Relatório

# Céu azul à frente?

## O estado da adoção da nuvem

intel Security

## Sumário

Agradecemos os 1.200 principais entrevistados da pesquisa pela participação e os seguintes altos executivos por compartilhar seus conhecimentos e pontos de vista neste relatório:

- Brent Conran, vice-presidente e CISO da Intel
- Brian Dye, vice-presidente corporativo da Intel Security
- Dimitra Liveri, diretora de segurança da informação e de redes da European Network and Information Security Agency (ENISA)
- Vanessa Pegueros, CISO da DocuSign, Inc.
- Jim Reavis, CEO da Cloud Security Alliance
- Dave Shackleford, analista da SANS e CEO da Voodoo Security
- Timothy Youngblood, CISO da Kimberly-Clark

## Uma nuvem para cada estação? Trata-se de uma questão de confiança.

Quase todos que ligam um dispositivo eletrônico consomem a computação na nuvem de alguma forma. Seja para a automação doméstica, seja para aplicativos de negócios que geram receita, todos nós dependemos da Amazon Web Services, do Microsoft Azure ou de outros provedores de nuvem que mantêm a disponibilidade de tais serviços. Ao pensarmos na evolução e no futuro da computação na nuvem, nosso uso dessa plataforma de computação crescerá e o impacto de nossa dependência da nuvem terá inúmeras ramificações para cada um de nós: consumidores e empresas. De acordo com nossa pesquisa, nos próximos 12 a 18 meses, a maior parte dos orçamentos de TI das empresas será gasto em recursos de nuvem pública. Algumas pessoas consideram esse um ponto crítico na TI.

Vejamos, então, as implicações dessa transição. Primeiro, as habilidades dos profissionais de tecnologia que trabalham nessas empresas precisarão evoluir de maneira significativa. Em segundo lugar, será necessário melhorar o nível de confiança na nuvem e, com isso, a visibilidade adicional de que todos precisamos para atingir esse nível de confiança.

Embora a nuvem já seja uma realidade, o futuro apresentará um escopo em expansão de seus recursos e não será surpresa nenhuma ver os serviços e aplicativos de infraestrutura crítica mudarem para a nuvem. Aliás, ao começarmos a especular sobre como será o data center corporativo do futuro, podemos pensar que o tipo Cloud First, ou "nuvem em primeiro lugar", será a distribuição padrão para os aplicativos, com exceção feita (apenas se fizer sentido) à hospedagem local.

Com a segurança adequada em funcionamento, o poder da computação na nuvem pode ser aproveitado para oferecer compatibilidade com novos aplicativos e ferramentas de negócios avançadas para aumentar a produtividade. No entanto, como será possível ver em nosso estudo, as empresas continuam a lutar contra problemas relacionados à confiança e à segurança.

Com o aumento de nossa dependência de tais plataformas de computação, temos a oportunidade de elevar o nível da confiança em harmonia com as expectativas das empresas e dos consumidores. A Cloud Security Alliance, uma organização comandada por voluntários que é líder em pesquisa técnica, estende o convite às empresas e às suas partes integrantes para participarem e conduzirem essa mudança transformacional.

*— Raj Samani, CTO da Intel Security para a Europa, Oriente Médio e África*
*— Jim Reavis, CEO da Cloud Security Alliance*

## Introdução

Uma vez que as exigências de negócios conduzem as empresas rapidamente rumo à computação na nuvem e além dos projetos e pilotos de pequena escala, quais são os principais problemas e tendências com os quais elas precisarão lidar? Como as empresas podem aproveitar os benefícios da nuvem sem comprometer a segurança e o controle?

Em uma pesquisa realizada por oito países, perguntamos a 1.200 tomadores de decisão de TI responsáveis pela segurança na nuvem em suas empresas sobre os planos deles para a adoção da nuvem, bem como quais são os maiores desafios e as prioridades de investimento deles para o próximo ano.

Neste relatório, examinamos as tendências de adoção da nuvem corporativa e como elas diferem entre software como serviço (SaaS), infraestrutura como serviço (IaaS), plataforma como serviço (PaaS), segurança como serviço (Security-as-a-Service) e também entre nuvem pública, privada ou híbrida. Analisamos também como as empresas de setores mais regulamentados estão tentando superar os problemas de conformidade relacionados à adoção da computação na nuvem.

Exploraremos também o que é mito e o que é real em relação aos maiores problemas de segurança na nuvem que as empresas enfrentam e analisaremos a eficácia dos investimentos em tecnologias de segurança na nuvem, incluindo criptografia, prevenção de perda de dados e muito mais.

Além disso, também examinaremos como as empresas estão enfrentando o desafio da nuvem adquirida pela TI oculta e ainda possibilitando que funcionários e departamentos obtenham acesso aos serviços de que precisam com a segurança necessária em funcionamento para proteger as informações corporativas. Neste relatório, avaliaremos também o grau de conhecimento dos riscos de segurança na nuvem entre os membros da diretoria.

