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

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

A modernização de sistemas legados e a governança de ti em instituições financeiras: uma análise sobre automação de processos (RPA) e compliance digital

Legacy systems modernization and it governance in financial institutions: an analysis on robotic process automation (RPA) and digital compliance

Vinicius Pereira Lensyk - Tecnólogo em Processos Gerenciais pelo Centro Universitário Internacional (UNINTER). Especialista em Análise de Sistemas, Governança de TI e Modelagem de Processos de Negócios em Ambientes Financeiros.

Resumo

A perenidade das instituições financeiras na era da economia digital depende intrinsecamente da capacidade de superar a obsolescência tecnológica sem comprometer a integridade dos dados e a conformidade regulatória. O presente artigo científico propõe uma investigação exaustiva e multidisciplinar sobre os desafios da modernização de sistemas legados em ambientes bancários, focando na aplicação de *Robotic Process Automation* (RPA) e na estruturação de frameworks de governança de TI. A metodologia adotada fundamenta-se em uma revisão narrativa de literatura, correlacionando os postulados de reengenharia de processos de Hammer (1990) com as diretrizes de governança do COBIT 2019 e as normas de segurança da informação da família ISO 27000. O estudo estrutura-se em cinco eixos temáticos de alta densidade, dissecando desde a arquitetura de sistemas legados e seus riscos operacionais, a implementação estratégica de RPA para eficiência, a gestão de *compliance* digital e proteção de dados, a integração de sistemas via APIs e microsserviços, até o alinhamento estratégico entre Negócios e Tecnologia (*Strategic Business-IT Alignment*). Os resultados teóricos demonstram que a modernização não é apenas uma atualização de *software*, mas uma reestruturação de processos que, quando bem governada, reduz custos operacionais (OPEX) e mitiga riscos sistêmicos. Conclui-se que o analista de negócios atua como o arquiteto dessa transformação, garantindo que a inovação tecnológica esteja subordinada aos objetivos estratégicos e regulatórios da instituição.

Palavras-chave: Governança de TI. Sistemas Legados. RPA. Compliance Digital. Processos Gerenciais.

Abstract

The longevity of financial institutions in the digital economy era intrinsically depends on the ability to overcome technological obsolescence without compromising data integrity and regulatory compliance. This scientific article proposes an exhaustive and multidisciplinary investigation into the challenges of modernizing legacy systems in banking environments, focusing on the application of Robotic Process Automation (RPA) and the structuring of IT governance frameworks. The adopted methodology is based on a narrative literature review, correlating Hammer's process reengineering postulates (1990) with COBIT 2019 governance guidelines and the ISO 27000 family information security standards. The study is structured into five high-density thematic axes, dissecting everything from the architecture of legacy systems and their operational risks, the strategic implementation of RPA for efficiency, digital compliance management and data protection, system integration via APIs and microservices, to the Strategic Business-IT Alignment. The theoretical results demonstrate that modernization is not merely a software update, but a restructuring of processes that, when well-governed, reduces operational costs (OPEX) and mitigates systemic risks. It is concluded that the business analyst acts as the architect of this transformation, ensuring that technological innovation remains subordinate to the institution's strategic and regulatory objectives.

Keywords: IT Governance. Legacy Systems. RPA. Digital Compliance. Managerial Processes.

1. Introdução

A arquitetura tecnológica que sustenta o sistema financeiro global enfrenta, no século XXI, um paradoxo estrutural de proporções críticas e sistêmicas: a necessidade premente, vital e inadiável

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

de inovação ágil para atender às demandas voláteis de um consumidor digitalizado colide frontalmente com a rigidez, a complexidade hermética e a obsolescência funcional dos sistemas legados (*mainframes*) que ainda processam a maioria esmagadora das transações bancárias mundiais. Nesse cenário de dicotomia profunda entre a arquitetura estática do legado e a funcionalidade fluida do novo, a Gestão de Processos Gerenciais e a Análise de Sistemas e Negócios emergem não como funções de suporte periférico, mas como disciplinas nucleares e estratégicas para a sobrevivência institucional em um mercado darwiniano. A literatura acadêmica especializada, ancorada em autores seminais como Laudon & Laudon (2014) e Weill & Ross (2004), aponta de forma contundente que a simples sobreposição de interfaces digitais modernas sobre núcleos de processamento arcaicos cria um débito técnico insustentável, resultando em vulnerabilidades de segurança cibernética, ineficiência operacional crônica e incapacidade de adaptação regulatória ágil. Portanto, a investigação científica rigorosa sobre metodologias que permitam uma transição segura, governada, auditável e eficiente desses ambientes complexos torna-se uma pauta de relevância acadêmica e pragmática urgente para a engenharia de software e a administração moderna de recursos tecnológicos.

