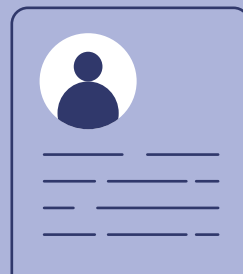


Riscos e benefícios da computação em nuvem



OPICE BLUM

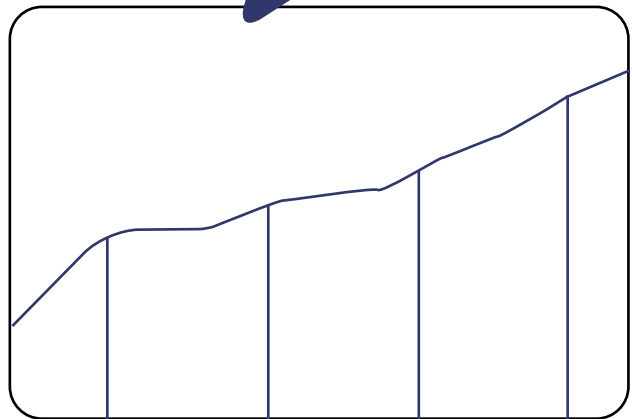
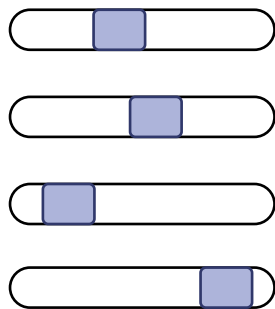
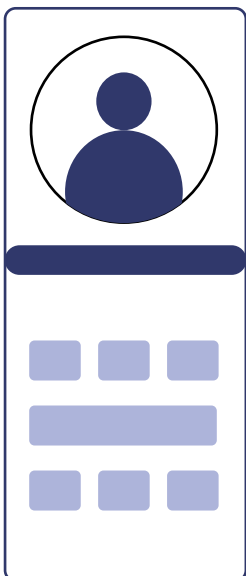
OPICE BLUM | BRUNO | VAINZOF



A computação em nuvem (*cloud computing*) refere-se à oferta de recursos de TI sob demanda por meio da internet. Na prática, trata-se da oferta em escala dos recursos físicos de *hardware* e de rede por provedores de serviços, sendo a nuvem o espaço no qual dados, *softwares*, aplicativos e serviços são hospedados.

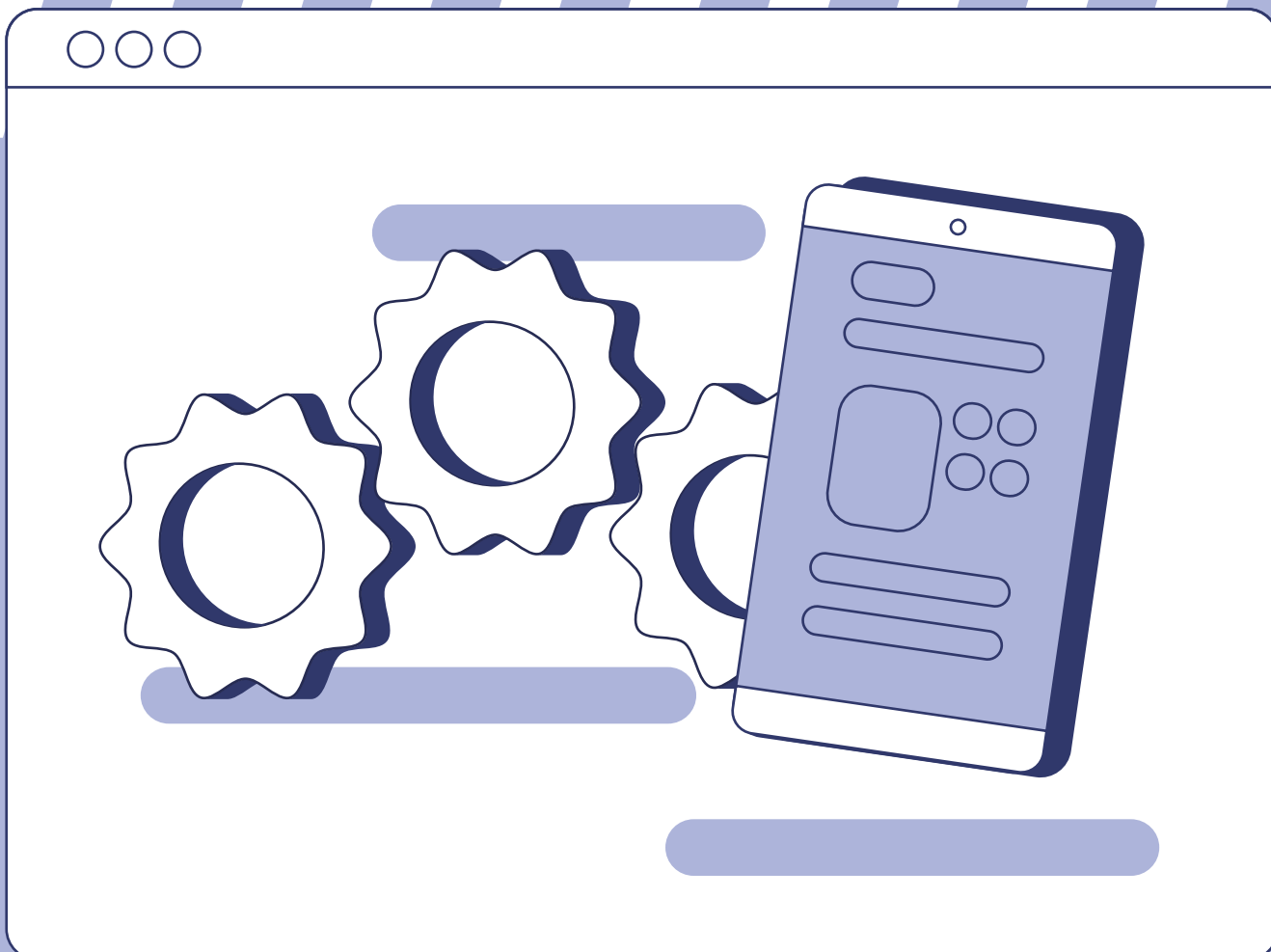
Existem três categorias de computação em nuvem¹:

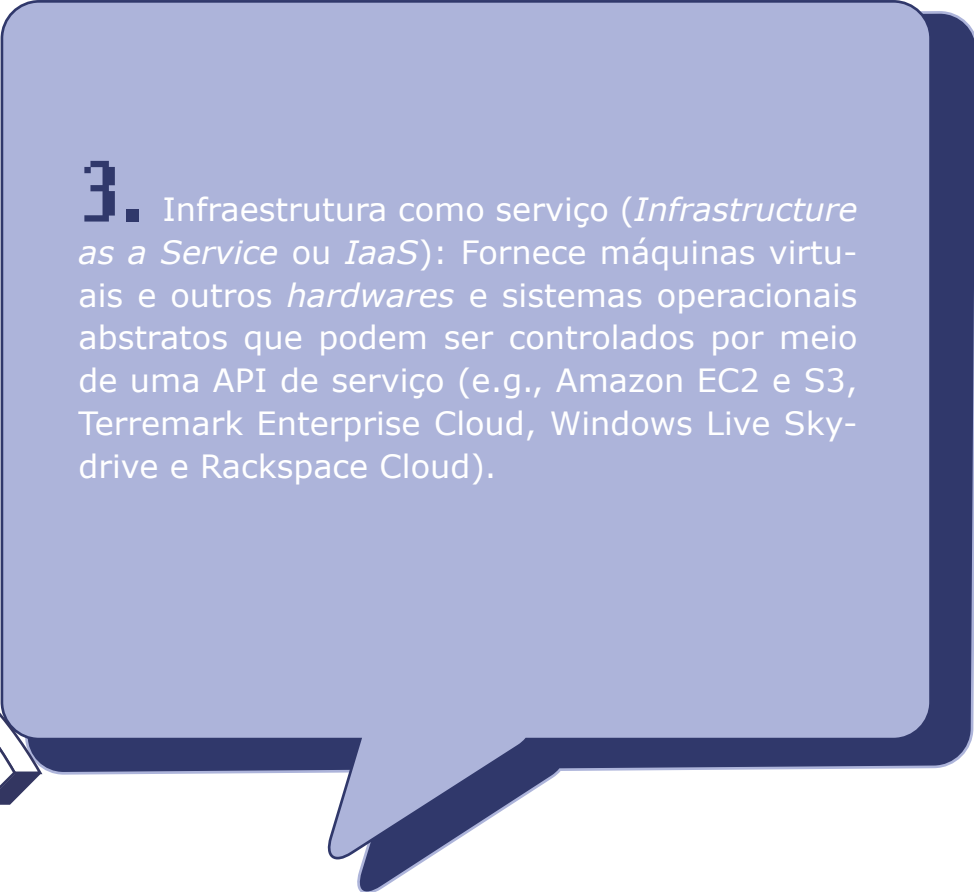
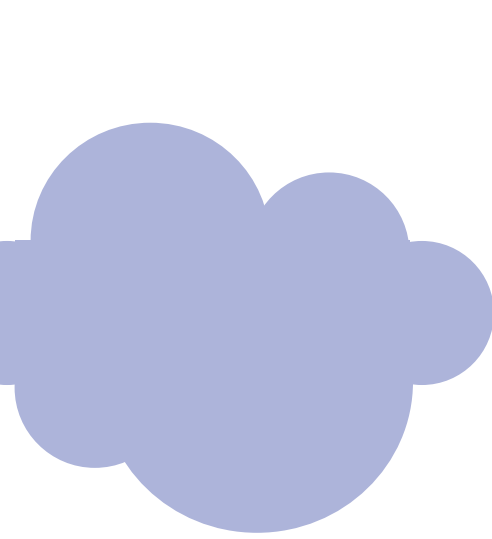
1. *Software como serviço (Software as a Service ou SaaS)*: É um *software* oferecido por provedor terceirizado, disponível sob demanda, geralmente configurável de modo remoto, via internet. Os exemplos incluem processamento de texto *on-line* e ferramentas de planilha, serviços de CRM e serviços de entrega de conteúdo da *web* (e.g., Salesforce CRM e Google Docs);