*"Fomos muito além dos adotantes iniciais (aqueles que estão testando e pilotando a nuvem) e chegamos à adoção total de uma variedade de diferentes tipos de nuvem. Estamos presenciando por toda a diretoria um verdadeiro reconhecimento de que este é o futuro da TI: mudar a computação para um utilitário."*

— Jim Reavis, CEO da Cloud Security Alliance

## TI corporativa eleva o investimento na nuvem

Os consumidores já vivem na nuvem e a usam diariamente para realizar tarefas variadas, de upload de fotos e acesso a e-mail ao backup de dados. Nossa pesquisa mostra que estamos agora em um ponto de inflexão semelhante, no qual a computação na nuvem se tornará o foco tecnológico predominante para a TI corporativa.

Embora o crescente investimento e adoção da nuvem por parte das empresas não seja uma grande surpresa, o ritmo acelerado em que isso está ocorrendo é significativo. Nossa pesquisa revela uma grande mudança para a TI corporativa, com a grande maioria dos orçamentos de TI das empresas sendo gasto com serviços de nuvem em menos de um ano e meio — e em ainda menos tempo que isso em alguns países (figura 1). Os entrevistados disseram que esperam que 80% do orçamento de TI da empresa deles sejam dedicados aos serviços de computação na nuvem nos próximos 16 meses. Empresas no Brasil e na Austrália esperam atingir essa marca de 80% no prazo de um ano.

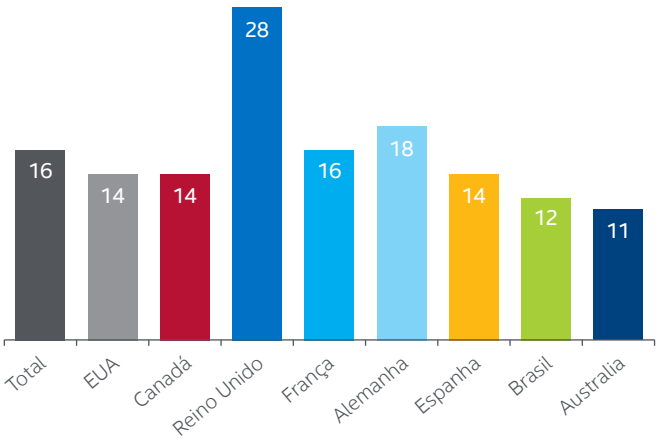


**Figura 1.** Número médio de meses para que 80% do orçamento de TI das empresas entrevistadas sejam compostos de serviços de computação na nuvem (por país).

*"Nossos parceiros de negócios estão aproveitando a natureza dinâmica da nuvem, a melhora na velocidade, o aumento da colaboração, a elasticidade dos serviços (ou seja, tudo o que torna a nuvem atraente) e estão agindo para aumentar isso porque, se você não o fizer, será pior para você. Como profissionais de segurança, temos de nos envolver e mostrar como a segurança pode ser a base."*

— Timothy Youngblood, CISO da Kimberly-Clark

A migração para os serviços de nuvem mencionada por nossos entrevistados será para distribuições de nuvem privada e pública. De acordo com nossa pesquisa, a nuvem privada é, no momento, o modelo de nuvem predominante nas empresas, com 51% da distribuição de nuvem delas sendo composta de nuvem privada. A nuvem pública constitui 30% e a nuvem híbrida representa 19% das distribuições de nuvem corporativas. Ao analisarmos quantos meses levará até que 80% do orçamento de TI de uma empresa sejam alocados para serviços de computação na nuvem, o prazo para as nuvens privadas diminui para apenas 15 meses.

*"Temos uma filosofia de 'nuvem em primeiro lugar' na DocuSign e percebemos que muitos de nossos clientes de diversos setores estão adotando a mesma abordagem. Trata-se de uma longa conversa com empresas em setores altamente regulamentados, como os de saúde e serviços financeiros. As equipes de TI nessas empresas estão em uma posição muito difícil, uma vez que os reguladores estão exigindo que elas provem que todas as medidas de segurança necessárias estejam em funcionamento antes da implementação. Elas sentem uma pressão incrível para investir o tempo necessário para provar isso aos reguladores, mas, ao mesmo tempo, as empresas as pressionam por mais eficiência, agilidade e que tudo seja feito mais rápido."*

— Vanessa Pegueros, CISO da DocuSign, Inc.

*"Saiba quais informações são apropriadas para se armazenar na nuvem e quais não são. Se há informações valiosas para a empresa, provavelmente é melhor que elas fiquem dentro dos limites do domínio da empresa e permaneçam em uma nuvem privada."*

— Eric Knapp, diretor global de segurança cibernética da Honeywell

É possível perceber as evidências de que a adoção dos serviços de nuvem atingiu o ponto crítico. As empresas estão usando uma média de 43 serviços de nuvem agora — embora seja importante observar algumas variações regionais significativas (figura 2). O Reino Unido, por exemplo, é o país mais lento em termos de adoção da nuvem (uma média de apenas 29 serviços de nuvem por empresa), enquanto as empresas brasileiras estão entre as que mais adotam serviços de nuvem (55 serviços de nuvem por empresa).