O problema central que norteia esta extensa, detalhada e profunda análise teórica reside na complexidade técnica de modernizar infraestruturas críticas de processamento financeiro sem interromper a continuidade dos negócios (*business continuity*) e sem violar os rigorosos, punitivos e complexos marcos regulatórios impostos por entidades governamentais, bancos centrais e normas internacionais de *compliance* financeiro. A hipótese central defendida e dissecada neste estudo é que a adoção estratégica de tecnologias de automação, especificamente o *Robotic Process Automation* (RPA), aliada a um framework robusto, documentado e disciplinado de Governança de TI (como o COBIT e os frameworks complementares ITIL e CMMI), oferece o caminho mais seguro e viável para a modernização incremental e sustentável. A estruturação deste artigo visa dissecar minuciosamente os mecanismos técnicos e gerenciais pelos quais a análise de negócios identifica gargalos em processos manuais repetitivos, propõe a automação inteligente e garante a integridade matemática dos dados na migração de sistemas monolíticos para arquiteturas distribuídas. Ao longo das próximas seções, será demonstrado com rigor acadêmico e metodológico como a aplicação técnica de conceitos de modelagem de processos (BPMN), segurança da informação em profundidade e arquitetura de microsserviços permite que as instituições financeiras transcendam as limitações físicas do legado, transformando a TI de um centro de custos passivo em um vetor de vantagem competitiva sustentável, auditável e resiliente.

2. Arquitetura de sistemas legados e a gestão do risco operacional

A persistência resiliente e problemática de sistemas legados no setor financeiro não é um acidente histórico, mas fruto de décadas de investimento maciço em plataformas robustas, geralmente

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

baseadas em linguagens como COBOL e outras tecnologias legadas, que oferecem uma estabilidade transacional e uma consistência de dados inigualável, porém, a um custo de manutenção, integração e evolução cada vez mais proibitivo e arriscado. A análise profunda, técnica e estrutural dessa arquitetura revela um monolito gigantesco de dados e regras de negócios entrelaçados de forma inextricável, onde a modificação de uma simples rotina de cálculo de juros compostos ou de taxas bancárias pode desencadear falhas catastróficas em cascata em módulos críticos de contabilidade, relatórios regulatórios federais e interfaces de atendimento ao cliente final. O risco operacional inerente e crescente a esses sistemas reside na escassez demográfica de mão de obra qualificada para mantê-los e na existência de uma "caixa preta" de regras de negócios que, muitas vezes, não estão documentadas em manuais, residindo apenas no código-fonte compilado há décadas e na memória tácita de colaboradores em vias de aposentadoria. A gestão de processos, nesse contexto, deve iniciar-se obrigatoriamente por um trabalho arqueológico de software e engenharia reversa, mapeando os fluxos de dados e as dependências lógicas antes de qualquer tentativa de migração ou refatoração.

O impacto negativo desses sistemas rígidos na agilidade de negócios é severo e mensurável; o indicador de *Time-to-Market* de novos produtos financeiros é drasticamente ampliado e prejudicado pela necessidade de testes de regressão manuais e exaustivos e pela dificuldade técnica de expor funcionalidades antigas através de interfaces modernas de APIs RESTful ou SOAP. Além disso, a segurança da informação em sistemas legados é frequentemente baseada em paradigmas perimetrais obsoletos, fundamentados na premissa falha de que a rede interna é segura e confiável, um paradigma que falha catastroficamente diante das ameaças persistentes avançadas (APTs), ransomwares modernos e da necessidade imperativa de abertura de dados via *Open Banking*. A modernização, portanto, não é apenas uma questão de eficiência econômica, mas de mitigação urgente de riscos cibernéticos e operacionais que podem levar à insolvência ou à intervenção regulatória. A literatura de engenharia de software, notadamente Pressman (2016), sugere que a estratégia de encapsulamento, onde o sistema legado é mantido como *backend* estável enquanto suas funções são expostas via camadas de abstração, é uma etapa intermediária válida, mas que não resolve o problema da dívida técnica subjacente e da escalabilidade horizontal necessária para picos de processamento na era digital.

A governança desses ambientes híbridos e complexos (legado + moderno) exige um controle rigoroso e disciplinado sobre o ciclo de vida das aplicações (ALM) e uma gestão de configuração de software impecável para evitar a divergência de versões e a perda de integridade dos ambientes de produção. O analista de negócios e sistemas deve atuar como o tradutor bilíngue entre as limitações técnicas do *mainframe* hostil e as exigências de experiência do usuário (*UX*) fluida das plataformas digitais móveis e web. A aplicação de frameworks internacionais de gestão de risco, como a ISO 31000, permite quantificar matematicamente o impacto financeiro e reputacional de falhas nesses

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

sistemas, justificando perante os conselhos de administração os investimentos massivos de capital (*CAPEX*) necessários para a sua substituição ou atualização gradual. A estratégia de "estrangulamento" (*Strangler Pattern*), conceituada por Fowler (2004), onde novas funcionalidades são construídas exclusivamente em novas plataformas modulares enquanto o sistema antigo é paulatinamente desativado função por função, apresenta-se como a metodologia mais segura e recomendada, exigindo, contudo, uma disciplina de gestão de projetos ferrenha e uma visão arquitetural de longo prazo que muitas organizações lutam para manter.

