CYBER READINESS
INSTITUTE

# FAQ sobre armazenamento na nuvem: Melhorar a segurança cibernética para trabalhadores remotos

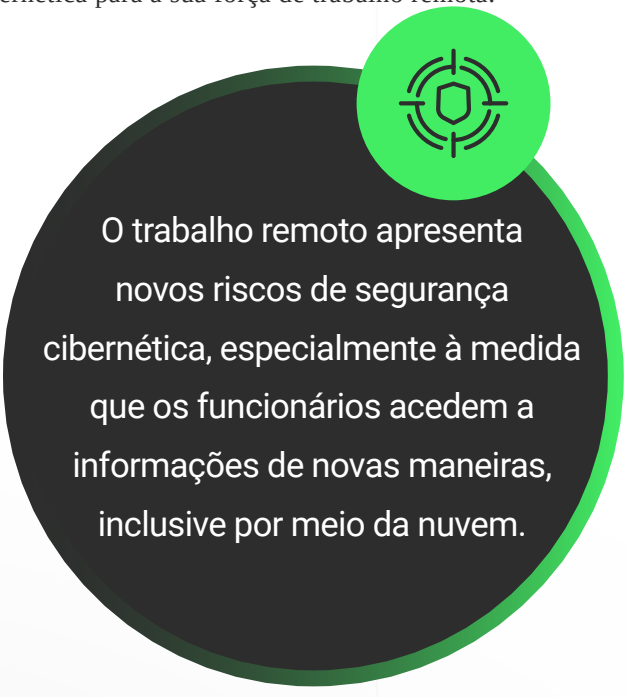
Em resposta à pandemia da COVID-19, a força de trabalho da maioria das empresas tornou-se remota. O trabalho remoto apresenta novos riscos de segurança cibernética, especialmente à medida que os funcionários acedem a informações de novas maneiras, inclusive por meio da nuvem.

Agora é a hora de avaliar como a sua empresa usa a nuvem. A nuvem tem vários recursos que podem ajudar a tornar o trabalho remoto mais prático, eficiente e seguro. Estas FAQ foram desenvolvidas para ajudar a gerência sénior de pequenas e médias empresas (PMEs) a familiarizarem-se com a terminologia da nuvem e a entenderem os fundamentos de como a nuvem pode melhorar a segurança cibernética para a sua força de trabalho remota.

## Ouço muito sobre “a nuvem”, mas quais são os princípios básicos que preciso de saber?

A “nuvem” refere-se a um grupo de computadores (conhecidos coletivamente como servidores) pertencentes e operados por uma empresa (normalmente chamada de Fornecedor de Serviços em Nuvem ou “CSP”) que fornece software ou armazenamento. Um cliente ou empresa licencia o uso do software e/ou armazenamento, normalmente numa base mensal com os custos mudando com base no uso semelhante aos custos mensais de serviços públicos.

O CSP é responsável por operar, manter e atualizar o hardware do computador (por exemplo, armazenamento, servidores), que está fisicamente localizado num centro de dados e não nas instalações do cliente. Como cliente, paga pelo uso dos serviços deles.






guide@cyberreadinessinstitute.com

# Quais são alguns dos termos comuns que irei ouvir quando falar com as pessoas sobre a nuvem?

### CENTROS DE DADOS

Pense em grandes armazéns cheios de computadores ligados à Internet e conhecidos coletivamente como “servidores”. Quando, como cliente, usa um serviço (por exemplo, Outlook), está essencialmente a alugar um espaço (armazenamento) e serviços (e-mail) para escrever, ler e enviar e-mails.

### SERVIDORES

Um conjunto de computadores e hardware ligados à Internet que fornecem algum tipo de serviço, armazenamento ou outra função.

### FORNECEDORES DE SERVIÇOS NA NUVEM (CSPS)

As empresas que prestam serviços a si como cliente. Alguns exemplos bem conhecidos são Microsoft, Google ou Amazon Web Services (AWS).