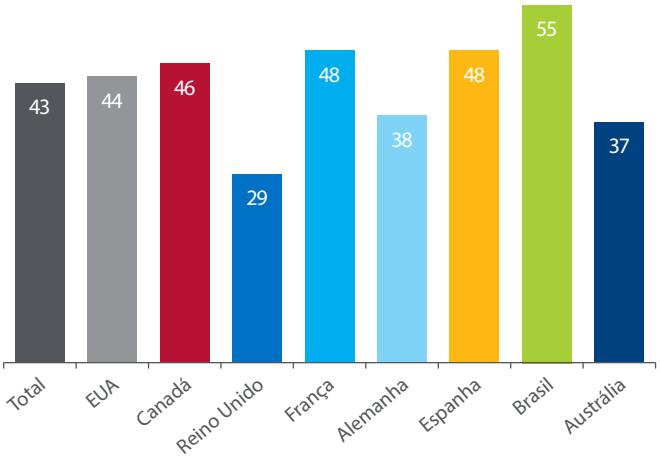


**Figura 2.** Número médio de serviços de nuvem que as empresas estão usando no momento (por país).

Obviamente, também haverá diferenças na taxa de adoção de diferentes tipos de plataformas de nuvem: pública, privada e híbrida ou gerenciada, bem como SaaS, IaaS e PaaS. Curiosamente, há também evidências de que a adoção varia de setor para setor. Em setores altamente regulamentados, como nos serviços financeiros, ainda há certa cautela quanto a mudar para a nuvem e os setores público e governamental também ficam para trás.

Ao examinarmos as tendências de adoção de nuvem, é fácil cair na armadilha e falar apenas do SaaS. Na realidade, nossa pesquisa revela que a maioria das empresas está planejando investir em todos os modelos de serviço de nuvem, mas (talvez de maneira surpreendente) o maior percentual (81%) é, na verdade, para a IaaS, em comparação com os 60% para o SaaS (figura 3). Esse percentual é seguido de perto pela Security-as-a-Service (79%), sendo que até mesmo o investimento planejado em PaaS (69%) é maior que o do SaaS.

Isso é confirmado pelo relatório da SANS, que também mostra que a IaaS será a maior área de crescimento das distribuições de nuvem corporativas no próximo ano.

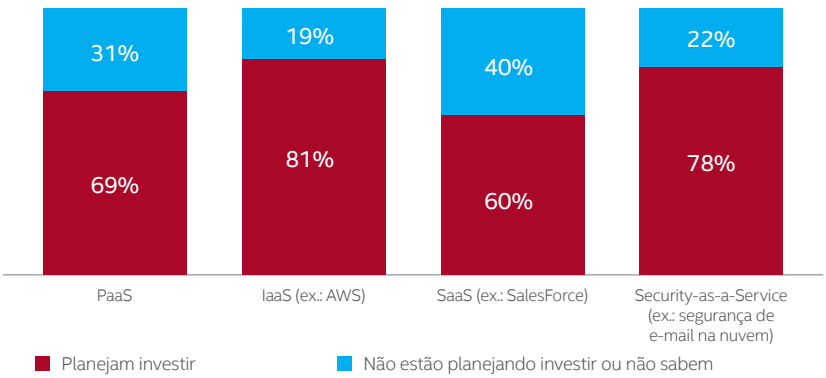


**Figura 3.** Em quais distribuições de nuvem sua empresa planeja investir?

*"A visibilidade de como o provedor de serviços de nuvem funciona e do que está acontecendo realmente inibe algumas análises de riscos e decisões de gerenciamento de riscos. Muitos regulamentos foram feitos antes da chegada da nuvem, os quais pressupunham que uma empresa tivesse controle total sobre a tecnologia de computação, o que já não ocorre mais com o advento da nuvem."*

— Jim Reavis, CEO da Cloud Security Alliance

*"Com certeza temos preocupações em relação às violações de dados. Muitas vezes elas acabam sendo ataques contra as credenciais de usuários que têm acesso legítimo ao serviço de nuvem e, consequentemente, ocorrem vazamentos de informações dessa forma."*

— Jim Reavis, CEO da Cloud Security Alliance

## Segurança e conformidade: a necessidade de melhor visibilidade

Quais são as implicações dessa maior adoção da nuvem para a segurança corporativa? Podemos ver dados adicionais importantes e confidenciais hospedados na nuvem. Aproximadamente 40% dos entrevistados da pesquisa da SANS, **Orchestrating Security in the Cloud** (Orquestrando a segurança na nuvem), dizem que processam ou armazenam dados confidenciais na nuvem.[1] Os tipos mais comuns de dados armazenados na nuvem são os de inteligência de negócios (52%), de contabilidade financeira (52%), de registros de funcionários (48%) e de informações pessoais de clientes (40%). O que desperta uma grande preocupação são os 13% das empresas que afirmaram não saber se têm dados confidenciais na nuvem. Muitos especialistas em segurança acreditam que esse número é, na verdade, muito maior, especialmente entre as empresas maiores. Um motivo para isso é que algumas empresas não querem admitir que não sabem, enquanto outras com operações e unidades de negócios espalhadas pelo mundo não sabem realmente se estão expostas dessa maneira.

