

6 Melhores práticas para o sucesso em ambientes de TI híbrida

Uma realidade na maioria dos departamentos de TI nos dias atuais, a TI híbrida é resultado da migração feita pelos CIOs de muitas de suas aplicações, infraestruturas e ferramentas de TI para a nuvem, mantendo, ao mesmo tempo, outros elementos fora dela. A operação e manutenção bem-sucedidas de um ambiente de TI híbrida podem ser afetadas positivamente pela adoção eficaz de seis práticas recomendadas.

Análise:

A TI híbrida ajuda as empresas a extrair mais valor de seus ativos já existentes e oferece a base para a geração de impacto nos negócios por meio de investimentos estratégicos em nuvem. O ambiente de TI híbrida é resultado da estratégia utilizada pelas empresas de migrar, de forma seletiva, parte da TI para a nuvem e, ao mesmo tempo, manter outras tecnologias em ambientes fora dela (consulte "[Leveraging Hybrid IT Now to Power Digital Transformation](#)").

O processo de migração de tecnologias para a nuvem deve ser gradual na maioria das empresas, enquanto, em muitas outras, a migração de toda a TI não faz sentido algum. Ambas as situações sugerem que a TI híbrida é o modelo operacional do futuro. Apesar disso, o gerenciamento eficaz dos ambientes híbridos envolve importantes fatores, visto que todo novo fornecedor de TI torna o ambiente de TI híbrida ainda mais complexo e abre precedentes para maiores conflitos por conta das variações entre os modelos de serviço. Essas variações podem gerar retrabalho e ineficiências para os negócios. Por exemplo, cada fornecedor utilizará seu próprio processo de reparo e manutenção, suas próprias ferramentas de teste e seus próprios protocolos de segurança.

Haverá a necessidade de práticas, ferramentas e protocolos padrão para lidar com funcionalidades em duplicidade no portfólio híbrido, além de processos e mecanismos de governança para inserção ou atualização de dados entre diferentes produtos. Os CIOs terão de repensar como operar a TI na era híbrida e desenvolver um roadmap para o sucesso nesse modelo que aborde cada uma das seguintes práticas recomendadas funcionais e técnicas sugeridas:

MELHORES PRÁTICAS FUNCIONAIS

- 1** A seleção de aplicações deve incluir uma avaliação estratégica das funcionalidades de negócios e dos modelos de entrega.
- 2** A equipe deve ter as novas habilidades necessárias à implementação e operação de um ambiente de TI híbrida.
- 3** Os serviços de suporte a portfólios diversificados devem lidar com as variações e limitações das políticas e dos SLAs de serviço dos fornecedores.

MELHORES PRÁTICAS TÉCNICAS

- 4** Aproveite a flexibilidade e a agilidade do modelo operacional de TI híbrida e não se deixe atrapalhar pela complexidade arquitetônica.
- 5** Ferramentas, processos e governança de integração devem produzir uma solução uniforme.
- 6** Controles e processos de segurança devem manter o ambiente de TI híbrida seguro.

Os CIOs têm diante de si a incrível oportunidade de ajudar suas empresas a transformar o uso do modelo operacional de TI híbrida, mas é preciso seguir uma estratégia para desenvolver o portfólio híbrido e definir quando usar a nuvem e quando manter soluções fora da nuvem. A alocação de pessoal deve também ser abordada no desenvolvimento e na operação da TI híbrida. Os serviços de suporte devem evoluir para lidar com os componentes na nuvem e fora da nuvem do ambiente de TI híbrida.

1. A seleção de aplicações deve incluir uma avaliação estratégica das funcionalidades de negócios e dos modelos de entrega.

[As equipes de TI precisam ser estratégicas ao decidir se serão utilizadas soluções na nuvem ou fora da nuvem.](#)

Para garantir a compreensão da estratégia pelas partes interessadas, os líderes de TI podem precisar definir claramente a posição da empresa em relação às funcionalidades de negócios que podem/devem ir para a nuvem e que devem permanecer fora da nuvem.