A documentação exaustiva e padronizada de processos (BPM) é a ferramenta fundamental e inegociável para mitigar o risco do conhecimento tácito não documentado que reside nas equipes de TI antigas. Em muitas instituições financeiras tradicionais, as regras de negócio vitais estão "na cabeça" de funcionários antigos ou "hardcoded" de forma obscura no sistema, sem documentação funcional associada. O levantamento detalhado e a modelagem gráfica desses processos em notação padrão internacional (BPMN) permitem que a organização retome o controle intelectual sobre suas operações, identificando redundâncias, gargalos de performance e oportunidades de otimização antes da automação ou migração. Sem esse mapeamento exaustivo e analítico, a tentativa de modernização corre o risco gravíssimo de apenas "automatizar o caos", perpetuando ineficiências processuais em uma plataforma tecnológica mais cara e complexa. A análise de negócios, portanto, precede a tecnologia; ela é a garantia lógica de que a nova arquitetura sistêmica refletirá as necessidades reais e atuais da instituição e não apenas as capacidades limitadas da ferramenta de software adquirida.

Por fim, a gestão do risco operacional em sistemas legados envolve também o planejamento estratégico de continuidade de negócios e recuperação de desastres (BCP/DR) em cenários de catástrofe tecnológica ou física. A dependência de hardware proprietário, obsoleto e sem suporte do fabricante cria um ponto único de falha (*Single Point of Failure*) que pode paralisar operações bancárias nacionais e gerar caos sistêmico. A migração planejada para infraestruturas de nuvem (*Cloud Computing*) pública, privada ou híbrida, embora complexa devido a questões de latência de rede e soberania de dados sensíveis, oferece uma resiliência elástica e uma redundância geográfica impossíveis de replicar em *data centers* locais tradicionais com custos viáveis. O papel da governança de TI é orquestrar essa transição delicada, garantindo que os níveis de serviço (SLA) acordados sejam mantidos e que a integridade transacional ACID (Atomicidade, Consistência, Isolamento e Durabilidade) — o ativo mais valioso de um banco — seja preservada intacta em cada etapa do processo de modernização tecnológica.

3. Robotic process automation (RPA) como vetor de eficiência e auditoria

A tecnologia disruptiva de *Robotic Process Automation* (RPA) emergiu no cenário corporativo global como uma solução tática de alto impacto e baixo atrito para preencher a lacuna

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

operacional entre os sistemas legados herméticos e a necessidade de processos digitais ágeis e integrados, atuando na camada de interface do usuário para automatizar tarefas repetitivas, baseadas em regras lógicas e de alto volume transacional. Diferente da integração tradicional via *backend*, que exige o desenvolvimento complexo, demorado e arriscado de APIs e alterações profundas no código-fonte legado, o RPA simula a ação humana no computador, interagindo com múltiplas aplicações heterogêneas (ERP, planilhas, sites web, terminais 3270, emuladores) de forma não invasiva e superficial. Para instituições financeiras, isso representa a capacidade revolucionária de automatizar processos críticos de *backoffice* — como conciliação bancária massiva, cadastro e validação de clientes, processamento de empréstimos consignados e geração de relatórios regulatórios complexos — com uma velocidade, consistência e precisão inalcançáveis pela força de trabalho humana, liberando o precioso capital intelectual dos colaboradores para atividades de análise, estratégia e relacionamento.

A implementação estratégica de RPA, contudo, exige uma análise de processos rigorosa, crítica e saneadora para evitar a perigosa automação de ineficiências pré-existentes. O princípio fundamental de "otimizar e padronizar antes de automatizar" é mandatório para o sucesso do projeto. O analista de negócios deve decompor o processo alvo em suas tarefas elementares, identificar as regras de decisão lógica binária e tratar as exceções de negócio antes de codificar o robô. A literatura especializada de Willcocks e Lacity (2016), corroborada por estudos sobre aplicações financeiras (Moffitt et al., 2018), destaca que o sucesso sustentável do RPA depende menos da tecnologia de automação em si e mais da governança corporativa sobre o que é automatizado e como é mantido. Robôs mal desenhados ou sem tratamento de erros podem replicar falhas em escala industrial ou falhar silenciosamente diante de pequenas alterações nas interfaces gráficas dos sistemas legados, criando um passivo operacional oculto gigantesco. Portanto, a criação de um Centro de Excelência (CoE) em RPA é vital para padronizar o desenvolvimento, monitorar a execução dos robôs em tempo real e gerenciar a manutenção do ciclo de vida das automações.

