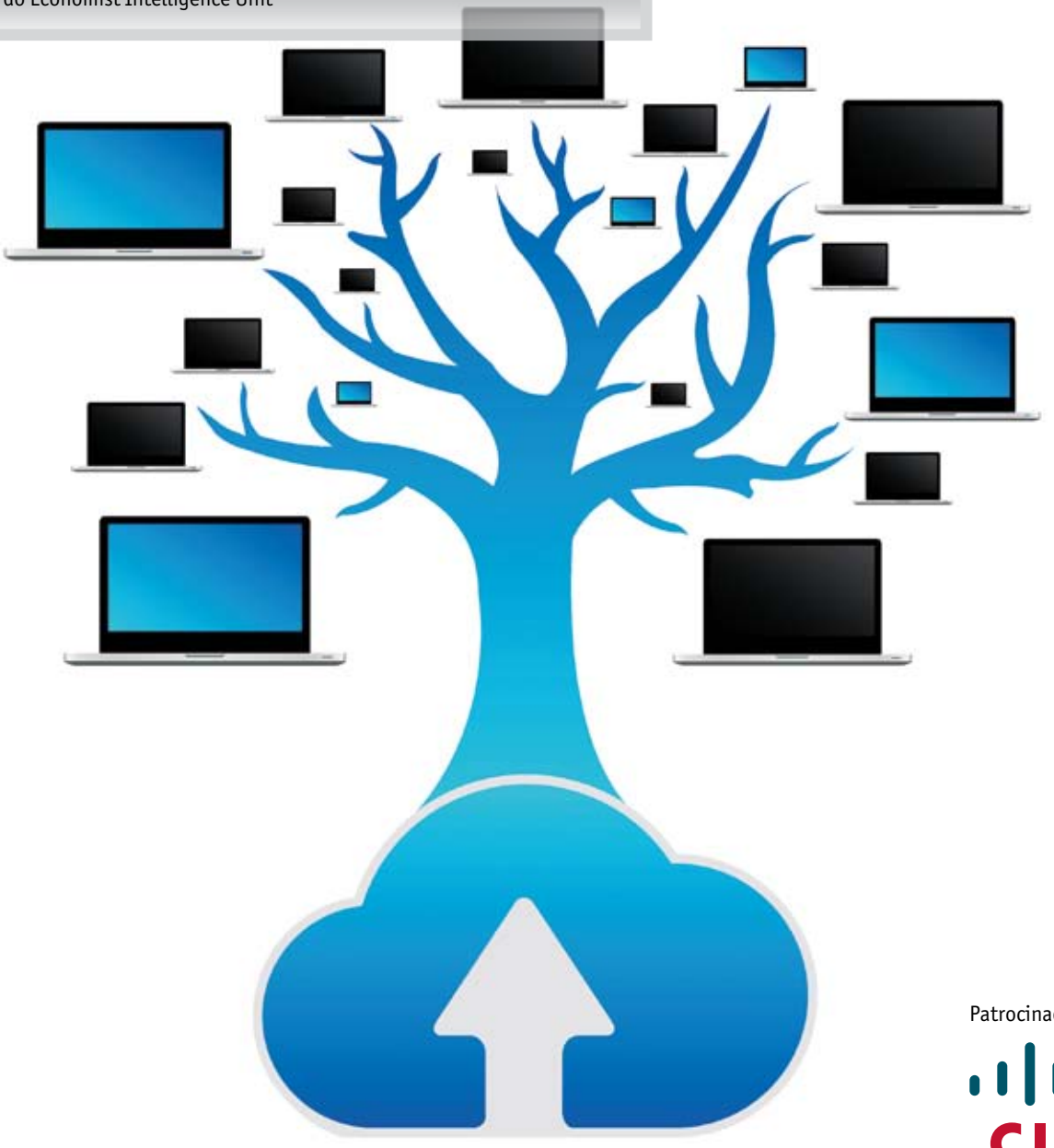
Economist Intelligence Unit

The Economist

Acesso seguro a dados em um universo móvel

Um relato do Economist Intelligence Unit



Patrocinado por

CISCO

Conteúdo

Prefácio

O uso crescente de dispositivos de comunicação do consumidor no local de trabalho e a necessidade de maximizar a produtividade de executivos e funcionários em movimento estão exigindo uma resposta das empresas. *O acesso seguro a dados em um universo móvel* explora como as empresas podem acomodar demandas crescentes pelo acesso móvel a informações comerciais e ao mesmo tempo minimizar os riscos de segurança aos dados de propriedade industrial. Como base para a pesquisa, o Economist Intelligence Unit conduziu em junho de 2012 uma pesquisa global com 578 executivos sêniores. A pesquisa explora como as empresas estão (ou deveriam estar) respondendo aos desafios atuais e emergentes decorrentes da tendência incontível do "traga o seu próprio dispositivo" (BYOD), além da crescente mobilidade dos funcionários em geral. Também realizamos diversas entrevistas mais detalhadas. As descobertas e opiniões expressas neste relatório não refletem necessariamente as opiniões do patrocinador. A autoria é de Lynn Greiner. Michael Singer e Justine Thody editaram o relatório e Mike Kenny foi responsável pelo layout. Gostaríamos de agradecer a todos os executivos que participaram da pesquisa e das entrevistas, incluindo aqueles que ofereceram as suas opiniões, mas preferiram o anonimato, por seu tempo e orientação valiosos.

Entrevistados

Lucy Burrow, diretora de TI, King's College London

Mike Cordy, diretor de tecnologia global, OnX Enterprise Solutions

Steve Ellis, vice-presidente executivo, Wells Fargo

Jay Leek, diretor de segurança de informações, Blackstone Group

Arturo Medina, diretor de tecnologia da informação, Ipsos Mexico

Bill Murphy, diretor de tecnologia, Blackstone Group

Al Raymond, vice-presidente, Aramark

Ashwani Tikoo, diretor de tecnologia, CSC Índia

Resumo executivo

No final da década de 90, surgiram os laptops portáteis e dispositivos móveis que permitiram que os executivos fossem produtivos até mesmo fora do escritório. Dispositivos como o ThinkPad da IBM e o BlackBerry da RIM introduziram uma era de equipamentos móveis multifuncionais que se mostraram irresistíveis aos diretores executivos. Hoje, a população mundial de funcionários móveis se expandiu além dos escritórios dos diretores e espera-se que, até 2015, chegue a 1,3 bilhão de pessoas, aproximadamente 38% da força de trabalho total, de acordo com a IDC, uma empresa de pesquisa tecnológica. De acordo com algumas estimativas, cerca de 76% das empresas atualmente apoiam uma política de BYOD, subitamente empurrando-as para a função de promover o acesso seguro aos dados em dispositivos que não lhes pertencem. A maioria das empresas afirma permitir que os funcionários usem dispositivos pessoais para tomar decisões mais eficazes, aproveitar oportunidades e trabalhar mais eficientemente com seus parceiros e clientes, ou seja, os mesmos motivos que levam as empresas a permitir o acesso móvel a dados em dispositivos pertencentes à empresa.

Em junho de 2012, o Economist Intelligence Unit conduziu uma pesquisa global patrocinada pela Cisco com 578 executivos sêniores para explorar as suas perspectivas sobre a segurança de dados em dispositivos móveis. As principais descobertas da pesquisa são:

- **A maioria dos executivos preocupa-se com as políticas de acesso móvel a dados da empresa.**

Quem participou da pesquisa?

A pesquisa entrevistou 578 executivos sêniores no mundo todo. Os entrevistados estavam sediados principalmente na América do Norte (29%), Europa Ocidental (25%) e a região da Ásia-Pacífico (27%), com o restante no Oriente Médio e África, América Latina e Europa Oriental. Do número total de entrevistados, 23% eram dos EUA, 10% da Índia, 7% do Canadá e 6% do Reino Unido. Em termos hierárquicos, 27% eram CEO, 17% eram vice-presidentes sêniores e 15% eram gerentes. Em relação ao tamanho da empresa, 55% delas tinham receita anual de US$ 500mi ou mais, com 22% com receita igual ou superior a US$ 10bi. Os entrevistados representaram uma variedade ampla de setores, em especial TI e tecnologia (13%), serviços financeiros (11%), serviços profissionais (11%) e energia e recursos naturais (9%). Funcionalmente, os entrevistados identificaram suas funções primárias como gestão geral, desenvolvimento comercial, financeiro e vendas e marketing. ■

Embora 42% dos entrevistados tenham declarado que a diretoria executiva precisa de acesso seguro e conveniente a dados estratégicos de planejamento para serem mais produtivos, somente 28% deles acreditam ser adequado que esses dados sejam acessíveis em dispositivos móveis. Cerca de metade dos entrevistados (49%) afirma que a complexidade de se proteger múltiplas fontes de dados e a falta de conhecimento sobre segurança e risco do acesso móvel (48%) são os principais desafios para as suas empresas.

- **Empresas maiores estão mais propensas a permitir o acesso móvel a dados críticos, mas também impõem regras mais rígidas.** Mais de 90% das empresas com receita superior a US$ 1 bi permitem acesso a dados via dispositivos pessoais ou corporativos. Contudo, mais da metade das empresas com receita superior a US$ 5bi permite acesso somente via dispositivos corporativos, enquanto um terço também permite acesso via dispositivos pessoais. Por outro lado, apenas 37% das empresas com receitas inferiores a US$ 500mi insistem em dispositivos corporativos, enquanto 47% também permitam acesso em dispositivos pessoais. Usuários móveis em grandes empresas devem, contudo, se manter nas linhas de dispositivos aprovados e devidamente verificados de acordo com as políticas.

- **Políticas móveis não devem negligenciar o uso de redes sociais.** Embora 56% dos entrevistados tenham políticas que englobam o uso de redes sociais através de dispositivos móveis, 33% dos executivos entrevistados não podem discutir o seu trabalho em plataformas de mídia social. Uma atenção especial às políticas de redes sociais pode permitir uma interação eficaz, protegendo os ativos de dados corporativos e evitando responsabilidade.

- **A infraestrutura disponível é a principal influência nas políticas da empresa sobre acesso móvel.** Embora 44% dos entrevistados declarem que a pressão dos executivos é uma das influências mais importantes sobre a política, este número é ofuscado pelos 60% que citam exigências de infraestrutura de TI. Isso indica que existe uma oportunidade para empresas que oferecem serviços de proteção e gerenciamento do acesso móvel.

A tendência de acesso móvel a dados é algo que não vai parar? A resposta simples é sim; dispositivos mais sofisticados que oferecem melhor experiência ao usuário servem apenas para acelerar a tendência. Isso significa que as políticas são obrigatórias, não opcionais. De acordo com os executivos entrevistados nesta pesquisa, envolver os funcionários na elaboração dessas políticas certamente aumenta a probabilidade de adesão. ■

Introdução

Adotar as políticas certas para o acesso móvel a dados está se tornando uma preocupação crescente para muitas empresas. Funcionários sêniores, assim como jovens contratados, precisam de acesso aos dados corporativos em qualquer lugar, a qualquer momento, em dispositivos móveis ou fixos. Muitas empresas estão percebendo que o suporte às políticas de dispositivo móvel podem resultar em dividendos na forma de maior engajamento e produtividade, incluindo maior receptividade em atuar fora do horário de trabalho. Locais de trabalho que aceitam a prática de BYOD também têm maior probabilidade de atrair funcionários com conhecimentos em tecnologia, o que geralmente ajuda a incentivar a inovação.

Conforme os dispositivos proliferam e o limite entre a TI corporativa e para o consumidor continuam a se misturar, os desafios que as empresas enfrentam ao adaptarem-se a esta mudança cultural crescerão. Expandir o escopo do acesso a dados comerciais apresenta riscos comerciais óbvios, além de desafios tecnológicos. Dispositivos portáteis podem ser perdidos ou roubados. Os indivíduos podem compartilhar os seus dispositivos com amigos ou parentes, aumentando o risco de vazamento de dados confidenciais. Frequentemente esses dados são acessados a partir de aplicativos não sancionados pela empresa. No entanto, tentar controlar os dispositivos que os funcionários levam para o trabalho, ou controlar como as pessoas usam os dispositivos fora do escritório é cada vez mais inútil para os departamentos de TI. Eles devem responder à vulnerabilidade crescente das redes de dados corporativos através da aplicação de proteções eficazes, tanto para protegerem os dados corporativos críticos, quanto para estarem em conformidade com os ambientes regulatórios em cada região na qual a empresa opera. ■

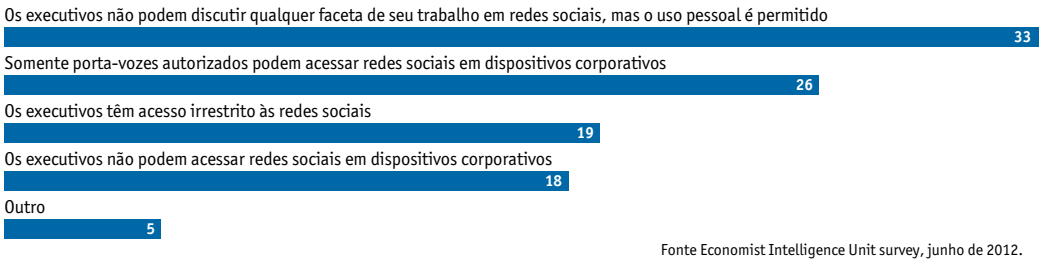
1 Mobilidade moderna: onde estamos agora?

Aproximadamente um bilhão de dispositivos inteligentes conectados foram colocados no mercado em 2011, um número que deve dobrar até 2016, de acordo com a IDC, uma empresa de pesquisa tecnológica. Esses dispositivos incluem produtos baseados em PCs, como laptops e netbooks, telefones celulares e tablets. A pesquisa do Economist Intelligence Unit mostrou que muitas pessoas usam vários dispositivos, muitas vezes uma combinação de laptop e smartphone, embora o uso de tablets esteja crescendo. A produção mundial de tablets no segundo trimestre de 2012 cresceu em 33,6% em relação ao primeiro trimestre e 66,2% em relação ao mesmo trimestre em 2011, de acordo com estimativas do IDC. Espera-se ver um crescimento significativo no uso de tablets após o lançamento da próxima geração de sistemas operacionais. Recursos de colaboração e comunicação adicionados aos novos tablets atrairão executivos com uma maior variedade de opções de acesso a dados do que os smartphones.

Fornecer a executivos em trânsito informações em seus dispositivos móveis permite que eles tomem decisões rápidas e informadas, especialmente em momentos cruciais como negociações, observa Ashwani Tikoo, diretor de tecnologia da CSC Índia, um fornecedor de serviços de TI. No segundo maior centro de operações da CSC global, Tikoo é responsável pelas políticas de segurança que protegem dados comerciais em dispositivos móveis. Ele afirma que a disponibilidade instantânea de dados permite que as equipes de vendas tomem as decisões certas naquele momento, em vez de fazer o cliente esperar. Para evitar a perda de dados, as políticas de segurança da CSC exigem criptografia de dados em todos os dispositivos móveis, incluindo dispositivos pessoais sob uma política de BYOD.

Evitar que os dados sejam armazenados em um dispositivo móvel é outra estratégia. Al Raymond, vice-presidente de gestão de privacidade e registros da Aramark, um fornecedor de serviços de alimentação nos EUA, declara que usuários autorizados, que precisam acessar informações da

Q **Políticas de redes sociais móveis para executivos**
Quais políticas sua empresa enfrenta acerca do uso de redes sociais em dispositivos corporativos? (% de entrevistados)



Fonte Economist Intelligence Unit survey, junho de 2012.

ESTUDO DE CASO Ipsos, uma abordagem híbrida

Em regiões como a América Latina, onde o contato face a face é preferível em pesquisas de mercado, os smartphones e tablets estão substituindo o lápis e papel como as ferramentas preferidas de pesquisa. A Ipsos, uma empresa de pesquisa de mercado global, adotou esta mudança no uso de dispositivos móveis em suas operações no México e em outros locais. A empresa opera atualmente em 84 países e tem 16.000 funcionários em regime de tempo integral. As suas pesquisas abrangem várias metodologias, seja online ou pessoalmente, resultando em mais de 70 milhões de entrevistas por ano mundialmente.

A Ipsos atualmente oferece dispositivos de propriedade da empresa a seus entrevistadores, mas está trabalhando em uma nova abordagem, segundo Arturo Medina, diretor de TI na Ipsos México. "Já que o custo de dispositivos móveis personalizados é muito alto, estamos adotando um modelo híbrido das políticas de BYOD", ele afirma.

No modelo híbrido em desenvolvimento, os entrevistadores podem escolher entre três modelos de smartphone compatíveis com o software de entrevistas da Ipsos. Os funcionários pagam pelo dispositivo através de descontos na folha de pagamento. Em circunstâncias normais, Medina diz que os funcionários tornam-se proprietários do dispositivo em 2-3 semanas.

A Ipsos fornece uma conexão por VPN a seus dados corporativos, enquanto o funcionário paga pelas outras funções do smartphone. A Ipsos gerencia os dispositivos para que possa apagar informações comerciais remotamente, se necessário. Os dados acessados no smartphone são criptografados, evitando algumas perdas. Os entrevistadores também devem aderir às políticas de uso corporativo. Medina observa que os entrevistadores têm a flexibilidade de usar um dispositivo em todos os lugares, e a empresa tem controle suficiente para proteger os seus dados. ■

empresa remotamente, o fazem através de uma rede privada virtual (VPN) segura em seus laptops ou dispositivos móveis. Nenhum dado, além dos e-mails, é armazenado no próprio dispositivo, tornando relativamente fácil a proteção de dados corporativos, caso o funcionário saia da empresa ou perca o dispositivo.

Existem desafios semelhantes em relação a redes sociais em dispositivos móveis fora do escritório, embora as políticas corporativas frequentemente restrinjam a participação dos executivos. Trinta e três por cento dos executivos que responderam à pesquisa do EIU declararam não poderem discutir qualquer faceta de seu trabalho em redes sociais, e outro quarto declarou que somente porta-vozes autorizados podem acessar redes sociais em dispositivos corporativos. Segundo a nossa pesquisa, o uso executivo das redes sociais continuará sendo restringido, seja através de políticas ou de acordos verbais, a fim de proteger as informações corporativas e limitar a responsabilidade jurídica.

Obviamente, diferentes posições na hierarquia da empresa têm acesso a diferentes tipos de dados, e nossa pesquisa rendeu algumas surpresas. Dentre os altos executivos, informações financeiras (60%) e de planejamento estratégico (42%) foram impulsionadores significativos da produtividade. Os gerentes buscam dados operacionais (44%) e dados de vendas e marketing (43%), enquanto funcionários em cargos inferiores precisaram acessar dados de clientes (42%) e operacionais (42%). De acordo com a nossa pesquisa, tomar decisões eficazes (52%) e aproveitar todas as oportunidades (42%) são os principais motivos pelos quais os executivos sêniores buscam acesso móvel a dados comerciais críticos. A conexão com terceiros, tais como fornecedores, tem uma posição especialmente alta na lista de empresas menores; 42% dos entrevistados em firmas com receita inferior a US$ 500mi listam isso como uma das 3 principais razões, comparado aos 37% de todas as firmas. Essa necessidade de se manter conectado ajudou a transformar o e-mail em um aplicativo imprescindível em dispositivos móveis, e ele continua sendo a ferramenta principal usada pelos executivos em nosso estudo para acessar dados comerciais remotamente (81%). ■

2 Perda, roubo e maus hábitos: o que as empresas estão fazendo para superar esses desafios?

Implementar sistemas para proteger os dados da empresa acessados por diversas plataformas diferentes é algo caro. Assim, não é de se surpreender que somente os participantes da pesquisa pertencentes às empresas maiores confiem nas estratégias de segurança de dados de suas empresas. Embora 45% dos entrevistados de empresas com receita anual igual ou superior a US$ 10 bilhões afirmem que sua empresa possui medidas de segurança de dados de última geração, isto cai para apenas 10% dos entrevistados de empresas menores (US$ 500 milhões). Além disso, mesmo entre as empresas com receitas entre US$ 500 mi e US$ 5 bi, aproximadamente um terço delas descrevem suas políticas corporativas como inadequadas ou completamente inadequadas.

No geral, os executivos que entrevistamos aceitam a necessidade de investimento, com 69% deles considerando o investimento em segurança como uma prioridade. Contudo, a nossa pesquisa indica que se deve fazer mais para educar os executivos acerca dos riscos de segurança. Algumas empresas que acreditam possuir um alto nível de segurança permitem, mesmo assim, práticas arriscadas. Por exemplo, dentre os executivos que afirmaram que suas empresas adotam práticas de segurança líderes de mercado (20%), 13% disseram não haver restrições em suas atividades nas redes sociais. Esta prática, obviamente, acarreta um risco de exposição acidental de informações confidenciais da empresa. A nossa pesquisa observou que o estabelecimento de políticas para o uso de redes sociais pode tanto permitir uma interação eficaz quanto ajudar a proteger os ativos de dados corporativos e evitar responsabilidade jurídica.

Com menos recursos que suas contrapartidas maiores, as empresas menores enfrentam desafios mais rigorosos na proteção de dados móveis. Aproximadamente 40% dos entrevistados de empresas com renda anual de US$ 500 mi ou menos descreveram as políticas de segurança de dados móveis na empresa como inadequadas ou completamente inadequadas. Assim como nas empresas maiores, as empresas menores com políticas estabelecidas por escrito podem avançar muito no sentido da proteção de dados corporativos a um custo relativamente baixo. Dispositivos vendidos nos últimos anos têm criptografia embutida que precisa somente ser ativada. Contudo, ferramentas adicionais de gestão são frequentemente necessárias para automatizar os processos de segurança, forçando as empresas menores a escolher entre comprar tecnologias de proteção ou adotar abordagens de menor custo, como manter os funcionários sob as políticas de segurança.

À medida que o poder de até mesmo o menor dos dispositivos móveis continua a aumentar, também aumenta o risco da perda de dados pelos motivos menos tecnológicos. A Kensington, fabricante de dispositivos periféricos para computadores nos EUA, afirma que mais de 70 milhões de smartphones são perdidos anualmente, e apenas 7% deles são recuperados. Laptops também não estão imunes, com a pesquisa da Kensington mostrando que 10% serão perdidos ou roubados ao longo da vida útil do PC. Três quartos das perdas ocorrem em trânsito ou enquanto o funcionário está trabalhando remotamente. Uma

Conhecendo a política de BYOD

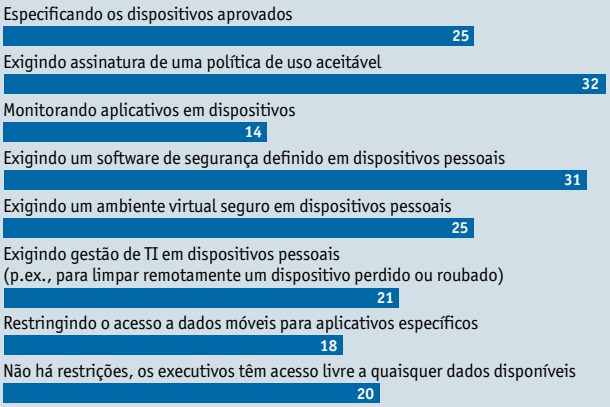
Uma vez que o modelo de BYOD é comparativamente novo, há poucos padrões da indústria já testados para tais políticas. Geralmente, se um funcionário deixa a empresa, voluntariamente ou não, os dados da empresa devem ser rapidamente removidos, de preferência sem interferir nas informações pessoais do funcionário. Políticas aceitáveis de uso para BYOD em geral incluem uma cláusula que permite isso. As empresas também podem se proteger legalmente, modificando suas políticas móveis existentes, segundo recomendações de um abstrato da National Law Review de junho de 2012. Políticas centradas em discriminação, assédio e oportunidades iguais de emprego, confidencialidade e proteção de segredos comerciais, além de políticas sobre adesão e ética também podem ser atualizadas para proteger as empresas contra o abuso das políticas móveis por parte do funcionário.

Para se protegerem contra práticas executivas arriscadas, muitas empresas instalam softwares no dispositivo do funcionário para travar os programas, criptografar os dados e realizar outras funções administrativas, tais como atualizar calendários ou fazer atualizações de segurança. Embora possa parecer invasivo para o funcionário, a maioria das políticas para dispositivos móveis exige algum tipo de controle de acesso administrativo remoto. Algumas empresas com políticas de BYOD esperam que seus executivos e funcionários certifiquem-se de que têm o software necessário em seus dispositivos, às suas próprias custas. Outros oferecem reembolso parcial ou total das despesas com programas exigidos especificamente para os negócios. Práticas adequadas de configuração e bom uso devem ser monitoradas e aplicadas centralmente, segundo Raymond, da Aramark, acrescentando que o treinamento regular para a conscientização sobre a segurança também faz com que os funcionários se lembrem sempre do acesso seguro a dados.

Raymond afirma que a sua empresa tem uma abordagem alternativa para a administração da segurança móvel para dispositivos. Os funcionários usam o dispositivo móvel unicamente como um visualizador, deixando os dados da empresa nos servidores corporativos, onde podem ser acessados com segurança e fazem a parte pesada da computação, e não no dispositivo em si. Os métodos para se fazer isso, inclusive o uso de tecnologia de desktop virtual e o acesso a dados por serviços na web como Salesforce.com, estão se ampliando porque o acesso móvel a redes seguras garante que as empresas controlem a criptografia, a autenticação e a gestão.

Arturo Medina, da Ipsos, que impõe controles semelhantes com base em rede, recomenda um diálogo constante com os funcionários para garantir a adesão e evitar downloads não autorizados de dados corporativos. "Deixe claro quais são os limites entre informações sensíveis e informações pessoais, além do que é arquivado como informação corporativa e o que é considerado informação pessoal", Medina aconselha. ■

Q **Políticas de BYOD**
Como sua empresa implementou a política BYOD para acesso a dados críticos? Selecione todos que se aplicam.
(% de entrevistados)



Fonte Economist Intelligence Unit survey, junho de 2012.

grande porcentagem desses equipamentos perdidos possui algum tipo de dado comercial.

O custo médio de uma violação de dados corporativos atingiu US$ 7,2 mi em 2010, de acordo com o Ponemon Institute, uma empresa de consultoria. Isso é mais do que o dobro do custo médio em 2005. Raymond, da Aramark, acredita que esses números são verdadeiros, dado o número e os tipos de violações, acrescentando que há centenas de pequenos incidentes todos os anos e alguns casos maiores que podem chegar a US$ 25mi–500mi.

Muitos casos de perda de dados móveis são resultado direto da falta de cuidado do usuário, o que é de grande preocupação para as empresas que tentam se proteger das violações de dados causadas por funcionários. O Estudo de *Custos de Violação de Dados* feito em 2011 pelo Ponemon observou que cerca de 30% a 40% das violações foram causadas por negligência, seguido por casos

de ataques maliciosos (43%). O estudo observou que 50% das violações em empresas italianas foram geradas por perda ou roubo de um dispositivo móvel. Somente a Alemanha (42%), a França (43%) e a Austrália (36%) apresentaram mais violações por ataques maliciosos do que aqueles causados por negligência. A Índia foi o único país cujas falhas de sistema ultrapassaram a negligência e os ataques maliciosos como causas de violações.

Algumas perdas notáveis de dados móveis ilustram a facilidade com que uma violação pode ocorrer. O Cancer Care Group, uma clínica de câncer em Indianápolis (EUA), perdeu dados pessoais de mais de 55.000 pacientes, além dos dados de seus funcionários, em julho de 2012, quando o laptop de um funcionário contendo arquivos de backup do servidor foi roubado de um veículo fechado. Os dados não estavam criptografados, contrariando as práticas recomendadas. O MD Anderson Cancer Center, uma clínica médica no Texas, EUA, sofreu duas violações entre junho e julho de 2012. Enquanto um incidente foi causado por um pen drive não criptografado perdido em um ônibus, o outro ocorreu quando um laptop, também sem criptografia, foi roubado da casa de um membro da equipe. Informações sobre mais de 30.000 pacientes foram comprometidas nas duas violações. Após a segunda violação, a instituição iniciou um projeto para criptografar todos os seus dados.

As empresas podem evitar muitas violações de dados ao adicionar proteção por senha aos dispositivos móveis, sejam eles laptops, smartphones ou dispositivos portáteis de armazenamento de dados, e ao criptografar completamente o disco ou pen drive.

Esses dispositivos também devem ter uma segurança física. Por exemplo, eles não devem ser deixados em veículos, mesmo se trancados. Telefones celulares e alguns PCs (equipados com tecnologia VPro da Intel) podem ser desativados e ter seus dados apagados remotamente caso sejam perdidos; quanto mais sensíveis forem os dados que eles contenham, mais importante deverá ser o uso de tais mecanismos, já que a criptografia pode ser quebrada. ■

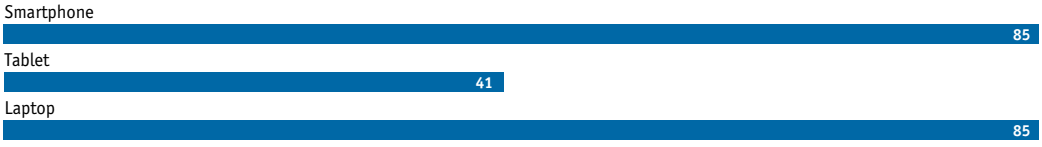
3 Cada vez mais dados em movimento: as tendências emergentes

Cerca de 90% das empresas do mundo permitem acesso móvel a dados críticos, de acordo com a União Internacional de Telecomunicações (ITU), uma agência das Nações Unidas. Dentre as empresas que não têm políticas formais de BYOD identificadas na pesquisa do EIU, 25% afirmam que planejam implantar um programa nos próximos 12-18 meses. Eles notam que este tipo de programa torna os funcionários mais motivados, uma observação confirmada por pesquisas independentes. De acordo com pesquisa conduzida em agosto de 2012 pela iPass, uma empresa de software móvel dos EUA, muitos funcionários trabalham até 20 horas adicionais não remuneradas por semana quando estão sempre conectados. Quase 90% dos entrevistados pela iPass afirmaram que a conectividade sem fio é um componente tão importante quanto a água e a eletricidade em suas vidas.

Embora mais funcionários estejam trabalhando fora do escritório, estabelecer um programa de acesso móvel incluindo BYOD não é uma opção para algumas empresas. Empresas bancárias e financeiras altamente regulamentadas têm políticas rígidas que proíbem o acesso de executivos a dados da empresa a partir de seus dispositivos pessoais. Steve Ellis, vice-presidente da Wells Fargo, observa que sua empresa está abordando o BYOD com cuidado e no momento está avaliando as opções. Ainda pode levar mais um ano para termos um plano formal, afirma Ellis. Outras empresas sem uma política formal de BYOD relatam a entrada de dispositivos pessoais escondidos. Antes da introdução da política formal móvel na Aramark há dez meses, as pessoas não tinham regras definidas sobre quais dispositivos e sistemas operacionais podiam ser conectados à rede da empresa. Com a nova política, implicando acesso baseado no cargo do funcionário e dispositivos e configurações aprovados, a empresa sabe exatamente quem tem acesso e a quais dados. "Não se trata mais de uma piscadinha e um balançar de cabeça", declarou Raymond. Quanto maior a visibilidade de seu programa, mais provável será que as pessoas o sigam.

Políticas a parte, a natureza dos dispositivos também mudou. Atualmente, pouco mais que um quarto (27%) do acesso a dados críticos ocorre a

Q **Dispositivos de acesso a executivos**
Quais dispositivos sua empresa oferece aos executivos para acesso a dados críticos?
Selecione todos que se aplicam.
(% de entrevistados)



Fonte Economist Intelligence Unit survey, junho de 2012.

ESTUDO DE CASO O EEOC dos EUA inicia um projeto piloto de mobilidade

O orçamento da Equal Employment Opportunity Commission (EEOC) para 2012 foi reduzido em aproximadamente 15%, de US$ 17,6mi para US$ 15mi. Com a necessidade de redução dos custos operacionais, a Diretora de Tecnologia e Informação Kimberly Hancher reduziu o orçamento para dispositivos móveis da agência pela metade. Para ajudar a preencher a lacuna, a agência lançou um projeto piloto de BYOD. O projeto focou em oferecer aos funcionários acesso ao e-mail da agência, calendários, contatos e tarefas. Como parte do projeto, alguns executivos sêniores receberam acesso "privilegiado" aos sistemas internos da agência.

Na fase inicial de teste, 40 voluntários devolveram seus aparelhos BlackBerry fornecidos pelo governo e passaram a usar os seus smartphones pessoais. A equipe de segurança de informação, jurídica e o sindicato criaram regras que equilibraram a privacidade do funcionário (políticas de mídia social, políticas de monitoramento) com a segurança governamental, como o regulamento do Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA SP 800-53 (também conhecido como "controles de segurança recomendados para sistemas de informação e organizações federais"). A segunda fase do programa iniciou em junho de 2012. O EEOC trabalhou com seus contratados para configurar o acesso ao e-mail da agência para funcionários participando do teste secundário. Aos demais 468 funcionários da agência usando dispositivos BlackBerry fornecidos pelo EEOC foram fornecidas três opções:

1. Devolver voluntariamente o BlackBerry e trazer para o trabalho um smartphone Android, Apple ou BlackBerry ou um tablet.