Sistemas de registro como o ERP são candidatos menos prováveis à nuvem como SaaS devido à sua típica complexidade, a um certo nível de customização e à independência de conectividade com a Internet ou de fatores externos para acesso ao software. Contudo, transferir aplicações ERP licenciadas para a nuvem por meio de uma migração IaaS pode ser uma manobra importante, capaz de proporcionar flexibilidade e agilidade e, ao mesmo tempo, dar oportunidade às empresas de continuar extraindo valor de suas licenças de aplicações.

Sistemas de engajamento, como o CRM e outras aplicações de front-end destinadas a conectar clientes a fornecedores, são candidatos mais prováveis ao SaaS, no qual a presença digital pode criar vantagem competitiva ou impulsionar o crescimento. Sistemas não tão complexos e propensos a mudanças frequentes para se manterem relevantes são igualmente bons candidatos ao SaaS.

A governança será necessária ou terá de ser mais rígida — isto é, "todos deverão seguir as regras" — na seleção de aplicações/tomada de decisões.

Por exemplo, é possível estabelecer uma estratégia que priorize a nuvem nas aplicações voltadas ao cliente, enquanto uma abordagem "ideal à finalidade" pode ser adotada para aplicações altamente integradas ou sigilosas. Nada disso terá importância sem um mecanismo de governança destinado a garantir o cumprimento das "regras".

Recomendações:

- A implantação de aplicações e serviços (nuvem vs. fora da nuvem) pode ser uma nova disciplina para a empresa. Desenvolva e aloque pessoal a essa atividade segundo necessário para abranger vários modelos de entrega.
- Atualize/crie uma estrutura que faça a seleção de aplicações e a tomada de decisões de maneira rápida e eficaz. A estrutura será acessada com mais frequência, e serão necessários resultados mais rápidos para compras na nuvem do que na maioria das compras históricas de soluções grandes e complexas fora da nuvem.

2. A equipe deve ter as novas habilidades necessárias à implementação e operação de um ambiente de TI híbrida.

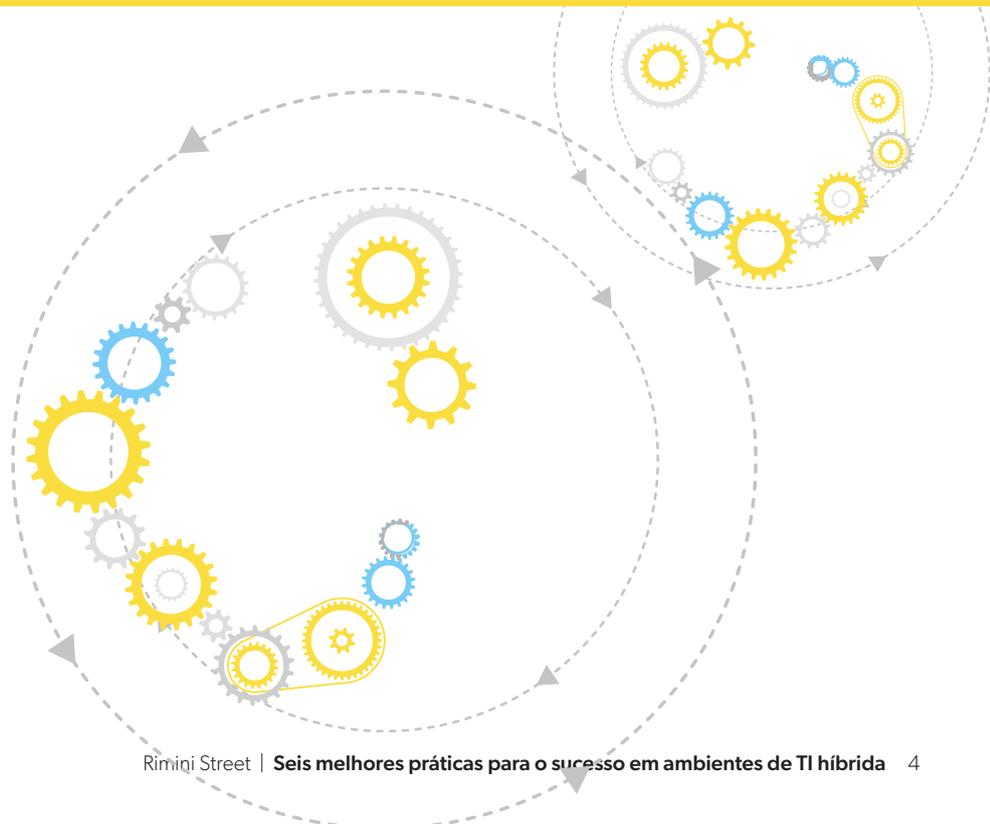
Para algumas empresas, habilidades como gerenciamento de plataformas e engenharia entre silos terão de ser formalizadas ou expandidas a fim de manter o ambiente de TI híbrida.