Além da eficiência operacional e redução de custos, o RPA desempenha um papel crucial e muitas vezes subestimado na auditoria interna e no *compliance* regulatório. Cada ação executada pelo robô digital é registrada em *logs* detalhados e timestamped, criando uma trilha de auditoria imutável, granular e 100% rastreável para fins de fiscalização. Em processos sensíveis e de alto risco, como a verificação de listas de sanções internacionais (OFAC), a prevenção à lavagem de dinheiro (AML) ou a validação de documentos para abertura de contas (*KYC - Know Your Customer*), a precisão algorítmica e determinística do robô elimina o erro humano por fadiga e o risco de fraude interna ou conluio. A automação garante matematicamente que a política de *compliance* seja executada estritamente conforme desenhada e aprovada, sem desvios subjetivos ou omissões operacionais, proporcionando uma segurança jurídica robusta para a instituição financeira diante de reguladores

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

estatais e auditores externos independentes.

A escalabilidade elástica da força de trabalho digital proporcionada pelo RPA permite que as instituições lidem com picos de demanda sazonal ou eventos de mercado imprevistos sem a necessidade de contratação e treinamento oneroso de força de trabalho temporária. Robôs de software podem trabalhar 24 horas por dia, 7 dias por semana, 365 dias por ano, sem pausas, férias ou encargos trabalhistas, aumentando drasticamente a capacidade de processamento (vazão) e a disponibilidade da organização. No entanto, a gestão dessa força de trabalho digital híbrida exige novas competências de TI e Negócios. É necessário monitorar a "saúde" e o desempenho dos robôs, gerenciar as credenciais de acesso e segredos (segurança de cofres de senhas) e orquestrar a fila de trabalho para garantir que os processos mais críticos e sensíveis ao tempo tenham prioridade de execução sobre rotinas de menor valor. A análise de sistemas deve evoluir para compreender as interdependências complexas entre os bots, os dados e os sistemas subjacentes, evitando que atualizações de software de terceiros quebrem as automações em produção.

A integração avançada do RPA com tecnologias cognitivas emergentes, como Reconhecimento Óptico de Caracteres (OCR) inteligente, Processamento de Linguagem Natural (NLP) e Inteligência Artificial (IA), expande o escopo da automação para processos que envolvem dados não estruturados e decisões probabilísticas, como a leitura e interpretação de contratos jurídicos, e-mails de clientes e imagens de documentos. Essa evolução, denominada *Intelligent Automation* (IA) ou Hiperautomação, permite que o sistema tome decisões baseadas em aprendizado de máquina supervisionado, encaminhando para análise humana apenas as exceções complexas ou ambíguas. Essa simbiose entre máquina e humano maximiza a eficiência operacional e eleva o nível de serviço ao cliente (SLA), permitindo respostas mais rápidas, precisas e personalizadas. O papel do gestor de processos é identificar estrategicamente as oportunidades onde essa inteligência híbrida pode gerar maior valor agregado e vantagem competitiva.

Por fim, a análise financeira do retorno sobre o investimento (ROI) em projetos de RPA deve considerar não apenas a redução de *Full-Time Equivalent* (FTE) e custos de folha de pagamento, mas também a mitigação de riscos operacionais, a melhoria da qualidade dos dados mestres e a velocidade de execução (*throughput*). Projetos de automação bem-sucedidos e bem governados frequentemente se pagam em menos de 12 meses, mas exigem um investimento contínuo em governança, infraestrutura e manutenção evolutiva. A tecnologia não é "instalar e esquecer"; é uma capacidade organizacional dinâmica que deve ser gerida como um ativo estratégico de longo prazo. A convergência harmoniosa entre a análise de processos de negócios, a engenharia de automação e a estratégia corporativa é o fator crítico que determina se o RPA será uma solução tática paliativa de curto prazo ou uma transformação estratégica estruturante de longo prazo para a instituição financeira.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

4. Governança de TI, proteção de dados e compliance digital

A governança de Tecnologia da Informação (TI) em instituições financeiras modernas transcende a mera gestão técnica de infraestrutura e suporte para se tornar um pilar central e indissociável da governança corporativa, essencial para assegurar que os vultosos investimentos em tecnologia gerem valor tangível e que os riscos cibernéticos e operacionais associados sejam mitigados a níveis aceitáveis. O framework internacional COBIT 2019 estabelece que a governança deve alinhar estrategicamente a TI aos objetivos de negócio, garantindo a entrega de benefícios, a otimização de riscos e recursos, e a transparência para as partes interessadas. Em um ambiente de transformação digital acelerada, onde dados são o ativo mais valioso e vulnerável, a governança de dados torna-se crítica e mandatória. É imperativo estabelecer políticas institucionais claras e auditáveis sobre a propriedade, a qualidade, a acessibilidade, a retenção e a segurança dos dados ao longo de todo o seu ciclo de vida, desde a captura na origem até o arquivamento legal ou descarte seguro e certificado.