### SOFTWARE ENQUANTO SERVIÇO (SAAS) (pronunciado “sass”)

Um CSP aloja nos seus servidores o software a que a sua empresa acede pela internet. É comum as empresas licenciarem o uso de muitos tipos de software, como e-mail (Google Mail), processador de texto (Microsoft Word), folhas de cálculo (Google Sheets), contabilidade (QuickBooks) e gestão de vendas (Salesforce). Essa é a maneira mais comum para pequenas empresas usarem a nuvem e exige o mínimo de manutenção para o cliente.

### PLATAFORMA ENQUANTO SERVIÇO (PAAS) (pronunciado “paz”)

Um CSP fornece a infraestrutura (por exemplo, um sistema operativo como o Windows) e o software que permite desenvolver, gerir e usar aplicações personalizadas (por exemplo, aplicações de gestão de stock ou pedidos móveis do cliente).

### INFRAESTRUTURA ENQUANTO SERVIÇO (IAAS) (pronunciado “eye-azz”)

Um fornecedor de serviços na nuvem hospeda fisicamente componentes que tradicionalmente estavam num centro de dados “local”, incluindo servidores, armazenamento, hardware de rede e software de servidor.

## Quais são os benefícios gerais de segurança ao mover operações e informações para a nuvem?

Os CSPs veem a segurança como uma ***função comercial central*** e reconhecem que a confiança é uma parte fundamental do seu modelo de negócios. Concentram-se em atualizar continuamente os serviços e a infraestrutura fornecidos para permitir soluções seguras para os seus clientes. Beneficia da sua experiência e foco contínuo em segurança.

***A infraestrutura física*** (por exemplo, servidores, routers, dispositivos de rede) está alojada em centros de dados de propriedade e mantidas pelo CSP. Isso normalmente a) Reduz os custos associados à manutenção, incluindo taxas de construção e manutenção, mas também b) Fornece recursos dedicados para proteger o local de problemas de segurança física.

Os CSPS acionam as ***economias de escala*** permitindo que aceda a recursos e serviços que excedem o que qualquer utilizador individual pode ser capaz de implantar. Por exemplo, os CSPs reúnem recursos para entender melhor os ataques cibernéticos mais recentes que os hackers estão a usar e para implantar soluções para proteger os seus serviços e os seus dados.

Os fornecedores de serviços na nuvem mais conceituados definirão claramente quais controlos de segurança possuem e quais são as suas responsabilidades quando se trata de usar os seus serviços. Caso contrário, ou se essa informação não vier de um fornecedor de serviços na nuvem que está a considerar, convém procurar outro fornecedor.

## À medida que migramos para a nuvem, quais são as responsabilidades contínuas da minha empresa em relação à segurança cibernética?

A sua principal responsabilidade é pelo comportamento dos seus funcionários. É responsável pela formação do seu pessoal sobre como evitar problemas e o que fazer se houver um problema. Precisa de ter a certeza de que eles compreendem que estar preparado para ataques cibernéticos é uma prioridade para a sua empresa.

**Existem princípios fundamentais a compreender no que diz respeito às responsabilidades de segurança para a sua empresa ao usar um CSP:**

- Em primeiro lugar, terceirizar serviços, funcionalidade ou infraestrutura para um CSP não significa terceirizar a sua responsabilidade de segurança. Um exemplo simples que se aplica a quase todos é a sensibilização e o acesso dos funcionários. Os seus funcionários sabem como detetar e-mails suspeitos? A sua empresa limita/restringe o acesso dos funcionários ao software (por exemplo, aplicações de contabilidade) com base na necessidade e nas suas responsabilidades?)
- Em segundo lugar, os invasores dedicam-se a enganar as pessoas (conhecido como “phishing”) como uma forma de obter acesso não autorizado. Mais de 90% dos hacks bem-sucedidos começam quando alguém clica numa ligação de e-mail suspeita. A formação em segurança cibernética para funcionários é muito importante, incluindo a prática de uma boa “higiene cibernética”, como não clicar em ligações de remetentes desconhecidos ou validar junto dos gestores os e-mails que solicitam informações confidenciais.
- Em terceiro lugar, o que acontece com os dados é quase sempre responsabilidade do cliente. Por exemplo, a fuga de dados financeiros confidenciais de clientes mal protegidos (pense em informações de cartão de crédito) que são carregados num CSP é responsabilidade do cliente, não do CSP. E os impactos sobre a reputação, jurídicos, financeiros e de conformidade, para citar alguns, também são da responsabilidade do cliente.

