RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

O framework Agility de transformação tecnológica regulada: uma metodologia baseada em risco para governança de tecnologia, modernização de sistemas, segurança de dados e resiliência operacional em instituições financeiras reguladas

The Agility Regulated Technology Transformation Framework: a risk-based methodology for technology governance, systems modernization, data security, and operational resilience in regulated financial institutions

El framework Agility de transformación tecnológica regulada: una metodología basada en riesgos para la gobernanza tecnológica, la modernización de sistemas, la seguridad de los datos y la resiliencia operativa en instituciones financieras reguladas

Antonio Garcia Junior
Agility Digital Technologies, LLC., Flórida, Estados Unidos
Autor correspondente: tony@agilitydigital.net
Breve biografia: fundador e proprietário da Agility Digital Technologies, LLC., com experiência profissional em liderança de tecnologia financeira, modernização, governança, arquitetura, dados, risco e resiliência operacional em ambientes bancários regulados.

Resumo:
Instituições financeiras enfrentam, de forma crescente, o desafio de modernizar ambientes tecnológicos legados ao mesmo tempo em que preservam governança efetiva, cibersegurança, proteção de dados, preparação regulatória e resiliência operacional. Bancos de pequeno e médio porte, cooperativas de crédito, fintechs, empresas de pagamentos e outras organizações financeiras reguladas podem enfrentar restrições específicas, pois precisam responder a expectativas tecnológicas e de supervisão complexas com recursos internos comparativamente limitados. Este artigo propõe o Agility Regulated Technology Transformation Framework (ARTTF), uma metodologia baseada em risco, estruturada, repetível e desenvolvida internamente para apoiar organizações financeiras reguladas na avaliação da maturidade tecnológica, identificação de riscos materiais, priorização de remediações e desenvolvimento de roteiros práticos de modernização. O framework integra seis domínios: governança de tecnologia e responsabilidade executiva; sistemas legados e arquitetura tecnológica; governança de dados, identidade e controle de acesso; riscos de nuvem, fornecedores e terceiros; cibersegurança, continuidade de negócios e recuperação; e auditabilidade, preparação regulatória e governança de remediações. A metodologia combina modelo de maturidade de cinco níveis, instrumento diagnóstico com 30 perguntas, priorização qualitativa de riscos, indicadores para dashboard executivo e planejamento de remediação por fases. Seu desenho se baseia em design science de sistemas de informação, literatura de transformação digital e orientações reconhecidas do setor financeiro e de cibersegurança dos Estados Unidos. Um cenário ilustrativo de banco comunitário demonstra como o framework pode converter preocupações tecnológicas fragmentadas em um programa priorizado de governança e modernização, sem substituir requisitos legais, regulatórios, de auditoria ou de supervisão específicos de cada instituição.

Palavras-chave:
Governança de TI. Modernização de sistemas. Segurança de dados. Resiliência operacional. Instituições financeiras.

Abstract:
Financial institutions increasingly face the challenge of modernizing legacy technology environments while maintaining effective governance, cybersecurity, data protection, regulatory readiness, and operational resilience. Smaller and mid-sized banks, credit unions,

fintech companies, payment organizations, and other regulated financial entities may face particular constraints because they must address complex technology and supervisory expectations with comparatively limited internal resources. This paper proposes the Agility Regulated Technology Transformation Framework (ARTTF), an internally developed, structured, and repeatable risk-based methodology designed to help regulated financial organizations assess technology maturity, identify material risks, prioritize remediation, and develop practical modernization roadmaps. The framework integrates six assessment domains: technology governance and executive accountability; legacy systems and technology architecture; data governance, identity, and access management; cloud, vendor, and third-party risk; cybersecurity, business continuity, and recovery; and auditability, regulatory readiness, and remediation governance. The methodology combines a five-level maturity model, a 30-question diagnostic instrument, qualitative risk prioritization, executive dashboard measures, and phased remediation planning. Its design draws on information-systems design science, digital-transformation literature, and recognized U.S. financial-sector and cybersecurity guidance, including NIST CSF 2.0 and FFIEC guidance. An illustrative community-bank scenario demonstrates how the framework can convert fragmented technology concerns into a prioritized governance and modernization program. The framework is intended as a practical management methodology and does not replace institution-specific legal, regulatory, audit, or supervisory requirements.

Keywords:
IT governance. Systems modernization. Data security. Operational resilience. Financial institutions.

Resumen:
Las instituciones financieras afrontan cada vez más el desafío de modernizar entornos tecnológicos heredados mientras mantienen una gobernanza eficaz, ciberseguridad, protección de datos, preparación regulatoria y resiliencia operativa. Los bancos pequeños y medianos, cooperativas de crédito, empresas fintech, organizaciones de pagos y otras entidades financieras reguladas pueden enfrentar restricciones particulares porque deben responder a expectativas tecnológicas y de supervisión complejas con recursos internos comparativamente limitados. Este artículo propone el Agility Regulated Technology Transformation Framework (ARTTF), una metodología estructurada, repetible, basada en riesgos y desarrollada internamente para ayudar a las organizaciones financieras reguladas a evaluar la madurez tecnológica, identificar riesgos materiales, priorizar la remediación y desarrollar hojas de ruta prácticas de modernización. El framework integra seis dominios de evaluación: gobernanza tecnológica y responsabilidad ejecutiva; sistemas heredados y arquitectura tecnológica; gobernanza de datos, identidad y gestión de accesos; riesgo de nube, proveedores y terceros; ciberseguridad, continuidad del negocio y recuperación; y auditabilidad, preparación regulatoria y gobernanza de la remediación. La metodología combina un modelo de madurez de cinco niveles, un instrumento diagnóstico de 30 preguntas, priorización cualitativa de riesgos, medidas para un panel ejecutivo y planificación de remediación por fases. Su diseño se basa en la ciencia del diseño de sistemas de información, la literatura de transformación digital y orientaciones reconocidas del sector financiero y la ciberseguridad de Estados Unidos. Un escenario ilustrativo de banco comunitario demuestra cómo el framework puede convertir inquietudes tecnológicas fragmentadas en un programa priorizado de gobernanza y modernización, sin sustituir requisitos jurídicos, regulatorios, de auditoría o supervisión específicos de cada institución.

Palabras clave:

Gobernanza de TI. Modernización de sistemas. Seguridad de datos. Resiliencia operativa. Instituciones financieras.

1. Introdução

A modernização tecnológica nos serviços financeiros não é um exercício puramente técnico. Ela modifica a forma como as instituições oferecem produtos, gerenciam riscos, protegem dados, interagem com clientes, dependem de terceiros e demonstram a eficácia dos controles a conselhos, auditores e supervisores. A pesquisa sobre transformação digital também enfatiza que uma transformação significativa exige mudanças nas estruturas, processos, capacidades e governança organizacionais, além da adoção de novas tecnologias (Vial, 2019). Em ambientes financeiros regulados, esse desafio mais amplo é intensificado por requisitos de segurança e solidez, segurança da informação, resiliência, proteção de dados, supervisão de terceiros e responsabilidade gerencial auditável.

O desafio é especialmente visível em instituições financeiras de pequeno e médio porte. Bancos comunitários e cooperativas de crédito podem operar serviços críticos de pagamentos, empréstimos, depósitos e informações de clientes com equipes de tecnologia e risco comparativamente pequenas. Fintechs e empresas de pagamentos podem crescer rapidamente enquanto se tornam mais dependentes de provedores de nuvem, parceiros bancários, APIs, plataformas de dados e serviços tecnológicos terceirizados. Em ambos os casos, as iniciativas de modernização somente criam valor quando a instituição consegue identificar quais riscos são materiais, estabelecer responsabilidades claras, sequenciar a remediação e preservar a continuidade durante a mudança.

As orientações do setor financeiro dos Estados Unidos tratam cada vez mais a governança de tecnologia, a arquitetura, a cibersegurança, a resiliência operacional, a autenticação e a gestão de terceiros como responsabilidades gerenciais interligadas. O manual Architecture, Infrastructure, and Operations do FFIEC enfatiza o planejamento de arquitetura e infraestrutura, a governança e gestão de riscos e o controle operacional de ativos, processos e terceiros interconectados (Federal Financial Institutions Examination Council [FFIEC], 2021a). O manual Business Continuity Management do FFIEC enquadra a continuidade como disciplina de gestão de riscos em toda a empresa, abrangendo tecnologia, operações, testes, comunicação e resiliência dos serviços críticos (FFIEC, 2019). As orientações interagências sobre terceiros afirmam ainda que o uso de terceiros não elimina a responsabilidade de uma organização bancária de operar com segurança, solidez e conformidade com os requisitos aplicáveis (Federal Deposit Insurance Corporation [FDIC] et al., 2023).