A conformidade estrita com legislações de proteção de dados e privacidade, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e a GDPR na Europa, impõe requisitos técnicos, jurídicos e processuais severos aos bancos e fintechs. O conceito de *Privacy by Design* exige que a privacidade e a segurança sejam incorporadas à arquitetura dos sistemas e processos desde a sua concepção inicial, e não como um adendo posterior ou camada superficial. Isso implica na implementação técnica de mecanismos avançados de anonimização e pseudo anonimização de dados, controle de acesso granular baseado em funções e necessidades (RBAC/ABAC) e criptografia robusta de dados em repouso (bancos de dados, backups) e em trânsito (redes, APIs). O analista de sistemas e negócios deve ter a competência de traduzir esses requisitos legais complexos em especificações técnicas funcionais e regras de negócio sistêmicas, garantindo que o software não apenas funcione, mas que opere rigorosamente dentro dos limites da legalidade, respeitando o consentimento e os direitos do titular dos dados.

O *Compliance* Digital em instituições financeiras envolve também a aderência mandatória a normas setoriais específicas e rigorosas, como as resoluções do Banco Central e do Conselho Monetário Nacional sobre segurança cibernética, terceirização de serviços e computação em nuvem. A instituição deve demonstrar capacidade comprovada de monitoramento contínuo de ameaças cibernéticas, gestão proativa de vulnerabilidades de software e hardware, e planos testados de resposta a incidentes de segurança. A implementação de um Centro de Operações de Segurança (SOC) operando 24/7 e o uso de ferramentas de SIEM (*Security Information and Event Management*) correlacionando eventos são mandatórios para detectar e responder a ataques em tempo real antes que se tornem violações de dados. A governança de TI deve assegurar que esses controles de segurança não sufoquem a agilidade e a inovação do negócio, buscando um equilíbrio dinâmico e inteligente

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

entre proteção e usabilidade, onde a segurança é vista como um habilitador de negócios digitais confiáveis e perenes.

A gestão de identidades e acessos (IAM - *Identity and Access Management*) é um componente crítico e fundamental da segurança em sistemas modernos distribuídos e legados centralizados. Com a proliferação de canais digitais, APIs abertas e o trabalho remoto híbrido, garantir inequivocamente que "quem é quem" e "quem pode fazer o quê" é um desafio técnico e processual complexo. A implementação de autenticação multifator (MFA) adaptativa e a gestão automatizada do ciclo de vida da identidade (admissão, movimentação de cargo e desligamento de colaboradores) devem ser auditadas rigorosamente para evitar contas órfãs e privilégios excessivos. Falhas nesse processo são a principal porta de entrada para fraudes internas, vazamento de dados e ataques de engenharia social. A governança deve estabelecer políticas de revisão periódica de acessos (recertificação), garantindo o princípio do menor privilégio (*Least Privilege*), onde cada usuário ou sistema tem acesso apenas ao estritamente necessário para o desempenho de sua função.

A auditoria de sistemas, independente e regular, é a linha de defesa final que válida a eficácia e a aderência da governança de TI. Auditores internos e externos examinam minuciosamente os controles gerais de TI (ITGC), a segurança física e lógica, e os controles de aplicativos para certificar a integridade, disponibilidade e confidencialidade das demonstrações financeiras e a conformidade regulatória. A automação de controles internos e a geração automática de evidências de auditoria reduzem significativamente o custo, o tempo e a fricção desses processos de verificação. O analista de negócios deve projetar sistemas e processos que sejam "auditáveis por padrão" (*audit by design*), com logs detalhados, trilhas de auditoria protegidas e rastreabilidade total das transações financeiras e administrativas. A transparência e a *accountability* proporcionadas por uma boa governança aumentam a confiança dos investidores, reguladores e clientes, reduzindo o custo de capital e o risco reputacional da instituição.

Conclui-se, neste eixo temático, que a governança de TI e a segurança da informação não são barreiras burocráticas à inovação, mas seus alicerces estruturais indispensáveis. Sem uma estrutura de controle robusta, madura e integrada, a velocidade da transformação digital pode levar a instituição financeira a um colapso operacional, financeiro ou reputacional irreversível. A integração cultural e processual entre as áreas de risco, *compliance*, segurança da informação, jurídico e desenvolvimento de sistemas (DevSecOps), alinhada aos princípios de Kim et al. (2016), é fundamental para criar uma cultura organizacional de responsabilidade compartilhada, onde a segurança e a conformidade são responsabilidade intrínseca de todos, desde o desenvolvedor de código júnior até o diretor executivo (CEO), garantindo a resiliência institucional frente às ameaças do século XXI.

