Redefinindo a Governança da Tecnologia de Nuvem Corporativa

As organizações de todo o mundo estão migrando rapidamente a infraestrutura de TI, software e outras tecnologias locais para os serviço em nuvem. Hoje, as organizações gastam quase metade do seu orçamento de TI em serviços de nuvem, e esse gasto está crescendo.[1] Os benefícios da utilização destes serviços são inegáveis, incluindo negociação de despesas de capital por taxas variáveis (ou seja, um modelo de pagamento por uso) e economias de escala, que os hiperescaladores em nuvem tipicamente oferecem. A tecnologia em nuvem permite maior velocidade e agilidade e acesso a um público mundial em um tempo menor em comparação com a infraestrutura e os serviços de TI locais. Além disso, o uso da nuvem permite que as organizações se concentrem no negócio principal e não na manutenção de centros de dados. Os serviços em nuvem também são constantemente aprimorados para permanecerem a frente da tecnologia.

No entanto, as organizações e suas práticas de governança não conseguiram acompanhar o ritmo de mudança da nuvem. Elas carecem das competências e dos conhecimentos necessários para governar eficientemente o uso da nuvem e seu risco associado; assim, eles são incapazes de otimizar seu valor. Adicionalmente, a adoção dos serviços em nuvem é geralmente percebida como mais dispendiosa quando vista a partir de uma perspectiva operacional ou como serviços em nuvem individuais, e isso se deve à falta de uma estrutura integrada definitiva ou padrão para governança em nuvem. Atualmente, as estruturas industriais não tratam especificamente do impacto da nuvem sobre governança de TI e processos de gestão. A computação em nuvem é um facilitador chave da transformação digital e tem uma consideração importante na governança digital. Assim, é importante que seja colocada maior ênfase na governança em nuvem para garantir que esteja alinhada com futuros requisitos de negócios.

Entendendo os Princípios da Governança em Nuvem

Para estabelecer os princípios da governança em nuvem, duas questões devem ser consideradas. Primeiro, como a governança de nuvem é diferente da governança de TI? A computação em nuvem converte ou abstrai hardware de TI e software em serviços, impactando quase todos os processos de governança e gestão de TI. Com a computação em nuvem, existe uma dependência maior de terceiros para infraestrutura e serviços de TI críticos em comparação com o ambiente de controle local de TI tradicional. Portanto, a governança de TI também deve ser adaptada. Segundo, por que uma governança de TI apropriada é tão importante? Devido à mudança fundamental da natureza dos serviços de TI introduzidos pela adoção da nuvem (ou seja, abordagens de segurança da informação, modelos de custos, habilidade exigida), os processos de governança de TI das organizações precisam ser adaptados para o novo modelo operacional introduzido pelo uso de infraestrutura e serviços em nuvem. Considerando a notável aceleração da migração em nuvem em todo o mundo, é importante que o conselho administrativo e a gestão executiva levem em conta vários

DAVID MAZULA | CISA, CISM

Parceiro da equipe de confiança digital na PricewaterhouseCoopers (PwC) África do Sul. Possui mais de 10 anos de experiência entregando auditorias de sistemas, auditorias internas, melhorias de processos de negócios e outros serviços de consultoria em diversas indústrias.

CASPER LAMPRECHT | CISA, CIA

Gerente Sênior da equipe de confiança digital na PwC África do Sul. Especializado em governança de TI e garantia de programa e projeto. Possui mais de 20 anos de experiência em gestão de projetos e 13 anos de experiência em riscos de TI e governança.

princípios quando fizerem a mudança para a nuvem. Práticas e controles rápidos e flexíveis são fundamentais, em vez de rígidos. Elas devem centralizar políticas, mas descentralizar a execução da política.[2] A **Figura 1** demonstra esses princípios.

O círculo externo representa as áreas de governança. O círculo interno é uma representação não exaustiva dos processos típicos de gestão de TI que a migração para a nuvem impacta.[3] A gestão executiva e os conselhos de diretores devem considerar os princípios da estrutura de governança na nuvem para ajudar a garantir um ambiente em nuvem bem administrado e agregando valor.

