RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 23/10/2026 | aceito: 28/10/2026 | publicação: 02/11/2026

Operações de nuvem e DevOps com prioridade à governança para instituições orientadas por missão: um modelo prático para confiabilidade, auditabilidade e inclusão digital

Governance-first cloud and DevOps operations for mission-driven institutions: a practical model for reliability, auditability and digital inclusion

Operaciones de nube y DevOps con prioridad en la gobernanza para instituciones orientadas por misión: un modelo práctico para la confiabilidad, la auditabilidad y la inclusión digital

Obede Bessa Rocha da Silva
Arquiteto Independente de Soluções em Nuvem e Pesquisador em DevOps

RESUMO
Instituições orientadas por missão dependem cada vez mais de práticas de computação em nuvem e DevOps; muitas delas, porém, operam com equipes reduzidas, processos legados e elevadas expectativas de continuidade, prestação de contas e confiança pública. Este artigo propõe um modelo operacional com prioridade à governança para ambientes institucionais de nuvem e DevOps. O modelo organiza as práticas em torno de cinco capacidades que se reforçam mutuamente: linha de base de arquitetura, padronização operacional, segurança e auditabilidade, observabilidade e resposta a incidentes, e capacitação da força de trabalho. Em vez de tratar a governança como uma camada documental aplicada após a implementação, o artigo a posiciona como um controle de engenharia que pode ser incorporado a arquiteturas de referência, guias operacionais (runbooks), planos de resposta (playbooks), rotinas de acesso e ciclos de melhoria contínua. O artigo destina-se a líderes e profissionais de TI de organizações do setor público, educacionais, sem fins lucrativos e de orientação comunitária que precisam modernizar a infraestrutura digital sem perder rastreabilidade nem disciplina operacional. O texto sintetiza padrões da prática profissional em arquitetura de nuvem, DevOps, segurança e engenharia de confiabilidade em um modelo aplicável, adaptável a instituições com diferentes níveis de maturidade.
Palavras-chave: governança de nuvem; DevOps; infraestrutura digital; tecnologia institucional; engenharia de confiabilidade; auditabilidade; resposta a incidentes; inclusão digital.

1 INTRODUÇÃO

A computação em nuvem e o DevOps transformaram os custos e a velocidade da infraestrutura digital. Nas organizações comerciais de tecnologia, a narrativa predominante costuma enfatizar a rapidez: ciclos de lançamento mais curtos, plataformas elásticas, automação e entrega contínua. Instituições orientadas por missão enfrentam as mesmas pressões técnicas, mas seu contexto operacional é diferente. Órgãos públicos, organizações educacionais, instituições sociais, igrejas, programas sem fins lucrativos e iniciativas comunitárias frequentemente precisam de infraestrutura moderna e, ao mesmo tempo, devem preservar a continuidade, a prestação de contas e controles compreensíveis. Mesmo sem grandes equipes especializadas em plataformas, seus sistemas sustentam serviços dos quais as pessoas dependem.

Nesses ambientes, a questão central não é simplesmente como migrar cargas de trabalho para plataformas de nuvem ou automatizar implantações. A questão mais difícil é como tornar governáveis as práticas de nuvem e DevOps: como garantir que as configurações sejam reproduzíveis, os

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 23/10/2026 | aceito: 28/10/2026 | publicação: 02/11/2026

incidentes possam ser diagnosticados, as decisões de acesso sejam auditáveis e o conhecimento operacional não permaneça restrito à memória de um único líder técnico. Governança, nesse sentido, não é burocracia. É o conjunto de práticas de engenharia e gestão que permite à instituição confiar em sua infraestrutura digital.

Este artigo apresenta um modelo com prioridade à governança para operações institucionais de nuvem e DevOps. O modelo foi concebido para organizações que precisam de uma ponte prática entre requisitos de governança de alto nível e o trabalho diário de engenharia. Não pretende substituir normas consolidadas nem arquiteturas de fornecedores. Em vez disso, traduz esses referenciais em um modelo operacional centrado em confiabilidade, segurança, auditabilidade e inclusão digital.

2 POR QUE A GOVERNANÇA DEVE INTEGRAR A PRÁTICA DE ENGENHARIA

A governança tradicional de TI frequentemente se manifesta em documentos de políticas, pontos formais de aprovação e revisões periódicas. Esses instrumentos continuam úteis, mas são insuficientes em ambientes de nuvem e DevOps, nos quais a infraestrutura pode ser alterada rapidamente, o acesso pode ser delegado entre serviços e desvios de configuração podem ocorrer sem visibilidade. Uma governança restrita a documentos tende a ficar defasada em relação ao sistema que deveria controlar.