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

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

5. Alinhamento estratégico de negócios e TI e a arquitetura de micros serviços

O Alinhamento Estratégico entre Negócios e Tecnologia da Informação (*Strategic Business-IT Alignment*) é considerado o "Santo Graal" da gestão corporativa moderna, referindo-se ao grau de harmonia e integração em que a missão, objetivos e planos da TI suportam, impulsionam e são suportados pela missão, objetivos e planos estratégicos do negócio. Em instituições financeiras, onde o produto comercializado é essencialmente digital (bits e bytes representando valor monetário e contratual), esse alinhamento não é opcional, mas existencial. A falta de sincronia entre as áreas resulta no fenômeno da "Shadow IT" (áreas de negócio contratando soluções tecnológicas à revelia da TI oficial), desperdício massivo de recursos financeiros em projetos que não geram valor agregado e perda irrecuperável de oportunidades de mercado por lentidão tecnológica (*Time-to-Market* elevado). O papel do Analista de Negócios Sênior e do Gestor de Processos é atuar como o elo de ligação diplomático e técnico (*liaison*), traduzindo a estratégia corporativa abstrata em um *roadmap* tecnológico concreto e garantindo que a TI seja proativa e inovadora na proposição de soluções que habilitem novos modelos de negócio.

A transição da arquitetura monolítica, rígida e acoplada dos sistemas legados para uma arquitetura moderna, flexível e desacoplada baseada em microsserviços é a manifestação técnica mais evidente desse alinhamento estratégico em busca de agilidade e escalabilidade. Microsserviços permitem que funcionalidades bancárias específicas (ex: consulta de saldo, transferência PIX, cálculo de score de crédito, emissão de boleto) sejam desenvolvidas, implantadas, atualizadas e escaladas de forma independente, sem afetar o restante do ecossistema. Isso confere uma flexibilidade tática enorme ao negócio, permitindo lançar novas *features* e correções em dias ou semanas, ao invés dos ciclos de meses típicos dos *mainframes*. A adoção de APIs (*Application Programming Interfaces*) padronizadas e seguras facilita a integração fluida com parceiros externos, startups e fintechs, viabilizando o modelo de negócios de *Banking as a Service* (BaaS) e a participação ativa no ecossistema competitivo do *Open Finance*.

A gestão e orquestração dessa arquitetura distribuída e granular, no entanto, introduz uma complexidade operacional e de monitoramento significativa que não existia no mundo monolítico. A orquestração de contêineres (ex: Kubernetes), a gestão da malha de serviços (*Service Mesh*), conforme abordada por Calcote e Butcher (2019), e a observabilidade distribuída (logs, métricas e rastreamento) tornam-se competências técnicas essenciais para a equipe de infraestrutura e operações. O alinhamento estratégico exige que a decisão de quebrar um monolito em microsserviços seja baseada estritamente em domínios de negócio (DDD - *Domain-Driven Design*), proposto por Evans (2003), e não apenas em preferências técnicas ou modismos tecnológicos. O analista deve mapear com precisão os contextos delimitados (*Bounded Contexts*) do negócio para garantir que a fronteira dos serviços de software reflita fielmente a realidade operacional e a linguagem onipresente da

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

organização, evitando o acoplamento excessivo que anularia os benefícios de agilidade da modularização.

A cultura DevOps e a adoção de metodologias ágeis de desenvolvimento (Scrum, Kanban, SAFe) são os processos organizacionais que operacionalizam esse alinhamento no dia a dia das equipes de produto. A aproximação colaborativa e contínua entre as equipes de desenvolvimento (Dev) e operações (Ops), aliada a ciclos curtos de entrega (sprints) e feedback contínuo do cliente final, garante que o produto de software evolua em sintonia fina com as necessidades reais e mutáveis do mercado. A gestão de portfólio de projetos de TI deve priorizar iniciativas baseadas em valor de negócio mensurável e auditável (*Business Value*), utilizando métricas financeiras como Valor Presente Líquido (VPL), Retorno sobre Investimento (ROI) e Custo do Atraso (*Cost of Delay*) para decidir onde alocar o capital. O alinhamento não é um estado estático a ser atingido uma única vez, mas um processo dinâmico, iterativo e contínuo de ajuste constante entre as capacidades tecnológicas disponíveis e as ambições comerciais da organização.

A inovação aberta (*Open Innovation*) e a colaboração estratégica com o ecossistema externo de fintechs e startups são extensões naturais do alinhamento estratégico moderno. Bancos tradicionais, por maiores que sejam, não conseguem inovar com excelência em todas as frentes sozinhos e na velocidade exigida pelo mercado. A capacidade de integrar soluções de terceiros de forma rápida, segura e transparente torna-se uma vantagem competitiva crucial. A governança de APIs e a gestão de parcerias tecnológicas tornam-se novas competências de negócio indispensáveis. O analista de negócios deve avaliar criteriosamente, através de estudos de *Make or Buy*, quando "construir dentro de casa" e quando "comprar, alugar ou integrar" soluções de mercado, considerando custos totais de propriedade (TCO), tempo de implementação, controle estratégico e diferenciação competitiva. Essa visão holística evita a síndrome do "não inventado aqui" e acelera a transformação digital da instituição.