Componentes de Governança da Nuvem e Risco

Existem 14 áreas principais de governança para a estrutura sugerida de governança em nuvem. É útil entender cada um desses tópicos da estrutura de governança em nuvem.

Estabeleça uma Estratégia em Nuvem e o Caso de Negócio

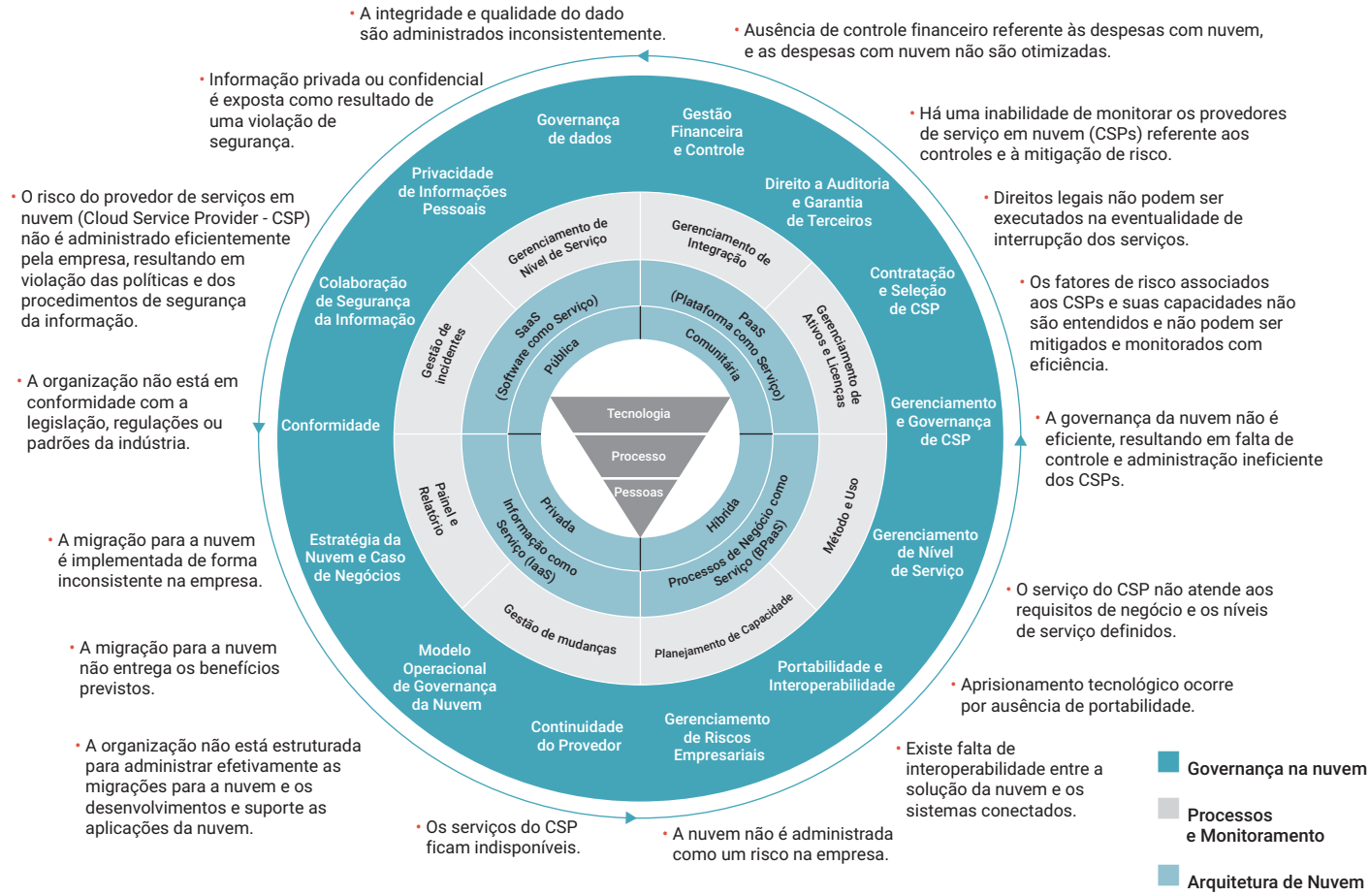
Uma estratégia em nuvem bem desenvolvida que é integrada a uma estratégia de negócios digitais de uma organização é um ponto de partida importante na jornada para adoção da nuvem. As organizações tipicamente optam por uma estratégia multinuvem e cloud first, mas não consideram a oportunidade da migração em nuvem ou como a nuvem possibilitará sua estratégia de negócios digitais. As organizações devem formular um caso de negócios e benefícios que considerem a estratégia em nuvem e as necessidades e benefícios associados da organização, o custo total de propriedade, e fatores estratégicos, como agilidade e eficiência.