A necessidade de um mecanismo prático de integração é, portanto, significativa. As instituições costumam manter inventários separados de achados de auditoria, riscos de cibersegurança, dívida arquitetural, problemas de qualidade de dados, preocupações com fornecedores, lacunas de recuperação de desastres e medidas regulatórias. Quando esses artefatos são gerenciados isoladamente, os líderes podem não dispor de uma visão consolidada de como as fragilidades tecnológicas interagem ou de quais ações devem ser priorizadas. Um programa atrasado de governança de identidades, por exemplo, pode afetar simultaneamente cibersegurança, preparação para auditorias, acesso de terceiros, proteção de dados e contenção de incidentes. Uma plataforma de middleware sem suporte pode gerar ao mesmo tempo riscos operacionais, de segurança, de integração e de continuidade.

Este artigo apresenta o Agility Regulated Technology Transformation Framework (ARTTF) como método prático para converter essas preocupações fragmentadas em um programa estruturado de transformação. O framework destina-se a bancos comunitários, bancos de pequeno e médio porte, cooperativas de crédito, fintechs, organizações de pagamentos, provedores de Banking-as-a-Service e outras organizações financeiras reguladas ou intensivas em dados. Foi concebido para apoiar patrocinadores executivos, líderes de tecnologia, profissionais de risco e conformidade, partes interessadas de auditoria interna, gerentes de programas e equipes de arquitetura no estabelecimento de uma base factual comum, na avaliação da maturidade, na priorização dos riscos e na construção de um roteiro executável.

O artigo oferece quatro contribuições práticas. Primeiro, define seis domínios integrados de avaliação que conectam governança, arquitetura, dados, risco de terceiros, cibersegurança, resiliência e preparação regulatória. Segundo, apresenta um modelo de maturidade de cinco níveis e um instrumento diagnóstico de 30 perguntas que podem ser usados em triagens iniciais e discussões executivas. Terceiro, define uma abordagem de mapa de calor de riscos com regras explícitas de escalonamento qualitativo, para que a pontuação simples não substitua o julgamento profissional. Quarto, apresenta um modelo de dashboard executivo e uma estrutura de roteiro em fases de 0-90 dias, 3-12 meses e 12-24 meses para converter os achados da avaliação em execução governada. Um caso ilustrativo demonstra a mecânica da abordagem sem utilizar dados confidenciais de clientes.

2. Fundamentos teóricos e regulatórios

2.1 Transformação digital como processo organizacional e de gestão de riscos

A transformação digital é comumente descrita como mudança organizacional possibilitada por combinações de tecnologias da informação, computação, comunicação e conectividade. Vial (2019) mostra que a transformação digital afeta a criação de valor e exige que as organizações enfrentem mudanças estruturais e barreiras à execução. Em uma instituição financeira, essas barreiras aparecem frequentemente como aplicações legadas, integração fragmentada, direitos decisórios pouco claros, propriedade de dados inconsistente, dependências de fornecedores, controles manuais, observabilidade insuficiente ou prioridades empresariais e regulatórias concorrentes.

Essa perspectiva é importante porque um roteiro de modernização concentrado apenas na substituição de tecnologia pode deixar de abordar o modelo operacional que criou o risco. A migração de um sistema central pode manter sem solução a propriedade de dados, fragilidades de acesso privilegiado, concentração de fornecedores ou governança de mudanças ineficaz. De forma inversa, uma iniciativa de governança que não enfrente sistemas obsoletos e restrições arquiteturais pode produzir documentação mais robusta sem reduzir a fragilidade operacional. Por isso, o ARTTF trata a transformação tecnológica como um problema combinado de governança, arquitetura, dados, segurança, resiliência e execução.

2.2 Integração entre governança, cibersegurança e risco corporativo

O NIST Cybersecurity Framework (CSF) 2.0 oferece uma taxonomia de alto nível que organizações de diferentes portes e níveis de maturidade podem utilizar para compreender, avaliar, priorizar e comunicar resultados de cibersegurança (Pascoe et al., 2024). A versão 2.0 acrescentou a função Govern e ampliou a ênfase na governança e no risco da cadeia de suprimentos, reforçando a necessidade de conectar a cibersegurança à tomada de decisões corporativas, em vez de tratá-la como programa técnico isolado. O NIST também enfatiza que o CSF descreve resultados, e não prescreve um único método de implementação, permitindo que as organizações adaptem a implementação ao seu perfil de risco.

As orientações do NIST sobre os Tiers do CSF podem ser usadas para caracterizar o rigor dos processos de governança e gestão de riscos de cibersegurança e contextualizar melhorias (Quinn et al., 2024). O modelo de maturidade de cinco níveis do ARTTF não é uma reformulação dos quatro Tiers do NIST CSF. Trata-se de uma escala diagnóstica desenvolvida internamente para apoiar uma avaliação mais ampla da transformação tecnológica em seis

domínios. Os resultados e Tiers do NIST CSF podem servir como referências informativas nas partes da avaliação relacionadas à cibersegurança, enquanto a pontuação de maturidade do ARTTF oferece uma visão gerencial entre domínios.

2.3 Arquitetura, tecnologia legada e dependência operacional

As orientações Architecture, Infrastructure, and Operations do FFIEC reconhecem que arquitetura tecnológica, infraestrutura e operações estão interligadas a ativos, processos e prestadores de serviços terceirizados (FFIEC, 2021a). Para instituições reguladas, as decisões de arquitetura influenciam disponibilidade, segurança, escalabilidade, dependência de fornecedores, movimentação de dados, complexidade das mudanças e oferta de produtos e serviços financeiros críticos. Isso torna a revisão de arquitetura uma atividade de gestão de riscos, além de uma atividade de design.

A tecnologia legada deve, portanto, ser avaliada não apenas pela idade, mas também por criticidade para o negócio, capacidade de suporte, exposição de segurança, complexidade de integração, recuperabilidade, concentração de conhecimento, risco de falha em mudanças e dependência de componentes obsoletos. O framework utiliza esses fatores para identificar prioridades de modernização e distinguir entre tecnologias que podem ser estabilizadas, tecnologias que devem ser desacopladas progressivamente e tecnologias que exigem substituição planejada.

2.4 Governança de dados, identidade e gestão de acessos

A governança de dados determina quais decisões devem ser tomadas sobre os dados e quem responde por elas. Khatri e Brown (2010) distinguem governança da gestão cotidiana e enfatizam direitos decisórios e responsabilização nos domínios de dados. Nos serviços financeiros, essas questões de governança estão diretamente ligadas à confiabilidade dos relatórios, à proteção de dados dos clientes, aos controles de fraude, ao risco de modelos, à análise de dados, à preparação para IA e às evidências regulatórias.

A gestão de identidades e acessos é igualmente transversal. As orientações de autenticação de 2021 do FFIEC enfatizam avaliação de riscos, segurança em camadas e práticas de autenticação mais robustas para clientes, empregados e terceiros que acessam sistemas e serviços (FFIEC, 2021b). Por isso, o framework avalia a governança de acessos em conjunto com classificação de dados, acesso privilegiado, segregação de funções, processos de admissão-movimentação-desligamento e revisão periódica de direitos, em vez de tratar a autenticação como controle isolado.

2.5 Nuvem, fornecedores e risco de terceiros

A modernização depende cada vez mais de provedores externos de tecnologia, plataformas de nuvem, produtos de software como serviço, parceiros fintech e fornecedores especializados. As orientações interagências de 2023 sobre terceiros estabelecem uma abordagem de ciclo de vida baseada em riscos, abrangendo planejamento, diligência e seleção, negociação contratual, monitoramento contínuo e encerramento (FDIC et al., 2023). As orientações também deixam claro que a organização bancária conserva a responsabilidade pela operação segura e sólida quando utiliza terceiros.

A adoção de nuvem cria considerações adicionais sobre responsabilidade compartilhada, concentração, transparência arquitetural, planejamento de saída, localização dos dados, identidade, monitoramento, resiliência e acesso contratual a evidências. O Tesouro dos Estados Unidos e o Financial Services Sector Coordinating Council publicaram recursos destinados a apoiar a adoção segura de nuvem e abordar preocupações com terceiros, terceirização, resiliência e transparência em instituições financeiras de diferentes portes (U.S. Department of the Treasury, 2024b). Por isso, o ARTTF incorpora a governança de nuvem e terceiros à mesma avaliação utilizada para arquitetura e resiliência operacional.

2.6 Cibersegurança, continuidade de negócios e resiliência operacional

O conceito de resiliência vai além da recuperação de desastres. As orientações do FFIEC enfatizam práticas de continuidade em toda a empresa, abrangendo tecnologia, operações, testes e comunicações, bem como a manutenção contínua dos sistemas e controles necessários para sustentar serviços críticos (FFIEC, 2019). O relatório Cybersecurity and Financial System Resilience de 2026 do OCC descreve cibersegurança, resiliência operacional e risco de terceiros como prioridades contínuas de supervisão no sistema bancário federal (Office of the Comptroller of the Currency [OCC], 2026). A NCUA também destaca exames direcionados, avaliações de risco, preparação e resiliência do sistema no setor de cooperativas de crédito (National Credit Union Administration [NCUA], 2026).

