Migração da Infraestrutura de TI On-Premise para Multicloud: Desafios no Contexto da Administração Pública Federal no Brasil e da Indústria Farmacêutica

Davi de França Carneiro[0000-0002-7318-6569], Nelson Gutemberg Rocha da Silva[0009-0000-4876-7129], Mauricio Barros Ottoni[0009-0006-3710-9239], Fabiano Alves da Silva[0009-0005-8189-0475]

Empresa Brasileira de Hemoderivados e Biotecnologia, Recife, PE, 51021-410, Brasil
{davi.carneiro, nelson.silva, mauricio.ottoni, fabiano.silva}@hemobras.gov.br

Resumo. Em muitas organizações, a infraestrutura de TI é um ponto crítico e está sujeita a monitoramento contínuo no processo de gestão estratégica de riscos. Ela deve ser capaz de fornecer suporte a serviços e sistemas de forma segura, com alto desempenho e baixa latência. Assim, as abordagens tradicionais de infraestrutura de TI, conhecidas como on-premise, precisam ser otimizadas, aliadas ao suporte dos serviços em nuvem. No contexto da administração pública federal no Brasil e da indústria farmacêutica, essa combinação é ainda mais desafiadora, pois envolve orientações de órgãos reguladores – como a Agência Nacional de Vigilância Sanitária (ANVISA), que se preocupa em manter as Boas Práticas de Fabricação dos produtos farmacêuticos (BPF) – e regulamentações recentes ou de certo modo incipientes do Governo Federal Brasileiro, quando se trata do uso de serviços em nuvem. Este trabalho, portanto, propõe uma estratégia de migração da infraestrutura de TI on-premise para multicloud, passando pelas fases da Engenharia de Requisitos (elicitação, análise e negociação, documentação, verificação e validação), a fim de gerenciar os principais aspectos jurídicos, financeiros e técnicos, incluindo equipamentos de rede, servidores, aplicações e serviços de suporte na indústria pública farmacêutica.

Palavras-chave: Governo Federal Brasileiro, Indústria Farmacêutica, Infraestrutura de TI, Migração para Nuvem.

1 Introdução

A crescente demanda das organizações por armazenamento e compartilhamento de dados e recursos tecnológicos, além da expansão de atividades remotas, com funcionários localizados em qualquer parte do mundo, provocam a necessidade de ações robustas que precisam ser implementadas pela equipe de Tecnologia da Informação (TI) [1].

Modelos tradicionais de infraestrutura de TI, conhecidos como on-premise, utilizam datacenters localizados dentro das dependências da empresa. Esse cenário, apesar de parecer seguro, possui gerenciamento e manutenção custosos, o que revela a carência de mão de obra disponível para realizar instalações, configurações e frequentes

Proceedings of the 27th Workshop on Requirements Engineering (WER24), August 07-09, 2024, Buenos Aires, Argentina.
DOI: 10.29327/1407529.27-31

manutenções preventivas ou emergenciais. O uso da nuvem traz uma nova realidade, com implantações simples, garantindo elasticidade de recursos, segurança e backups que podem ser recuperados em situações adversas [2]. Será que a nuvem é a solução para todos os problemas que envolvem a infraestrutura de TI? À primeira vista, parece a solução dos sonhos. No entanto, para uma organização originalmente constituída com um modelo on-premise e, particularmente no universo da administração pública federal no Brasil e da indústria farmacêutica, os desafios podem ser ainda maiores.

As demais seções deste artigo estão organizadas da seguinte forma: seção 2 descreve o referencial teórico; seção 3 detalha o modelo de gestão de infraestrutura de TI on-premise; seção 4 destaca o modelo de gestão de infraestrutura de TI em nuvem; seção 5 descreve as legislações aplicáveis; seção 6 mostra o processo de validação farmacêutica para soluções em nuvem; seção 7 traz a nossa principal contribuição, construindo uma estratégia para gerir os requisitos de migração da infraestrutura on-premise para nuvem; por fim, a seção 8 descreve as conclusões deste trabalho.

2 Referencial Teórico

A administração pública federal no Brasil dispõe de legislações consideradas recentes e ainda pouco implementadas na prática para viabilizar a imersão dos órgãos públicos federais em um modelo de contratação de softwares e serviços em nuvem, a exemplo da Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 [3]. Requisitos mínimos de segurança também foram definidos através da Instrução Normativa nº 05, de 30 de agosto de 2021, para proteção dos dados e documentos com grau de sigilo [4].