Em todos os tipos de distribuição de nuvem, manter a conformidade na nuvem é a maior preocupação de acordo com 72% dos entrevistados da pesquisa da SANS. O verdadeiro desafio aqui está relacionado à visibilidade, com mais da metade (58%) dos entrevistados da pesquisa da SANS citando como o maior problema a falta de visibilidade das operações do provedor de nuvem.

## Nuvens negras à frente? As ameaças para o século XXI

Nossa pesquisa sugere que é o momento de reavaliar quais são as ameaças reais à nuvem, com evidências da existência de uma lacuna entre a percepção e a realidade.

Na maioria dos países, a principal preocupação em relação ao uso do SaaS são os incidentes de segurança de dados, conforme mencionado por mais de um em cada cinco entrevistados (22%). As violações de dados também estão entre as principais preocupações para IaaS e nuvens privadas. Existem algumas diferenças regionais, principalmente na Austrália, onde o tempo de inatividade é a principal preocupação.

Mas qual é a realidade?

À medida que mais perguntas foram feitas, menos de um quarto (23%) das empresas disse que realmente sofria com violações ou perda de dados por parte de seus provedores de serviços de nuvem e apenas um em cada cinco entrevistados sofreu com acesso não autorizado aos dados ou serviços. A pesquisa da SANS mostra um nível ainda mais baixo de violações de dados na nuvem, com apenas 9% dos entrevistados tendo já sofrido algum incidente em nuvens públicas ou com SaaS ou aplicativos de nuvem privada.

Na verdade, os incidentes e problemas mais comuns que os entrevistados tiveram com os serviços de nuvem foram a migração de serviços e de dados, os custos altos e o pouco valor oferecido ou a falta de visibilidade das operações do provedor de nuvem (figura 4).

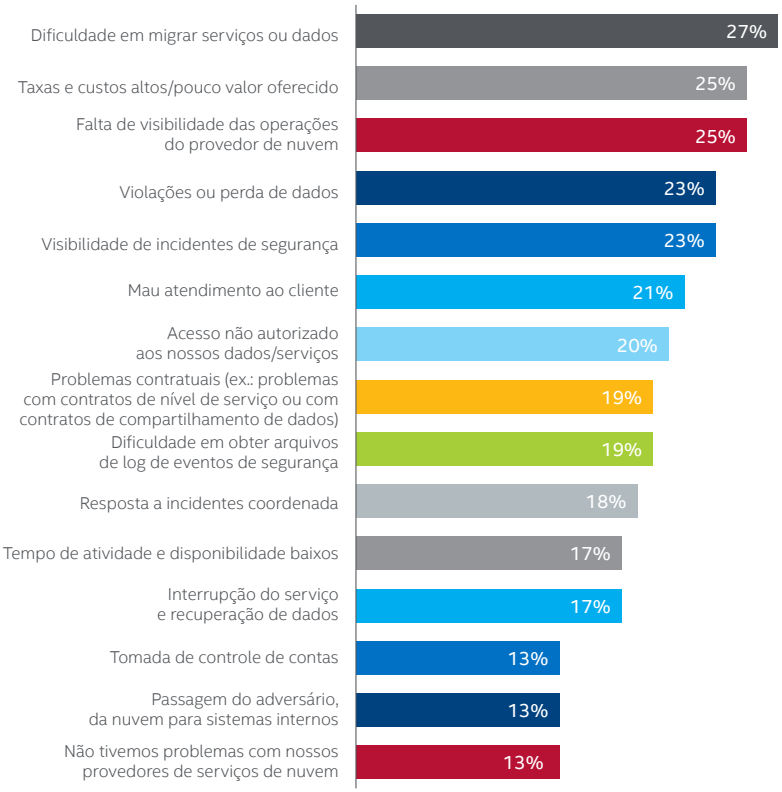


**Figura 4.** No que diz respeito à segurança na nuvem, quais problemas a sua empresa teve com os provedores de serviços de nuvem?

Quando analisamos as ameaças específicas à segurança na nuvem identificadas pelos entrevistados, descobrimos que malware e redes de bots são os principais problemas para as distribuições de nuvem privada (33%), enquanto os ataques de negação de serviços são considerados as principais ameaças para as nuvens públicas (36%).

*"As empresas precisam incorporar segurança ao DevOps e os dois elementos mais críticos são o monitoramento contínuo e a detecção de alterações."*

— Dave Shackleford, analista da SANS e CEO da Voodoo Security

Outros riscos à segurança na nuvem surgem possivelmente por meio do rápido aumento ou diminuição do dimensionamento dos serviços, embora isso seja mais um problema de disponibilidade e de continuidade dos negócios para o qual as empresas precisam se planejar. Outra característica fundamental da adoção da nuvem é a ascensão do DevOps, que são os ciclos cada vez mais rápidos de desenvolvimento, teste e distribuição de aplicativos. Incorporar uma segurança robusta a esse ambiente de desenvolvimento contínuo é vital para acompanhar essas mudanças rápidas e para ser alertado de qualquer possível risco à segurança associado a elas.