O pool de especialização na nuvem é menor do que a demanda por essas habilidades. A demanda por habilidades de integração de nuvem para nuvem e de nuvem para fora da nuvem será alta, mas elas serão difíceis de encontrar. Será mais fácil compor equipes que, coletivamente, tenham experiência em segurança, rede, engenharia de soluções etc. do que alocar alguns indivíduos com um amplo leque de habilidades. Por exemplo, com relação à equipe do Centro de Excelência em Nuvem (CCOE), a Gartner observa o seguinte: "Tal equipe deve ser normalmente liderada por um arquiteto de nuvem sênior com conhecimento prático em operações de negócios e de TI".

Para empresas sem muitas ações de terceirização, será necessário contratar ou treinar especialistas em áreas como gerenciamento de fornecedores, contratação de serviços e gerenciamento de serviços. Diante da grande dificuldade de alocar habilidades de negócios, a migração para a nuvem pode ser uma oportunidade de requalificação/reciclagem de treinamento. Talvez seja necessário o apoio dos líderes para convencer a equipe a aprender algo novo. Por outro lado, as oportunidades de reciclagem de treinamento podem ajudar a reter/elevar o moral dos funcionários que buscam uma experiência mais ampla em nuvem.

Recomendações:

- Avalie a necessidade de obter habilidades técnicas, como engenharia entre silos, segurança de nuvem, gerenciamento de plataformas e integração.
 - Nas situações em que for difícil alocar habilidades, considere adotar uma abordagem de equipe para obter o complemento integral e busque oportunidades de reciclar o treinamento da equipe interna, em vez de contratar novos funcionários.
 - Combine esforços de alocação de pessoal com oportunidades de requalificação para eliminar o possível temor de deslocamento de pessoal.
- Pondere sobre a necessidade de obter habilidades funcionais, como gerenciamento de fornecedores, gerenciamento de serviços e seleção estratégica.
- Avalie a ideia de requalificar ou reciclar o treinamento da equipe interna para preencher as lacunas de habilidades relacionadas à nuvem.



3. Os serviços de suporte a portfólios diversificados devem lidar com as variações e limitações das políticas e dos SLAs de serviço dos fornecedores.

A complexidade dos serviços de suporte pode se intensificar rapidamente à medida que novos fornecedores são incorporados ao ambiente de TI híbrida.

A maioria dos fabricantes de software dá suporte apenas a seu próprio código. A oferta deles é limitada, e eles normalmente não detêm a propriedade nem dão suporte a customizações e integrações. Nas situações que requerem suporte, ou quando ocorre um incidente de reparo e manutenção em uma solução multifornecedor, uma abordagem de responsabilização unificada à coordenação de serviços de suporte pode reduzir acusações e respostas do tipo "prove que o problema é meu" e "esse não é o meu código" dadas por fornecedores de nuvem e fora da nuvem e, espera-se, reduzir os tempos de suporte e elevar a qualidade.