Sem uma estratégia em nuvem cuidadosamente considerada e documentada, as organizações enfrentam várias fontes de risco, incluindo:

- Uma migração para a nuvem que é implementada inconsistentemente em toda a empresa. Diferentes divisões organizacionais e unidades de negócios podem utilizar diferentes abordagens para a adoção da nuvem e aplicar diferentes princípios, que podem ter implicações adversas para o negócio na entrega dos seus objetivos.

FIGURA 1

Estrutura de Governança da Nuvem



- Uma migração para a nuvem que não entrega os benefícios e o valor previsto. Alguns dos benefícios da nuvem, como agilidade, podem ser impedidos.
- Risco de dependência de terceiros com pouca clareza e não administrado. Isso pode levar a problemas tais como interrupções do sistema, falhas de segurança e não conformidade com as normas.
- Risco de privacidade e segurança cibernética com pouca clareza e não administrado. Isso pode resultar em violações da segurança cibernética e não conformidade com as leis e normas de privacidade.

Criar um Modelo Operacional de Governança em Nuvem

Modelo operacional de governança em nuvem refere-se à estrutura organizacional, funções e responsabilidades, recursos, competências e processos de negócios que habilitam os serviços em nuvem. A nuvem suporta um modelo operacional de negócios e uma estratégia de negócios digitais da organização, assim o modelo operacional de TI, incluindo o modelo operacional de governança de TI, deve ser alinhado com a nuvem. O modelo operacional de TI deve estar alinhado com o modelo operacional de negócios através de consulta com as partes interessadas do negócio. Uma vez que o modelo operacional de TI está alinhado, o modelo operacional de governança de TI deve ser adaptado ao risco e aos desafios colocados pela nuvem.

As fontes de risco que podem acompanhar um modelo operacional de governança em nuvem inadequado incluem:

- A organização não deve estar estruturada de maneira que administre eficientemente a migração, o desenvolvimento e o suporte de aplicativos para a nuvem.
- As atividades em nuvem não podem suportar a estratégia de negócios, o que podederia expor a organização a fatores de risco não administrados.
- Os custos da nuvem podem ser excessivos, não imediatamente identificáveis (ou seja, ocultos) ou não administrados.

Busque Conformidade com a Nuvem

Reguladores e outras partes interessadas importantes, esperam conformidade com leis, regras, normas e padrões da industria.[4] Alguns dos requisitos de conformidade com os quais as organizações devem aderir incluem a EU General Data Protection Regulation (GDPR), a South African Protection of Personal Information Act (POPIA), South African Consumer Protection Act 68 of 2008, os padrões da International Organization for Standardization (ISO) (por exemplo, ISO 22316:2017) e os padrões Payment Card Industry (PCI) standards. Os hiperescaladores em nuvem também devem estar em conformidade com vários padrões da industria, e é por isso que é importante que uma organização que adota serviços em nuvem integre a nuvem aos processos de conformidade.