As indústrias farmacêuticas no Brasil são regidas pela ANVISA (Agência Nacional de Vigilância Sanitária), que instituiu a RDC nº 658, de 30 de março de 2022, descrevendo as diretrizes de boas práticas de fabricação (BPF). Isso inclui os sistemas computadorizados, que precisam passar por etapas bem conhecidas de validação: Qualificação de Projeto (QP), Qualificação de Instalação (QI), Qualificação de Operação (QO) e Qualificação de Desempenho (QD) [5]. Na nuvem, no entanto, esses procedimentos são desafiadores, pois a solução está sob controle dos provedores. Uma estratégia de migração, portanto, deve ser capaz de lidar com requisitos legais, técnicos e financeiros para implementar essa mudança, que não será apenas estrutural, mas cultural.

3 Gestão de Infraestrutura de TI On-Premise

Na gestão de infraestrutura de TI on-premise, os dados, sistemas e hardwares são armazenados e gerenciados em um datacenter dedicado dentro da organização. A seguir, destacam-se os principais benefícios e desafios desse tipo de gestão tradicional [6, 7].

Benefícios:

- Liberdade e controle sobre o hardware, software e dados, podendo a organização executar upgrades, modificações e configurações;

- Maior conectividade e disponibilidade dos recursos de TI, sem interferências externas. Servidores acessíveis, mesmo com uma queda no link de internet;
- Maior conformidade com a política de segurança e privacidade de dados, permitindo maior controle sobre os dados sigilosos da organização;
- Custos previsíveis ao longo do tempo, apesar do elevado valor de investimento inicial, permitindo que a empresa planeje adequadamente o orçamento de TI;
- Alta performance dos recursos, uma vez que, estando interconectados localmente, os administradores têm controle direto sobre hardwares e softwares.

Desafios:

- A manutenção do hardware envolve maior planejamento para atualizar equipamentos obsoletos e realizar manutenções preventivas frequentes;
- A segurança digital em rede local exige um firewall robusto, sistemas de detecção de intrusões e políticas de acesso físico e lógico aos recursos de TI;
- As ações de backup e recuperação dos dados dependem de sistemas eficientes e planos eficazes de recuperação de desastres, em caso de falhas;
- A escalabilidade também se torna um entrave, pois a infraestrutura deve acompanhar o crescimento da empresa e suportar maiores demandas por recursos.

Ao aderir à abordagem de infraestrutura on-premise, as organizações deverão avaliar benefícios e desafios, além de custos e preferências de gerenciamento de dados.

4 Gestão de Infraestrutura de TI em Ambientes Multicloud

Diferentemente da estrutura apresentada na seção 3, a multicloud permite que as organizações utilizem duas ou mais plataformas de nuvem, dependendo, em geral, de uma nuvem pública. Há uma combinação de serviços e sistemas contratados, de modo que é possível aproveitar as vantagens individuais de cada fornecedor. A seguir, destacam-se os principais benefícios e desafios desse tipo de gestão [8, 9].

Benefícios:

- Flexibilidade. É possível escolher serviços de provedores distintos, conforme critérios de desempenho, localização, preço, segurança e conformidade;
- Mudança rápida de tecnologias. A organização pode adotar rapidamente as melhores tecnologias de qualquer fornecedor;
- Redundância. Usando várias nuvens, a organização reduz sua vulnerabilidade a interrupções e o tempo de inatividade que não foi planejado;
- Conformidade e localização. Políticas e regulamentos podem exigir que os dados da organização sejam armazenados em locais específicos. Assim, é possível escolher provedores de nuvem que atendam a essas necessidades;

- Escalabilidade e performance. Os recursos podem ser ampliados, de acordo com a carga de trabalho da empresa.

Desafios:

- Gestão complexa. Gerenciar vários provedores de nuvem exige habilidades e ferramentas de monitoramento, segurança e otimização de recursos;
- Segurança. É importante garantir junto ao provedor que os recursos de nuvem estejam protegidos de ataques e de violações de segurança;
- Integração. Integrar sistemas e serviços entre diferentes provedores de nuvem pode ser complexo, visto que as organizações devem garantir que suas cargas de trabalho se comuniquem efetivamente e troquem dados de maneira fluida;
- Custo. A multicloud pode ajudar na otimização de custos, mas também pode levar a gastos ocultos, como taxas de transferência de dados entre provedores de nuvem, e aumentar a complexidade na previsão de gastos de infraestrutura.

Utilizar a infraestrutura multicloud torna-se um caminho rumo à melhoria operacional e impulsiona, nas organizações, a inovação digital e a mitigação de riscos.

5 Legislações Aplicáveis na Administração Pública Federal Brasileira para Soluções em Nuvem

A Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, estabelece o modelo de contratação de software e de serviços de computação em nuvem [3], e a Instrução Normativa (IN) nº 05, de 30 de agosto de 2021, dispõe sobre os requisitos mínimos de segurança da informação para utilização dessas soluções [4].

A portaria, publicada pela Secretaria de Governo Digital, é uma medida administrativa que estabelece normas orientadas pelos principais órgãos de controle e considera as boas práticas, a legislação e a jurisprudência relacionada às contratações de software e de serviços em nuvem [3]. Essa portaria apresenta 27 tópicos, dentre os quais destacam-se: i) detalhamento dos termos e definições que deverão ser utilizados para o processo de contratação; ii) delimitação do escopo e balizadores dos modelos de contratações; iii) orientações sobre as diretrizes estratégicas para o uso de software em computação em nuvem; iv) definição do objeto que deverá ser utilizado para as contratações, considerando o tipo de software pretendido; v) definição do modelo de licenciamento; vi) modalidade de remuneração; vii) vigência e a identificação dos tipos de serviços agregados; viii) privacidade e segurança da informação; ix) definição dos valores da contratação; x) análise da amostra do objeto; xi) forma de quantificação e estimativa prévia do volume de serviços; xii) utilização de catálogos de soluções de TI, com condições padronizadas na contratação de software; xiii) verificação da qualidade dos serviços; xiv) vigência dos contratos; xv) gerenciamento dos riscos e xvi) governança da contratação dos serviços de computação em nuvem.

Migrar para a nuvem requer um rigor no tratamento da segurança dos dados e dos documentos que possuam grau de sigilo. A IN nº 05, publicada pelo Gabinete de

Segurança Institucional (GSI) do governo brasileiro, promove essa segurança, preservando os interesses nacionais, a segurança e a integridade do Estado [4]. A IN possui 8 capítulos e 28 artigos que envolvem: i) classificação de informação; ii) definição de procedimentos de classificação de informação, considerando os graus de sigilo apresentados na tabela 1; iii) medidas para garantir a proteção e o controle de acesso às informações classificadas; iv) regulamentação da transmissão e o transporte de informações classificadas e v) diretrizes para a gestão de documentos classificados.

Essas legislações exigem que o datacenter esteja localizado em território brasileiro ou com uma cópia armazenada no Brasil, por motivos de segurança e de soberania.

Tabela 1. Classificação da informação e grau de sigilo.

Ostensiva	Transparência ativa.
	Transparência passiva.
Sigilosa classificada em grau de sigilo	Reservada – Prazo máximo de restrição de acesso de 5 anos.
	Secreta – Prazo máximo de restrição de acesso de 15 anos.
	Ultrassecreta – Prazo de restrição de acesso de 25 anos, prorrogável por uma única vez, e por período não superior a 25 anos, limitado ao máximo de 50 anos.
Sigilosa protegida por legislação específica	Sigilo decorrente de direitos de personalidade.
	Sigilo de processos e procedimentos.
	Informação de natureza patrimonial.
Pessoal	Prazo máximo de restrição de acesso de 100 anos, independente de classificação de sigilo e quando se referir à intimidade, vida privada, honra e imagem das pessoas.

Um catálogo de serviços foi disponibilizado pela administração central do governo brasileiro para as contratações feitas pelos órgãos, conforme detalhado em [10] e [11].

6 Validação Farmacêutica em Ambientes Multicloud para Atendimento às Regulamentações da ANVISA

Na indústria farmacêutica, para softwares contendo requisitos de impacto em boas práticas de fabricação (BPF), é necessário que haja um processo de validação, a fim de garantir a segurança, qualidade e eficácia dos medicamentos finais. Essa validação passa por quatro etapas: Qualificação de Projeto (QP); Qualificação de Instalação (QI); Qualificação de Operação (QO); Qualificação de Desempenho (QD) [5]. Software, hardware e componentes de rede precisam ser validados para que a unidade opere em sintonia com BPF [12]. Com isso, a validação de um sistema em ambiente multicloud apresenta desafios únicos. A necessidade de validar o hardware, que pode estar localizado em diferentes partes do mundo, destaca-se como o principal desses desafios.

Quando se trata de empresa pública federal, essa restrição se limita ao território nacional, conforme orientação da IN nº 05, detalhada na seção 5 deste estudo [4].

No entanto, para a ANVISA, não há restrições quanto ao uso dedicado do hardware ao software, permitindo assim que sistemas com impacto em BPF sejam implementados em redes públicas ou privadas. Isso não simplifica o processo de validação, já que, durante a QI, uma etapa crucial da validação, é necessário verificar se o sistema foi instalado conforme as especificações pré-aprovadas. No caso de componentes-padrão de hardware, essa etapa pode ser realizada com base nas especificações do hardware da nuvem [13]. Em um ambiente multicloud, onde o software pode estar distribuído entre vários servidores, cada um desses servidores precisa passar pelo processo de QI.

Em um ambiente on-premise, a QI poderá ser realizada presencialmente e evidenciada por fotos e documentos emitidos pelo fornecedor do hardware. Já no ambiente multicloud, a única evidência possível são as especificações do hardware, uma vez que não se tem o acesso físico aos ambientes dos servidores. Assim, é fundamental que os hardwares da multicloud tenham sua especificação detalhada para a conclusão da QI. Conforme [13]: "As empresas reguladas devem manter um inventário de seus sistemas computadorizados." Por isso, todos os componentes precisam ser listados e validados.

Em resumo, a validação de sistemas na multicloud, de acordo com a ANVISA, requer uma abordagem sistemática, documentada e orientada ao cumprimento das regulamentações aplicáveis e garantia da qualidade e segurança dos produtos farmacêuticos.

7 Estratégia de Gestão de Requisitos para Migração da Infraestrutura de TI On-Premise para Multicloud

Segundo um estudo da Gartner, realizado em 2021, é previsto que até 2025, cerca de 85% das organizações irão utilizar computação em nuvem [14].

Neste artigo, tendo-se em mente as legislações aplicáveis mostradas na seção 5, é explorada uma estratégia de gestão de requisitos para facilitar a migração da infraestrutura de TI on-premise para multicloud, conforme apresentada na figura 1. Esse processo é realizado em quatro etapas: i) avaliação da infraestrutura atual; ii) revisão dos requisitos de hardware; iii) gestão e monitoramento dos requisitos durante a migração do ambiente e iv) plano de testes. A construção dessa proposta tomou como base o estudo feito por [15], contendo um plano de migração para a nuvem do Exército Brasileiro.

Alterações nos requisitos de hardware podem ter um impacto significativo no software. Assim, eles precisam ser cuidadosamente identificados e detalhados [16]. Nesse sentido, deve-se avaliar a estrutura on-premise atual antes de realizar a migração.

Quando se trata de um sistema mantido por uma indústria farmacêutica, esse sistema encontra-se inicialmente em estado validado, ou seja, passou por todas as etapas de validação da ANVISA, incluindo os requisitos de software e hardware, os quais foram elicitados, analisados e negociados, documentados, verificados e validados. Logo, a avaliação da infraestrutura atual será apoiada pela documentação levantada durante a QI do software. Essa documentação garante que o estado validado do ambiente on-premise não foi alterado, mantendo as configurações aprovadas do hardware.

Após a análise do estado validado do software, de imediato já se têm os requisitos de software e hardware, uma vez que estes foram mapeados durante o processo de validação do software. Esses requisitos, porém, precisarão ser revisados, diante da

necessidade de mudança na infraestrutura, principalmente os requisitos não funcionais ligados à infraestrutura e aos servidores.

Após esse refinamento e atualização de requisitos, a gestão e monitoramento da migração é fundamental para garantir segurança e transparência para o usuário final. Inicialmente, deve-se garantir que todos os hardwares do ambiente multicloud, que irão suportar o software a ser migrado, sejam mapeados e mantenham todos os mesmos requisitos elencados. Com hardware de origem e destino compatíveis, haverá o mínimo de impacto no sistema que já se encontra validado, com alterações mínimas no código, caso seja necessária alguma adaptação no endereço de apontamento dos servidores, ou em uma parametrização pontual do software para o ambiente multicloud [17].

Durante o processo de migração dos dados, considerando os mesmos requisitos elencados durante a validação inicial do sistema, o banco de dados é o requisito fundamental a ser mantido para uma segura migração dos dados. Com o banco de dados compatível, um exportação e importação dos dados através do mesmo SGBD garante que os dados sejam transferidos para a nuvem sem que haja um comprometimento de integridade.

Como última etapa, o plano de testes preconizado no Guia de Validação da ANVISA será seguido durante a QO e a QD, momento em que os testes funcionais garantem o sucesso da migração do sistema entre os ambientes.

Fig. 1. Etapas da estratégia de migração.