Trabalhar com vários fornecedores no portfólio híbrido cria a possibilidade de SLAs conflitantes (ou no mínimo incompatíveis). Por exemplo, é possível que o tempo de resposta garantido para interrupções de um fornecedor seja maior que o de outro, e isso pode se transformar em um problema de SLA se o segundo fornecedor não for capaz de cumprir com o SLA pelo fato de estar aguardando a resposta do primeiro.

Processos e governança relacionados a cada aspecto do suporte – incluindo, sem limitação, design de soluções, testes, backups, recuperação de interrupções e coordenação de tempos de inatividade planejados – devem ser compatíveis na governança e nos processos internos de vários fornecedores.

Em ambientes fora da nuvem, a empresa tem controle quase total sobre a forma como os serviços de suporte são entregues. Mas, em ambientes híbridos, normalmente os fornecedores controlam como e quando algumas atividades críticas de suporte acontecem. Por exemplo, um fornecedor de nuvem pode atualizar seu ambiente de teste apenas mensalmente, e outro pode limitar o número de testes permitido por mês. Qualquer política pode implicar a necessidade urgente de um teste sincronizado entre vários fornecedores. Esse é apenas um dos aspectos de suporte que podem ser afetados no modelo híbrido.

As empresas precisam identificar claramente seus próprios serviços de suporte, os serviços de propriedade dos fornecedores e os serviços "intermediários" que precisam ser negociados ou acordados. O conceito de abordar o grupo intermediário se aplica a todos os fornecedores integrados ao ambiente de TI híbrida.

Recomendações:

- Estabeleça uma matriz RACI (responsável, aprovador, consultado, informado) de "responsabilidades" para cada fornecedor.
- Como sugestão, unifique os serviços de reparo e manutenção de Nível 3 na nuvem e fora da nuvem em um parceiro de suporte capaz de orquestrar serviços de vários fornecedores.
- Considere também o uso de um provedor de AMS para operação e gerenciamento do portfólio de TI híbrida de produtos e serviços na nuvem e fora da nuvem. Nessa abordagem, uma organização (formada por equipes internas ou por AMS externo) é responsável por executar e manter soluções em todo o portfólio e tem pessoal e habilidades operacionais para isso. Isso reduz os problemas de interrupções e responsabilização que podem ocorrer quando vários fornecedores são individualmente responsáveis por partes distintas da solução total.

Um dos desafios do modelo de TI híbrida é que a arquitetura pode rapidamente se tornar um tanto complicada. À medida que mais componentes são adicionados ao portfólio híbrido, aumenta a necessidade de priorizar a integração. Da mesma forma, a segurança se torna mais desafiadora com o acréscimo de cada novo provedor à combinação.

1. Aproveite a flexibilidade e a agilidade do modelo operacional de TI híbrida e não se deixe atrapalhar pela complexidade arquitetônica.

Apesar de proporcionar flexibilidade e agilidade às empresas, a TI híbrida também gera despesas gerais de arquitetura.

Um número cada vez maior de provedores, opções e alternativas pode gerar complicações arquitetônicas que levam a um ambiente de TI mais complexo. Por exemplo, como evitar funcionalidades em duplicidade entre provedores que oferecem recursos sobrepostos (ou escolher uma delas)? E se for necessário configurar os recursos em duplicidade para ambas as ofertas dos provedores para que elas funcionem corretamente?

A colocalização agrava ainda mais a complexidade arquitetônica e gera uma situação em que a empresa é proprietária dos servidores nos quais executa suas aplicações, mas um terceiro é proprietário das instalações físicas nas quais estão os servidores. O cliente tem autoridade sobre o hardware e o software, mas a instalação de armazenamento tem autoridade sobre a manutenção e a segurança dos equipamentos. Isso pode requerer controles adicionais nas situações em que data centers de vários locatários estejam envolvidos. Os desafios da colocalização devem ser também levados em consideração na escolha de provedores e produtos a serem incluídos no portfólio híbrido.