CSPs devem ser avaliados de acordo com as políticas de privacidade organizacional e os mecanismos de monitoramento devem ser instalados para garantir conformidade contínua com os requisitos de privacidade.

Fontes comuns de risco que podem surgir de uma falha de integração da nuvem aos processos de conformidade incluem:

- A organização pode não estar em conformidade com a legislação, normas ou padrões da industria local ou internacional.
- A organização pode perder sua(s) licença(s) para operar (p. ex.: perda do direito de processar informações pessoais devido a contravenção de regras de privacidade).

Foco em Colaboração com a Segurança da Informação

Usar os serviços em nuvem não garante automaticamente a segurança da informação.[5] As funções e as responsabilidades entre os provedores de serviço de nuvem (cloud service providers - CSPs) e o cliente devem ser bem definidas para os processos e controles de segurança cibernética. Responsabilidade compartilhada associada aos tipos de serviços em nuvem que estão sendo utilizados devem também ser considerados.[6]

Fontes comuns de risco associadas à colaboração inadequada ou ineficiente da segurança da informação incluem:

- A organização não administra eficientemente o risco do CSP, resultando em violação das políticas e dos procedimentos de segurança da informação da organização.
- A entidade que está utilizando os serviços em nuvem não considera e implementa suficientemente os controles complementares de cliente-usuário, o que pode resultar em lacunas no ambiente de controle e elevar a exposição da entidade ao risco.
- Os mecanismos de monitoramento não estão instalados para garantir que o CSP continue implementando as medidas de segurança da informação acordadas e contratadas.

QUER SABER MAIS?

- Leia *Continuous Oversight in the Cloud. https://www.isaca.org/continuous-oversight*
- Saiba mais, discuta e colabore com a governança em nos fóruns Online da ISACA. *https://engage.isaca.org/onlineforums*

As organizações devem adotar e implementar uma estrutura de governança de dados e processos de gestão de dados apropriados, tais como gestão de qualidade de dados, cobrindo os dados em nuvem.

Proteja a Privacidade de Informações Pessoais

A administração deve realizar uma avaliação cuidadosa do risco de privacidade antes de adotar qualquer serviço em nuvem.[7] CSPs devem ser avaliados de acordo com as políticas organizacionais de privacidade e mecanismos de monitoramento devem ser instalados para garantir conformidade contínua com os requisitos de privacidade. Além disso, processos adequados de gestão de incidentes devem ser estabelecidos para garantir que existam proteções para lidar com incidentes quando ocorrerem.

Possíveis riscos associados a falha de proteção de informações pessoais incluem:

- Potencial exposição de informação privada ou confidencial devido a violação de segurança
- Potencial não conformidade com regras e normas que podem ter impactos adversos, como sanções, prejuízos financeiros, ou danos a reputação para a organização

Garantir a Gonvernaça de Dados para Permitir Digitalização

A governança de dados é um facilitador essencial para as organizações conduzidas por dados e digitalização. As organizações podem aproveitar múltiplos serviços relacionados a dados em nuvem para análise preditiva, vantagem competitiva e benefícios comerciais. A administração deve estabelecer controles para garantir a integridade, precisão, confidencialidade, disponibilidade e totalidade da informação armazenada e processada na nuvem.

A administração inconsistente de integridade e qualidade de dados é um risco fundamental associado a governança de dados. As organizações devem adotar e implementar uma estrutura de governança de dados e processos de gestão de dados apropriados, tais como gestão de qualidade de dados, cobrindo os dados em nuvem.

Monitorar a Administração Financeira

Para prevenir o crescimento descontrolado e a escalada de gastos em nuvem, é essencial priorizar o monitoramento centralizado e o relatório de custos da nuvem, além da avaliação, otimização e previsão contínua de gastos da nuvem. A administração deve estabelecer os processos e controles tais como etiquetagem, relatórios e alocação de custos. Etiquetagem é importante para a correta alocação de custos dentro da organização à medida que o uso da nuvem cresce.