## Como a mudança para a nuvem melhora a nossa prontidão cibernética em relação à gestão da identidade do utilizador (por exemplo, palavras-passe e autenticação)?

Muitos fornecedores de serviços na nuvem têm equipas dedicadas à segurança cibernética e podem responder a incidentes em tempo real, identificando quando os problemas começam e tomam medidas para mitigar a quantidade de danos. Um grande fornecedor de serviços na nuvem recebe mais de 200 milhões de tentativas de início de sessão **por dia**. Este fornecedor pode aprender rapidamente quando um novo tipo de ataque ameaça as suas palavras-passe e tomar medidas para evitar que isso o afete a si ou aos seus utilizadores.

## Como a mudança para a nuvem melhora a prontidão cibernética relacionada com a manutenção do software atualizado?

Manter o software atualizado é um grande benefício para os clientes e muitas vezes um ponto de venda importante para os fornecedores de serviços na nuvem, especialmente ao implementar uma solução SaaS ou PaaS. Quando muda para um serviço na nuvem, o fornecedor é responsável por manter as atualizações de software atuais sem que precise de fazer nada.

No entanto, este recurso pode ter uma desvantagem, pois os utilizadores podem não estar prontos para se adaptar aos novos recursos tão rápido quanto as empresas de serviços na nuvem os implementam. Se isso se aplica à sua empresa, deve perguntar se há uma **opção de atualização adiada** para a sua licença de software na nuvem. Lembre-se de que os funcionários ainda podem ser responsáveis por atualizar o software que está no seu computador, tablet ou telemóvel individual.

## Como a mudança para a nuvem melhora a nossa prontidão cibernética em relação à prevenção de e-mails de phishing?

O phishing é difícil de resolver, pois usa fraude por engenharia social (às vezes, especificamente adaptado ao indivíduo, chamado ***spear-phishing***) para entrar numa aplicação ou aceder a dados confidenciais (por exemplo, informações de início de sessão e palavra-passe).

Dito isto, os fornecedores de e-mail na nuvem podem aprender e responder rapidamente a ataques de phishing **assim que os mesmos são conhecidos**. Os fornecedores de e-mail na nuvem podem fornecer serviços para ajudar a relatar e impedir que e-mails de phishing conhecidos cheguem aos seus funcionários. Em última análise, a melhor linha de defesa é um ***utilizador bem treinado*** que sabe como são os e-mails de phishing e o que fazer (e não fazer!) quando os vê.

O uso de um fornecedor de serviços na nuvem melhora a prontidão cibernética da sua empresa na gestão da identidade do utilizador, mantendo o software atualizado e evitando e-mails de phishing.

## Como a mudança para a nuvem melhora a nossa prontidão cibernética em relação ao uso de USBs e unidades de armazenamento removíveis?

Migrar para a nuvem representa uma melhoria dramática, pois não há dispositivos de "armazenamento multimédia" removíveis necessários para usar software baseado na nuvem. Tudo o que a nuvem requer é um utilizador com um início de sessão, um navegador e uma ligação à Internet. USBs e unidades de armazenamento removíveis tornam-se irrelevantes, desde que dê formação aos seus utilizadores sobre como usar a nuvem para armazenar, transferir e aceder a informações de que precisam.

Ainda será responsável por manter a segurança nos dispositivos físicos, que permitem unidades de armazenamento removíveis e podem impedir o cliente de aceder aos serviços. Um benefício, no entanto, é que, embora um dispositivo individual (por exemplo, desktop) possa ser comprometido por um ataque de USB, os serviços “vivem” na nuvem e são acessíveis a partir de um dispositivo não infetado. Este é um poderoso recurso de nuvem que ajuda a proteger a continuidade dos seus negócios.

## Como a nuvem me ajuda se ocorrer um incidente cibernético?

Os fornecedores de serviços na nuvem gastam muito tempo e dinheiro garantindo que os seus serviços não sejam interrompidos por um incidente cibernético. Os CSPs oferecem ferramentas de software que podem ajudar a isolar a causa raiz (por exemplo, serviços de registo de eventos, atividades suspeitas) de um incidente para reduzir a possibilidade de acontecer novamente. Os centros de dados CSP também possuem fortes controlos de segurança física, proteção de energia e prevenção de incêndio, para que tenha a certeza de que a infraestrutura física real de TI está bem protegida.

## Os nossos funcionários estão a usar os seus smartphones para trabalhar. Como o uso de serviços na nuvem me ajuda a reduzir o risco relacionado com a segurança cibernética?

Precisa de estar ciente de como os seus utilizadores estão a aceder às suas aplicações, sistemas e informações. Deve criar uma política de segurança móvel que se aplique a todos os utilizadores, independentemente do dispositivo que estão a usar. A nuvem oferece os mesmos benefícios gerais de segurança para os funcionários, independentemente de eles usarem o smartphone ou outro tipo de dispositivo. É importante lembrar que os smartphones oferecem a maior superfície de ameaça e cada empresa deve ser diligente na sua política de segurança móvel.

### Sobre o Cyber Readiness Institute

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para a partilha de recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). O programa de prontidão cibernética online está disponível em chinês, inglês, francês, espanhol, português, árabe e japonês. Entre em contacto connosco com perguntas, comentários ou histórias de sucesso (**guides@cyberreadinessinstitute.org**).

## Como priorizo o que mover para a nuvem?

Não existe uma resposta “universal”. A maioria das empresas tem o que é chamado de ambiente "híbrido" que usa uma combinação de serviços na nuvem com soluções autogeridas e locais (por exemplo, uma empresa pode usar a sua configuração de rede para um pequeno escritório e serviço de e-mail fornecido por CSP.) Aqui estão algumas considerações:

- O software ou serviço faz interface diretamente com a Internet? Muitas empresas movem as suas aplicações de e-mail e gestão de relacionamento com o cliente (CRM) para a nuvem, pois são aplicações de missão crítica cujos servidores tradicionalmente exigem muita manutenção. A maioria das empresas hoje também obtém o seu software comercial básico (ou seja, processamento de texto, folhas de cálculo, contabilidade) por meio de uma assinatura SaaS.
- Quão difícil seria? Algumas funções são muito mais fáceis de migrar do que outras. Por exemplo, mover o seu e-mail ou armazenamento de ficheiros para a nuvem é simples. No entanto, sistemas móveis como folha de pagamento ou contabilidade que envolvem muitos dados históricos podem ser muito mais complexos.
- Quais são os custos relativos? Ao comparar os custos entre usar a nuvem e fazer você mesmo, certifique-se de que conta também o tempo e as despesas de fazê-lo no local. Não se trata apenas do custo de hardware e software - é o momento de configurar, atualizar, manter e solucionar problemas do seu sistema.
- Avalie os aspetos de segurança aprimorados do uso da nuvem. Pense em possíveis interrupções nos seus negócios, bem como na perda das suas informações - especialmente as informações mais valiosas.

## Como a mudança para a nuvem afetará o nosso fluxo de trabalho atual e o que os nossos funcionários precisam de fazer?

A resposta a esta pergunta dependerá do que mover para a nuvem. Mover o e-mail para a nuvem normalmente resulta em poucas mudanças, ao passo que mover o seu software de contabilidade para a nuvem pode representar uma interrupção dramática, exigindo gestão de mudanças para os seus utilizadores e para a sua empresa.

## Qual é o impacto do uso da nuvem, se houver, na forma como interajo com os meus fornecedores e clientes?

A resposta simples é: depende. As empresas usam a nuvem para atingir objetivos diferentes em projetos muito diversos. No entanto, mudar para a nuvem geralmente libera tempo e dinheiro que gastaria em recursos de TI (servidores, redes, etc.). Na maioria dos casos, usar a nuvem tornará mais fácil e seguro transferir ou partilhar informações com os seus clientes e fornecedores.