Por fim, embora as aplicações modernas sejam projetadas para interoperabilidade, uma combinação de soluções em nuvem e fora da nuvem aumenta a complexidade arquitetônica nos pontos de contato. Exemplos disso incluem elementos de dados — (centro de custos, ID de funcionário, número do cliente etc.) que provavelmente serão incluídos em produtos de vários provedores, mas não necessariamente definidos de maneira semelhante em todos os produtos. Embora a empresa possa ajustar as definições de dados de seus sistemas fora da nuvem (o que não é garantido, principalmente em soluções mais antigas), ela provavelmente não pode alterar definições em produtos de nuvem. Nas situações em que dados, processos e segurança transcendem provedores e modelos de entrega, essas variações devem ser tratadas antes da fase de integração.

Aproveite a flexibilidade e agilidade do modelo híbrido para se adaptar rapidamente à evolução dos negócios.

As mudanças ocorrem com mais frequência nos ambientes de TI híbrida. Isso é um resultado direto da maioria dos componentes de nuvem ainda em evolução. Também é um "recurso" das funcionalidades de nuvem, projetadas para ser substituídas à medida que soluções melhores chegam ao mercado. Atividades operacionais, como controle de versões de produtos, serão fundamentais para garantir que o ambiente de TI híbrida possa resistir à mudança.

Ao medir a adaptabilidade dos ambientes híbridos, avalie a facilidade de interconexão entre provedores e produtos distintos. Isso também pode ser descrito como o nível de interoperabilidade ou a quantidade de esforço necessária para a integração.

Recomendações:

- Mantenha os produtos fora da nuvem quando fizer sentido utilizá-los como base para a implantação de soluções de nuvem no entorno. Bons candidatos à retenção de licenças fora da nuvem incluem aplicações como as de ERP, nas quais a alta integração é necessária, customizações existentes que atenderam a requisitos exclusivos e/ou quando nenhuma solução de SaaS for capaz de oferecer paridade funcional.
- Crie agilidade e flexibilidade no ambiente híbrido migrando para a nuvem funcionalidades que não exigem alta integração, que requerem mudanças frequentes ou rápidas para manter a empresa competitiva e que podem ser facilmente substituídas à medida que soluções melhores são disponibilizadas.
- Assegure-se de produzir um design arquitetônico de TI híbrida flexível o bastante para integrar, remover ou desativar soluções rapidamente. Estabeleça o monitoramento contínuo de gargalos ou pontos de falha gerados pela variedade de provedores, por sua diversidade e por possíveis atritos entre nuvem e fora da nuvem.

2. Ferramentas, processos e governança de integração devem produzir uma solução uniforme.

Um dos principais motivos da migração para pacotes integrados de produtos é a integração direta. Diante da atual decomposição dos pacotes e de sua aquisição por meio de vários fornecedores, a integração passa a ser uma das mais altas prioridades.

Novas arquiteturas orientadas a serviços, arquiteturas de serviços em nuvem e estruturas de integração foram disponibilizadas para facilitar a viabilização da TI híbrida.

Quando os processos são divididos entre produtos, não há garantia intrínseca da realização integral e precisa de um processo entre os produtos. A integração de processos deve se tornar uma disciplina, já que não é automaticamente garantida (como provavelmente seria em um pacote de produtos).

A integração de dados, que é a forma mais familiar de integração, terá um aumento na prioridade porque a integridade dos dados, os direitos de acesso e uso, a propriedade e a sincronização podem se tornar complexas entre fornecedores devido à variedade cada vez maior de endpoints.