8 Conclusão

A administração pública federal brasileira estabelece normas, tais como a Portaria SGD/MGI nº 5.950 e a IN nº 05 do GSI, para contratações seguras de sistemas em nuvem, embora, na prática, a implementação dessas orientações ainda esteja um pouco incipiente, já que muitos órgãos públicos são muito dependentes do método on-premise.

As indústrias farmacêuticas, por sua vez, precisam seguir um processo de validação específico, com qualificações para garantir o atendimento às regulamentações da ANVISA e manter a conformidade com as boas práticas de fabricação (BPF). Nos ambientes multicloud, o maior desafio ocorre no momento da QI, já que a infraestrutura pertence a terceiros, de maneira distribuída e, muitas vezes, desconhecida pelo cliente.

Portanto, para realizar a migração de uma infraestrutura de TI on-premise para multicloud, foi proposta uma estratégia dividida em quatro etapas: i) avaliação da

infraestrutura atual; ii) revisão de requisitos de hardware; iii) gestão e monitoramento dos requisitos durante a migração e iv) plano de testes. Essas etapas garantem a manutenção do estado validado do sistema computadorizado, seguindo as diretrizes da ANVISA. Como trabalho futuro, espera-se a avaliação dos resultados que serão obtidos com a aplicação prática da estratégia de migração apresentada neste artigo.

Referências

1. Tanenbaum, A.S.: Computer Networks. 4ª ed. Editora Campus, Amsterdam, Holanda (2003)
2. On-premises vs cloud: quais são as maiores diferenças?, https://codebit.com.br/blog/on-premises-vs-cloud-quais-sao-as-maiores-diferencas, último acesso em 25/03/2024
3. Portaria SGD/MGI n.º 5.950, de 26 de outubro de 2023, https://www.gov.br/governodigital/pt-br/contratacoes/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023, último acesso em 25/03/2024
4. Instrução Normativa n.º 05, de 30 de agosto de 2021, https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684, último acesso em 25/03/2024
5. Carneiro, D.F., Da Silva, N.G.R., Ottoni, M.B., Gomes, I.I.: Um Modelo Híbrido de Gestão de Requisitos para Desenvolvimento e Aquisição de Softwares na Indústria Farmacêutica. 26º Workshop de Engenharia de Requisitos (WER23), Porto Alegre, RS, Brasil (2023)
6. APIPASS, https://apipass.com.br/on-premise/, último acesso em 25/03/2024
7. O que é on-premise, quais são as suas características e diferenças do sistema cloud?, https://rockcontent.com/br/blog/o-que-e-on-premise/, último acesso em 25/03/2024
8. Multicloud management: challenges for technology, people, process, https://www.networkworld.com/article/969187/multcloud-management-challenges-for-technology-people-processes.html, último acesso em 25/03/2024
9. Multicloud: benefícios e desafios de adotar essa estratégia, https://www.supero.com.br/blog/multicloud-vantagens-e-desafios-de-adotar-essa-estrategia/, último acesso em 25/03/2024
10. Pregão Eletrônico nº 29/2018, https://www.gov.br/gestao/pt-br/acesso-a-informacao/licitacoes-e-contratos/licitacoes-e-contratos/licitacoes/pregao/2018/pregao-eletronico-no-29-2018, último acesso em 25/03/2024
11. Pregão eletrônico SRP nº 18/2020, https://www.gov.br/gestao/pt-br/assuntos/central-de-compras/transparencia/licitacoes/2020/pregao-eletronico-srp-no18-2020-central-de-compras, último acesso em 25/03/2024
12. Fontes, P.R.F.S., et al.: Validação de sistemas computadorizados como metodologia da garantia da qualidade: caso em uma indústria farmacêutica (2018)
13. ANVISA: Guia para Validação de Sistemas Computadorizados. Guia n.º 33/2020. Versão 1
14. Uso da computação em nuvem está em constante crescimento, https://valor.globo.com/patrocinado/dino/noticia/2023/10/03/uso-da-computacao-em-nuvem-esta-em-constante-crescimento.ghtml, último acesso em 25/03/2024
15. Morais, N.S.: Proposta de modelo de migração de sistemas de ambiente tradicional para nuvem privada para o Polo de Tecnologia da Informação do Exército brasileiro (2015)
16. Cysneiros, L.M., Leite, J.C.S.P.: Requisitos não funcionais: da elicitação ao modelo conceitual. PhD Tese, PUC-RJ (2001)
17. Sousa, A., et al.: Elicitação e Especificação de Requisitos em Sistemas Embarcados: Uma Revisão Sistemática. CIbSE, p. 606 (2015)