2. Devolver o BlackBerry e aceitar um telefone celular fornecido pelo governo somente com recursos de voz.

3. Manter o BlackBerry entendendo que o EEOC não tem aparelhos de reposição.

Os gerentes do EEOC relataram resultados positivos do projeto piloto até o momento. Os funcionários pagam por seus próprios pacotes de voz e dados e a agência cobre as licenças para o software de gestão. O Sr. Hancher do EEOC observou que, para alguns funcionários, o custo pode ser um problema, e uma questão pendente é se a agência poderá oferecer algum tipo de reembolso parcial dos serviços de dados e voz. Hancher nota que o sucesso foi alcançado através do envolvimento de funcionários, sindicato e departamento jurídico desde o início do processo. ■

partir de smartphones, de acordo com a nossa pesquisa. Os entrevistados esperam que isso aumente para mais de um terço (35%) nos próximos 12-18 meses, com outros 30% de dados críticos acessados por outros dispositivos móveis, em relação ao atual um quinto. Com o advento de novos softwares e seus dispositivos associados, os tablets devem se tornar um janela móvel mais amplamente usada para dados corporativos de executivos, talvez substituindo smartphones um dia, de acordo com um artigo da revista *The Economist* (outubro de 2011). A tela maior expande a gama de dados que podem ser visualizados eficazmente e, junto com teclados externos, eles permitem uma interação mais fácil com aplicativos.

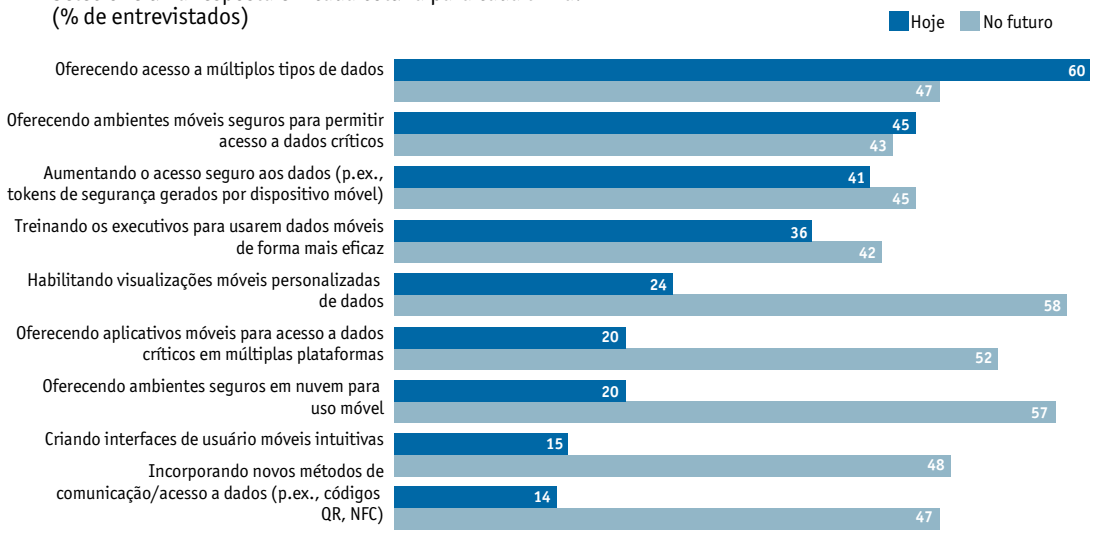
Curiosamente, embora 42% dos entrevistados tenham declarado que os altos executivos precisam de acesso seguro e conveniente a dados estratégicos de planejamento para serem mais produtivos, somente 28% acreditam que é adequado que esses dados sejam acessíveis em dispositivos móveis. O principal desafio é, não surpreendentemente, a preocupação sobre segurança potencial e outros riscos. Todavia, somente 11% dos entrevistados em nossa pesquisa declararam que sua empresa não oferece acesso a dados críticos fora do escritório. ■

4 Como as empresas podem garantir políticas móveis eficazes?

Os entrevistados claramente reconhecem as vantagens de se permitir o acesso móvel a dados e estão cientes dos investimentos necessários. Algumas das medidas que as empresas precisam adotar para proteger os dados corporativos acessados por dispositivos móveis podem ser colocadas em prática remotamente. Atualmente, os gerentes de TI podem adicionar recursos de segurança aos laptops, smartphones e tablets, frequentemente usando as ferramentas de gestão existentes. Eles também podem separar os dados da empresa dos dados pessoais, além de duplicar e armazenar dados comerciais em redes corporativas. Desktops virtuais oferecem acesso móvel seguro a dados em laptops pessoais. Essas proteções permitem que os funcionários móveis recuperem os dados em caso de perda ou dano ao dispositivo com esforço mínimo. De acordo com os entrevistados, essas medidas permitirão que mais executivos no futuro acessem dados corporativos com segurança a partir de qualquer computador.

Para os altos executivos que viajam muito, menos tempo gasto na atualização de protocolos de segurança significa mais tempo para o trabalho. No futuro, a segurança de dados será fortalecida com a ajuda de tecnologias integradas diretamente

Q Autorização móvel
De que modos sua empresa autoriza o acesso a dados críticos hoje e como isso pode mudar no futuro? Selecione uma resposta em cada coluna para cada linha.
(% de entrevistados)



Fonte Economist Intelligence Unit survey, junho de 2012.

aos aplicativos que protegem os dados em si, dificultando a intercepção e o uso indevido, declarou Tikoo da CSC. "Os aplicativos devem ser capazes de reconhecer que estou trabalhando em um iPad ou numa tela de 5 polegadas e processar os dados de forma adequada".

Raymond afirma que, embora não haja essa necessidade em seus negócios, ambientes separados para uso comercial e pessoal são importantes. Contudo, haverá consequências se as políticas adjacentes ou quaisquer outras medidas de segurança não forem aplicadas. Ele afirma que é sempre surpreendido quando conversa com seus colegas sobre como o nível de segurança em grandes empresas é apenas ilusório. As palavras estão lá, mas não são cumpridas.

A Ipsos, uma empresa de pesquisa global, exige que cada funcionário conclua um curso de treinamento sobre segurança pela intranet corporativa, o que é uma boa relação custo-benefício para atingir os funcionários em 84 países. Embora o programa tenha sido desenvolvido internamente, produtos comercialmente disponíveis para segurança que podem ser personalizados para as necessidades locais são prontamente disponibilizados por organizações como o Instituto de Segurança Nacional dos EUA (NSI). Os funcionários também devem assinar uma política de uso aceitável de dispositivos móveis que cobre tudo, desde o tipo de dados que eles podem acessar a partir de um dispositivo móvel até as regras sobre a força de senhas.

Outras proteções de segurança exigem uma atitude confiável por parte dos usuários. Embora os dispositivos móveis devam ter senhas, a Coalfire, uma empresa de auditoria, estima que atualmente apenas metade dos dispositivos pessoais possuam. Os funcionários em um programa de BYOD devem concordar que, se seus dispositivos pessoais forem roubados ou perdidos, a responsabilidade do departamento de TI inclui a exclusão remota das informações em dispositivos pessoais para proteger os dados da empresa.

Há obviamente uma maneira para que a maioria das empresas conscientizem a equipe sobre as questões de segurança decorrentes do acesso móvel de dados da empresa. A pesquisa indicou que executivos fora da Europa e da América do Norte apresentam maior resistência às políticas de segurança de dados em dispositivos pessoais. Ainda assim, em um mundo cada vez mais interconectado, falhas de segurança em uma região podem afetar as empresas subsidiárias (e seus clientes) em outro local. ■

5 Conclusão

O acesso de dados móveis não só irá expandir, como a tendência não pode ser interrompida. Dispositivos sem gerenciamento e segurança já se infiltraram no ambiente comercial, colocando os dados das empresas em risco e abrindo uma porta para ataques através de dispositivos comprometidos. Quase um terço dos entrevistados em nossa pesquisa relatam políticas de dispositivo móvel inadequadas em suas empresas. Estabelecer políticas sensatas e exequíveis é o primeiro passo para alcançar um programa de acesso móvel a dados viável.

Executivos que classificam suas políticas de dispositivos como líderes de mercado indicam que usam os dados móveis para tomar decisões mais eficazes e colaborativas, evitar a perda de oportunidades e trabalhar de forma mais eficaz com os parceiros e clientes. Para garantir que esse acesso não comprometa os dados comerciais, os executivos podem querer priorizar os programas que reduzem o risco e apoiar investimentos em serviços de dados e segurança.

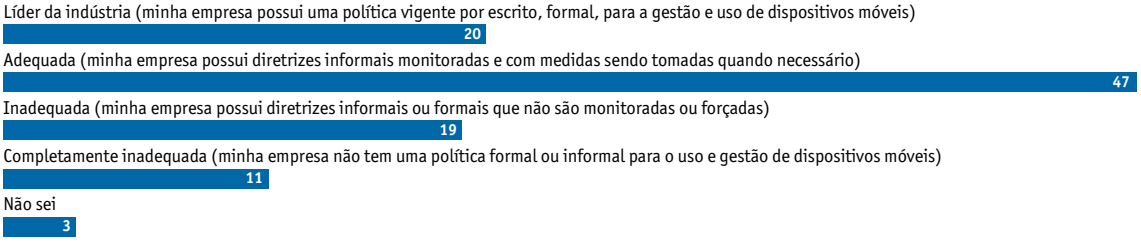
Dispositivos conectados estão se tornando cada vez mais uma parte integrante dos negócios globais. O tipo de dispositivo em uso está evoluindo, com os tablets sendo o dispositivo preferido atualmente. Podemos esperar um crescimento significativo no uso de tablets após o lançamento da próxima geração de sistemas operacionais, que darão aos tablets uma variedade maior de opções de acesso a dados do que os smartphones. Segundo os analistas, isso será uma faca de dois gumes, já que os tablets serão dispositivos complementares aos sistemas existentes, não substitutos.

No futuro, a proteção de dados críticos pode significar a criação de exigências ainda mais rigorosas ao acesso. A mudança para o uso dos tablets em negócios fora do escritório, por exemplo, abrirá um novo conjunto de desafios, já que irá encorajar os executivos a buscar acesso móvel a uma gama mais ampla de dados. Isso vai exigir que muitas empresas comecem a ver a questão sob uma nova perspectiva, dos dispositivos e seus pontos fracos até a infraestrutura disponível aos próprios usuários. ■

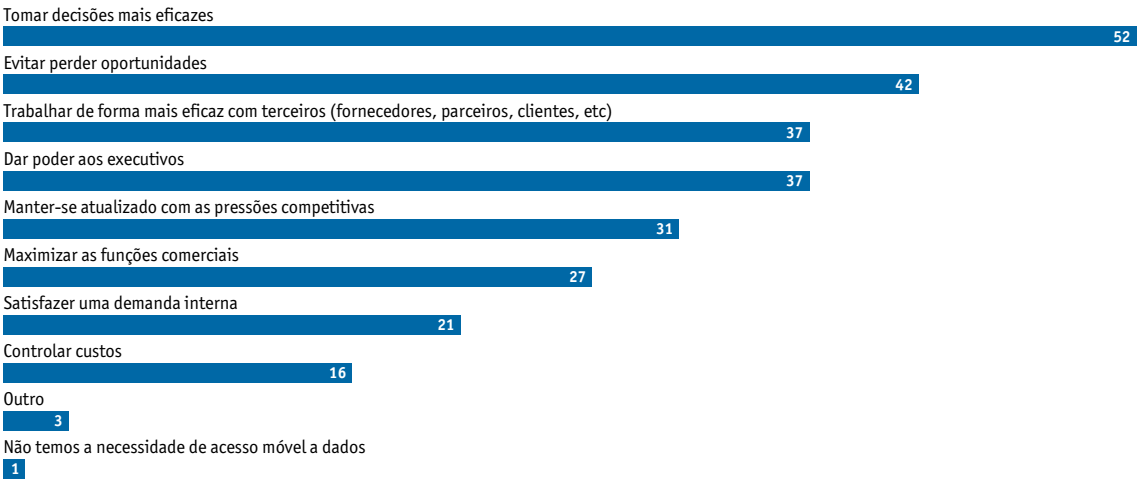
Apêndice: resultados da pesquisa

As porcentagens podem não somar 100% devido ao arredondamento ou à capacidade dos entrevistados de escolher múltiplas respostas.

Com base em suas observações, como a política de dispositivos móveis em sua empresa se compara a de seus concorrentes no setor?
(% de entrevistados)

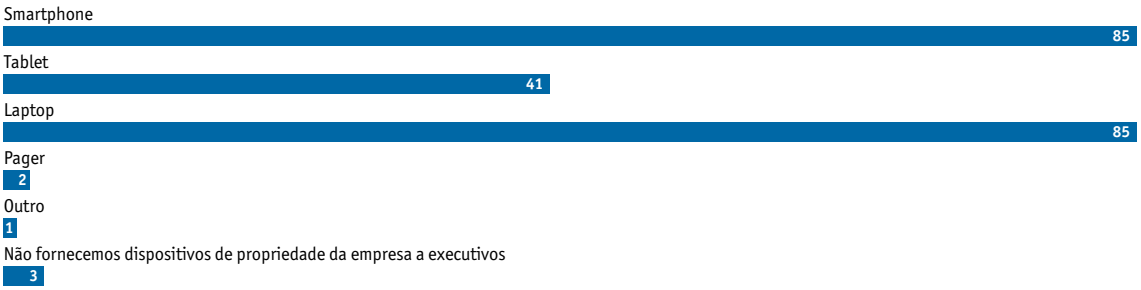


Quais fatores líderes de negócios estão motivando a necessidade de acesso de dados críticos a partir de dispositivos móveis?
Selecione até três.
(% de entrevistados)



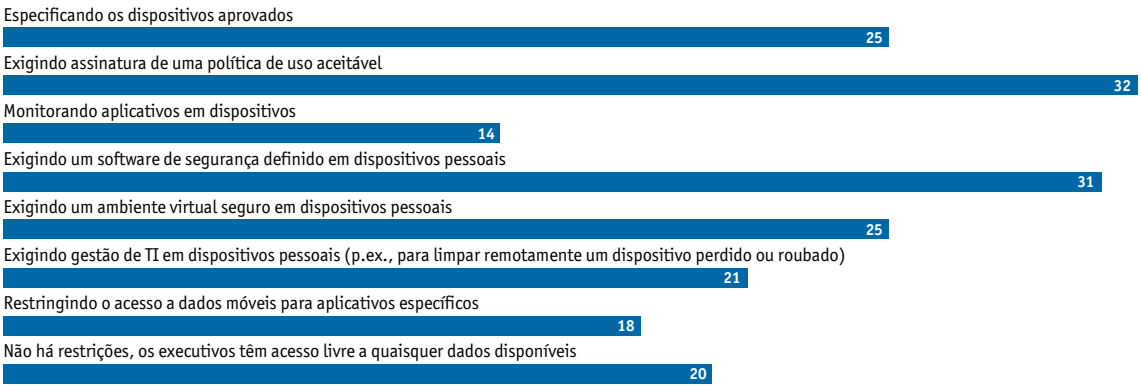
Sua empresa permite o acesso a dados críticos fora do escritório?
(% de entrevistados)

Quais dispositivos sua empresa oferece aos executivos para acesso a dados críticos?
Selecione todos que se aplicam.
(% de entrevistados)

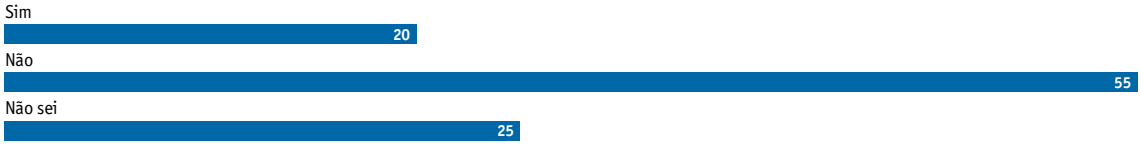


Sua empresa permite que os executivos levem seus próprios dispositivos (política BYOD) e usá-los em vez de usar dispositivos da empresa para acessar dados críticos?
(% de entrevistados)

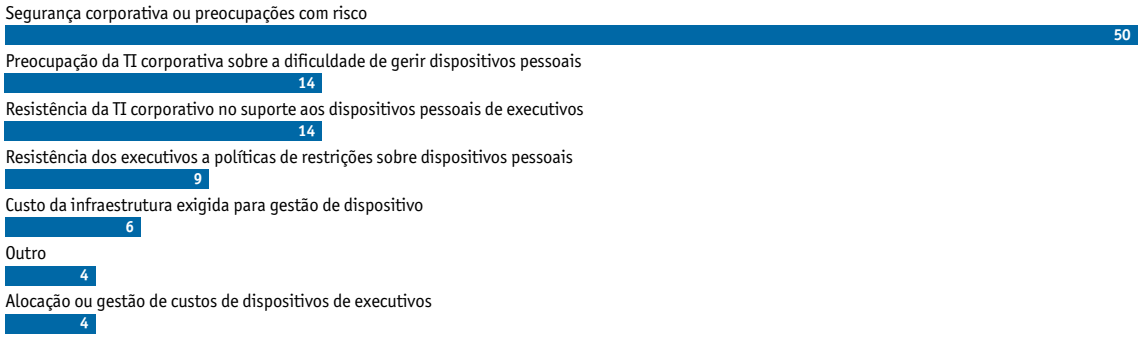
Como sua empresa implementou a política BYOD para acesso a dados críticos?
Selecione todos que se aplicam.
(% de entrevistados)



Sua empresa planeja implementar BYOD (política "traga seu próprio dispositivo") para acessar dados críticos?
(% de entrevistados)

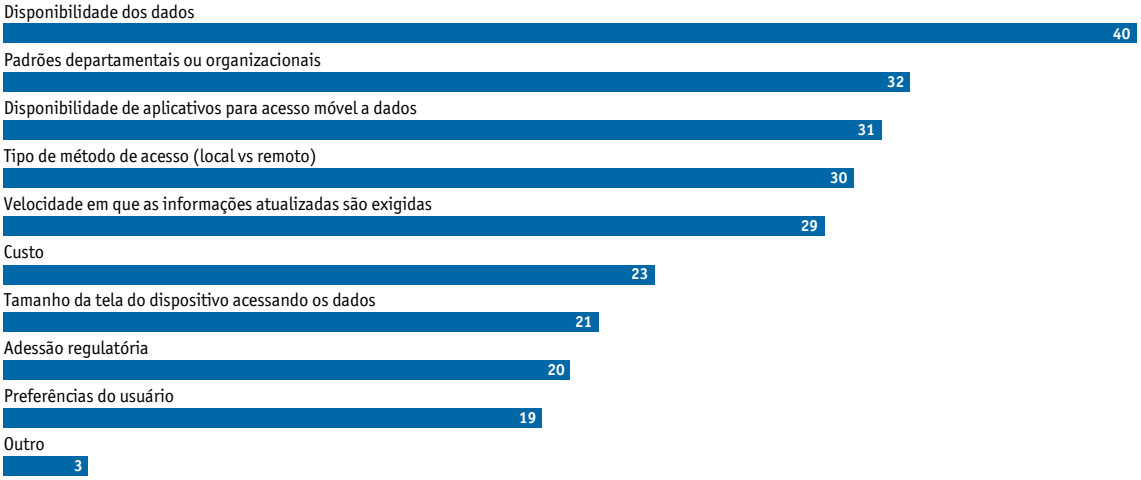


Qual você acredita ser o maior obstáculo à implementação da política BYOD para acesso a dados críticos?
(% de entrevistados)

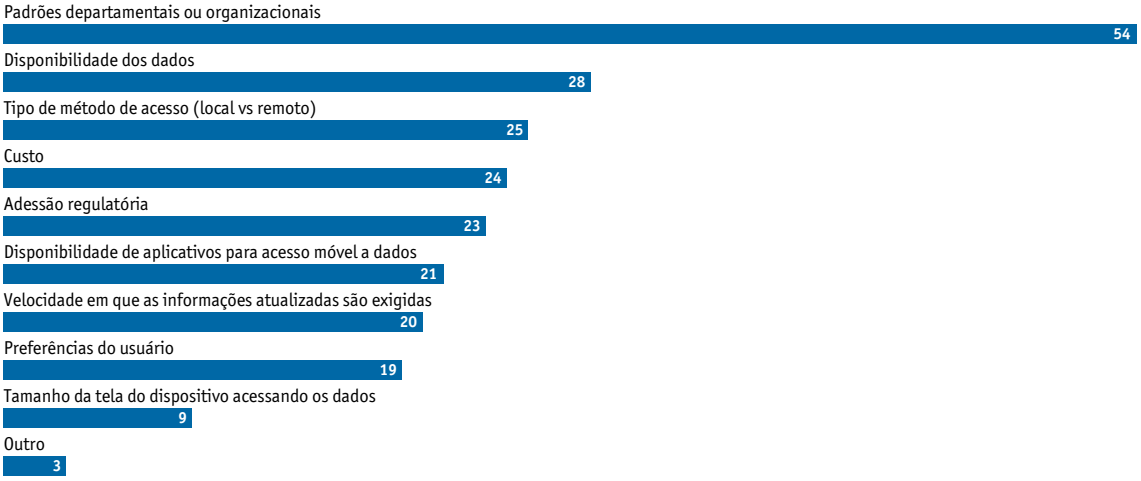


Em sua opinião, quais são os maiores desafios que sua empresa enfrenta em relação ao acesso seguro a dados críticos por dispositivos móveis, propriedade da empresa ou do executivo?
Selecione até quatro.
(% de entrevistados)

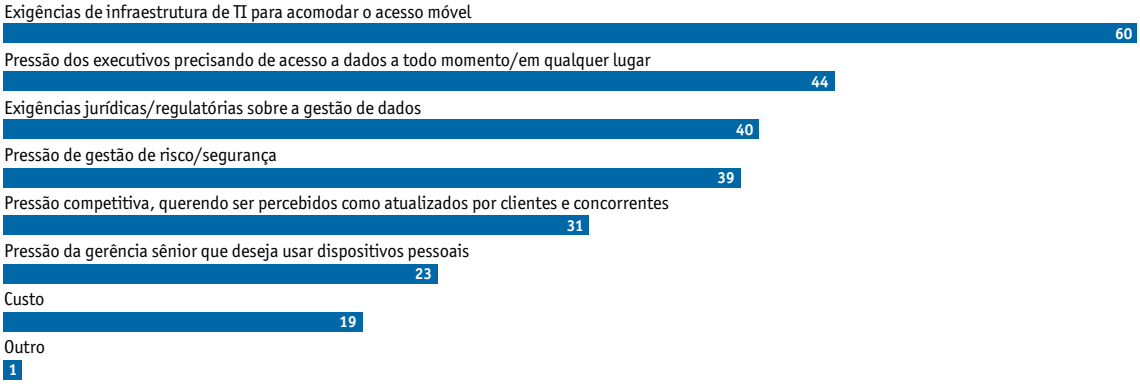
Além de seu cargo, o que determina quais dados são/estarão disponíveis aos dispositivos móveis?
Selecione até três.
(% de entrevistados)