À medida que o portfólio de aplicações se torna mais diversificado e distribuído por meio da TI híbrida, você pode aproveitar as funcionalidades robustas presentes nas ferramentas mais recentes para habilitar com mais facilidade a integração direta.

Normalmente, os fornecedores de SaaS e de nuvem utilizam terminologias diferentes em seus processos de TI. Caso ainda não exista, pode ser necessário criar um centro de excelência (COE) de integração para gerenciar o portfólio híbrido. O CEO de integração pode ajudar a superar as "barreiras de linguagem" entre fornecedores e desenvolver processos comuns, quando necessário.

Os atuais padrões de ferramentas de integração podem rapidamente se tornar inadequados à medida que o portfólio se expandir para um cenário de nuvem múltipla. Talvez seja necessário adicionar ferramentas modernas de integração de plataforma como serviço (iPaaS) ao kit de ferramentas de integração para lidar com os requisitos de nuvem para nuvem e de nuvem para fora da nuvem.

O mecanismo de integração a ser usado, a propriedade de dados e processos e a integridade da integração são exemplos de áreas nas quais a governança terá de se expandir para acomodar a natureza multifornecedores dos portfólios híbridos.

Recomendações:

- Desenvolva especialização em conhecimento multifornecedores. Isso será de grande valia para atender aos requisitos e restrições de integração que não são contemplados pelos conectores pré-empacotados dos fornecedores. Defina a integração como uma parte substancial dos custos de aplicações.
- Encontre um equilíbrio entre software de integração implantado internamente e plataforma de integração como serviço (iPaaS).
- Estabeleça um COE de integração para gerenciar as interconexões de seu ambiente de TI híbrida.

3. Controles e processos de segurança devem manter o ambiente de TI híbrida seguro.

Segurança da infraestrutura: a combinação da arquitetura fora da nuvem com as arquiteturas compartilhadas dos diversos fornecedores de nuvem em um modelo de TI híbrida aumenta a quantidade de pontos de controle e os tipos de controles envolvidos.

Haverá tantas variações de processos e protocolos de segurança de infraestrutura quanto de fornecedores no portfólio híbrido, e alguns talvez não sejam compatíveis. Além disso, a segurança consistente de um componente pode ser minimizada pela segurança superficial de outro. Embora a segurança do ambiente físico do fornecedor de nuvem seja mantida pelo fornecedor, os clientes devem garantir que a infraestrutura de nuvem esteja operacionalmente protegida.

Segurança de aplicações: a segurança das ferramentas e aplicações de SaaS é, de modo geral, aceitável, apesar de haver tantas variações envolvidas quanto fornecedores.

São necessários processos de segurança robustos para manter o portfólio híbrido protegido. O uso de uma tecnologia unificadora, como login único ou portais, pode facilitar o acesso a aplicações e ferramentas, mas talvez não elimine conflitos em designs individuais de segurança. Alguns produtos oferecem proteção no nível do elemento de dados, por exemplo, enquanto outros oferecem proteção por tipo de registro, o que pode gerar um conflito que precisa ser solucionado no design de segurança mestre da empresa.

Proteger um ambiente de TI híbrida envolve garantir que os controles multifornecedores reduzam a exposição em cada ponto de contato de fornecedor.

Cada novo fornecedor no portfólio aumenta a exposição de segurança e a possibilidade de que alguma força externa (por exemplo, um funcionário descontente ou alguém que encontre/procure por falhas na infraestrutura) se utilize disso para "invadir". Resultados de uma pesquisa recente da Cowen demonstraram que 37% dos entrevistados identificaram a Segurança de nuvem como uma das principais prioridades em termos de gastos. E, no período pré-pandemia da COVID, mais de 90% dos entrevistados projetavam ampliar seus orçamentos de segurança em 2020 (no entanto, houve uma queda de 6% nos resultados pós-COVID, embora a segurança continue tendo a maior expectativa de crescimento em relação ao ano anterior no período pós-pandemia). Embora os CIOs reconheçam o fato e estejam se planejando para ele, as empresas devem estar dispostas a aceitar certo nível de risco ao adicionar produtos de nuvem a seus portfólios de TI híbrida.