Fontes comuns de risco associadas à gestão de risco financeiro incluem:

- A ausência de controle financeiro a respeito dos custos da nuvem pode resultar em organizações não otimizando a utilização da nuvem ou entrega do valor esperado.
- Uma abordagem isolada de gestão de custos de computação em nuvem pode não ser ideal. Isso pode retardar ou interromper a adoção de nuvem, prejudicar a inovação ou reduzir a qualidade da oferta de serviço.
- A expansão da nuvem (crescimento descontrolado) ou a subutilização dos recurso em nuvem pode resultar em maiores gastos associados.

Considere o Direito de Auditar Garantia de Terceiros

Garantia continua sendo um desafio, especialmente nos casos de CSPs relativamente pequenos cujos processos e estruturas de governança não são formalizados. CSPs menores podem não ser capazes de pagar provedores de garantia independentes para emitir relatórios da organização de serviço. Eles podem também ser incapazes de lidar com múltiplas solicitações para auditar ou realizar autoavaliações de risco de vários graus de detalhamento. As organizações devem considerar incluir o direito de auditar e o envio de relatórios de garantia de terceiros em contratos com CSP. Isso é especialmente importante em relação aos fornecedores de Software como um serviço (Software-as-a-Service - SaaS) porque SaaS geralmente cria uma caixa preta em que o ambiente de controle e risco do fornecedor não é visível para o cliente.

Infelizmente, falha em monitorar os CSPs por mitigação e controles de risco é uma fonte comum de risco emprerial. Isso pode resultar em risco desconhecido e não administrado, levando a interrupção das operações de negócios diárias.

Selecione Cuidadosamente e Contrate CSPs

A diligência prévia, seleção e contratação de fornecedores são importantes para garantir que as organizações protejam seus direitos legais. Os contratos de CSP são geralmente documentos padrão de alto nível que são unilaterais, oferecendo pouco recurso para os clientes. Atenção especial deve ser dada à propriedade,

particularmente no caso de um contrato de SaaS, em que usuários podem investir volumes de recursos significativos, particularizando a solução em nuvem para os seus propósitos.[8]

Fatores de risco comuns incluem:

- As organizações podem não ser capazes de impor direitos legais na eventualidade de interrupção de serviços e litígios sobre questões como propriedade ou movimentação de CSPs. Isso pode levar a prejuízos financeiros ou longas batalhas jurídicas para as organizações.
- As organizações podem não entender os fatores de risco associados aos CSPs e suas capacidades de endereçá-los, dessa forma podem não conseguindo mitigá-los e monitorá-los eficientemente.

Atinja Gestão e Governança Eficazes de CSP

Os acordos de governança e a gestão de CSPs, seja utilizada informação como serviço (Information as a Service - IaaS), plataforma como serviço (Platform as a Service - PaaS) ou SaaS, são partes importantes do combate ao efeito caixa preta típico dos provedores de serviço. As organizações devem sempre reter a responsabilidade pela governança.[9] Elas não podem delegar governança para CSPs. As organizações devem administrar proativamente os provedores de nuvem e ter fortes estruturas de governança interna que se alinhem às estratégias de negócios, especialmente com planos de transformação digital ou roteiros abrangentes.

Se as organizações não puderem governar os fornecedores de nuvem eficientemente, o resultado pode ser falta de controle e gestão ineficiente de CSPs.

Atenção ao Acordo de Nível de Serviço

Organizações devem monitorar e gerenciar ativamente os níveis de serviço do CSP. Relatórios e reuniões periódicas de nível de serviço são essenciais para garantir que os provedores de serviço atendam os requisitos da organização. Esse não é um novo conceito para a maioria das equipes de TI; no entanto, as organizações devem considerar aproveitar as ferramentas modernas e específicas da nuvem para monitorar os níveis de serviço acordados. Sem essas ferramentas, as organizações correm o risco de que os serviços do CSP deixem de atender aos requisitos de negócios ou aos níveis de serviço definidos.

Garantir Portabilidade e Interoperabilidade

As organizações devem considerar a migração potencial a partir do CSP quando o provedor é apontado para garantir que o bloqueio do fornecedor não ocorre em razão de falta de portabilidade. As organizações devem incluir assistência a migração nos contratos de fornecedor e pensar em classificar os serviços em nuvem que consomem para determinar a velocidade de portabilidade necessária. De outra forma, podem enfrentar a falta de interoperabilidade entre a solução em nuvem e os sistemas conectados, criando ilhas de informação e problemas de integração.

Priorizar o Gerenciamento de Risco Empresarial

As organizações devem integrar o risco da nuvem aos processos de gestão de risco empresarial e informar sobre risco periodicamente. A administração deve definir claramente as funções e responsabilidades em relação à gestão de risco na nuvem.[10]

Se uma organização deixar de tratar a nuvem como risco para a toda a organização, a adoção da nuvem pode falhar e apresentar mais problemas do que progresso para a organização.

As organizações devem incluir assistência a migração nos contratos de fornecedor e pensar em classificar os serviços em nuvem que consomem para determinar a velocidade de portabilidade necessária.

Considerar a Continuidade do CSP

As organizações devem arquitetar a recuperação de desastres e a continuidade na nuvem como parte das suas soluções em nuvem e não devem presumir que a recuperação automática ocorrerá. Se eles falharem em fazer isso, é possível que os serviços do CSP fiquem indisponíveis.[11]

Conclusão

Governança da nuvem é emergente. A utilização da nuvem altera os processos padrão de governança de TI local (p. ex.: SaaS e IaaS influenciam a natureza dos processos de gestão e governança do fornecedor). A nuvem possui impacto fundamental nos serviços de TI, que altera o perfil de risco. Os processos de governança de TI existentes projetados para serviços de TI locais não estão alinhados com os desafios e o risco apresentado pela adoção e a migração para a nuvem. A estrutura de governança

em nuvem proposta oferece um modelo integrado dos aspectos mais importantes da governança em nuvem e contribui para uma governança em nuvem eficiente.

Notas finais

1 FutureCIO, "Half of IT Budgets Will Go to the Cloud," 16 February 2022, *https://futurecio.tech/half-of-it-budgets-will-go-to-the-cloud*

2 Wood, T.; D. Bartoletti; *Adapt Your Governance Framework for Cloud*, Forrester, USA, 2018

3 ITIL and Office of Government Commerce (OGC), *Service Operation*, p33–78, The Stationery Office (TSO), UK, 2007, *http://www.teraits.com/pitagoras/marcio/itil/OGC_ITIL_v3_5_Service_Operation.pdf*

4 Heyink, M.; *An Introduction to Cloud Computing: Legal Implications for South African Firms*, Version 2, Law Society of South Africa, South Africa, 2014, *https://www.lssa.org.za/wp-content/uploads/2019/12/LSSA-Guidelines_Introduction-to-Cloud-Computing-Legal-Implications-2012.pdf*

5 Neely, M.; "Securing an Evolving Cloud Environment," *ISACA® Journal*, vol. 3, 2014, *https://www.isaca.org/archives*

6 Vohradsky, D.; "Cloud Risk—10 Principles and a Framework for Assessment," *ISACA Journal*, vol. 5, 2012, *https://www.isaca.org/archives*

7 Woo, T.; D. Bartoletti; *Adapt Your Governance Framework for Cloud*, Forrester, USA, 2018

8 *Op cit* Heyink

9 Kirkpatrick, J.; "Governance in the Cloud," *ISACA Journal*, vol. 5, 2011, *https://www.isaca.org/archives*

10 Raval, V.; "Risk Landscape of Cloud Computing," *ISACA Journal*, vol. 1, 2010, *https://www.isaca.org/archives*

11 Shacklett, M.; "Rethinking Disaster Recovery for the Cloud," *CIO Magazine*, 6 December 2018