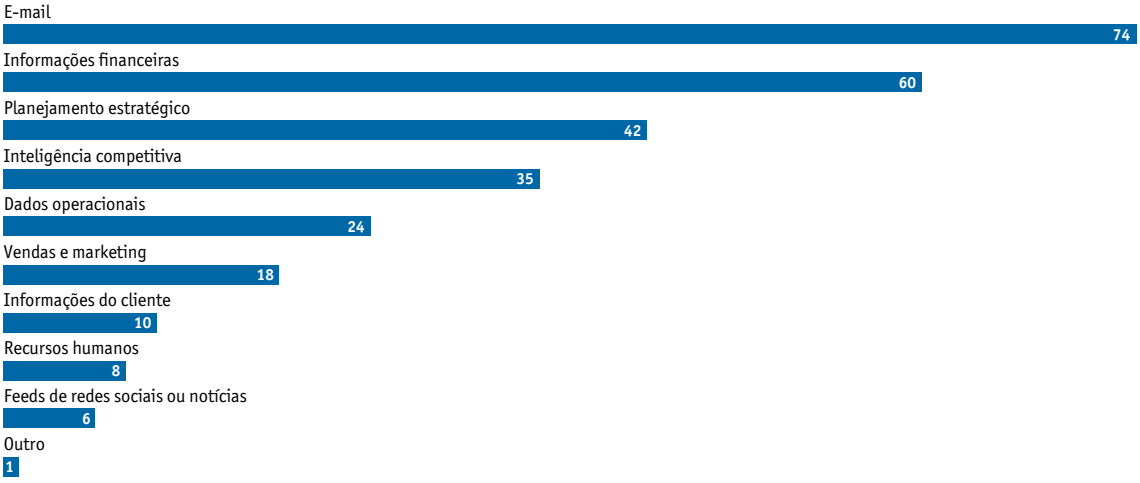
O que determina quais usuários podem/poderão acessar dados críticos em dispositivos móveis?
Selecione até três.
(% de entrevistados)



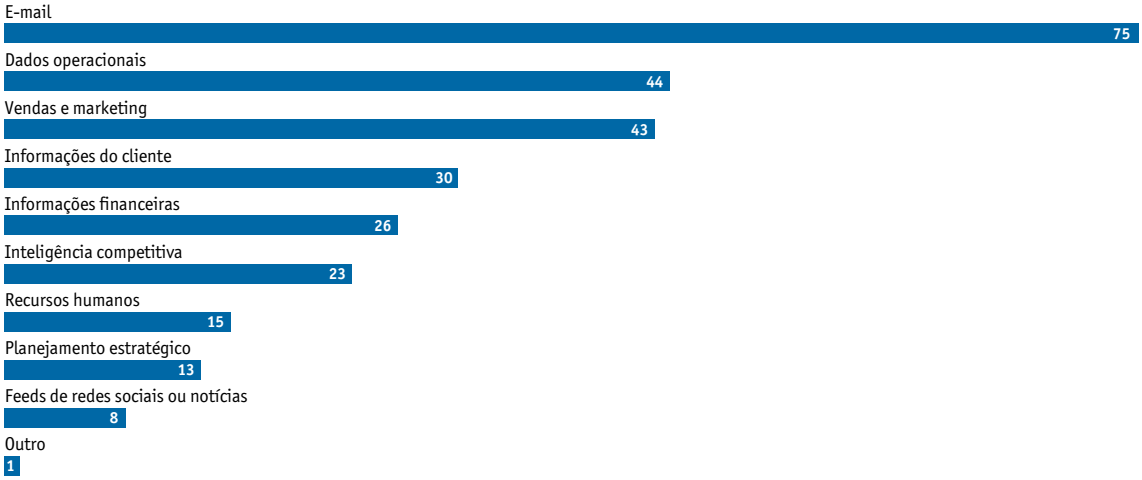
Quais são as influências mais importantes sobre as políticas da empresa e abordagens para criação de uma estratégia de aplicativos e dispositivos móveis?
Selecione até três.
(% de entrevistados)



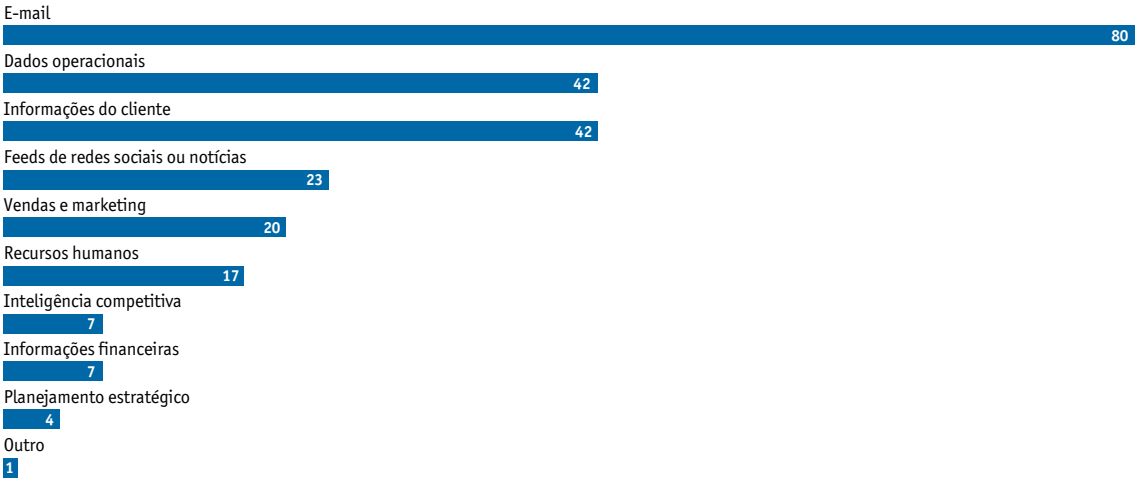
Quais informações listadas devem ser entregues de forma segura e conveniente para que as funções a seguir sejam mais produtivas?
—Executivos de nível C
Selecione até três para cada função.
(% de entrevistados)



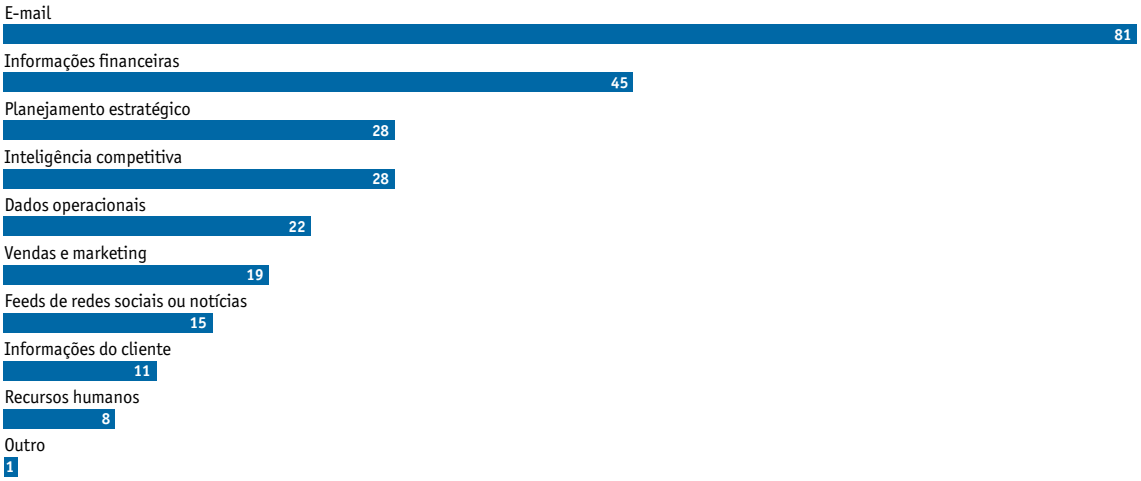
Quais informações listadas devem ser entregues de forma segura e conveniente para que as funções a seguir sejam mais produtivas?
—Gerentes comerciais
Selecione até três para cada função.
(% de entrevistados)



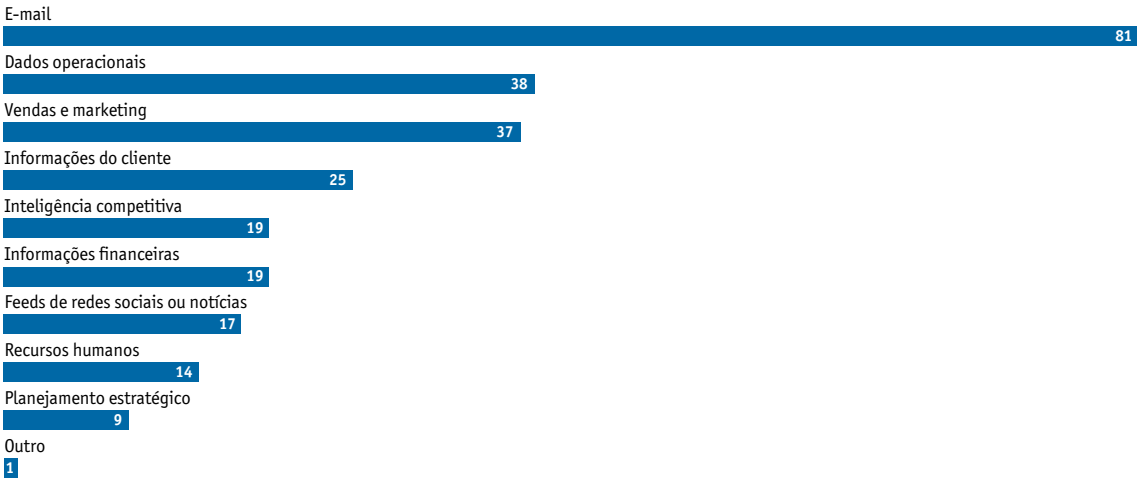
Quais informações listadas devem ser entregues de forma segura e conveniente para que as funções a seguir sejam mais produtivas?
—Funcionários
Selecione até três para cada função.
(% de entrevistados)