Validar a eficácia dos controles de segurança no portfólio híbrido pode ser desafiador, visto que o cliente não terá um nível detalhado de visibilidade da segurança dos fornecedores de nuvem.

Ao mesmo tempo, a maioria dos fornecedores não se mostra receptiva a testar a segurança de seus produtos ou de seus ambientes. Certas políticas e controles legais também têm o poder de limitar o que pode ser testado no ambiente do fornecedor.

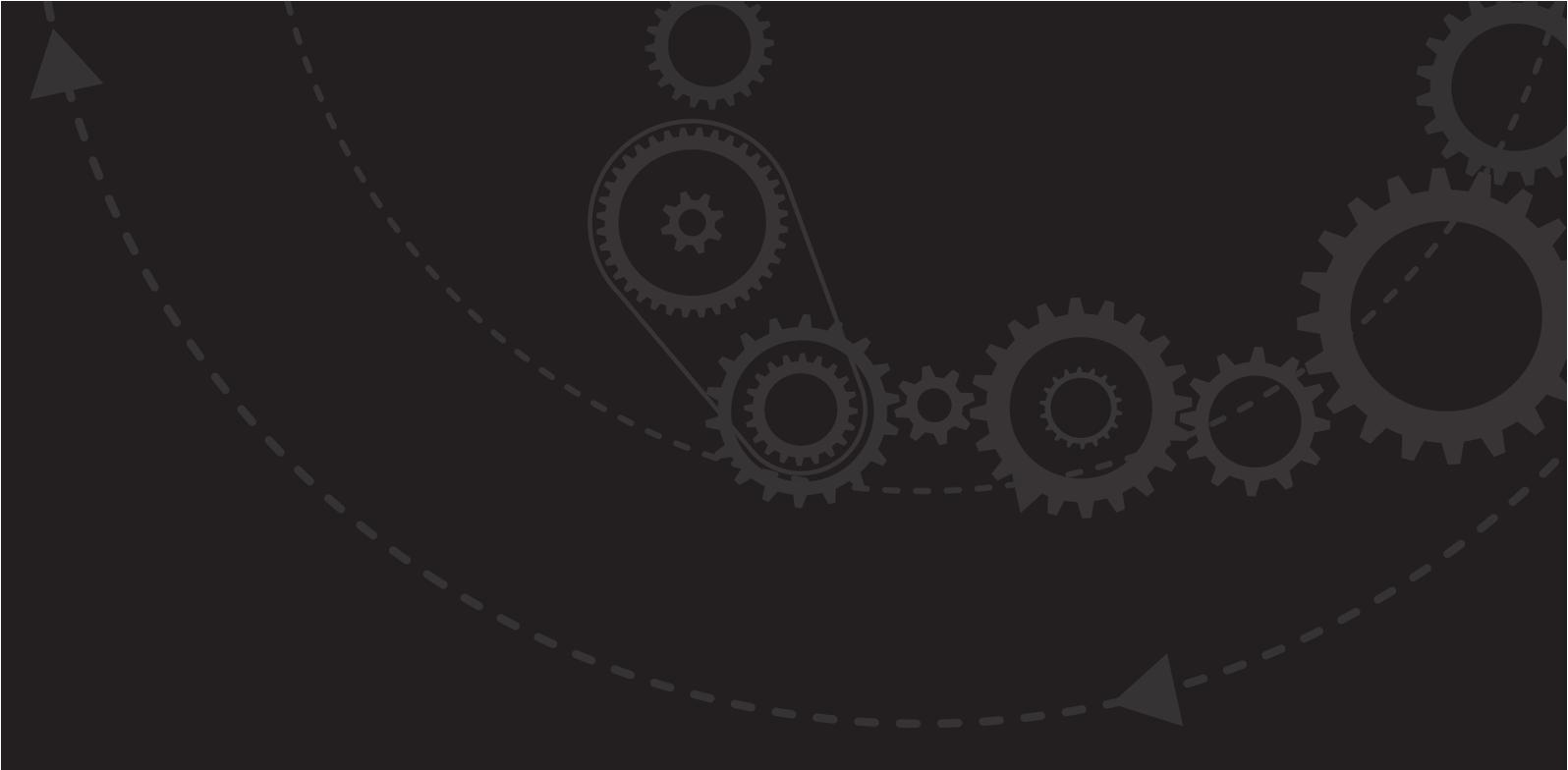
Recomendações:

- Alinhe os processos e controles de segurança em todo o portfólio.
- Defina responsabilidades pelos serviços de segurança de infraestrutura e aplicações. Dê atenção especial à definição e atribuição de propriedade de identidades e controles de gerenciamento de acesso.
- Determine o quanto a empresa está disposta a confiar "na nuvem".
- Desenvolva uma auditoria de segurança e medidas de eficácia que considerem a falta de visibilidade dos serviços de nuvem.



CONCLUSÃO

Os benefícios de um ambiente de TI híbrida são significativos e valem qualquer complexidade adicional, mas é importante lidar proativamente com os fatores críticos para o sucesso. Adotar estas seis práticas recomendadas pode melhorar significativamente o sucesso geral da implantação do modelo de TI híbrida, além de ajudar você a navegar pelos desafios da migração para a nuvem.



Rimini Street®

riministreet.com/br
contato@riministreet.com
twitter.com/riministreet
[linkedin.com/company/rimini-street](https://www.linkedin.com/company/rimini-street)

A Rimini Street, Inc. (Nasdaq: RMNI) é fornecedora global de produtos e serviços de software corporativo, maior provedora de suporte independente a produtos de software Oracle e SAP e parceira da Salesforce®. A empresa oferece serviços de suporte e AMS integrados e ultrarresponsivos, que permitem a licenciados de softwares corporativos uma economia de custos significativa, liberando recursos para inovar e obter melhores resultados nos negócios. Empresas da Global Fortune 500, de médio porte, do setor público e outras organizações de uma ampla variedade de setores têm na Rimini Street uma provedora de produtos e serviços de software corporativo de confiança.

© 2021 Rimini Street, Inc. Todos os direitos reservados. "Rimini Street" é uma marca registrada da Rimini Street, Inc. nos Estados Unidos e em outros países, e Rimini Street, o logotipo da Rimini Street e suas combinações, e outras marcas marcadas por TM são marcas comerciais da Rimini Street, Inc. Todas as outras marcas comerciais são de propriedade dos respectivos donos e, a menos que especificado de outra forma, a Rimini Street não tem afiliação, endosso ou associação com os detentores de tais marcas comerciais nem com outras empresas aqui citadas. Este documento foi criado pela Rimini Street, Inc. ("Rimini Street") e não é patrocinado por, endossado por ou afiliado a Oracle Corporation, SAP SE ou qualquer outra parte. Exceto se expressamente disposto por escrito, a Rimini Street não assume nenhuma responsabilidade por qualquer garantia expressa, implícita ou estatutária relacionada às informações apresentadas, incluindo, sem limitação, qualquer garantia implícita de comercialização ou adequação a uma finalidade específica. A Rimini Street não será responsável por qualquer indenização punitiva, por danos diretos, indiretos, patrimoniais, extrapatrimoniais ou por custos adicionais decorrentes do uso ou da incapacidade de uso dessas informações. A Rimini Street não oferece declarações ou garantias em relação à precisão ou à integridade das informações fornecidas por terceiros e reserva-se o direito de fazer alterações em informações, serviços ou produtos a qualquer momento. LR-73498 | BR-091521