No ARTTF, a resiliência é avaliada por meio da criticidade dos serviços, objetivos de recuperação, mapeamento de dependências, testes de backup e restauração, preparação para incidentes, governança de crises, monitoramento, redundância arquitetural, dependências de recuperação de fornecedores e capacidade da organização de manter ou restaurar serviços financeiros críticos. Essa visão mais ampla reduz o risco de que um programa de backup tecnicamente bem-sucedido seja confundido com resiliência operacional.

2.7 Tecnologia emergente e preparação para IA

A análise avançada de dados e a inteligência artificial podem ampliar a eficiência e o apoio à decisão, mas também aumentam a importância da qualidade dos dados, explicabilidade, segurança, governança de terceiros e responsabilização da gestão. O AI Risk Management Framework do NIST oferece uma estrutura voluntária para gerenciar riscos que os sistemas de IA representam para organizações e para a sociedade (Tabassi, 2023). O trabalho do Tesouro para o setor financeiro identifica privacidade de dados, dependências de terceiros, cibersegurança, vieses, governança e conformidade como considerações relevantes na adoção de IA em serviços financeiros (U.S. Department of the Treasury, 2024a). O Financial Stability Board também identifica dependências de terceiros, risco cibernético, risco de modelos, qualidade dos dados e governança entre as vulnerabilidades importantes relacionadas à IA nas finanças (Financial Stability Board [FSB], 2024).

O ARTTF não é um framework de governança de IA. Em vez disso, trata a preparação para IA como resultado de capacidades fundamentais mais robustas: governança responsável, dados confiáveis, acesso controlado, arquitetura segura, supervisão eficaz de terceiros, mudanças auditáveis e operações resilientes. As instituições podem ampliar o instrumento diagnóstico com perguntas específicas sobre IA quando casos de uso de análise avançada ou IA forem materiais para o escopo.

3. Metodologia

3.1 Orientação aplicada de design science

O framework foi desenvolvido como artefato metodológico orientado à prática. A design science em sistemas de informação se concentra na criação e aplicação de artefatos destinados a melhorar capacidades humanas e organizacionais em um domínio de problema definido (Hevner et al., 2004). Peffers et al. (2007) descrevem um processo de pesquisa em design science que inclui identificação do problema, definição de objetivos, design e desenvolvimento, demonstração, avaliação e comunicação. O desenvolvimento do ARTTF segue essa lógica em nível aplicado: identifica um problema gerencial recorrente na transformação tecnológica regulada, especifica as capacidades necessárias para enfrentá-lo, concebe um artefato repetível de avaliação e priorização, demonstra seu uso por meio de um caso ilustrativo e comunica limitações e oportunidades de futura avaliação empírica.

A metodologia combina três fontes de conhecimento. A primeira consiste em orientações públicas reconhecidas de reguladores financeiros e órgãos de normalização dos

Estados Unidos, utilizadas para identificar temas recorrentes de governança, arquitetura, cibersegurança, resiliência, dados, acesso e terceiros. A segunda é a literatura de sistemas de informação sobre transformação digital, governança de dados e design science. A terceira é a experiência profissional do autor em liderança de tecnologia financeira, modernização, governança, arquitetura, dados, risco e iniciativas de resiliência operacional em ambientes bancários regulados. O framework não reproduz programa de exame, scorecard ou catálogo proprietário de controles de um regulador. Ele traduz princípios recorrentes em uma sequência gerencial de avaliação e planejamento da transformação.

Este artigo não reivindica validação empírica em uma amostra estatisticamente representativa de instituições. O caso ilustrativo da Seção 9 é hipotético e serve apenas para demonstrar a mecânica de pontuação, priorização, comunicação executiva e desenvolvimento do roteiro. Pesquisas futuras devem avaliar a consistência entre avaliadores, a validade preditiva e os resultados práticos em instituições de diferentes tipos e portes.

3.2 Princípios de design

Tabela 1. Princípios de design do Agility Regulated Technology Transformation Framework

Princípio de design	Significado operacional
Baseado em riscos, e não orientado por checklist	A profundidade da avaliação e a prioridade de remediação devem refletir criticidade para o negócio, relevância regulatória, impacto sobre clientes e dados, exposição e dependência operacional.
Responsabilização executiva	Todo achado material deve ter responsável, caminho decisório, data-alvo e mecanismo de escalonamento.
Orientação por evidências	As conclusões devem ser rastreáveis a documentos, entrevistas, inventários, configurações, métricas, evidências de testes ou outros artefatos de análise.
Integração entre domínios	Um achado pode afetar vários domínios; a metodologia deve evitar pontuações isoladas que ocultem riscos interconectados.
Proporcionalidade	A profundidade da avaliação deve refletir porte, complexidade, produtos, modelo tecnológico, dependência de terceiros e perfil de risco da instituição.
Modernização com resiliência	Mudanças no estado-alvo devem melhorar escalabilidade e eficiência sem enfraquecer segurança, continuidade, auditabilidade ou controle.
Capacidade de ação	A avaliação deve terminar com ações priorizadas, sequenciamento, dependências, responsáveis e decisões executivas, e não com uma lista estática de observações.
Repetibilidade	Domínios principais, perguntas, definições de pontuação e estruturas de reporte devem ser suficientemente consistentes para apoiar reavaliação e análise de tendências.

Nota. Os princípios destinam-se a orientar o julgamento profissional; não substituem requisitos legais ou de supervisão específicos da instituição.

3.3 Escopo e uso pretendido

O framework foi concebido para diagnósticos iniciais, revisões de preparação regulatória, avaliações de modernização, programas de melhoria da governança, due diligence, planejamento de remediação e governança da transformação. Pode ser utilizado como avaliação empresarial completa ou ter seu escopo limitado a um subconjunto de domínios, unidades de negócio, plataformas ou serviços críticos. Uma avaliação completa deve estabelecer limites de escopo, sistemas e serviços materiais, terceiros importantes, dados críticos, contexto regulatório e principais iniciativas de transformação antes do início da pontuação.

Os usuários pretendidos incluem CIOs, CTOs, CISOs, CROs, líderes de risco de tecnologia, responsáveis por conformidade, líderes de dados, arquitetos empresariais, líderes de programas, partes interessadas de auditoria interna e consultores externos. O framework não pretende criar certificação, classificação regulatória ou conclusão jurídica. Uma pontuação de maturidade 4 ou 5 não estabelece conformidade, e uma pontuação menor não estabelece por si só uma violação regulatória. A pontuação é uma ferramenta gerencial de priorização e diálogo.

4. O Agility Regulated Technology Transformation Framework

4.1 Ciclo de entrega em seis fases

Tabela 2. Ciclo de seis fases do ARTTF

Fase	Objetivo principal	Resultados representativos
Fase 1 - Alinhamento executivo e confirmação do escopo	Definir contexto do negócio, direcionadores regulatórios, escopo, serviços críticos, partes interessadas, critérios de sucesso, cronograma e governança.	Termo de abertura; declaração de escopo; mapa de partes interessadas; lista de documentos solicitados; hipóteses iniciais de risco.
Fase 2 - Descoberta do estado atual e coleta de evidências	Analisar governança, arquitetura, aplicações, infraestrutura, nuvem, fornecedores, dados, controles, continuidade, achados de auditoria, práticas de mudança e reporte.	Avaliação do estado atual; inventário; registro de evidências; mapa de dependências; registro preliminar de riscos.
Fase 3 - Avaliação de lacunas baseada em riscos e avaliação da maturidade	Avaliar práticas atuais frente às orientações selecionadas, requisitos do negócio, apetite de risco e resultados-alvo; identificar causas-raiz e lacunas interconectadas.	Pontuações de maturidade; matriz de lacunas; mapa de calor de riscos; registro de problemas; observações executivas.
Fase 4 - Design do estado-alvo e roteiro de modernização	Traduzir achados em modelos operacionais-alvo, governança, arquitetura, melhorias de controles, sequenciamento e prioridades de investimento.	Modelo do estado-alvo; blueprint de arquitetura; RACI; plano de controles; roteiro de modernização; resumo do impacto nos negócios.
Fase 5 - Apoio direcionado à implementação	Fornecer apoio à governança e implementação sem atuar como empresa de alocação de pessoal, MSP, fornecedor de testes de invasão ou de operações contínuas de segurança.	Plano de implementação; dashboard de governança; rastreador de fornecedores; registro de problemas e riscos; evidências de controles; procedimentos atualizados.

Fase	Objetivo principal	Resultados representativos
Fase 6 - Reporte executivo, evidências de auditoria e melhoria contínua	Estabelecer reporte sustentável, métricas, rotinas de governança, evidências, reavaliação e lições aprendidas.	Relatório executivo; pacote para o conselho; evidências de auditoria; dashboard de remediação; backlog de melhorias; linha de base para reavaliação.