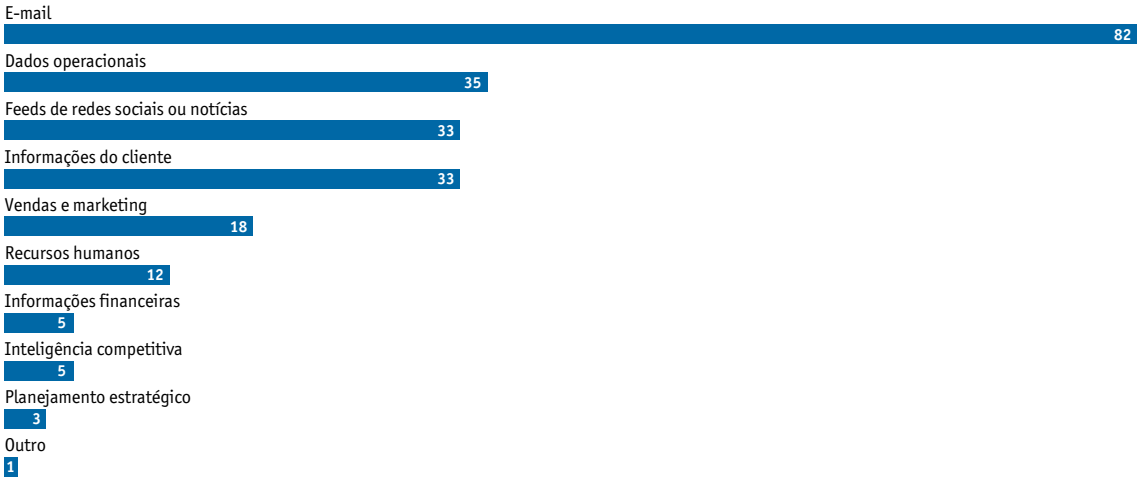
Quais desses tipos de informações/mídias são adequadas para acesso por dispositivos móveis?
—Executivos de nível C
Selecione até três para cada função.
(% de entrevistados)



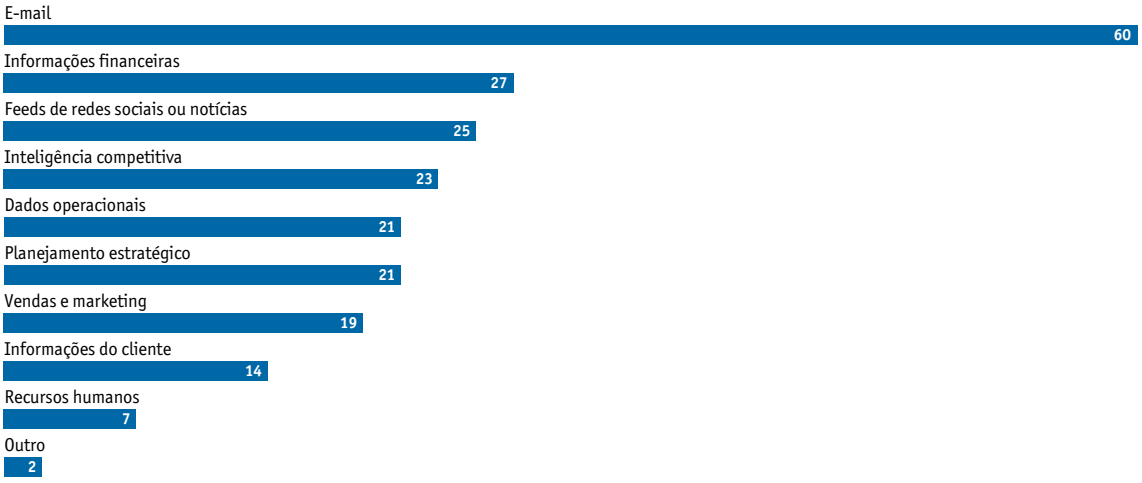
Quais desses tipos de informações/mídias são adequadas para acesso por dispositivos móveis?
—Gerentes comerciais
Selecione até três para cada função.
(% de entrevistados)



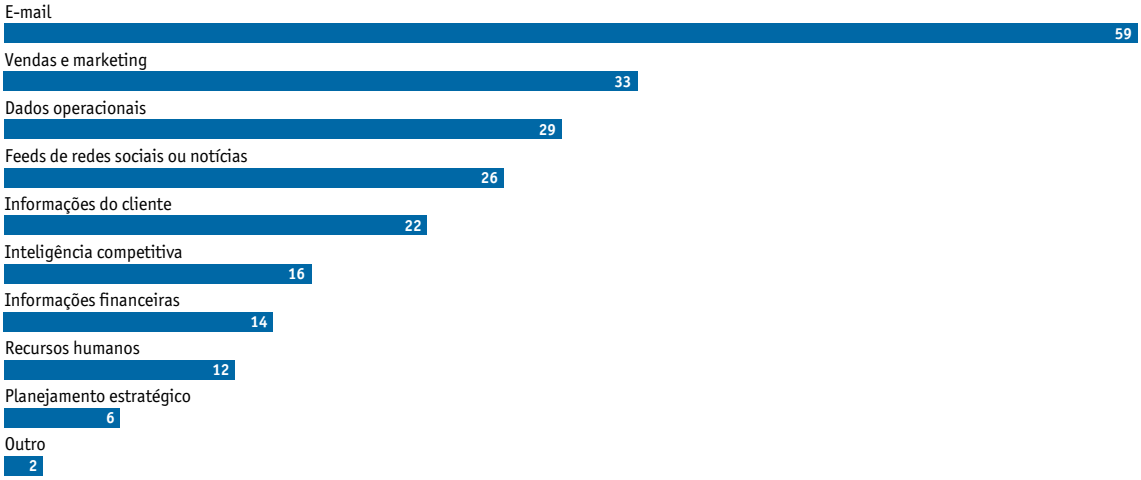
Quais desses tipos de informações/mídias são adequadas para acesso por dispositivos móveis?
—Funcionários
Selecione até três para cada função.
(% de entrevistados)



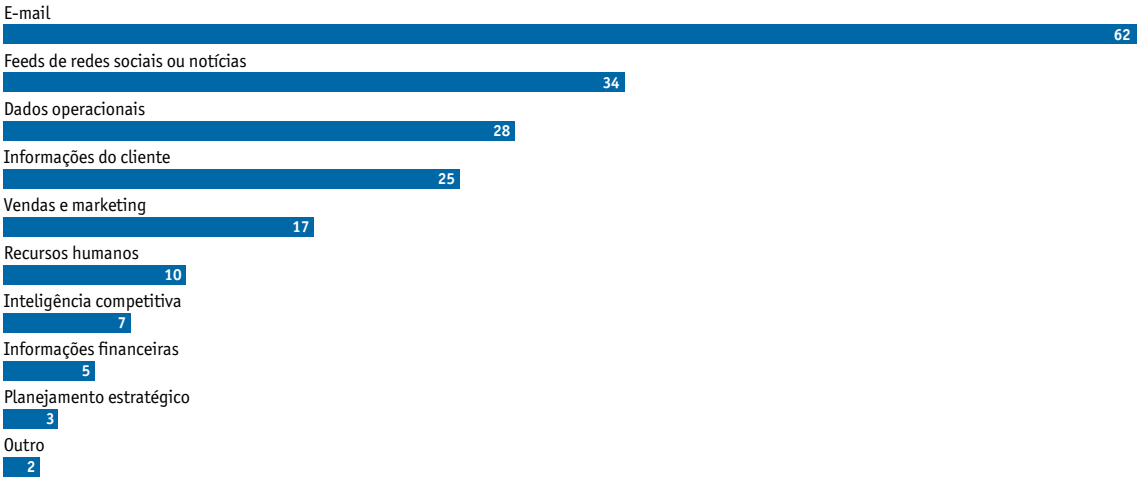
Quais desses tipos de informações/mídias são adequadas para acesso por dispositivos móveis de armazenamento em nuvem?
—Executivos de nível C
Selecione até três para cada função.
(% de entrevistados)



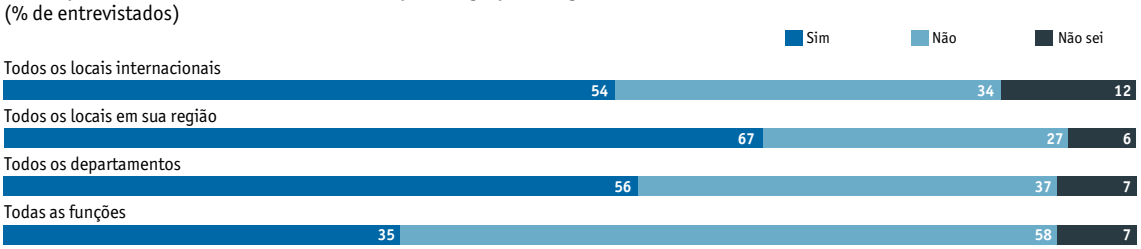
Quais desses tipos de informações/mídias são adequadas para acesso por dispositivos móveis de armazenamento em nuvem? —Gerentes comerciais
Selecione até três para cada função.
(% de entrevistados)



Quais desses tipos de informações/mídias são adequadas para acesso por dispositivos móveis de armazenamento em nuvem? —Funcionários
Selecione até três para cada função.
(% de entrevistados)



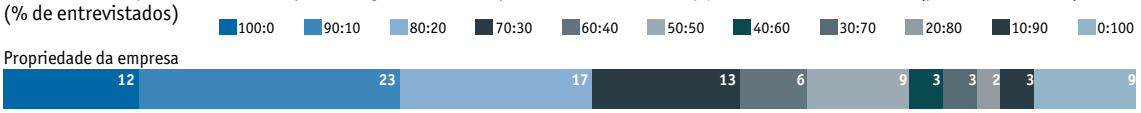
Sua empresa oferece acesso móvel aos dados para os grupos a seguir?
(% de entrevistados)



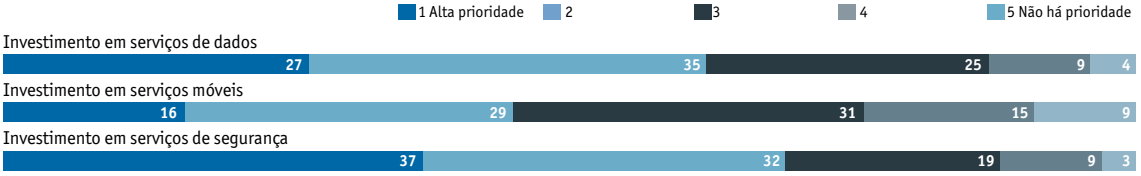
Sua empresa tem políticas vigentes para uso aceitável de redes sociais (p.ex., Facebook, Twitter) em dispositivos corporativos?
(% de entrevistados)

Quais políticas sua empresa enfrenta acerca do uso de redes sociais em dispositivos corporativos?
(% de entrevistados)

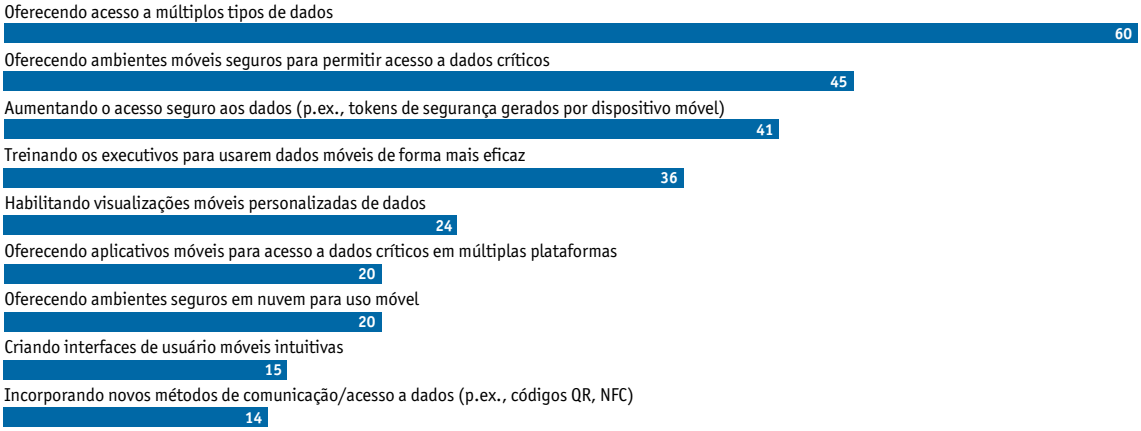
Qual é a proporção de tempo que você usa em dispositivos móveis que são propriedade da empresa em comparação a dispositivos pessoais para sua empresa?
Deslize o botão para escolher uma porcentagem relevante que reflete como cada opção deve ser considerada (p.ex., 60% a 40%).
(% de entrevistados)