Um modelo operacional com prioridade à governança incorpora a governança ao fluxo de trabalho de engenharia. Ele exige que as equipes definam arquiteturas de referência antes de implantações ad hoc, codifiquem padrões reproduzíveis de configuração, documentem rotinas de incidentes antes das emergências e integrem registros, permissões, rotinas de backup e históricos de mudanças à superfície normal de projeto. Essa orientação acompanha o movimento mais amplo em direção à segurança desde a concepção, à engenharia de confiabilidade e à conformidade contínua.

Essa necessidade é especialmente visível em instituições com missões sociais ou públicas. Uma organização de pequeno porte pode não descrever seu trabalho como engenharia de plataforma, mas ainda precisa de gestão confiável de identidades, disciplina de backup, revisão de acessos, inventário de ativos, continuidade de serviços e capacitação técnica. Quando essas práticas estão ausentes, a modernização pode aumentar o risco: a instituição adquire novas ferramentas, mas perde clareza operacional.

3 O MODELO COM PRIORIDADE À GOVERNANÇA

O modelo proposto reúne cinco capacidades. Cada uma pode ser implementada de forma incremental,

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 23/10/2026 | aceito: 28/10/2026 | publicação: 02/11/2026

mas os resultados mais robustos surgem quando elas se reforçam mutuamente. A linha de base de arquitetura define o modelo operacional desejado. A padronização operacional transforma esse modelo em rotinas reproduzíveis. Segurança e auditabilidade tornam as decisões rastreáveis. Observabilidade e resposta a incidentes garantem que falhas possam ser detectadas e gerenciadas. A capacitação da força de trabalho torna o modelo sustentável ao converter conhecimento técnico em capacidade institucional compartilhada.

Tabela 1 – Capacidades do modelo com prioridade à governança para operações institucionais de nuvem e DevOps

Capacidade	Controles Práticos	Resultado Institucional
Linha de base de arquitetura	Arquiteturas de referência, classificação de ambientes, objetivos de backup e recuperação, modelo de identidade e responsabilidade pelos serviços.	Um mapa compartilhado da infraestrutura digital e da postura de risco da instituição.
Padronização operacional	Guias operacionais, planos de resposta, padrões de configuração, rotinas de mudança, inventário de ativos e acompanhamento de fornecedores e acordos de nível de serviço (SLAs).	Menor variabilidade, integração mais rápida e menor dependência de conhecimento não documentado.
Segurança e auditabilidade	Acesso com privilégio mínimo, revisão periódica de acessos, requisitos de registro, retenção de evidências e mapeamento entre políticas e controles.	Decisões rastreáveis e maior preparo para revisões internas ou externas.
Observabilidade e resposta a incidentes	Monitoramento, encaminhamento de alertas, revisão de registros, níveis de gravidade de incidentes, revisão pós-incidente e indicadores de integridade dos serviços.	Diagnóstico mais rápido, recuperação mais disciplinada e aprendizado com falhas.
Capacitação da força de trabalho	Capacitação aplicada, hábitos de documentação, iniciativas de inclusão digital e orientação técnica baseada em funções.	Operações sustentáveis e participação mais ampla na transformação digital.

3.1 Linha de Base de Arquitetura

Uma linha de base de arquitetura constitui a representação mínima viável e confiável do ambiente tecnológico da instituição. Ela identifica serviços críticos, responsáveis, dependências, ambientes, modelos de acesso, expectativas de recuperação e riscos conhecidos. Em ambientes de nuvem, a linha de base também deve abranger a estrutura de contas ou projetos, a segmentação de rede, os limites de identidade, as configurações padrão de registro, as responsabilidades por backups e as condições em

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 23/10/2026 | aceito: 28/10/2026 | publicação: 02/11/2026

que serviços gerenciados são preferíveis a componentes administrados pela própria instituição.
A linha de base deve ser simples o bastante para ser mantida. Uma falha comum é produzir um documento de arquitetura extenso demais para ser atualizado. Para instituições menores, uma arquitetura de referência compacta, um catálogo de serviços e um registro de decisões podem oferecer mais valor prático do que um repositório de arquitetura abrangente, porém desatualizado.