4.2 Seis domínios integrados de avaliação

Tabela 3. Domínios integrados de avaliação

ID	Domínio	Escopo	Principais famílias de referência
D1	Governança de tecnologia e responsabilização executiva	Direitos decisórios, responsabilização, propriedade dos riscos, políticas, fóruns de governança, alinhamento estratégico, reporte executivo e ao conselho, apetite de risco e supervisão gerencial.	Função Govern do NIST CSF 2.0; conceitos de gestão/AIO do FFIEC; governança de riscos corporativos.
D2	Sistemas legados e arquitetura tecnológica	Ciclo de vida de aplicações e infraestrutura, arquitetura-alvo, dívida técnica, integrações, APIs, dependências de nuvem e locais, escalabilidade, observabilidade, complexidade de mudanças e sequenciamento da modernização.	FFIEC Architecture, Infrastructure, and Operations; literatura de transformação digital.
D3	Governança de dados, identidade e gestão de acessos	Propriedade, classificação, qualidade e linhagem de dados, governança de acessos, acesso privilegiado, processos de admissão-movimentação-desligamento, segregação de funções e confiabilidade dos relatórios.	Literatura de governança de dados; orientações do FFIEC sobre autenticação e acesso; resultados do NIST.
D4	Nuvem, fornecedores e risco de terceiros	Inventário e classificação por risco de terceiros, due diligence, contratação, SLAs, monitoramento contínuo, concentração, responsabilidade compartilhada na nuvem, quartas partes, resiliência e planejamento de saída.	Orientações interagências de 2023 sobre terceiros; recursos do Tesouro sobre nuvem; governança da cadeia de suprimentos do NIST.
D5	Cibersegurança, continuidade de negócios e recuperação	Governança de segurança, gestão de vulnerabilidades, monitoramento, resposta a incidentes, backups, testes de recuperação, RTO/RPO, gestão de crises, continuidade de serviços críticos e dependências de resiliência.	NIST CSF 2.0; FFIEC Business Continuity Management; prioridades de resiliência do OCC e da NCUA.
D6	Auditabilidade, preparação regulatória e governança da remediação	Mapeamento de controles, evidências, achados de auditoria e exames, acompanhamento de mudanças regulatórias, adesão a políticas, propriedade dos problemas, validação da remediação, reporte e governança do encerramento.	Temas de supervisão do FFIEC/OCC; governança do NIST; práticas de controles internos e evidências.

4.3 Modelo de maturidade de cinco níveis

O modelo de maturidade oferece uma linguagem comum para descrever a institucionalização das práticas. Avalia se as responsabilidades e controles são informais ou repetíveis, se estão documentados e são executados de forma consistente, se a gestão mede desempenho e risco e se a organização estabeleceu melhoria contínua e resiliência. A escala é intencionalmente ampla o suficiente para ser aplicada aos seis domínios, permitindo que evidências específicas de cada domínio determinem a pontuação.

Uma pontuação de maturidade somente deve ser atribuída após a análise de evidências adequadas ao escopo. Respostas de entrevistas, por si só, não devem sustentar pontuação alta

quando documentação, evidências operacionais, testes, métricas ou histórico de problemas contradizem a prática declarada. Da mesma forma, a ausência de um documento formal não deve impor automaticamente uma pontuação baixa se a organização puder demonstrar mecanismo equivalente, controlado e repetível.

Tabela 4. Escala de maturidade do ARTTF

Nível	Classificação	Definição	Características típicas
1	Reativo	As práticas são informais, fragmentadas, dependentes de pessoas ou orientadas principalmente por eventos. A responsabilidade e as evidências são limitadas.	Alta variabilidade; lacunas materiais podem ser desconhecidas; a remediação é principalmente reativa.
2	Em desenvolvimento	Existem controles e responsabilidades básicos, mas a execução é inconsistente entre equipes, sistemas ou períodos.	Visibilidade parcial; exceções recorrentes; métricas limitadas; evidências inconsistentes.
3	Definido	As práticas são documentadas, atribuídas, padronizadas e geralmente repetíveis dentro do escopo definido.	Funções e processos são claros; há evidências disponíveis; as exceções são gerenciadas.
4	Gerenciado	As práticas são medidas, baseadas em riscos, monitoradas e integradas à governança e ao reporte gerencial.	Métricas, limites, testes, análise de tendências e remediação responsável estão estabelecidos.
5	Otimizado / Resiliente	As práticas são integradas, adaptáveis, melhoradas continuamente e comprovadamente resilientes em condições variáveis.	Aprendizado contínuo; automação quando adequada; testes de cenários; resposta rápida; otimização estratégica.

Nota. Este modelo de maturidade de cinco níveis é uma escala diagnóstica do ARTTF e não deve ser apresentado como equivalente ao modelo de quatro Tiers do NIST CSF.

4.4 Lógica de pontuação da maturidade

Cada pergunta diagnóstica recebe pontuação de 1 a 5 de acordo com as definições da Tabela 4. A pontuação de um domínio é a média aritmética das cinco perguntas atribuídas a ele. A pontuação geral padrão de maturidade é a média das pontuações dos seis domínios. A ponderação igual é adequada para um diagnóstico empresarial inicial porque evita criar aparência de precisão antes que a instituição tenha estabelecido seu perfil de risco. As organizações podem adotar pesos baseados em risco quando houver justificativa documentada — por exemplo, uma organização de pagamentos pode atribuir maior peso à resiliência cibernética e à dependência de terceiros, enquanto uma instituição em um grande programa de modernização do sistema central pode enfatizar arquitetura e dados.

A pontuação deve ser acompanhada por um indicador de confiança das evidências, como Alta, Média ou Baixa. Uma pontuação baseada em políticas, evidências de sistemas, métricas, resultados de testes e histórico de problemas deve ter maior confiança do que aquela baseada principalmente em entrevistas. Quando as evidências forem contraditórias, o

avaliador deve registrar a contradição e utilizar a menor pontuação sustentada até que a divergência seja resolvida.

5. Instrumento diagnóstico de 30 perguntas

5.1 Questionário principal

O diagnóstico principal contém cinco perguntas para cada um dos seis domínios. O instrumento destina-se a entrevistas estruturadas e análise de evidências, não a uma lista de autocertificação. Cada pergunta deve ser apoiada por uma breve nota de evidência, uma pontuação de maturidade de 1 a 5 e qualquer observação de risco resultante. As perguntas podem ser complementadas de acordo com os produtos da instituição, perímetro regulatório, serviços críticos, fornecedores materiais e programas ativos de transformação.

Tabela 5. Diagnóstico principal de 30 perguntas do ARTTF

Nº	Domínio	Pergunta diagnóstica	Pontuação (1-5)
1	D1	A estratégia tecnológica, as prioridades de risco e as principais decisões de modernização são governadas por fóruns executivos claramente definidos e com direitos decisórios documentados?	
2	D1	Há responsáveis formalmente designados para riscos tecnológicos materiais, controles, serviços críticos e ações de remediação?	
3	D1	As políticas e normas tecnológicas estão sujeitas a processos definidos de aprovação, exceção, revisão e descontinuação?	
4	D1	Os riscos tecnológicos e de cibersegurança estão integrados à gestão de riscos corporativos, ao apetite de risco e ao reporte executivo e ao conselho?	
5	D1	Os relatórios gerenciais utilizam KPIs/KRIs relevantes para decisão, limites, tendências e critérios de escalonamento, em vez de apenas métricas de atividade?	
6	D2	A instituição mantém um inventário confiável de aplicações, infraestrutura, integrações, dependências críticas, situação do ciclo de vida e propriedade de negócio?	
7	D2	Tecnologias em fim de vida, sem suporte, de alta complexidade ou alta dependência são identificadas e governadas por planos documentados de ciclo de vida e remediação?	
8	D2	Existe arquitetura-alvo e roteiro de modernização documentados e alinhados à estratégia de negócio, às prioridades de risco e à resiliência dos serviços críticos?	
9	D2	Integrações e APIs são governadas por práticas definidas de arquitetura, segurança, dados, versionamento, propriedade e monitoramento?	
10	D2	Dívida técnica, complexidade de mudanças, exceções de arquitetura e dependências de modernização são medidas e incorporadas às decisões de investimento?	
11	D3	Proprietários de dados, data stewards, elementos de dados críticos, requisitos de classificação e responsabilização pela qualidade dos dados estão claramente definidos?	
12	D3	Problemas de qualidade, linhagem, conciliação e reporte de dados são medidos, investigados e remediados com base no impacto empresarial e regulatório?	
13	D3	Os processos de admissão-movimentação-desligamento estão integrados à governança de identidades para que o acesso seja tempestivo, rastreável e removido quando deixar de ser justificado?	
14	D3	Direitos de acesso privilegiado e de alto risco estão sujeitos a autenticação robusta, aprovação, registro, monitoramento e recertificação periódica?	

Nº	Domínio	Pergunta diagnóstica	Pontuação (1-5)
15	D3	Conflitos de segregação de funções e exceções de acesso são identificados, avaliados quanto ao risco, limitados no tempo e revisados por gestão responsável?	
16	D4	A instituição mantém um inventário completo e classificado por risco de terceiros, serviços de nuvem, subcontratados materiais e dependências tecnológicas?	
17	D4	A due diligence avalia segurança, resiliência, condição financeira, tratamento de dados, apoio regulatório, concentração e capacidades operacionais de forma proporcional ao risco?	
18	D4	Contratos e SLAs tratam de segurança, direitos sobre dados, notificação de incidentes, direitos de auditoria e acesso, resiliência, subcontratação, desempenho, encerramento e necessidades de saída?	
19	D4	Terceiros materiais estão sujeitos a monitoramento contínuo de desempenho, risco, controles, incidentes e condição financeira com limites definidos de escalonamento?	
20	D4	Risco de concentração, lacunas de responsabilidade compartilhada na nuvem, substituibilidade, portabilidade de dados e planos de saída e transição são avaliados para fornecedores críticos?	
21	D5	As práticas de monitoramento, registro, alertas, gestão de vulnerabilidades e escalonamento de incidentes de cibersegurança são baseadas em riscos e eficazes para sistemas e serviços críticos?	
22	D5	O programa de resposta a incidentes é testado por meio de exercícios que incluem tomada de decisões executivas, comunicações, fornecedores, jurídico/conformidade e coordenação da recuperação?	
23	D5	Análises de impacto no negócio, RTOs, RPOs, dependências de recuperação e planos de continuidade estão atualizados para produtos e serviços financeiros críticos?	
24	D5	As capacidades de backup, restauração, failover e recuperação de desastres são testadas com frequência e escopo compatíveis com a criticidade do serviço e os cenários de ameaça?	
25	D5	Fragilidades significativas de resiliência, pontos únicos de falha, exposição a ransomware e restrições de recuperação são acompanhados por uma remediação com responsáveis?	
26	D6	Os controles tecnológicos materiais podem ser mapeados a evidências documentadas que demonstrem design, responsabilidade, operação, testes e tratamento de exceções?	
27	D6	Achados de auditoria, exames, conformidade e risco são governados por um processo comum de gestão de problemas com responsáveis, prazos, evidências e validação?	
28	D6	A instituição mantém um processo estruturado para identificar mudanças regulatórias ou de supervisão aplicáveis à tecnologia e traduzi-las em ações?	
29	D6	Políticas, procedimentos, normas, evidências de sistemas, resultados de testes e aprovações gerenciais estão organizados para serem apresentados com eficiência em auditorias ou exames?	
30	D6	Itens de remediação vencidos, recorrentes ou de alta gravidade são escalonados à direção executiva e ao conselho ou comitê adequado, com decisões claras e aceitação de riscos?	

5.2 Expectativas de evidências e disciplina de pontuação

Uma resposta diagnóstica deve ser documentada em quatro campos: pontuação, evidências analisadas, observação e referência da ação ou risco. As evidências típicas incluem regimentos de governança, materiais de conselhos ou comitês, políticas e normas, inventários de ativos e aplicações, diagramas de arquitetura, registros de fornecedores, contratos, relatórios de revisão de acessos, métricas de vulnerabilidade, registros de incidentes, resultados de testes de backup e recuperação, achados de auditoria, rastreadores de problemas, dashboards e registros de mudanças. O objetivo não é maximizar o volume de documentação, mas estabelecer rastreabilidade entre a pontuação e a prática institucional observável.

As pontuações devem descrever institucionalização, não aspiração. Uma política recém-aprovada sem evidências operacionais geralmente sustenta uma pontuação Em desenvolvimento ou Definida, dependendo do escopo da implementação; ela não deve sustentar automaticamente maturidade Gerenciada. Por outro lado, um processo maduro pode ser sustentado por evidências automatizadas e histórico operacional consistente, ainda que a organização utilize terminologia diferente da adotada pelo framework. Os avaliadores devem documentar práticas compensatórias, em vez de forçar conformidade artificial.

O questionário é deliberadamente conciso. Uma avaliação completa deve desdobrar cada pergunta em subtestes baseados no escopo e na materialidade. Por exemplo, a Pergunta 24 pode exigir análises separadas de design de backup imutável, testes de restauração, isolamento para recuperação cibernética, failover de serviços críticos, dependências de recuperação e evidências de recuperação dos fornecedores. Portanto, o instrumento de 30 perguntas deve ser entendido principalmente como diagnóstico executivo e organizador do programa de trabalho.

6. Modelo de avaliação e priorização de riscos

6.1 Escalas de probabilidade e impacto

O modelo de riscos utiliza uma matriz 5 × 5 de probabilidade e impacto como recurso de comunicação. Como as matrizes qualitativas de risco podem gerar falsa precisão, compressão de faixas e ordenação ambígua, a pontuação numérica não deve ser usada como único fundamento das decisões de remediação (Cox, 2008). Por isso, o ARTTF combina a pontuação-base com fatores explícitos de escalonamento, criticidade dos serviços, relevância regulatória e julgamento profissional.

Tabela 6. Escala de probabilidade

Pontuação	Nível	Interpretação
1	Rara	Não esperada em condições normais; controles preventivos robustos e exposição limitada.
2	Improvável	Plausível, porém infrequente; a exposição é limitada ou os controles são geralmente eficazes.
3	Possível	Pode ocorrer em condições realistas; existem fragilidades ou dependências conhecidas.
4	Provável	Espera-se que ocorra ou se repita sem remediação; há evidências de fragilidade dos controles ou eventos repetidos.
5	Quase certa	Ativa, recorrente, altamente exposta ou fortemente evidenciada como iminente/persistente.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

Tabela 7. Escala de impacto

Pontuação	Nível	Interpretação
1	Limitado	Efeito localizado; sem consequência material para clientes, regulamentação, finanças ou serviços críticos.
2	Moderado	Interrupção ou falha de controle gerenciável, com impacto empresarial contido.
3	Significativo	Impacto operacional, sobre clientes, dados, auditoria, finanças ou gestão que exige resposta coordenada.
4	Grave	Impacto sério sobre serviços críticos, dados sensíveis, postura regulatória, perdas financeiras ou operações sustentadas.
5	Severo / Crítico	Potencial de interrupção ampla ou prolongada, danos graves a clientes ou dados, exposição regulatória significativa ou ameaça a serviços essenciais.

6.2 Mapa de calor de riscos e faixas-base de prioridade

A pontuação-base de risco é calculada como Probabilidade × Impacto, gerando um valor de 1 a 25. As faixas padrão de prioridade são Baixa (1-4), Moderada (5-9), Alta (10-14) e Crítica (15-25). Essas faixas são pontos de partida e devem ser calibradas ao apetite de risco e à política de gestão de problemas da instituição. A matriz não deve se sobrepor a requisitos obrigatórios de remediação, compromissos de auditoria, achados regulatórios ou vulnerabilidades críticas conhecidas.

Figura 1. Mapa de calor de riscos do ARTTF (pontuação-base)

Impact → Likelihood ↓	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Nota. Faixas-base: Baixa = 1-4; Moderada = 5-9; Alta = 10-14; Crítica = 15-25. As pontuações são um recurso de priorização, não uma estimativa quantitativa da perda esperada.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

6.3 Fatores qualitativos de escalonamento

Tabela 8. Fatores de escalonamento da prioridade de risco

Fator de escalonamento	Gatilho	Tratamento
Importância regulatória ou de supervisão	O achado está relacionado a compromisso regulatório, achado de exame, requisito legal, problema formal de auditoria ou expectativa material de supervisão.	Elevar a prioridade quando o atraso puder gerar exposição regulatória, jurídica ou de exame.
Dependência de serviço crítico	O achado afeta pagamentos, depósitos, empréstimos, acesso de clientes, identidade, segurança, processamento central ou outro serviço essencial.	Elevar quando a falha puder prejudicar produto/serviço crítico ou dependência de recuperação.
Dados sensíveis / impacto sobre clientes	O achado pode expor de forma material dados confidenciais, de clientes, financeiros, de autenticação ou regulados.	Elevar quando a sensibilidade, escala ou potencial de uso indevido dos dados for material.
Exposição externa / explorabilidade	A fragilidade está voltada para a internet, é explorada ativamente, facilmente abusada ou ligada a credenciais fracas ou acesso privilegiado.	Elevar com base em inteligência de ameaças, evidências de vulnerabilidade ou exposição.
Concentração de terceiros / substituibilidade	Um fornecedor crítico possui poucos substitutos, dependências opacas, capacidade de saída inadequada ou risco de concentração.	Elevar quando a instituição tiver controle limitado ou poucas alternativas de recuperação.
Fragilidade de recuperação	Os controles não foram testados, a restauração é incerta, RTO/RPO não podem ser demonstrados ou permanecem pontos únicos de falha.	Elevar quando a falha puder prolongar a interrupção ou tornar incerta a recuperação.
Problema recorrente / vencido	O mesmo problema se repetiu, ultrapassou datas-alvo ou permaneceu aberto em revisões anteriores.	Elevar para refletir governança de remediação ineficaz e exposição acumulada.