Obviamente, não devemos tirar conclusões precipitadas baseadas nos resultados da pesquisa de que as violações de dados na nuvem não são uma ameaça grave à segurança ou de que nunca acontecem. Devemos considerar a possibilidade de violações de dados subdeclaradas quando estas não são divulgadas a agências de imposição da lei ou reguladores. E, claro, quando as violações de dados na nuvem ocorrem realmente, as consequências são muitas vezes significativas. Embora a lacuna entre a percepção e a realidade em relação à ameaça contra a segurança na nuvem precise ser preenchida até certo ponto, a pesquisa sugere que o investimento e o planejamento quanto à mitigação de riscos de violação importantes precisam ser equilibrados com algumas das ameaças mais comuns do dia a dia para sistemas corporativos e dados na nuvem. Entre essas ameaças estão problemas de migração, mau atendimento ao cliente e problemas contratuais, bem como ameaças à segurança específicas, como negação de serviço, malware e violação de contas.

## Risco e segurança na nuvem: o ponto cego dos executivos de nível "C"

*"Diretorias e executivos de nível 'C' começam a reconhecer amplamente que a segurança na nuvem é um elemento crítico de qualquer negócio e que ela deve ser levada a sério."*

— Vanessa Pegueros, CISO da DocuSign, Inc.

Nossa pesquisa mostra um alto nível de envolvimento na tomada de decisão de segurança na nuvem por parte da gerência sênior — não apenas do diretor de TI, do CIO e do CISO, mas muitas vezes também do CEO e do CFO. No entanto, a gerência sênior compreende totalmente os riscos de segurança?

Quando se trata de nuvens públicas, parece haver uma lacuna perturbadora quanto ao conhecimento, por parte da diretoria, das implicações de segurança no armazenamento de dados confidenciais na nuvem pública. (Veja a figura 5). Apenas 34% dos entrevistados acreditam que a gerência sênior na empresa deles compreende totalmente as implicações, enquanto um em cada cinco afirma que os executivos de nível "C" não têm nem ideia ou apenas compreendem parcialmente esses riscos. Há uma lacuna ainda maior no Reino Unido, onde apenas 15% acreditam que a gerência sênior na empresa deles compreende totalmente os riscos de armazenar dados na nuvem pública. Compare isso com o Brasil (49%) e a Austrália (47%), onde o grau de conhecimento é muito maior entre os membros da diretoria.

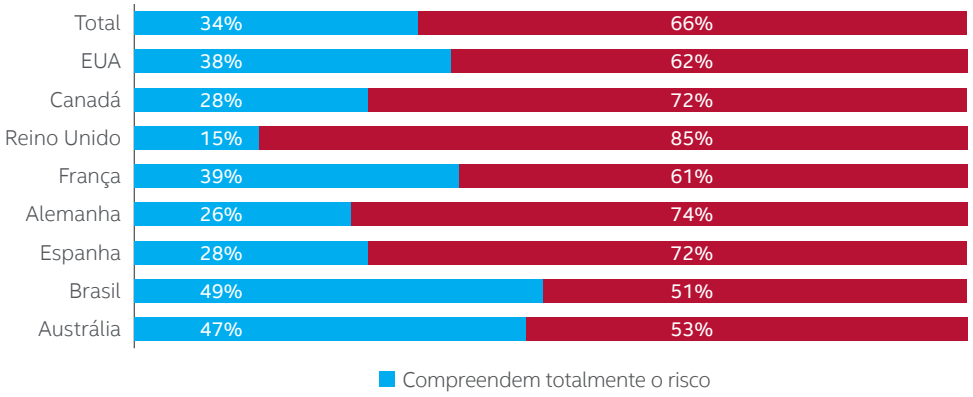


**Figura 5.** Você acha que os executivos/gerência sênior compreendem as implicações de segurança no armazenamento de dados confidenciais na nuvem pública?

*"Conhecimento é poder. Temos um programa bem intensivo de conscientização da segurança com foco na educação de todos os nossos funcionários sobre o valor das informações. É o que chamo de nosso 'firewall humano'."*

— Timothy Youngblood, CISO da Kimberly-Clark

Embora as violações de dados importantes e as consequências financeiras e de reputação transformaram a segurança de dados em uma preocupação prioritária para muitos CEOs e para os outros executivos de nível "C", nossa pesquisa sugere que ainda há necessidade de mais educação para aumentar o conhecimento e a compreensão dos riscos associados ao armazenamento de dados confidenciais na nuvem.

## A TI oculta: risco ou oportunidade?

A maioria dos entrevistados em nossa pesquisa diz que a TI oculta exerce um impacto negativo na capacidade da empresa deles de manter os serviços de nuvem seguros e protegidos, com 10% indicando que ela deixa suas empresas expostas a um risco significativo.

Proteger a TI oculta continua a ser um grande desafio: 52% das linhas de negócios ainda esperam que a TI proteja seus serviços de nuvem fornecidos por departamentos não autorizados. Além disso, quase um quarto dos entrevistados (23%) disse que esses departamentos fornecem sua própria segurança sem a ajuda da TI.

*"A TI oculta é a nova TI. O modelo antigo esgotou-se. Quanto mais lutamos contra isso, menos nos concentramos no trabalho necessário para sua proteção. Precisamos aceitar que a TI oculta é a realidade atual e concentrar a nossa energia para gerenciá-la com segurança."*

— Vanessa Pegueros, CISO da DocuSign, Inc.

A visibilidade da TI oculta departamental é geralmente maior para o SaaS do que para a IaaS. No entanto, em todas as instâncias, pelo menos um quinto dos entrevistados não sabe se a TI oculta está ocorrendo em cada departamento de suas empresas. Os níveis de TI oculta são mais altos nos departamentos de vendas, de pesquisa e desenvolvimento e de marketing. O maior ponto de interrogação paira sobre o departamento jurídico. Aproximadamente 37% dos nossos entrevistados não souberam dizer se esse departamento está adquirindo nuvem sem o conhecimento do departamento de TI.

Como as empresas estão lidando com a TI oculta? Os métodos mais comuns são:

- Monitoramento de atividade de banco de dados (49%).
- Firewalls de última geração (41%).
- Gateways da Web (37%).

Outra tática é trabalhar com o departamento de finanças para ser alertado quanto aos relatórios de despesas enviados para serviços de nuvem.

Há uma divisão notável na maneira de lidar com a TI oculta quando ela é descoberta. Quase metade dos entrevistados (46%) bloqueia o acesso, enquanto 37% migram a TI oculta para um serviço aprovado.

*"As pessoas estão apenas tentando fazer o seu trabalho. Se não conseguirmos atendê-las, elas procurarão ajuda em outro lugar. A TI e o CIO devem ser o agente e aceitar os serviços de nuvem e de SaaS."*

— Brent Conran, vice-presidente e CISO da Intel

## A confiança na nuvem está crescendo?

À primeira vista, os números de destaque da nossa pesquisa mostram um nível relativamente baixo de confiança na computação na nuvem em comparação com a TI hospedada local ou internamente. Não surpreendentemente, a nuvem pública é o modelo menos confiável (figura 6).

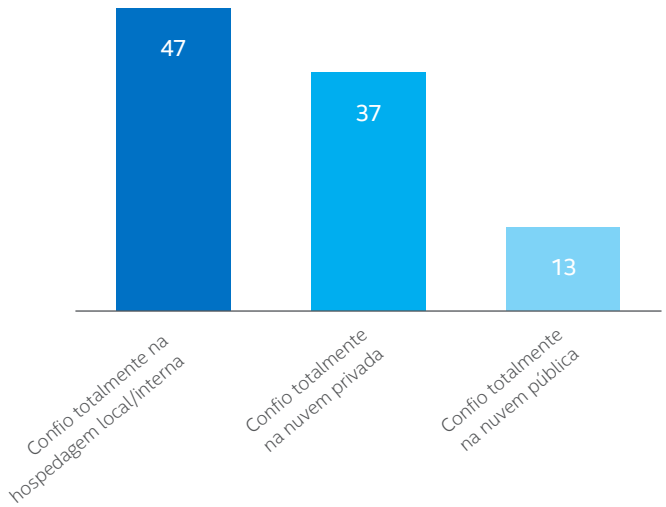


**Figura 6.** "O quanto você confiaria nas seguintes opções para manter os dados confidenciais da sua empresa protegidos?"

Mais significativamente, o panorama geral mostra um nível global crescente de confiança na computação na nuvem em relação ao ano passado — 77% das empresas afirmam que suas organizações confiam mais na computação na nuvem agora do que há um ano (figura 7).

*"Uma nova era está chegando para os provedores de nuvem. Estamos em um período de transição, mas acredito que essas novas disposições regulamentares ajudarão o investimento e a confiança para que nos sintamos mais à vontade com os serviços de nuvem."*

— Dimitra Liveri, diretora de segurança da informação e de redes da European Network and Information Security Agency (ENISA)

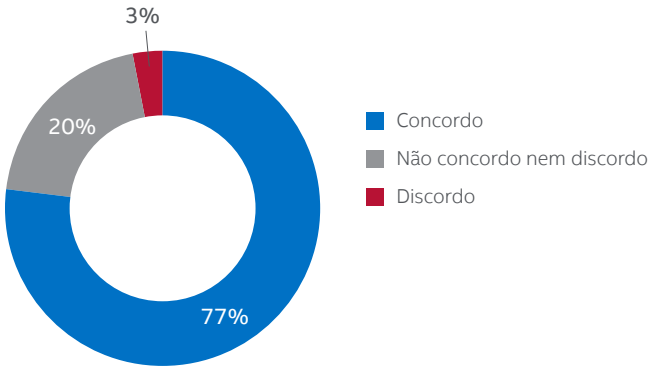


**Figura 7.** Aqueles que concordam com a afirmação "Minha empresa confia mais na computação na nuvem agora do que há 12 meses".

Com dois regulamentos significativos aguardando a votação da Comissão Europeia, 2016 promete ser um grande ano para usuários e provedores de nuvem na Europa. Os regulamentos consistem no regulamento geral de proteção de dados e na diretiva de segurança da informação de redes da União Europeia. Eles ajudarão a reforçar a confiança na segurança na nuvem? Os especialistas acreditam que sim.