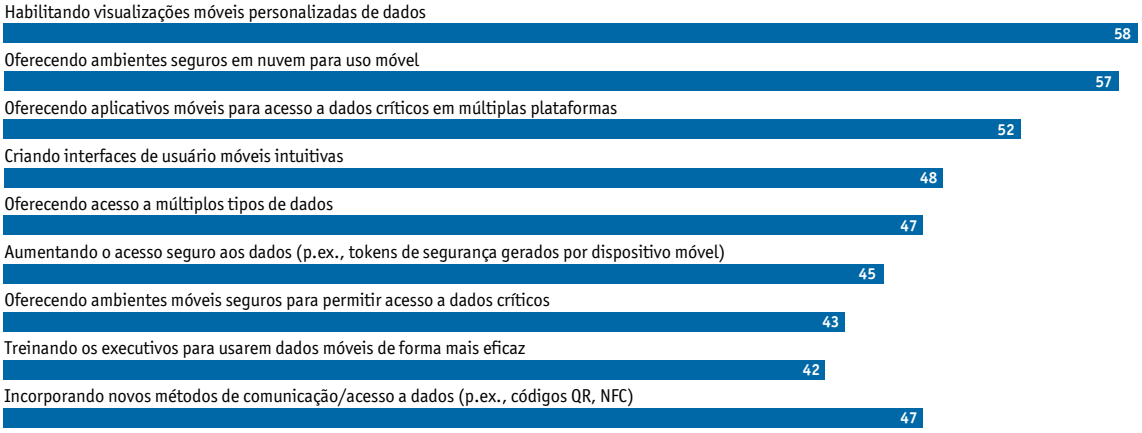
Como sua empresa prioriza as estratégias a seguir?
Classifique em uma escala de 1 a 5, onde 1=Alta prioridade e 5=Não há prioridade.
(% de entrevistados)



De que modos sua empresa autoriza o acesso a dados críticos hoje e como isso pode mudar no futuro? —Hoje
Selecione uma resposta em cada coluna para cada linha.
(% de entrevistados)



De que modos sua empresa autoriza o acesso a dados críticos hoje e como isso pode mudar no futuro? —No futuro
Selecione uma resposta em cada coluna para cada linha.
(% de entrevistados)



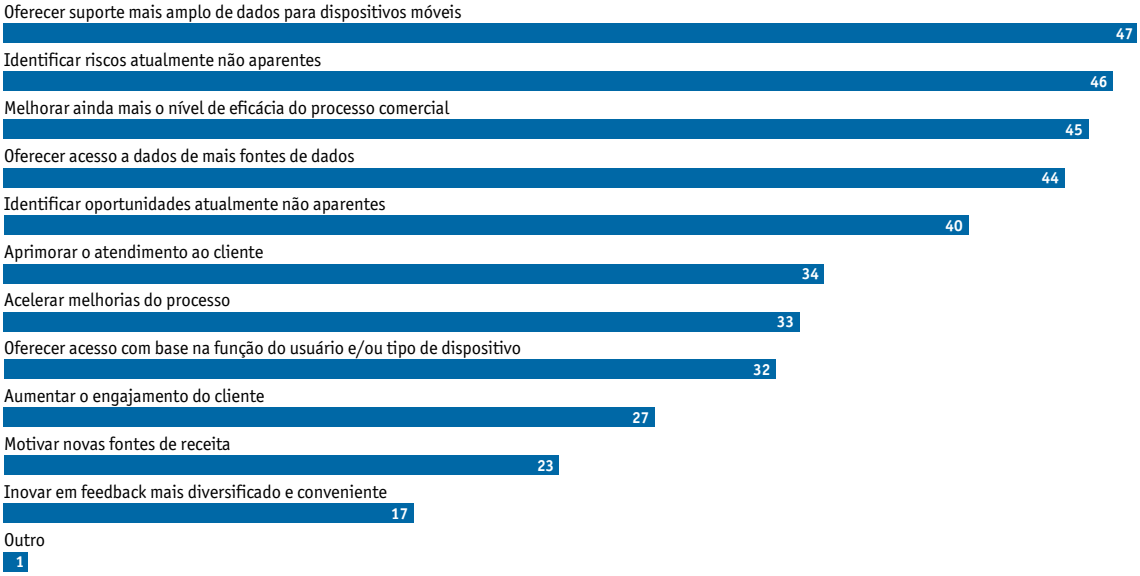
Qual é a proporção de dados críticos que você acessa por canais móveis atualmente?
0 total deve ser de 100%

	Média
Móvel via smartphone	26,9
Móvel em outros dispositivos (p.ex., tablet)	21,7
Acesso não móvel	59,8

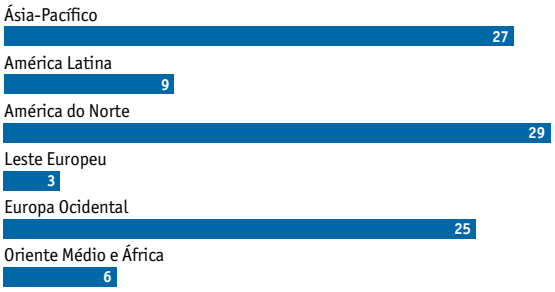
Qual será a proporção de dados críticos que você acessará por canais móveis nos próximos 12-18 meses?
0 total deve ser de 100%

	Média
Móvel via smartphone	34,5
Móvel em outros dispositivos (p.ex., tablet)	30,2
Acesso não móvel	42,8

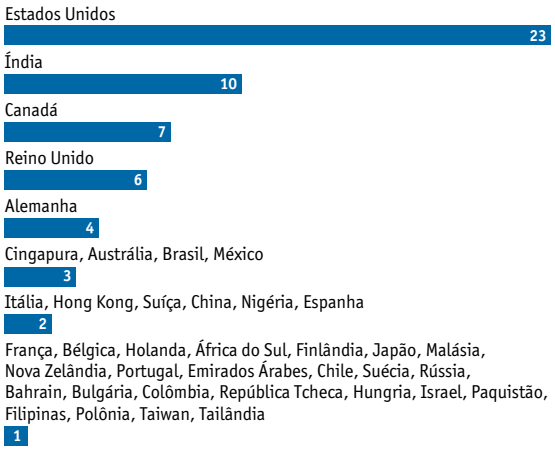
Nos próximos 12–18 meses, o que sua empresa espera fazer para acessar dados críticos que atualmente não pode/consegue fazer?
Selecione todos que se aplicam.
(% de entrevistados)



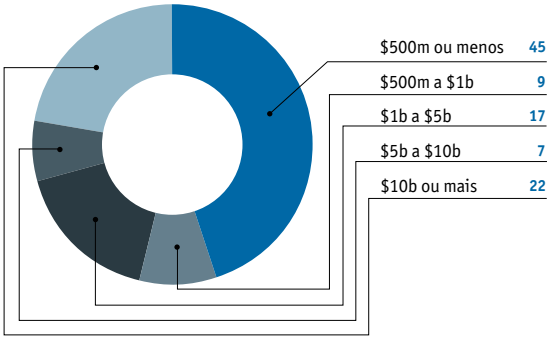
Em qual região você está?
(% de entrevistados)



Em que país você está?
(% de entrevistados)

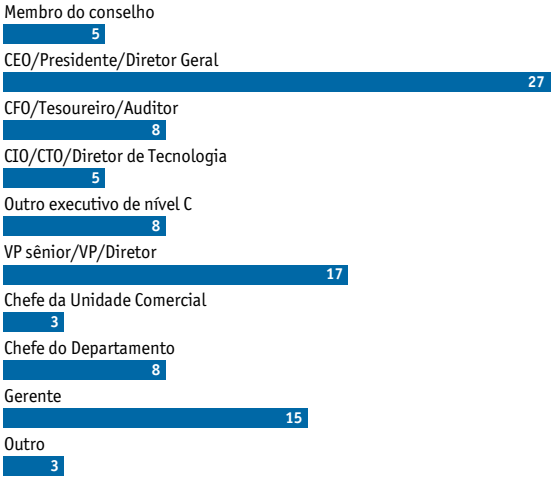


Qual é a renda anual global de sua empresa (em dólares)?
(% de entrevistados)

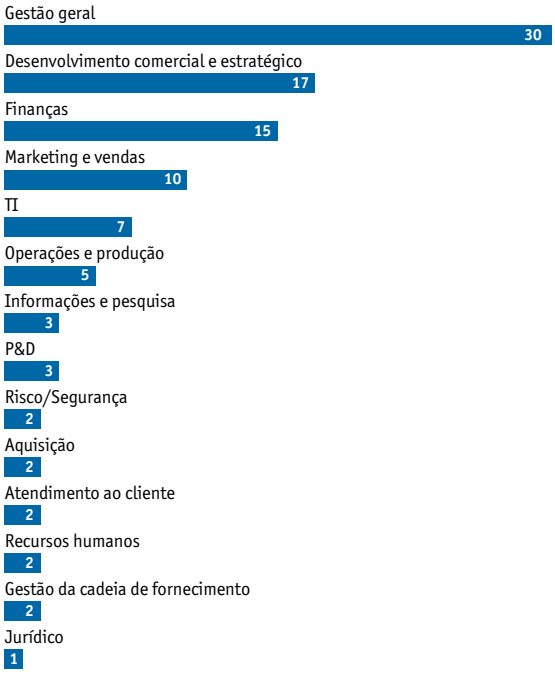


Qual é o seu setor primário?
(% de entrevistados)

Qual das opções a seguir melhor descreve seu cargo?
(% de entrevistados)



Qual é a sua principal função?
(% de entrevistados)



Embora todo esforço tenha sido feito para verificar a exatidão destas informações, nem o The Economist Intelligence Unit Ltd., nem o patrocinador desta pesquisa aceitam qualquer responsabilidade ou obrigação por consequência da confiança depositada neste white paper ou qualquer informação, opinião ou conclusão contidos neste white paper.

Capa: Shutterstock

Londres
26 Red Lion Square
Londres
WC1R 4HQ
Reino Unido
Tel: (44 20) 7576 8000
Fax: (44 20) 7576 8476
E-mail: london@eiu.com

Nova York
750 Third Avenue
5º andar
Nova York, NY 10017
Estados Unidos
Tel: (1 212) 554 0600
Fax: (1 212) 586 0248
E-mail: newyork@eiu.com

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

Geneva
Boulevard des
Tranchées 16
1206 Geneva
Suíça
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com