Uma prática recomendada é preservar a pontuação-base original e registrar separadamente a prioridade final da gestão. Por exemplo, uma pontuação-base 12 pode ser designada Crítica por se tratar de um achado regulatório vencido que afeta um serviço crítico de pagamentos. Essa abordagem mantém a transparência da pontuação e evita manipular probabilidade ou impacto apenas para alcançar a prioridade desejada.

7. Dashboard executivo de riscos tecnológicos

7.1 Design do dashboard

O dashboard executivo traduz os detalhes da avaliação em um conjunto limitado de indicadores relevantes para decisão. Deve responder a quatro perguntas: qual é a atual postura de maturidade e risco? Quais riscos exigem decisões executivas? A remediação está avançando no ritmo necessário? As iniciativas de modernização estão melhorando ou aumentando a resiliência? Portanto, o dashboard deve combinar indicadores de maturidade, risco, remediação, resiliência, arquitetura, terceiros e auditoria, em vez de reportar apenas atividades de cibersegurança.

As métricas devem ser definidas com responsável, lógica de cálculo, fonte de dados, limite, frequência e caminho de escalonamento. Um dashboard sem limites pode se tornar um

artefato de reporte, e não um controle gerencial. Da mesma forma, um número excessivo de métricas pode ocultar os poucos problemas que exigem ação. O ARTTF recomenda uma visão executiva compacta, apoiada por detalhamentos operacionais mais profundos.

Tabela 9. Medidas recomendadas para o dashboard executivo

Indicador	Definição	Frequência	Uso executivo
Maturidade tecnológica geral	Pontuação média de maturidade dos domínios mais nível de confiança das evidências.	Trimestral	Tendência e meta por ciclo de avaliação.
Maturidade dos domínios	Pontuações de maturidade D1-D6.	Trimestral	Destacar domínios abaixo da meta ou em declínio.
Riscos tecnológicos Críticos / Altos	Quantidade e tendência de itens Críticos e Altos em aberto.	Mensal	Escalonar imediatamente novos itens Críticos.
Remediação vencida	Número e percentual de problemas além da data-alvo aprovada.	Mensal	Escalonar itens materiais vencidos e prorrogações repetidas.
Achados regulatórios / de auditoria	Achados em aberto por gravidade, idade, prazo e situação de validação.	Mensal	Separar compromissos que exigem evidência formal de encerramento.
Exposição crítica a legados	Serviços críticos dependentes de tecnologia sem suporte ou de alto risco.	Trimestral	Acompanhar marcos de descontinuação, contenção e desacoplamento.
Terceiros de alto risco	Fornecedores materiais com problemas abertos de controles, desempenho, resiliência ou contrato.	Mensal	Incluir situação de concentração e do plano de saída.
Exceções de acesso privilegiado	Contas/exceções de alto risco fora das políticas ou dos requisitos de recertificação.	Mensal	Escalonar privilégios sem responsável, obsoletos, compartilhados ou excessivos.
Conformidade com SLA de patches / vulnerabilidades	Percentual de vulnerabilidades materiais remediadas dentro do SLA definido com base em riscos.	Mensal	Segmentar por exposição e criticidade para o negócio.
Sucesso de testes de backup / recuperação	Serviços críticos com testes bem-sucedidos e evidenciados de restauração/failover.	Trimestral	Acompanhar testes com falha e dependências de recuperação não comprovadas.
Preparação para exercícios de incidentes / crises	Situação e encerramento de lições de exercícios de mesa ou recuperação.	Trimestral / Semestral	Escalonar achados não resolvidos e de alto impacto dos exercícios.
Taxa de encerramento da remediação	Itens encerrados e validados de forma independente em relação aos abertos no período.	Mensal	Monitorar crescimento do backlog e recorrência.
Saúde dos marcos de modernização	Marcos críticos do roteiro dentro do prazo, em risco ou atrasados.	Mensal	Vincular atrasos à exposição de risco e às decisões executivas.
Decisões executivas necessárias	Decisões em aberto sobre financiamento, aceitação de riscos, sequenciamento, fornecedores ou escopo.	Mensal	Manter registro de decisões com responsável e prazo.

7.2 Cadência de governança

Uma cadência prática de governança combina revisões mensais de remediação e transformação, revisões trimestrais de riscos executivos e comunicação periódica ao conselho ou a comitês do conselho, conforme o modelo de governança da instituição. Riscos críticos

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

não devem esperar por uma reunião agendada. O dashboard deve preservar o histórico das decisões, a aceitação aprovada de riscos, mudanças nas datas-alvo e a justificativa de decisões materiais de sequenciamento. Isso cria um vínculo auditável entre os achados da avaliação e a responsabilização executiva.

8. Roteiro de remediação e modernização

8.1 Princípios do roteiro

O roteiro converte os achados de risco e maturidade em ações sequenciadas. A ordem não deve ser determinada apenas pela maior pontuação numérica de risco. Algumas ações são pré-requisitos de outras: uma instituição pode precisar estabelecer propriedade das aplicações e mapeamento de dependências antes de racionalizá-las com segurança; pode precisar estabilizar a recuperação de backups antes de iniciar uma migração de infraestrutura de alto risco; e pode precisar de propriedade e classificação de dados antes de implementar análise avançada em escala.

Por esse motivo, o ARTTF utiliza três horizontes de planejamento. Os primeiros 0-90 dias enfatizam governança, evidências, redução urgente da exposição e ganhos rápidos. O horizonte de 3-12 meses institucionaliza controles e executa modernizações de complexidade média. O horizonte de 12-24 meses trata de transformação estrutural, grandes mudanças de plataforma, arquitetura de dados, engenharia de resiliência e melhoria contínua. O cronograma deve ser adaptado ao perfil de risco da instituição, capacidade de recursos, restrições dos fornecedores e compromissos regulatórios.

Tabela 10. Roteiro em fases de remediação e modernização

Horizonte	**Ações prioritárias**	**Entregáveis representativos**	**Resultado gerencial esperado**
0-90 dias - Estabilizar e estabelecer controle	Confirmar governança executiva e responsáveis; validar inventários de serviços críticos e tecnologia; identificar ativos críticos sem suporte; encerrar lacunas urgentes de acesso privilegiado e autenticação; validar backup/restauração de serviços críticos; classificar fornecedores materiais; criar registro unificado de problemas; estabelecer plano de encerramento regulatório e de auditoria; definir princípios decisórios do estado-alvo.	Regimento de governança; responsáveis/RACI; inventário crítico; registro dos principais riscos; ganhos rápidos validados; linha de base do dashboard executivo; plano de remediação de 90 dias.	Riscos desconhecidos ou sem responsável tornam-se visíveis; a exposição imediata é contida; os executivos passam a ter uma base factual comum.
3-12 meses - Institucionalizar e modernizar	Implementar arquitetura-alvo e ondas de modernização; formalizar governança de dados; fortalecer IAM/PAM e recertificação de acessos; melhorar práticas de vulnerabilidade e observabilidade; estabelecer governança de nuvem e fornecedores; testar BCP/DR e resposta a incidentes; melhorar ciclo de vida das políticas; automatizar evidências quando prático; executar remediações de alta prioridade.	Arquitetura-alvo; backlog de modernização; modelo operacional de governança de dados; monitoramento de fornecedores; evidências de recuperação testadas; controles melhorados; tendência mensurável de remediação.	Os controles tornam-se repetíveis e mensuráveis; a dívida técnica crítica e as lacunas de resiliência começam a diminuir.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

Horizonte	Ações prioritárias	Entregáveis representativos	Resultado gerencial esperado
12-24 meses - Transformar e otimizar	Executar grande modernização de legados/core; desacoplar integrações e fortalecer arquitetura de APIs/plataformas; modernizar arquitetura de dados; implementar engenharia de resiliência e testes de dependências; otimizar modelo operacional de nuvem; automatizar governança e reporte; preparar casos de análise avançada/IA sobre bases controladas; incorporar reavaliação contínua.	Plataformas modernizadas; arquitetura resiliente; melhores bases de dados; métricas contínuas; governança otimizada; reavaliação que demonstre melhoria da maturidade.	O risco estrutural é reduzido; modernização e resiliência se reforçam; a melhoria contínua é institucionalizada.

8.2 Regras de priorização e sequenciamento

1. Tratar exposições imediatas de segurança, clientes, regulamentação e serviços críticos antes do trabalho de otimização.

2. Estabelecer responsabilidades e evidências antes de utilizar pontuações de maturidade em decisões de investimento.

3. Resolver lacunas fundamentais de identidade, recuperação, inventário e dependências que possam comprometer a modernização posterior.

4. Sequenciar a modernização por capacidade de negócio e dependência, e não apenas pela idade da aplicação.

5. Utilizar contenção quando a substituição imediata for impraticável, mas definir um marco explícito de saída ou modernização.

6. Tratar dependências de fornecedores e nuvem como parte da arquitetura do serviço, incluindo planejamento de recuperação e saída.

7. Integrar compromissos de auditoria e regulatórios ao mesmo roteiro usado para a transformação tecnológica.

8. Exigir decisões executivas para riscos aceitos, prorrogações repetidas de prazo, reduções materiais de escopo e mudanças que afetem serviços críticos.