*"O primeiro ponto de partida para a segurança corporativa na nuvem pública é perguntar: quais são os limites de responsabilidade? O que você, como empresa, consegue controlar totalmente e o que o provedor de nuvem é obrigado a gerenciar? Você precisa avaliar os controles de todo o espectro da segurança, incluindo segurança de dados, gerenciamento de identidade e aplicação de políticas. Haverá coisas que você não conseguirá controlar mais, principalmente em nível de rede."*

— Dave Shackleford, analista da SANS e CEO da Voodoo Security

## Prioridades de investimento em segurança na nuvem

As prioridades de investimento em segurança variam entre os diferentes tipos de distribuições de nuvem. As empresas estão usando uma média de três soluções de segurança para proteger seus aplicativos de SaaS. A mais comum é a criptografia de arquivos (60%), seguida por segurança de e-mail (55%).

Para a IaaS, as empresas estão usando uma média de quatro soluções de segurança. As mais comuns são firewalls (70%) e criptografia (62%). A nuvem privada também tem uma média de quatro soluções de segurança, com firewalls sendo a mais comum (67%).

As quatro principais áreas da Security-as-a-Service nas quais as empresas planejam investir são as mesmas em que elas já estão investindo: proteção de e-mail, proteção na Web, antimalware e firewall de aplicativo (figura 8). Essa tendência indica que as empresas estão planejando melhorar e expandir os serviços de segurança com base na nuvem que elas já têm em funcionamento.

A pesquisa da SANS também destaca algumas áreas fundamentais de investimento em segurança na nuvem nos próximos 18 meses. Entre essas estão varredura de vulnerabilidades, autenticação multifator, prevenção de perda de dados, gerenciamento de log, sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS), gerenciamento de eventos e informações de segurança (SIEM) e serviços de agente de segurança de acesso à nuvem (CASBs).

De acordo com o relatório da Gartner, *Market Guide for Cloud Access Security Brokers* (Guia de mercado para agentes de segurança de acesso à nuvem), os CASBs, em especial, são uma área de alto crescimento. A Gartner prevê que "até 2020, 85% das grandes empresas usarão um produto de agente de segurança de acesso à nuvem em seus serviços de nuvem, percentual que hoje está pouco abaixo de 5%".[2] Nossa pesquisa confirma isso. Apesar de que os CASBs são um serviço relativamente novo, 36% das empresas estão usando esses serviços para proteger seus aplicativos de SaaS e 32% usam esses serviços para monitorar as implementações de nuvem adquiridas pela TI oculta. Quase um quarto (24%) das empresas também planeja investir em um CASB como serviço no futuro.

*"Compreender o que está acontecendo em seu ambiente de nuvem (por exemplo, entre a base de usuários e a equipe de vendas) é realmente algo crítico, sendo que as ferramentas que permitem o gerenciamento com maior segurança serão algo que olharei com mais atenção. Precisamos também de ferramentas que ajudem a automatizar processos, como resposta a incidentes, e que nos permitam fazer mais com o que temos no momento."*

— Vanessa Pegueros,
CISO da DocuSign, Inc.

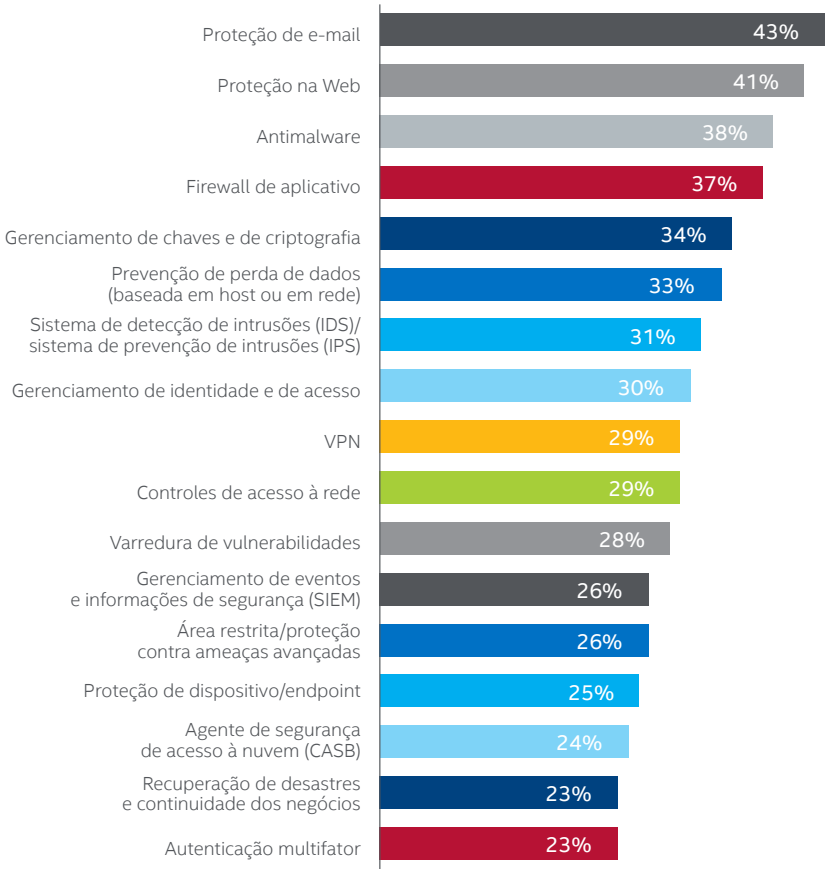


**Figura 8.** Em quais áreas da Security-as-a-Service a sua empresa planeja investir?

Das empresas que usam um serviço de nuvem pública, pouco mais de um terço (34%) afirmou ter uma solução unificada com integração total e gerenciamento central entre seus sistemas locais e de nuvem híbrida. Portanto, ainda há espaço para melhorias nesse ponto.