Por fim, o alinhamento estratégico exige uma liderança transformacional e visionária que fomente uma cultura digital em toda a organização, do estagiário ao conselho de administração. A tecnologia deve ser desmistificada e entendida por todos não como uma caixa preta mágica, mas como uma ferramenta lógica de empoderamento do negócio. A capacitação contínua e cruzada das equipes de negócio em conceitos tecnológicos fundamentais e das equipes de TI em conceitos bancários e financeiros cria uma linguagem comum e um entendimento compartilhado que reduzem atritos, eliminam barreiras de comunicação e potencializam a colaboração sinérgica. O sucesso da modernização bancária não reside apenas na qualidade do código escrito, mas na capacidade da organização de aprender, adaptar-se e alinhar seus recursos tecnológicos à sua visão de futuro de forma coesa, disciplinada e estratégica.

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

6. Conclusão

A extensa, minuciosa e densa jornada analítica e investigativa percorrida ao longo das seções deste artigo científico permite consolidar, de forma fundamentada, a tese de que a modernização de sistemas legados e a implementação de uma governança de TI robusta em instituições financeiras não constituem meros projetos técnicos de atualização de parque tecnológico ou conformidade burocrática, mas sim imperativos estratégicos de sobrevivência, resiliência e competitividade em um cenário econômico digital e globalizado. Foi demonstrado, através da revisão narrativa de literatura e da análise conceitual aprofundada dos paradigmas arquiteturais, que a manutenção inercial de arquiteturas monolíticas obsoletas representa um risco sistêmico inaceitável e crescente, tanto pela ótica da ineficiência operacional e custos de manutenção insustentáveis, quanto pela perspectiva crítica da segurança cibernética, da integridade dos dados e da conformidade regulatória exigida pelos órgãos fiscalizadores. A gestão de processos gerenciais, quando instrumentalizada pela análise de negócios profissional e pela tecnologia da informação de ponta, fornece o arcabouço metodológico necessário para decompor a complexidade dos sistemas antigos e reconstruí-los sobre bases modernas, ágeis, escaláveis e auditáveis.

A implementação estratégica de *Robotic Process Automation* (RPA) revelou-se, ao longo da análise detalhada, como uma ferramenta tática de potência extraordinária para a transição digital suave e eficiente. Ao automatizar a "camada de colagem" entre sistemas díspares e eliminar o trabalho manual repetitivo, o RPA não apenas gera eficiências de custo imediatas e libera o precioso capital humano para atividades analíticas nobres, mas também atua como um vetor poderoso de *compliance* e auditoria, garantindo matematicamente que as regras de negócio e políticas institucionais sejam executadas com precisão, consistência e rastreabilidade total. Contudo, a tecnologia por si só é insuficiente e perigosa se não for gerida adequadamente; sua eficácia e segurança dependem umbilicalmente de uma governança rigorosa que evite a proliferação descontrolada de robôs não gerenciados (*Shadow RPA*) e garanta o alinhamento estrito com a arquitetura de segurança da informação e os objetivos de negócio.

A governança de TI e a proteção de dados emergiram nesta investigação como os pilares de confiança e legitimidade sobre os quais o sistema financeiro digital moderno se sustenta. Em um cenário de ameaças cibernéticas sofisticadas, persistentes e globais, e de regulações de privacidade de dados cada vez mais estritas e punitivas (como a LGPD), a capacidade institucional de demonstrar controle efetivo, monitoramento contínuo e resposta incidente rápida é tão vital para a reputação e a continuidade do banco quanto a sua própria solvência financeira e liquidez. A arquitetura de microsserviços e a integração via APIs padronizadas, discutidas no âmbito do alinhamento estratégico, provaram ser os habilitadores técnicos fundamentais que permitem aos bancos tradicionais competirem em velocidade, flexibilidade e inovação com as fintechs nativas digitais,

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

viabilizando novos modelos de negócio colaborativos e abertos como o *Open Finance* e o *Banking as a Service*.

Ademais, a pesquisa evidenciou de forma contundente e transversal que o fator humano, a cultura organizacional e a liderança são determinantes absolutos no sucesso ou fracasso da modernização tecnológica. A figura do Analista de Negócios Sênior e do Gestor de Processos destacou-se como o elemento aglutinador e tradutor capaz de conectar os dialetos técnicos da engenharia de software com as necessidades comerciais e regulatórias do negócio, mediando conflitos de prioridade e alinhando expectativas de entrega. A adoção de metodologias ágeis e a cultura DevOps não são apenas mudanças procedimentais de trabalho, mas transformações profundas de *mindset* que exigem liderança visionária e visão estratégica de longo prazo. A capacitação contínua das equipes, a retenção de talentos e a gestão do conhecimento tácito e explícito são essenciais para evitar que a modernização tecnológica resulte apenas em uma nova geração de sistemas legados incompreensíveis e ingovernáveis no futuro próximo.