9. Reavaliar a maturidade e o risco residual após remediações materiais ou grandes ondas de modernização.

10. Preservar a rastreabilidade do achado ao risco, à ação, às evidências, à validação e ao encerramento.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

9. Aplicação ilustrativa

9.1 Instituição hipotética e escopo

O caso a seguir é fictício e fornecido exclusivamente para demonstrar a mecânica do framework. Não representa cliente, instituição financeira, avaliação ou conclusão regulatória reais.

O HarborView Community Bank (HCB) é modelado como um banco comunitário regional hipotético com aproximadamente US$ 3 bilhões em ativos, modelo operacional misto entre agências e canais digitais, várias centenas de empregados e dependência material de um provedor de core bancário, aplicações de clientes hospedadas em nuvem, fornecedores de pagamentos e serviços tecnológicos terceirizados. A gestão planeja um programa plurianual de modernização digital, mas acumulou problemas de auditoria em aberto, integrações ponto a ponto, propriedade de dados inconsistente e diversas relações de alta dependência com fornecedores. O escopo da avaliação abrange os seis domínios do ARTTF e se concentra em serviços críticos de depósitos, pagamentos, canais digitais, informações de clientes e relatórios financeiros.

9.2 Resultados ilustrativos de maturidade

Tabela 11. Resultados ilustrativos de maturidade do HCB

Domínio	Descrição	Pontuação	Interpretação ilustrativa
D1	Governança de tecnologia e responsabilização executiva	2,8	Existem fóruns de governança definidos, mas a atribuição de responsabilidades e os limites de KRIs são inconsistentes.
D2	Sistemas legados e arquitetura tecnológica	1,8	Vários componentes críticos estão envelhecendo; a arquitetura-alvo e o mapeamento de dependências estão incompletos.
D3	Governança de dados, identidade e gestão de acessos	2,2	Existem controles de acesso, mas propriedade dos dados, governança de acessos privilegiados e recertificação precisam ser fortalecidas.
D4	Nuvem, fornecedores e risco de terceiros	2,0	Os fornecedores materiais são conhecidos, mas concentração, planejamento de saída e monitoramento contínuo são inconsistentes.
D5	Cibersegurança, continuidade de negócios e recuperação	2,4	As operações de segurança estão estabelecidas, mas evidências de recuperação e testes de resiliência entre fornecedores estão incompletos.
D6	Auditabilidade, preparação regulatória e governança da remediação	2,6	Existe acompanhamento de problemas, mas achados vencidos e qualidade das evidências exigem governança executiva mais robusta.
Geral	Maturidade com pesos iguais	2,3	Classificação geral: Em desenvolvimento.

A pontuação geral ilustrativa de 2,3 indica que o HCB estabeleceu diversas práticas fundamentais, mas não possui institucionalização consistente em arquitetura, governança de

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

terceiros, gestão de dados e acessos e recuperação. A observação mais importante não é a média em si, mas o perfil desigual de maturidade. Um banco pode manter operações de cibersegurança relativamente maduras e ainda carregar risco material por meio de tecnologia sem suporte, planejamento fraco de saída de fornecedores ou dependências de recuperação não testadas.

9.3 Riscos prioritários ilustrativos

Tabela 12. Registro ilustrativo e priorização de riscos

ID	Risco	P	I	Prioridade-base / final	Justificativa do escalonamento	Tratamento imediato
R1	Middleware sem suporte que sustenta integrações críticas de pagamentos	4	5	20 - Crítica	Dependência conectada externamente, conhecimento interno limitado, serviço crítico de pagamentos.	Conter exposição; confirmar opções de fornecedor/suporte; acelerar plano de desacoplamento/substituição.
R2	Contas privilegiadas com recertificação incompleta e propriedade inconsistente	4	4	16 - Crítica	Alto privilégio e acesso a sistemas sensíveis; relevância para auditoria.	Recertificação emergencial; remover acessos obsoletos; implementar governança e monitoramento de PAM.
R3	A restauração de serviços críticos não foi demonstrada de ponta a ponta entre os principais fornecedores	3	5	15 - Crítica	Fragilidade de recuperação e dependência de terceiros.	Executar teste de restauração/failover; validar RTO/RPO e dependências de fornecedores; encerrar lacunas de evidências.
R4	Contrato de provedor material de nuvem não possui disposições suficientemente detalhadas de saída/transição	3	4	12 - Alta	Preocupações de concentração e substituibilidade.	Revisar contrato e plano de saída; definir requisitos de portabilidade de dados e transição.
R5	Achado de auditoria de alta gravidade ultrapassou a data-alvo após duas prorrogações	3	4	12 - Crítica (escalonada)	Fator de governança recorrente/vencido e compromisso de auditoria.	Escalonamento executivo; plano de recuperação; validação independente antes do encerramento.
R6	Elementos de dados críticos não possuem responsáveis e limites de qualidade formalmente atribuídos	3	3	9 - Moderada	Afeta confiabilidade dos relatórios e preparação para modernização/análise de dados.	Estabelecer propriedade e modelo operacional de qualidade dos dados no horizonte de 3-12 meses.

9.4 Visão ilustrativa do dashboard executivo

Tabela 13. Dashboard executivo ilustrativo

Indicador	Estado atual	Meta	Situação	Comentário executivo
Maturidade geral	2,3 - Em desenvolvimento	Meta 3,0 em 12 meses	Amarelo	Arquitetura e TPRM são os domínios mais baixos.
Riscos críticos	4	Meta ≤ 1 em 90 dias	Vermelho	R1, R2, R3 e R5 exigem acompanhamento executivo.
Riscos altos	1	Tendência de queda	Amarelo	R4: risco de saída da nuvem.
Remediação vencida	7 itens; 2 materiais	Nenhum item material vencido	Vermelho	R5 exige plano de recuperação e ação de governança.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

Indicador	Estado atual	Meta	Situação	Comentário executivo
Exposição crítica a legados	3 serviços críticos	Todos com plano financiado de modernização/contenção	Vermelho	Middleware de pagamentos é a prioridade máxima.
Terceiros de alto risco	6; 2 com problemas em aberto	Todos com monitoramento ativo e postura de saída	Amarelo	Exige revisão contratual e de concentração.
Exceções de acesso privilegiado	14	Zero exceção de alto risco sem responsável ou obsoleta	Vermelho	Recertificação imediata em andamento.
Testes de recuperação	3 de 5 serviços críticos testados de ponta a ponta	5 de 5	Amarelo	A restauração entre fornecedores deve ser concluída.
Marcos de modernização	2 em risco	Nenhum marco crítico sem decisão executiva	Amarelo	O mapeamento de dependências atrasa o sequenciamento da arquitetura.

9.5 Roteiro ilustrativo

Nos primeiros 90 dias, o HCB estabeleceria um único fórum executivo de remediação, validaria o inventário de serviços críticos, aplicações e fornecedores, concluiria a recertificação de acessos privilegiados, realizaria um teste completo de recuperação dos serviços de maior criticidade, estabeleceria um plano de recuperação para problemas de auditoria vencidos e definiria marcos de contenção e substituição para o middleware de pagamentos sem suporte. Essas ações reduziriam a exposição imediata e melhorariam a base de evidências para a modernização de prazo mais longo.

Durante os meses 3-12, o HCB executaria a primeira onda de modernização da arquitetura, formalizaria a propriedade dos dados e os limites de qualidade, melhoraria a gestão de acessos privilegiados, fortaleceria o monitoramento de nuvem e fornecedores, concluiria testes de continuidade de negócios e recuperação de desastres dos serviços críticos e racionalizaria os processos de gestão de problemas e evidências de controles. O objetivo seria alcançar o nível Definido em todos os domínios e estabelecer práticas Gerenciadas nas áreas de maior risco.

Durante os meses 12-24, o HCB continuaria desacoplando integrações legadas, implementaria a arquitetura-alvo de plataformas e dados, melhoraria a engenharia de resiliência e os testes de dependências, automatizaria determinadas evidências e relatórios de risco e estabeleceria um modelo operacional para análise de dados responsável e preparação para IA. Uma reavaliação formal compararia a maturidade dos domínios, o risco residual, problemas vencidos, evidências de recuperação e resultados da modernização com a linha de base original.

10. Discussão

A proposição central do ARTTF é que risco tecnológico e modernização tecnológica devem ser gerenciados por meio de uma perspectiva executiva comum. As instituições financeiras frequentemente organizam responsabilidades por funções especializadas — cibersegurança, infraestrutura, arquitetura, dados, gestão de fornecedores, conformidade, auditoria interna e execução de programas. A especialização é necessária, mas pode fragmentar a responsabilização quando a instituição precisa decidir quais ações de transformação são mais importantes. O framework cria um vocabulário compartilhado sem exigir que essas funções sejam reunidas em uma única equipe.