¹ European Network and Information Security Agency – ENISA. 2009. *Cloud Computing - Benefits, risks and recommendations for information security*. Disponível em: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport. Acesso em: 1º dez. 2022.

2. Plataforma como serviço (*Platform as a Service* ou *PaaS*): Permite que os clientes desenvolvam novos aplicativos usando APIs implantadas e configuráveis remotamente. As plataformas oferecidas incluem ferramentas de desenvolvimento, gerenciamento de configuração e plataformas de implantação (e.g., Microsoft Azure, Force e Google App Engine);



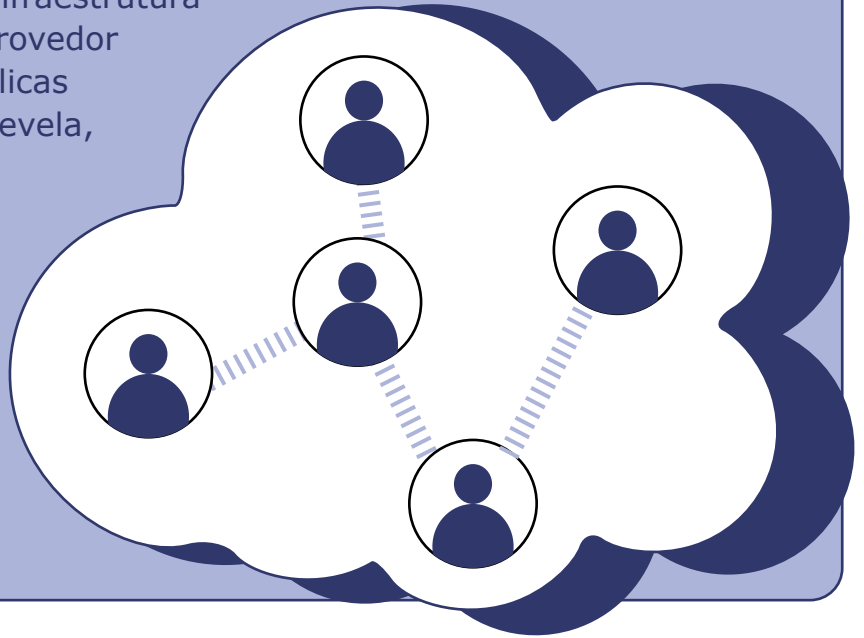


3. Infraestruturas como serviço (*Infrastructure as a Service* ou *IaaS*): Fornece máquinas virtuais e outros *hardwares* e sistemas operacionais abstratos que podem ser controlados por meio de uma API de serviço (e.g., Amazon EC2 e S3, Terremark Enterprise Cloud, Windows Live Skydrive e Rackspace Cloud).





Uma nuvem será pública quando pertencer a um provedor público, ou seja, um fornecedor de serviço terceirizado. Nesse caso, toda a infraestrutura de suporte é de propriedade do provedor e gerenciada por ele. Nuvens públicas estão disponíveis, como o nome revela, publicamente, e qualquer organização pode se inscrever.