## Resumo

A adoção da nuvem nas empresas está se aproximando rapidamente de um ponto crítico, com as empresas afirmando que 80% do orçamento de TI delas serão destinados à nuvem em 16 meses ou menos.

Existem muitos incentivos persuasivos que conduzem as empresas rumo à nuvem, incluindo maior agilidade, inovação mais rápida e eficiências de custo. No entanto, com tamanha variedade de opções de distribuição de nuvem, existem desafios de segurança inerentes. Uma vez que a nuvem é ou será o repositório de dados corporativos tão vitais, as empresas devem levar em consideração o seguinte:

- Os controles de segurança e a conformidade são responsabilidades compartilhadas entre as empresas e os provedores de serviços de nuvem. Pergunte ao seu provedor de serviços sobre os controles de segurança deles e verifique se a geração de relatórios está incluída no seu contrato de nível de serviço (SLA). No entanto, é essencial para a empresa proteger o que está sob o controle deles na nuvem (dados, aplicativos ou cargas de trabalho) e integrar isso aos planos de arquitetura da nuvem deles.

*"Mesmo que você tenha terceirizado e esteja usando a nuvem, você não terceirizou a sua responsabilidade. Você não pode dizer: 'Olha, foi a Amazon'."*

— Brent Conran, vice-presidente e CISO da Intel

- As principais áreas de investimento de segurança na nuvem incluem criptografia de dados, gerenciamento de identidade e de acesso, prevenção de perda de dados e proteção de e-mail. As empresas também estão investindo cada vez mais na Security-as-a-Service e em outros serviços que ajudam a orquestrar a segurança em vários provedores e ambientes, mais notavelmente os CASBs.
- Embora as distribuições de nuvem de TI oculta continuem a ser um desafio, uma vez que elas podem expor dados da empresa a um maior risco, as empresas de TI devem trabalhar em conjunto com as unidades de negócios para encontrar um caminho mais seguro para permitir que os usuários implementem suas próprias distribuições de nuvem. A TI pode recuperar o controle e a visibilidade ao atuar como agente e redirecionar os usuários de negócios a alternativas de serviços de nuvem mais seguros.
- Embora muitas diretorias estejam cada vez mais envolvidas na tomada de decisões relacionadas à segurança na nuvem, há evidência de uma lacuna preocupante no conhecimento e na compreensão desses riscos. Uma maior conscientização em relação a isso é necessária, uma vez que há maior envolvimento dos CIOs e CISOs nas reuniões de diretoria com outros executivos de nível "C". A repercussão financeira e o dano à reputação sofrido pelas empresas em algumas violações de dados importantes recentes devem ser um incentivo para que os altos executivos tornem a segurança de dados (interna ou na nuvem) uma prioridade.

## Metodologia

A pesquisa envolvendo 1.200 tomadores de decisão responsáveis pela segurança na nuvem das empresas deles foi realizada pela Vanson Bourne em junho de 2015. Os entrevistados selecionados eram provenientes da Austrália, Brasil, Canadá, França, Alemanha, Espanha, Reino Unido e Estados Unidos, incluindo uma variedade de empresas, de 251 a 500 funcionários até as com mais de 5.000 funcionários.

## Sobre a Intel Security

A McAfee agora é parte da Intel Security. Com sua estratégia Security Connected, sua abordagem inovadora para a segurança aprimorada por hardware e a exclusiva Global Threat Intelligence, a Intel Security está sempre empenhada em desenvolver soluções de segurança proativas e comprovadas e serviços para a proteção de sistemas, redes e dispositivos móveis para uso pessoal ou corporativo no mundo todo. A Intel Security combina a experiência e o conhecimento da McAfee com a inovação e o desempenho comprovados da Intel para tornar a segurança um elemento essencial em toda arquitetura e plataforma de computação. A missão da Intel Security é oferecer a todos a confiança para viver e trabalhar de forma segura no mundo digital. **www.intelsecurity.com**

1. *SANS: Orchestrating Security in the Cloud* (SANS: orquestrando a segurança na nuvem), escrito por Dave Shackleford, setembro de 2015 (patrocinado pela Intel Security)
2. Relatório da Gartner, *Market Guide for Cloud Access Security Brokers* (Guia de mercado para agentes de segurança de acesso à nuvem), escrito por Craig Lawson, Neil MacDonald e Brian Lowans, 22 de outubro de 2015

**McAfee. Part of Intel Security.**
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com