Uma segunda contribuição é a separação explícita entre maturidade e risco. A maturidade pergunta quão consistente e eficazmente uma capacidade está institucionalizada. O risco pergunta o que pode acontecer, qual a probabilidade, qual pode ser a gravidade do impacto e que contexto adicional altera a prioridade. Uma baixa pontuação de maturidade pode não gerar risco alto imediato quando o processo atende a um serviço de baixa criticidade e exposição limitada. De forma inversa, uma organização geralmente madura ainda pode ter uma única vulnerabilidade crítica ou dependência de recuperação não testada que exija ação imediata. Tratar maturidade e risco como conceitos separados, porém conectados, ajuda a evitar interpretações simplistas.

Uma terceira contribuição é o uso da confiança das evidências. As avaliações de tecnologia dependem frequentemente de entrevistas com líderes que compreendem os processos pretendidos, mas podem não perceber exceções locais. Registrar a confiança das evidências torna a incerteza visível e direciona testes de acompanhamento. Também sustenta reavaliações mais confiáveis, porque as melhorias podem ser avaliadas por meio de evidências operacionais, e não apenas por mudanças de percepção.

O framework também enfatiza a relação entre modernização e resiliência operacional. A modernização pode reduzir riscos ao eliminar sistemas sem suporte, reduzir processos manuais, melhorar observabilidade, fortalecer identidade e simplificar integrações. Também pode aumentar riscos quando a migração introduz novas dependências, enfraquece o design de recuperação, cria concentração ou altera responsabilidades operacionais mais rapidamente do que a governança consegue se adaptar. Por isso, um roteiro baseado em riscos trata a resiliência como requisito de design da modernização, e não como controle posterior à implementação.

Para instituições de pequeno e médio porte, a proporcionalidade é especialmente importante. O objetivo não é reproduzir o modelo de pessoal, documentação ou ferramentas de um grande banco global. É demonstrar que a governança e os controles são adequados ao porte, complexidade, produtos, dados, dependência tecnológica e perfil de risco da instituição. A mesma pergunta diagnóstica pode, portanto, levar a expectativas de evidências diferentes em um banco comunitário, uma plataforma fintech e uma grande empresa de pagamentos.

O framework também pode apoiar a transferência de conhecimento. Como os domínios, perguntas, definições de pontuação, abordagem de mapa de calor, medidas do dashboard e horizontes do roteiro estão documentados, equipes internas podem reutilizar o método em reavaliações periódicas, governança de projetos, revisões de fornecedores e planejamento executivo. Essa repetibilidade pode reduzir a dependência de avaliações pontuais e ajudar as instituições a desenvolver capacidade interna de gestão de riscos tecnológicos.

11. Limitações e pesquisas futuras

O ARTTF possui várias limitações. Primeiro, o artigo atual apresenta uma metodologia conceitual e aplicada, e não um modelo preditivo empiricamente validado. A escala de cinco níveis e as perguntas diagnósticas ainda não foram testadas quanto à confiabilidade estatística em uma população representativa de instituições financeiras. Segundo, a pontuação qualitativa de riscos depende do julgamento do avaliador. Embora os requisitos de evidências e os fatores de escalonamento reduzam a subjetividade, diferentes avaliadores ainda podem chegar a pontuações distintas. Terceiro, as obrigações jurídicas e regulatórias específicas de cada instituição variam conforme licença, regulador, produto, geografia, dados e atividade; um framework generalizado não pode substituir análise jurídica, de conformidade ou de supervisão sob medida.

Quarto, o framework utiliza deliberadamente um conjunto compacto de 30 perguntas. Isso favorece a usabilidade executiva, mas significa que um trabalho completo deve desdobrar as perguntas em procedimentos detalhados e testes de evidências. Quinto, o risco tecnológico muda rapidamente. Condições de ameaças, expectativas regulatórias, arquiteturas de nuvem, casos de uso de IA, dependências de fornecedores e produtos evoluem; por isso, os critérios diagnósticos devem ser revisados periodicamente e submetidos a controle de versão.

Pesquisas futuras devem avaliar o framework por meio de múltiplos estudos de caso em bancos comunitários, cooperativas de crédito, empresas fintech e organizações de

pagamentos. Questões úteis incluem consistência entre avaliadores, relação entre melhorias de maturidade e encerramento de problemas, efeito da confiança das evidências na precisão da pontuação, valor de diferentes pesos dos domínios e se o sequenciamento do roteiro melhora o tempo do ciclo de remediação ou reduz achados recorrentes. Trabalhos futuros também podem desenvolver extensões específicas para processamento de pagamentos, Banking-as-a-Service, gestão patrimonial e adoção responsável de IA.

12. Considerações finais

Organizações financeiras reguladas precisam se modernizar preservando controle, segurança, auditabilidade e continuidade. Esses objetivos costumam ser gerenciados em programas separados, embora as dependências tecnológicas subjacentes sejam compartilhadas. O Agility Regulated Technology Transformation Framework oferece um método integrado para conectar essas preocupações por meio de seis domínios, um modelo de maturidade de cinco níveis, um diagnóstico de 30 perguntas, priorização de riscos, comunicação executiva e planejamento da transformação em fases.

O framework é intencionalmente prático. Começa com alinhamento executivo e evidências, distingue maturidade de risco e termina com um roteiro que atribui responsabilidades e sequenciamento. O caso ilustrativo mostra como uma instituição pode passar de observações fragmentadas a uma visão consolidada dos riscos tecnológicos e prioridades de modernização. O resultado mais importante não é uma pontuação numérica de maturidade, mas uma narrativa gerencial defensável que explique o que é material, por que é importante, quem é responsável, quais evidências sustentam a conclusão e qual ação deve ocorrer em seguida.

Quando utilizada de forma adequada, a metodologia pode apoiar preparação regulatória, remediação de auditorias, modernização de sistemas, governança de dados e acessos, supervisão de terceiros, cibersegurança e resiliência operacional. Foi concebida para complementar — e não substituir — frameworks reconhecidos e orientações de supervisão. Seu valor reside em traduzir esses princípios em um processo executivo repetível para priorizar e governar a transformação tecnológica em ambientes financeiros regulados.

13. Declarações

Conflito de interesses: o autor é fundador e proprietário da Agility Digital Technologies, LLC., e desenvolveu o framework descrito neste artigo. Essa afiliação é declarada porque o framework leva o nome da empresa.

Financiamento: nenhum financiamento externo foi recebido para a elaboração deste artigo metodológico.

Declaração de ética: este artigo não envolve participantes humanos, animais ou dados confidenciais de clientes. O caso ilustrativo é inteiramente hipotético.

Disponibilidade de dados: nenhum conjunto de dados empíricos foi criado ou analisado. Todos os dados e pontuações de casos apresentados para demonstração são hipotéticos.

14. Referências

Cox, L. A., Jr. (2008). What's wrong with risk matrices? Risk Analysis, 28(2), 497-512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, & Office of the Comptroller of the Currency. (2023). Interagency guidance on third-party relationships: Risk management. https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html

Federal Financial Institutions Examination Council. (2019). Business Continuity Management booklet. FFIEC Information Technology Examination Handbook. https://www.ffiec.gov/news/press-releases/2019/pr-11-14

Federal Financial Institutions Examination Council. (2021a). Architecture, Infrastructure, and Operations booklet. FFIEC Information Technology Examination Handbook. https://www.ffiec.gov/news/press-releases/2021/pr-06-30

Federal Financial Institutions Examination Council. (2021b). Authentication and Access to Financial Institution Services and Systems guidance. https://www.ffiec.gov/news/press-releases/2021/pr-08-11

Financial Stability Board. (2024). The financial stability implications of artificial intelligence. https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105. https://aisel.aisnet.org/misq/vol28/iss1/6/

Khatri, V., & Brown, C. V. (2010). Designing data governance. Communications of the ACM, 53(1), 148-152. https://doi.org/10.1145/1629175.1629210

National Credit Union Administration. (2026). 2025 cybersecurity and credit union system resilience report. https://ncua.gov/news/publication-search/cybersecurity/2025-cybersecurity-and-credit-union-system-resilience-report

Office of the Comptroller of the Currency. (2026). 2026 cybersecurity and financial system resilience report. https://www.occ.treas.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/index-cybersecurity-and-financial-system-resilience-report.html

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Quinn, S., Pascoe, C., Barrett, M., Scarfone, K., & Witte, G. (2024). NIST Cybersecurity Framework 2.0: Quick-start guide for using the CSF Tiers (NIST SP 1302). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1302

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

U.S. Department of the Treasury. (2024a, December 19). Treasury releases report on the uses, opportunities, and risks of artificial intelligence in financial services. https://home.treasury.gov/news/press-releases/jy2760

U.S. Department of the Treasury. (2024b, July 17). Treasury and the Financial Services Sector Coordinating Council publish new resources on effective practices for secure cloud adoption. https://home.treasury.gov/news/press-releases/jy2467

U.S. Department of the Treasury. (2026, February 19). Treasury releases two new resources to guide AI use in the financial sector. https://home.treasury.gov/news/press-releases/sb0401

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003