A análise da evolução dos sistemas bancários demonstrou que a tecnologia não é um fim em si mesma, mas um meio poderoso para alcançar eficiência, segurança e satisfação do cliente. A modernização deve ser encarada como uma jornada contínua e não como um destino estático. As instituições que compreendem essa dinâmica investem não apenas em software e hardware, mas em inteligência de processos, arquitetura corporativa e governança de dados. A capacidade de orquestrar ecossistemas complexos, integrando sistemas legados robustos com novas tecnologias digitais, define a agilidade e a resiliência da instituição financeira. O equilíbrio entre a inovação disruptiva e a estabilidade operacional é o desafio constante que exige uma governança madura e uma gestão de TI alinhada aos propósitos do negócio.

Outro ponto crucial levantado pelo estudo é a interdependência entre a modernização tecnológica e a sustentabilidade econômica das instituições financeiras. A redução do custo total de propriedade (TCO) dos sistemas de TI, alcançada através da desativação de mainframes caros, da automação de processos manuais e da migração para a nuvem, libera recursos financeiros para investimentos em inovação e novos produtos. A eficiência operacional gerada pela tecnologia moderna permite que os bancos ofereçam serviços mais competitivos, com tarifas menores e melhor experiência para o usuário, garantindo sua relevância em um mercado cada vez mais comoditizado e disputado. A análise de negócios fornece as métricas e os estudos de viabilidade necessários para priorizar esses investimentos e demonstrar o retorno para os acionistas.

Conclui-se, portanto, com base em todo o exposto e argumentado, que o futuro das instituições financeiras reside inequivocamente na sua capacidade de orquestrar uma metamorfose contínua, governada e inteligente, onde a tecnologia é fluida, os processos são otimizados e a governança é onipresente. A convergência epistemológica, técnica e prática entre a Ciência da

Ano V, v.2 2025 | submissão: 22/09/2025 | aceito: 24/09/2025 | publicação: 26/09/2025

Computação, a Administração de Empresas e a Engenharia de Processos forma o arcabouço intelectual necessário para enfrentar os desafios complexos do século XXI. As organizações que logram êxito em integrar a robustez e a confiabilidade do legado com a agilidade e a inovação do digital, sob a égide de uma governança ética, transparente e eficiente, não apenas sobrevivem às turbulências do mercado, mas lideram a redefinição do sistema financeiro global. A modernização é, em última análise, um processo contínuo de adaptação evolutiva, guiado pela inteligência analítica humana e potencializado pela força bruta da automação digital.

Referências

CALCOTE, Lee; BUTCHER, Zack. **Istio: Up and Running**. Sebastopol: O'Reilly Media, 2019.

COBIT 2019. **COBIT 2019 Framework: Introduction and Methodology**. Schaumburg: ISACA, 2018.

EVANS, Eric. **Domain-Driven Design: Tackling Complexity in the Heart of Software**. Boston: Addison-Wesley, 2003.

FOWLER, Martin. **StranglerFigApplication**. MartinFowler.com, 2004.

HAMMER, Michael. **Reengineering Work: Don't Automate, Obliterate**. Harvard Business Review, v. 68, n. 4, p. 104-112, 1990.

ISO/IEC 27001. **Information technology - Security techniques - Information security management systems - Requirements**. Geneva: International Organization for Standardization, 2013.

KIM, Gene; DEBOIS, Patrick; WILLIS, John; HUMBLE, Jez. **The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations**. Portland: IT Revolution Press, 2016.

LAUDON, Kenneth C.; LAUDON, Jane P. **Management Information Systems: Managing the Digital Firm**. 13. ed. Boston: Pearson, 2014.

MOFFITT, Kevin C.; ROZARIO, Andrea M.; VASARHELYI, Miklos A. **Robotic Process Automation for Financial and Accounting Applications**. Journal of Emerging Technologies in Accounting, v. 15, n. 1, p. 1-10, 2018.

PRESSMAN, Roger S. **Engenharia de Software: Uma Abordagem Profissional**. 8. ed. Porto Alegre: McGraw-Hill, 2016.

WEILL, Peter; ROSS, Jeanne W. **IT Governance: How Top Performers Manage IT Decision Rights for Superior Results**. Boston: Harvard Business School Press, 2004.

WILLCOCKS, Leslie; LACITY, Mary. **Service Automation: Robots and the Future of Work**. Warwickshire: Steve Brookes Publishing, 2016.