3.2 Padronização Operacional

A padronização operacional converte a arquitetura em práticas reproduzíveis. Guias operacionais (runbooks) e planos de resposta (playbooks) são artefatos centrais. Um guia operacional descreve como executar uma tarefa conhecida, como integrar um usuário, restaurar um backup, renovar uma credencial ou validar uma implantação. Um plano de resposta descreve como reagir a uma classe de eventos, como indisponibilidade de serviço, suspeita de comprometimento de conta ou problemas de integridade de dados.
A padronização não elimina o julgamento profissional. Ela reduz o número de situações em que decisões precisam ser tomadas sob pressão e com informações incompletas. Também cria uma base de capacitação para integrantes menos experientes da equipe, favorecendo a inclusão digital dentro da própria instituição.

3.3 Segurança e Auditabilidade

Segurança e auditabilidade devem ser tratadas como requisitos de engenharia. Controles de acesso, registro de eventos, retenção de evidências e revisão de configurações precisam ser definidos antes que um sistema se torne crítico. O NIST Cybersecurity Framework 2.0 destaca a governança como função central que determina como o risco de segurança cibernética é compreendido e gerenciado. Em ambientes institucionais, isso significa que as equipes técnicas devem ser capazes de explicar não apenas se determinado controle existe, mas por que existe, quem é responsável por ele e como as evidências de seu funcionamento são preservadas.
Os princípios de confiança zero são úteis porque promovem verificação explícita, privilégio mínimo e avaliação contínua das relações de confiança. Para organizações menores, o ponto de partida prático pode ser modesto: centralizar a identidade, eliminar contas compartilhadas, documentar acessos privilegiados e revisar permissões periodicamente.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 23/10/2026 | aceito: 28/10/2026 | publicação: 02/11/2026

3.4 Observabilidade e Resposta a Incidentes

A observabilidade fornece os sinais necessários para gerenciar a confiabilidade. O monitoramento e o registro de eventos devem estar alinhados à criticidade do serviço. Nem todo sistema requer o mesmo nível de instrumentação, mas cada serviço crítico deve ter um responsável, uma definição de integridade, expectativas de alerta e um fluxo de tratamento de incidentes. A engenharia de confiabilidade de sites popularizou os objetivos de nível de serviço e os orçamentos de erro como formas de conectar o trabalho de engenharia à confiabilidade percebida pelo usuário. Mesmo quando uma instituição não adota formalmente SRE, o princípio permanece válido: a confiabilidade deve ser descrita em termos relevantes para as pessoas que dependem do serviço.

A revisão pós-incidente é igualmente importante. Uma revisão com prioridade à governança não se limita à causa técnica. Ela avalia se a organização dispunha de rotinas adequadas de detecção, documentação, acesso, backup, escalonamento e comunicação. O resultado deve ser um conjunto reduzido de melhorias cujo progresso possa ser acompanhado até a conclusão.

3.5 Capacitação da Força de Trabalho e Inclusão Digital

A inclusão digital é frequentemente discutida como acesso à tecnologia por comunidades externas. As instituições também precisam de inclusão digital interna: funcionários e voluntários devem compreender os sistemas que utilizam, os riscos que administram e as rotinas que mantêm os serviços confiáveis. A capacitação deve, portanto, estar vinculada a artefatos operacionais. Um guia operacional não é apenas um controle; é também um objeto de aprendizagem. Um plano de resposta não é apenas uma ferramenta para incidentes; é também uma forma de distribuir a capacidade de julgamento por toda a organização.

Essa perspectiva é particularmente importante em organizações orientadas por missão, nas quais o trabalho tecnológico frequentemente ultrapassa os limites formais dos cargos. O objetivo não é transformar cada parte interessada em engenheiro. O objetivo é criar compreensão compartilhada suficiente para que as decisões tecnológicas se tornem mais transparentes, resilientes e alinhadas ao propósito institucional.

4 ROTEIRO DE IMPLEMENTAÇÃO

As organizações podem adotar o modelo por meio de um roteiro em etapas. O roteiro é intencionalmente leve, pois muitas instituições não podem interromper suas operações para executar

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 23/10/2026 | aceito: 28/10/2026 | publicação: 02/11/2026

um amplo programa de transformação.

• Etapa 1: Estabelecer a linha de base. Identificar serviços críticos, responsáveis, dependências, contas privilegiadas, rotinas de backup e riscos não resolvidos.