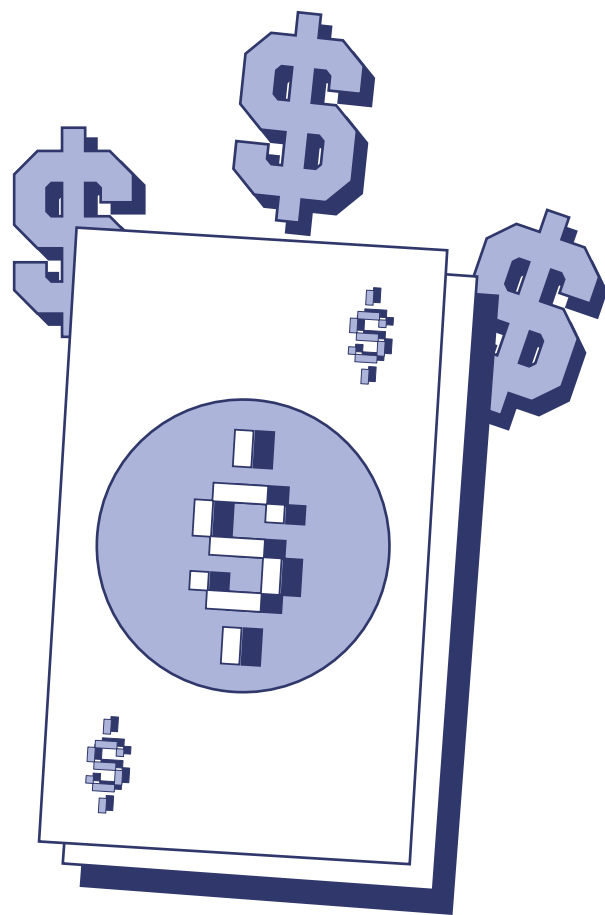
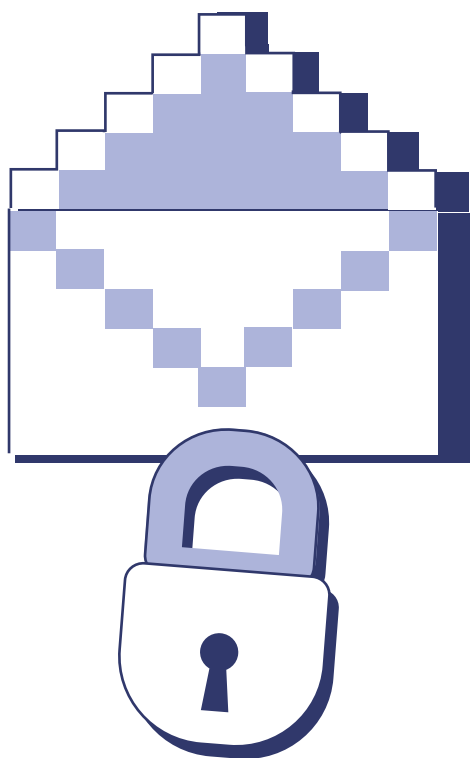


A nuvem será privada, por sua vez, quando tiver seus serviços construídos de acordo com os princípios da computação em nuvem, mas acessíveis apenas dentro de uma rede privada. A nuvem privada apresenta a vantagem de armazenamento de informações confidenciais do negócio, pois a infraestrutura é hospedada dentro da companhia. Já a chamada nuvem híbrida consiste em uma mistura das duas anteriores, possuindo provedores públicos e privados. Serviços em nuvens híbridas são oferecidos a um número limitado de partes.





Por se tratar de um serviço sob demanda, a computação em nuvem oferece a vantagem de redução de custos, visto que permite ao cliente trocar despesas fixas, como a manutenção de *datacenters* e servidores físicos, por despesas variáveis, por meio de um sistema de cobrança de pagamento conforme o uso (*pay-as-you-go*). Isso também proporciona maior flexibilidade, uma vez que é possível aumentar ou diminuir facilmente a infraestrutura tecnológica de acordo com as necessidades do cliente. Ademais, a computação em nuvem permite ampliar atividades para novas regiões geográficas de maneira facilitada. Com provedores disponibilizando infraestrutura em todo o mundo, é possível implantar aplicativos em vários locais físicos com apenas alguns cliques.



A computação em nuvem tem também potencial significativo para melhorar a segurança da informação. Isso porque, de maneira geral, investimentos em medidas de segurança são mais baratos quando implementados em grande escala – como ocorre na computação em nuvem. A mesma quantidade de investimento em segurança, seja de medidas defensivas, como filtragem, ou recursos humanos, compra melhor proteção. Desse modo, defesas baseadas em nuvem podem ser mais robustas, escaláveis e econômicas. Essas vantagens explicam o aumento dos gastos com *IaaS* e *PaaS* em nuvens públicas no Brasil, que atingiram cerca de US\$ 3 bilhões só em 2021².