• Etapa 2: Padronizar as tarefas mais frequentes. Criar guias operacionais concisos para integração de usuários, alterações de acesso, backups, verificações de recuperação e manutenção rotineira.

• Etapa 3: Definir classes de incidentes. Acordar níveis de gravidade, fluxos de escalonamento, comunicações, captura de evidências e expectativas para revisões pós-incidente.

• Etapa 4: Incorporar segurança e auditabilidade. Mapear políticas a controles, programar revisões de acesso, preservar registros de sistemas críticos e documentar exceções.

• Etapa 5: Ensinar o modelo operacional. Utilizar guias operacionais, planos de resposta e lições de incidentes como materiais de capacitação para partes interessadas técnicas e não técnicas.

O roteiro deve ser avaliado pela maturidade operacional, e não pelo volume de documentos. Indicadores úteis incluem a capacidade da equipe de identificar os responsáveis pelos serviços, restaurar um backup crítico, explicar acessos privilegiados, reproduzir uma configuração, encaminhar um incidente e capacitar um novo participante sem depender integralmente da memória informal.

5 RISCOS E COMPENSAÇÕES

O modelo com prioridade à governança envolve compensações. O excesso de padronização pode retardar a experimentação. A padronização insuficiente pode tornar os sistemas frágeis. O equilíbrio adequado depende do risco institucional, da criticidade dos serviços e da maturidade da equipe. Uma regra útil é padronizar os pontos em que uma falha causaria dano institucional e preservar a flexibilidade onde o aprendizado constitui o principal objetivo.

Outro risco é a governança meramente performática: produzir documentos que atendam a uma lista de verificação de auditoria, mas não influenciem as operações. Esse risco pode ser reduzido vinculando cada artefato de governança a uma rotina operacional. Uma política deve corresponder a um controle; um controle deve corresponder a evidências; e as evidências devem poder ser recuperadas pelas pessoas responsáveis pelo serviço.

6 CONCLUSÃO

As práticas de nuvem e DevOps podem ajudar instituições orientadas por missão a modernizar sua infraestrutura, mas a modernização sem governança pode aumentar a fragilidade. Um modelo operacional com prioridade à governança trata a confiabilidade, a segurança, a auditabilidade e a

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 23/10/2026 | aceito: 28/10/2026 | publicação: 02/11/2026

transferência de conhecimento como responsabilidades de engenharia. Ao incorporar a governança a arquiteturas de referência, guias operacionais, planos de resposta, rotinas de acesso, observabilidade e capacitação, as instituições podem criar uma infraestrutura digital não apenas moderna, mas também compreensível e confiável.

O modelo apresentado é intencionalmente prático. Seu valor não reside em acrescentar mais uma camada de terminologia, mas em ajudar as instituições a desenvolver hábitos reproduzíveis que protejam a continuidade e ampliem a participação na transformação digital.

AGRADECIMENTOS

O autor utilizou o OpenAI ChatGPT como apoio na redação, no refinamento estrutural e na organização editorial. O autor analisou e revisou o manuscrito e assume responsabilidade por seu conteúdo final. O artigo não inclui figuras, imagens nem dados experimentais gerados por inteligência artificial.

REFERÊNCIAS

[1] IEEE Computer Society, “Author Information: IT Professional.” [Online]. Disponível em: https://www.computer.org/csdl/magazine/it/write-for-us

[2] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST, fev. 2024. [Online]. Disponível em: https://www.nist.gov/cyberframework

[3] S. Rose, O. Borchert, S. Mitchell e S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, ago. 2020. [Online]. Disponível em: https://doi.org/10.6028/NIST.SP.800-207

[4] B. Beyer, C. Jones, J. Petoff e N. R. Murphy, Site Reliability Engineering: How Google Runs Production Systems. Sebastopol, CA, EUA: O'Reilly Media, 2016. [Online]. Disponível em: https://sre.google/sre-book/table-of-contents/

[5] AWS, “AWS Well-Architected Framework.” [Online]. Disponível em: https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html

[6] Google Cloud, “DORA: DevOps Research and Assessment.” [Online]. Disponível em: https://dora.dev/

[7] Cloud Security Alliance, “Cloud Controls Matrix.” [Online]. Disponível em: https://cloudsecurityalliance.org/research/cloud-controls-matrix

[8] IEEE, “IEEE Submission and Peer Review Policies.” [Online]. Disponível em: https://journals.ieeeauthorcenter.ieee.org/submit-your-article-for-peer-review/ieee-submission-and-peer-review-policies/

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.