² Lobo, Ana Paula. Mercado de nuvem brasileiro tem receita estimada em R\$ 18 bilhões. Convergência Digital, 3 ago. 2021. Disponível em: <https://www.convergenciadigital.com.br/Cloud-Computing/Mercado-de-nuvem-brasileiro-tem-receita-estimada-em-R%24-18-bilhoes-57725.html>. Acesso em: 3 dez. 2022.



Dado o custo reduzido e a flexibilidade nela implicados, a migração para a computação em nuvem é atraente para algumas empresas que, muitas vezes, imaginam que, ao terceirizar recursos de TI, terão todos os problemas relativos à segurança da informação solucionados – o que não é verdade. As economias de escala e a flexibilidade da nuvem trazem também riscos específicos, já que a concentração de recursos e de dados representa alvo mais atraente para os invasores.

Os riscos cibernéticos da computação em nuvem devem ser devidamente avaliados antes da celebração de um contrato com o provedor. Devem ser levadas em conta questões como nível de segurança oferecido, atribuição de responsabilidades, procedimento em caso de incidentes e existência de transferência internacional de dados pessoais.





Ao mapear os riscos relativos à computação em nuvem, a Agência Europeia para a Segurança das Redes e da Informação (Enisa) aponta, por exemplo, a perda de governança: ao utilizar infraestruturas de nuvem, o cliente necessariamente cede o controle ao provedor em uma série de questões que podem afetar a segurança³. Ao mesmo tempo, os instrumentos que regem a prestação do serviço podem apresentar lacunas nas defesas de segurança. Outro risco apontado diz respeito a falhas de isolamento: recursos compartilhados e espalhados em diversas localidades são características definidoras da computação em nuvem. Essa categoria de risco abrange falha de mecanismos que separam armazenamento, memória, roteamento e até reputação entre diferentes inquilinos da nuvem.

A maioria das questões legais envolvidas na computação em nuvem atualmente será resolvida durante a avaliação do contrato (ou seja, ao fazer comparações entre diferentes provedores) ou durante as negociações. O cenário mais comum, no entanto, é a seleção entre diferentes contratos oferecidos no mercado, uma vez que eles costumam ser padronizados e, portanto, não passíveis de negociação. No entanto, podem existir oportunidades para clientes em potencial de serviços em nuvem escolherem provedores cujos contratos sejam negociáveis.





Ao contrário dos serviços de internet tradicionais, as cláusulas contratuais padrão podem merecer revisão adicional devido à natureza da computação em nuvem. As partes de um contrato devem prestar atenção especial a direitos e obrigações relacionados a notificações de violações de segurança, transferências de dados, criação de trabalhos derivados, mudança de controle e acesso a dados por entidades de fiscalização. Como a nuvem pode ser usada para terceirizar infraestrutura interna crítica, e a interrupção dessa infraestrutura pode ter efeitos abrangentes, as partes devem considerar cuidadosamente se as limitações padrão de responsabilidade representam adequadamente suas alocações, dado o uso da nuvem pelas partes, ou responsabilidades pela infraestrutura⁴.

A computação em nuvem apresenta também riscos relativos à proteção de dados. Em alguns casos, pode ser difícil para o cliente da nuvem (na sua função de controlador) verificar efetivamente as práticas de tratamento do provedor e, assim, ter certeza de que os dados são tratados de forma legal. Esse problema é agravado em casos de múltiplas transferências de dados, sobretudo internacionalmente. Por outro lado, alguns provedores de nuvem fornecem informações sobre suas atividades de tratamento de dados, principalmente em suas políticas de privacidade e garantia de certificações reconhecidas – que deverão ser avaliadas previamente à contratação da nuvem.

⁴ European Network and Information Security Agency – ENISA. 2009. *Cloud Computing - Benefits, risks and recommendations for information security*. Disponível em: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport. Acesso em: 1º dez. 2022.



Por fim, ao optar pela migração para a computação em nuvem, é fundamental ter em mente que nem todos os riscos podem ser transferidos para o provedor: se um risco levar ao fracasso de um negócio, produzir danos graves à reputação ou tiver implicações legais, é difícil ou impossível para qualquer outra parte arcar com compensações. A realização de uma *due diligence*, que leve em consideração não apenas os benefícios da contratação de computação em nuvem para a empresa, mas os riscos relativos à segurança da informação e à proteção de dados, é capaz de prevenir a futuros prejuízos ao negócio.

Nossa equipe está à disposição para auxiliar e esclarecer dúvidas sobre o tema.

contato@opiceblum.com.br



OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF