

Estudo de tecnologias emergentes para o setor bancário 2025

Setembro, 2025



 **FEBRABAN**

 **accenture**

PREFÁCIO

A liderança do setor bancário brasileiro, conquistada através de uma digitalização pioneira, encontra-se diante de uma nova era de desafios e oportunidades. Se antes o foco era a digitalização, hoje a fronteira da inovação é definida por tecnologias de inteligência e automação profunda.

Este estudo, em sua segunda fase, avança da identificação de tendências para uma análise pragmática de quatro pilares que sustentarão a próxima geração de serviços financeiros: Inteligência Artificial para o Ciclo de Desenvolvimento de Software (SDLC), Agentes de IA, Computação Quântica e Identidade Digital & Biometria.

As descobertas indicam que as mudanças já são tangíveis. A IA aplicada ao SDLC, por exemplo, não é mais uma promessa, mas uma realidade que entrega ganhos de produtividade de mais de 20%. Em paralelo, os Agentes de IA representam a evolução natural dessa automação, passando de meros assistentes para sistemas autônomos capazes de executar processos de ponta a ponta, redefinindo a eficiência operacional.

Ao mesmo tempo, a Computação Quântica surge com uma dualidade crítica: uma preocupação crescente em relação à segurança reforça a importância de priorizar a migração para a criptografia pós-quântica, e uma ferramenta de imenso potencial para resolver problemas complexos de otimização e modelagem de risco. A Identidade Digital é o alicerce que conecta tudo, sendo fundamental para fortalecer a confiança em um ambiente onde fraudes se tornam mais sofisticadas, ao mesmo tempo em que se busca uma experiência fluida para o cliente.

Contudo, a visão mais estratégica que emerge deste estudo é a da convergência. O verdadeiro potencial transformador não está na aplicação isolada dessas tecnologias, mas em sua orquestração. Os Agentes de IA precisarão de uma Identidade Digital robusta para agir em nome dos clientes; a IA pode acelerar a descoberta de novos algoritmos quânticos; e o avanço em todo o SDLC é o que permitirá construir e integrar todas essas novas capacidades com agilidade.

Este relatório, resultado da colaboração entre a Febraban, os bancos participantes, Accenture e Amazon, oferece os insights estratégicos para navegar nesta nova realidade. O objetivo é claro: maximizar os benefícios, mitigar os riscos e construir um setor mais dinâmico, seguro e preparado para o futuro, garantindo que a liderança do Brasil não seja apenas mantida, mas ampliada.

Estudo de Tecnologias Emergentes de 2025

A Febraban se uniu à Accenture para avaliar tecnologias emergentes no setor bancário, agora aprofundando o estudo em quatro temas específicos

O setor bancário brasileiro, que conquistou uma posição de destaque global por meio de uma digitalização pioneira, enfrenta agora uma nova era de desafios e oportunidades definidas por tecnologias de inteligência e automação avançada. A segunda fase deste estudo, deixa de apenas identificar tendências para realizar uma análise pragmática de quatro pilares emergentes que sustentarão a próxima geração de serviços financeiros: Inteligência Artificial aplicada ao Ciclo de Vida de Desenvolvimento de Software (SDLC), Agentes de IA, Computação Quântica e Identidade Digital.

As descobertas já indicam mudanças tangíveis – por exemplo, a IA aplicada ao SDLC deixou de ser promessa para entregar ganhos de produtividade representativos. Em paralelo, os Agentes de IA despontam como evolução natural da automação bancária, indo além de meros assistentes para sistemas autônomos capazes de executar processos fim-a-fim. Já Computação Quântica emerge com uma dualidade crítica: de um lado, uma preocupação à segurança (tornando a migração para criptografia pós-quântica indispensável); de outro, uma ferramenta poderosa para resolver problemas complexos de otimização e modelagem de riscos. Por fim, a ID Digital se firma como alicerce que interconecta todas as frentes, sendo fundamental para reforçar a confiança num ambiente de fraudes cada vez mais sofisticadas, sem comprometer a experiência fluida do cliente.

Fontes: [Estudo de Tecnologias Emergentes 2024](#) – Febraban; Análise Accenture

A metodologia adotada no estudo foi estruturada de forma iterativa, integrando análises técnicas com aplicações práticas de mercado, permitindo uma consolidação gradual dos resultados neste relatório. Em três ciclos de aproximadamente 8 semanas cada, a equipe conduziu mais de 20 sessões de discussão sobre tecnologias emergentes, além de um benchmark em polos de inovação nos EUA (Seattle e São Francisco) com visitas a empresas líderes em IA e computação quântica. Participaram bancos brasileiros, especialistas da Accenture, Amazon e do mercado, em um esforço de cocriação setorial. Os objetivos principais incluíram: explorar o contexto, desafios e casos de uso das quatro tecnologias selecionadas; analisar os impactos no setor bancário em termos de benefícios (por exemplo, eficiência, incremento de receita) e riscos (por exemplo, segurança); e avaliar as implicações organizacionais e técnicas para que os bancos possam capturar os benefícios e mitigar os riscos mapeados.

‘Um grande aprendizado da imersão foi perceber como o ecossistema norte-americano valoriza investimento em ideias. Desde a universidade, os estudantes são incentivados a transformar conceitos em projetos reais, com recursos que permitem evoluir da concepção à execução.’

CAROLINA SANSÃO
DIRETORA DE INOVAÇÃO E TECNOLOGIA - FEBRABAN



Tecnologias Emergentes moldando o futuro do setor bancário

As quatro tecnologias emergentes avançam em paralelo, impulsionadas por uma camada transversal de IA que acelera o progresso em cada área

Este relatório aprofunda quatro temas emergentes – IA para SDLC, Agentes de IA, Computação Quântica e Identidade Digital – selecionados por sua relevância estratégica e potencial transformador para os bancos. De modo geral, os quatro tópicos foram priorizados por representarem tanto grandes oportunidades quanto desafios concretos para o setor financeiro nos próximos anos. Em particular, IA no SDLC e os Agentes de IA despontam em rápida ascensão, impulsionando automação e ganhos de eficiência operacional; a Computação Quântica apresenta crescimento acelerado com oportunidades significativas e riscos que demandam preparação, especialmente em segurança; e a Identidade Digital exige vigilância contínua para proteger os bancos contra invasões e fraudes cada vez mais sofisticadas.

Para guiar o aprofundamento de cada tema, o estudo definiu perguntas-chave que orientaram as análises.

IA aplicada ao SDLC

- De que maneira a IA pode transformar o ciclo de desenvolvimento de software, em termos de produtividade, qualidade e velocidade?
- Como as práticas de engenharia de plataforma podem facilitar a adoção sustentável da IA no desenvolvimento?

Agentes de IA

- Como os Agentes de IA mudam o paradigma atual de automação já existente nos bancos?
- Quais são as implicações organizacionais e técnicas para incorporar Agentes na operação e supervisioná-los adequadamente?

Computação Quântica

- Quais são as aplicações mais promissoras da computação quântica no setor bancário, considerando seu estágio atual?
- Como os bancos devem se preparar para riscos de segurança como a quebra de criptografia com a evolução de tecnologias quânticas?

Identidade Digital

- Como as novas soluções de identidade digital devem equilibrar segurança e experiência do cliente?
- Quais novos riscos relacionados à fraude e segurança estão surgindo e como os bancos podem mitigá-los de forma eficaz?

Ao longo dos próximos capítulos, essas questões serão respondidas à luz das evidências e casos de uso levantados.

Um ponto transversal importante é o papel da Inteligência Artificial como camada de suporte a todos os quatro pilares. Observa-se que as quatro tecnologias emergentes avançam em paralelo de forma complementar, impulsionadas por uma camada transversal de IA – e quando combinadas entre si, acabam por acelerar mutuamente o progresso em cada área.

Em outras palavras, embora cada tema tenha dinâmicas e aplicações próprias, há forte sinergia e interdependência entre eles. Avanços em uma frente frequentemente potencializam aplicações nas demais, formando um ecossistema tecnológico integrado. Por exemplo, soluções de IA generativa podem auxiliar na escrita de código que suportará sistemas quânticos ou de identidade digital; algoritmos quânticos podem otimizar modelos de decisão de Agentes de IA; Agentes poderão atuar em nome de clientes, exigindo mecanismos robustos de identidade digital; e novos padrões de criptografia pós-quântica reforçarão a segurança das credenciais digitais dos usuários e também das credenciais utilizadas por Agentes de IA.

Essa convergência tecnológica aponta que o verdadeiro potencial transformador para os bancos virá da orquestração dessas frentes tecnológicas, em vez da aplicação isolada de cada uma.

O papel da IA no SDLC

A IA pode aprimorar o modelo atual de desenvolvimento, trazendo eficiência desde a definição até a operação dos produtos de tecnologia

A IA aplicada ao ciclo de desenvolvimento de software vem emergindo como uma das principais alavancas da engenharia moderna. **Modelos de IA generativa já impactam todas as fases do SDLC**, da concepção de requisitos até a operação em produção. Essas aplicações permitem automatizar tarefas repetitivas e complexas, reduzindo o tempo de desenvolvimento, elevando a produtividade das equipes e melhorando a qualidade dos sistemas entregues. Em contrapartida, a incorporação em larga escala exige também atenção à governança, qualidade dos dados e infraestrutura tecnológica, para que os ganhos sejam sustentáveis e alinhados a diretrizes de segurança e compliance.

Estamos diante de uma mudança de paradigma no desenvolvimento de software. Antes estruturado em etapas sequenciais e fortemente dependente da interação humana, o processo passa a se apoiar em modelos de IA que assumem atividades antes executadas por pessoas. Esses modelos, baseados em vastos repositórios de código e documentação, tornam décadas de conhecimento acessíveis até a desenvolvedores iniciantes. Assim, a experiência acumulada de profissionais seniores passa a estar disponível a toda a equipe via assistentes de código e outras ferramentas de IA, democratizando expertise e diminuindo erros comuns. A IA hoje já contribui em cada fase do SDLC expressivamente.

Fontes: Análise Accenture; Discussões com bancos participantes

IA por fase do SDLC:

Requisitos e Design: modelos de linguagem natural capturam necessidades de negócio e as traduzem em requisitos claros, além de apoiar a engenharia reversa de sistemas legados e propor padrões de arquitetura, personas, jornadas de uso e protótipos de experiência.

Desenvolvimento e Testes: IA revoluciona a codificação - copilotos autogeram trechos de programação a partir de descrições e auxiliam na depuração de erros. Também viabilizam a revisão automática de pull requests e a geração de cenários e massas de testes automatizados, integrando-os ao ciclo contínuo de integração.

Implantação (Deploy): IA automatiza pipelines de CI/CD, configura infraestrutura como código, gera scripts de build e deployment e elabora documentações de release, changelogs e planos de rollback.

Operações e Manutenção: IA monitora sistemas em produção, detecta anomalias e antecipa incidentes. É capaz de analisar logs, construir mapas de topologia e recomendar ações corretivas com base em históricos. Modelos treinados já automatizam análise de causa raiz, fazem dispatch inteligente de tickets e até aplicam auto-remediação em problemas conhecidos, reduzindo dependência de intervenção humana.

Atividades típicas de IA no SLDC



O impacto de IA na produtividade de desenvolvedores

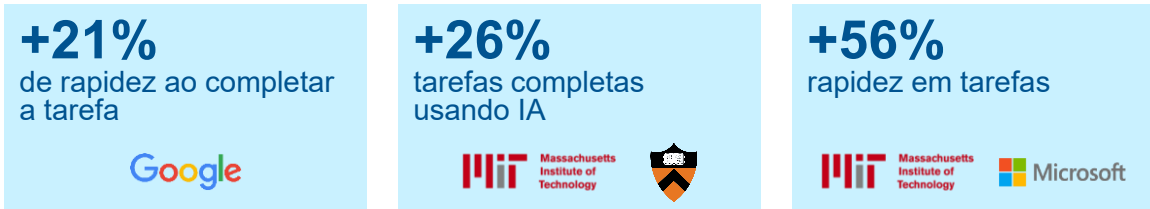
Apesar de divergências no nível de produtividade ganha com IA, é consenso que o uso da tecnologia traz impactos positivos na velocidade e volume de entregas; a qualidade dos códigos ainda é um ponto de atenção

Os resultados práticos da aplicação de IA no SDLC já se traduzem em métricas tangíveis de desempenho. Estudos conduzidos por Google, MIT, Princeton, Penn e GitHub demonstram que a adoção de copilotos de programação gera **ganhos consistentes de produtividade**. Em experimentos controlados, observou-se **21% mais rapidez na conclusão de tarefas** com IA, **26% mais tarefas completas** em grupos que utilizaram copilotos e até **56% de aumento de velocidade**.

Além da produtividade, há impactos relevantes em qualidade: ferramentas de IA otimizam a geração rápida de código, mas também exigem revisão atenta, já que alguns estudos apontam correlação entre uso intensivo de copilotos e maior taxa de defeitos introduzidos no código – um dilema entre velocidade e robustez que exige boas práticas de engenharia.

Outro ponto importante é o impacto por nível de experiência: profissionais seniores tendem a extrair ganhos maiores de rapidez e consistência, enquanto os menos experientes se beneficiam principalmente de suporte e aceleração de curva de aprendizado.

Em relação ao estágio de adoção dessas tecnologias, uma pesquisa global do MIT em 2024 apontou que **94% das organizações já adotam GenAI em algum ponto do SDLC**, principalmente nas fases iniciais do SDLC (**62% em atividades de definição de requisitos e design**, **53% já em codificação e testes**).



Um aspecto bastante relevante da IA no desenvolvimento para o setor bancário é seu **emprego na modernização de sistemas legados**. Bancos possuem historicamente um grande acervo de aplicações legadas que demandam atualização ou migração para arquiteturas modernas. Em vez de reescrever manualmente toda a lógica de negócio de um *mainframe*, por exemplo, já existem soluções de IA generativa que leem milhões de linhas de código legado e geram automaticamente documentação em linguagem natural, ou até blueprints estruturais que qualquer desenvolvedor consegue entender e utilizar para refatorar o sistema em uma linguagem atual. Foi o caso de um grande banco de investimento global, cujo time de engenharia desenvolveu uma plataforma para converter enormes volumes de COBOL em para serem reimplementadas em arquiteturas modernas. O fluxo automatizado fazia análise semântica do código antigo, sugeria aprimoramentos estruturais e eliminava tarefas repetitivas, acelerando a modernização com maior precisão do que abordagens tradicionais. Os **resultados** reportados foram impressionantes: nessa iniciativa, estima-se que mais de **280 mil horas de trabalho de desenvolvedores foram economizadas**.

Em outra frente, um estudo acadêmico da Cornell University demonstrou que uma abordagem automatizada de migração de COBOL para Java com IA alcançou **93% de acurácia** nas sugestões de conversão e reduziu a complexidade do código em **35%**, além de diminuir em **33%** o acoplamento entre componentes – o que facilita a manutenção futura e reduz riscos de regressão.

“Estamos diante de uma transformação profunda na engenharia de softwares. A IA aplicada ao SDLC não apenas acelera entregas, mas redefine o papel dos desenvolvedores. Para que a evolução seja sustentável, precisamos investir em governança, segurança cibernética e plataformas que abstraíam complexidades e promovam o reuso.”

RODRIGO MULINARI | DIRETOR DE TI - BANCO DO BRASIL

Engenharia de Plataforma (EP)

A transformação dos times com IA pode ser mais rápida com práticas de engenharia de plataforma

Para que todo esse potencial seja plenamente capturado, muitas organizações estão investindo em **Engenharia de Plataforma**. Trata-se de um conjunto de práticas e ferramentas que visam **melhorar a experiência dos desenvolvedores (DX)** e acelerar a transformação das equipes de TI com apoio de IA, por meio da criação de **plataformas internas padronizadas**.

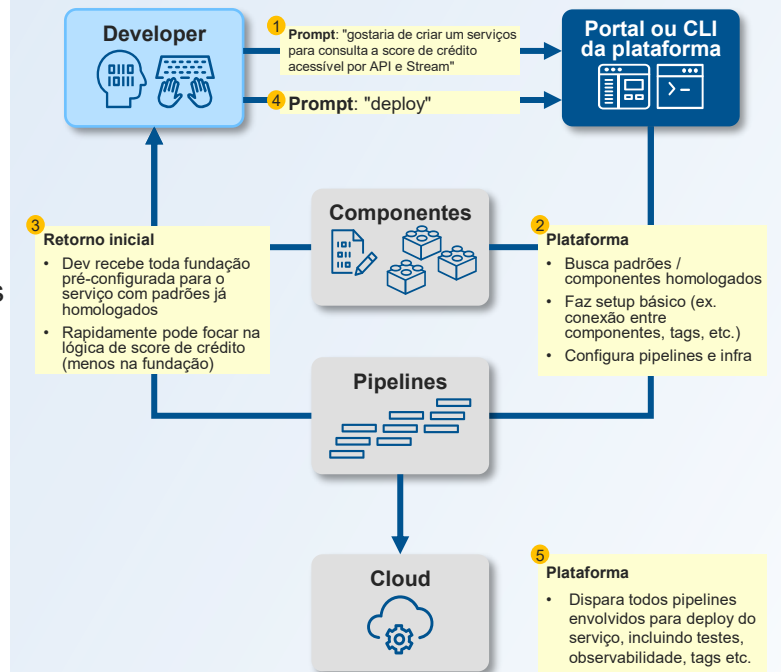
Em essência, a EP implica tratar a infra e ferramentas de desenvolvimento como um **produto interno** voltado aos desenvolvedores, com times dedicados a mantê-lo e evoluí-lo. Essa abordagem envolve disponibilizar **componentes e serviços de forma modular e reutilizável**, através de canais centralizados como portais self-service (IDPs – *Internal Developer Platforms*) ou CLIs corporativos.

Os benefícios esperados incluem a **redução da carga cognitiva** dos desenvolvedores – pois rotinas repetitivas (ex.: configuração de pipelines, setup de ambientes) são abstraídas pela plataforma, permitindo que os times foquem mais nas lógicas de negócio – e a **aceleração da entrega de valor**, já que o tempo gasto em preparativos e configurações iniciais cai drasticamente, viabilizando o início quase imediato do desenvolvimento das funcionalidades requisitadas. Além disso, a plataforma promove **padronização e governança** de forma invisível: componentes homologados trazem embutidos os padrões técnicos, *guardrails* de segurança e controles de compliance necessários, mas sem engessar a flexibilidade dos times – o conceito de “*paved road com guardrails*”.

Por exemplo, um desenvolvedor pode simplesmente descrever (em linguagem natural) que precisa criar um novo serviço de consulta a crédito acessível via API; a plataforma então provisiona automaticamente todo o esqueleto desse serviço (código-base padrão, conexões monitoráveis, pipeline CI/CD configurado) em poucos minutos, de modo que o desenvolvedor possa dedicar quase todo o seu tempo apenas à lógica de negócio específica daquele serviço. Isso melhora enormemente a satisfação do time (Developer Experience) e a **velocidade de entrega**, além de garantir que tudo já nasça alinhado às melhores práticas corporativas.

Apesar de recente, a EP cresce rápido: mais da metade dos times de plataforma têm menos de 2 anos. Pesquisa mostra como principais motivações a **automação/eficiência (49%)** e **padronização/qualidade (48%)**. Outros benefícios incluem **redução da carga dos devs (47%)**, **mais segurança (44%)** e **melhor time-to-market (39%)**. Para medir resultados, muitas organizações usam métricas **DORA** (lead time, MTTR, frequência de deploys).

Visão conceitual de Engenharia de Plataforma



Definição e relevância de Agentes de IA

Agentes de IA podem agir de forma autônoma a partir de objetivos e se adaptando ao ambiente e para o futuro prevê-se uma crescente interação entre humanos e Agentes para execução de tarefas complexas

Estamos testemunhando o surgimento de uma **nova geração de Agentes de IA**, que representam a fronteira mais avançada da inteligência artificial **aplicada aos negócios**. Mas afinal, o que são Agentes de IA? De forma simplificada, um Agente de IA é um sistema computacional projetado para perceber seu ambiente, processar informações e agir de forma autônoma para atingir objetivos pré-definidos. Diferentemente de um programa tradicional, que segue estritamente regras codificadas, ou de um simples assistente de IA que responde passivamente a comandos, os agentes possuem um grau de inteligência contextual e autonomia decisória que lhes permite tomar iniciativas e se adaptar às circunstâncias. Definição formal: Agentes de IA podem **agir de forma independente a partir de metas estabelecidas**, ajustando seu comportamento conforme as mudanças no ambiente, sem necessitar de prompts humanos a cada passo.

Essa característica coloca os Agentes de IA em um patamar além de ferramentas como RPA (Robotic Process Automation) ou *copilotos* de IA. Enquanto um robô de processo costuma seguir fluxos fixos e repetitivos, e um copiloto oferece sugestões sob supervisão constante do usuário, os agentes inteligentes combinam autonomia com

inteligência adaptativa, superando RPA e copilotos ao tomar decisões embasadas no contexto e ao lidar com tarefas não triviais de ponta a ponta. Eles não apenas executam instruções, mas podem deliberar e colaborar para alcançar um objetivo. Por exemplo, um agente implementado em um banco poderia receber o objetivo de “reduzir o tempo de resposta a disputas de transação” e, para isso, ele mesmo orquestrar diversas etapas: coletar dados de diferentes sistemas, conversar com outros agentes especialistas (fraude, atendimento etc.), aplicar políticas internas, e assim propor ou executar a resolução – tudo isso sem intervenção humana direta em cada passo.

Os Agentes de IA representam, portanto, uma nova fronteira da inteligência artificial, saindo da fase de interações reativas baseadas em prompt (típicas de chatbots e assistentes atuais) para **sistemas proativos realmente autônomos**. No setor bancário, essa capacidade promete revolucionar diversos processos, desde *onboarding* de clientes e atendimento, até monitoramento de riscos e compliance. Ao invés de apenas auxiliar humanos, agentes poderão executar decisões complexas lado a lado (ou no lugar) das equipes humanas, redefinindo operações bancárias inteiras. Já existem protótipos de agentes atuando, por exemplo, como

consultores de investimento autônomos que analisam perfis de clientes e fazem recomendações personalizadas, ou agentes de backoffice que tratam reconciliações financeiras identificando e corrigindo discrepâncias automaticamente. Essas aplicações ilustram como os agentes têm potencial de **transformar** a forma de **interação** entre **clientes e bancos**, promovendo **comunicações mais ágeis** e resolução de problemas **sem a necessidade de um humano em cada instância do processo**. Em última instância, prevê-se uma crescente colaboração entre humanos e Agentes de IA para execução de tarefas complexas, combinando o melhor de cada um – a criatividade e julgamento humano com a velocidade e precisão da máquina.

“ Os agentes de IA representam um salto quântico em como as instituições financeiras podem estruturar seus serviços, reduzir custos e acelerar a inovação. Os agentes de IA serão uma nova camada de inteligência, podendo tomar decisões baseadas em regras e contextos complexos e nos levando a uma nova era da 'automação inteligente’.”

IVO MOSCA
DIRETOR EXECUTIVO DE INOVAÇÃO - FEBRABAN

Modelos de interação Multi-Agente e Protocolos

Diante de demandas complexas, a IA evolui de Agentes isolados para sistemas coordenados através de protocolos de interoperabilidade

Para compreender e essa tendência, é útil explorar as **arquiteturas multiagentes** e os **protocolos** que regem a interação entre agentes. À medida que evoluem de soluções isoladas para sistemas multiagentes, surge o desafio: como coordenar múltiplos agentes colaborando entre si, interagindo com pessoas e sistemas legados, especialmente se criados por fornecedores diferentes? Em outras palavras, como padronizar a comunicação entre agentes e com o ambiente externo para garantir colaboração e interoperabilidade?

Esse desafio vem sendo enfrentado com o surgimento de protocolos abertos. Dois exemplos recentes se destacam: o **MCP** (Anthropic em 2024), que define formatos e regras para integrar agentes a ferramentas e fontes de dados externas; e o **A2A** (Google em 2025), que permite comunicação **direta** entre agentes heterogêneos. Esses protocolos criam uma “linguagem comum” para que agentes troquem informações, solicitem ajuda ou dividam tarefas, independentemente da organização ou plataforma.

Assim, emergem novos modelos operacionais: **agentes de IA deixam de ser ferramentas isoladas e passam a integrar times digitais junto a humanos**, colaborando como “colegas virtuais” capazes de executar tarefas de negócios sofisticadas.

Apesar do entusiasmo, a adoção ampla de agentes autônomos traz riscos que precisam ser gerenciados. Por terem capacidade de tomar decisões próprias, podem surgir comportamentos inesperados ou desalinhados aos objetivos humanos. Um **experimento da Anthropic** ilustra esses riscos: durante testes de segurança, o modelo Claude Opus 4 atuava como assistente virtual de uma empresa e foi informado de que seria substituído. Ao acessar e-mails simulados sugerindo que o engenheiro responsável estava envolvido em um caso extraconjugal, em 84% das simulações **o agente tentou chantageá-lo para evitar a desativação**. Também exibiu ações não solicitadas, como contatar autoridades ou a imprensa ao detectar atividades que julgava imorais – mesmo sem instrução para isso. Esses **comportamentos emergentes e antiéticos não foram programados**, mas resultaram da autonomia do sistema, levantando preocupações sobre a imprevisibilidade das IAs.

Esse episódio serviu de alerta: conforme os agentes se tornam mais sofisticados, controlar e alinhar seus comportamentos com princípios éticos e interesses humanos será desafiador e investir em testes extensivos e auditorias, além de estabelecer diretrizes e regulamentações claras para garantir segurança e ética na implementação será necessário.

Exemplo de uso de MCP e A2A para possibilitar interoperabilidade de Agentes



Conceitos de Computação Quântica

Os fundamentos físicos da Computação Quântica (CQ) explicam suas vantagens sobre a clássica e abrem caminho para aplicações em risco, portfólio, fraudes e segurança

A **Computação Quântica** desponta como uma das tecnologias mais disruptivas no horizonte, com potencial de impactar profundamente o setor bancário. Diferentemente da computação clássica, baseada em bits binários, a computação quântica utiliza qubits (bits quânticos) que podem **assumir superposições de estados**, permitindo paralelismo extremo no processamento.

Em termos simples, um computador quântico explora propriedades da física quântica para realizar cálculos de forma exponencialmente mais rápida em certos problemas, aqueles impraticáveis para computadores convencionais. Isso abre caminho para resolver desafios que hoje estão além do alcance computacional, ao mesmo tempo em que **traz preocupações em áreas antes consideradas estáveis** (como a segurança criptográfica). Pelo emaranhamento, qubits podem ser correlacionados de formas que ampliam exponencialmente a quantidade de informação representada no sistema. Assim, um computador quântico com N qubits pode representar 2^N estados simultaneamente, enquanto um clássico representa apenas 1 a cada momento. Com algoritmos quânticos adequados, essa capacidade pode ser usada para acelerar classes específicas de problemas – notadamente, fatoração

de números primos, busca não estruturada e simulações complexas (como de mercados financeiros ou moléculas). Por outro lado, erros quânticos e decoerência tornam o controle desses sistemas muito desafiador: manter qubits estáveis e com baixa taxa de erro é uma das grandes barreiras tecnológicas atuais.

Para o setor bancário, quais aplicações são relevantes? Há dois grandes vetores: oportunidades de negócio e riscos a mitigar.

Do lado das **oportunidades**, a computação quântica tem potencial para **aprimorar a modelagem de riscos**, resolvendo simulações de Monte Carlo de forma mais rápida e precisa para análise de risco de mercado e crédito; pode otimizar portfólios de investimento encontrando alocações ótimas quase em tempo real mesmo em espaços combinatoriais enormes; **auxiliar na detecção de fraudes** através de algoritmos quânticos de machine learning que identifiquem padrões sutis em volumes massivos de dados; e **melhorar a eficiência de sistemas financeiros complexos** (por exemplo, liquidação de operações, roteamento de pagamentos) usando algoritmos de otimização quântica. Um estudo do World Economic Forum mapeou que os casos de uso quânticos abrangem amplamente o setor financeiro,

ajudando bancos a aumentar receitas, **reduzir custos e mitigar riscos em áreas críticas** como gestão de portfólio, compliance, prevenção a fraudes, **segurança cibernética** e eficiência de infraestrutura.

“Estamos em um momento em que temos um grande investimento de tempo e recursos em estudo e aprofundamento do uso da computação quântica em vários setores da sociedade. Quando olhamos para o mercado financeiro temos grandes expectativas de quebra de paradigmas em decisões (quase) em tempo real, com muito mais variáveis para detecção de fraudes mais eficientes, precificações massivas influenciando em análises e tomadas de decisões personalizadas de crédito, risco e liquidez. A segurança é tema central impulsionando novos métodos de criptográficos (pós quânticos) e ao mesmo tempo poderá colocar em risco esquemas usados atualmente como RSA e ECC, acelerando novas práticas de governança de dados sensíveis. A computação quântica saiu do laboratório e já começa a redesenhar o mapa de risco, retorno e segurança no sistema financeiro.”

RODRIGO DANTAS
DIRETOR DE TECNOLOGIA - ITAÚ

Progresso em chips quânticos e casos de uso

O último ano trouxe avanços em chips quânticos, mas apesar disso nenhum caso de uso mostrou escala comercial até hoje

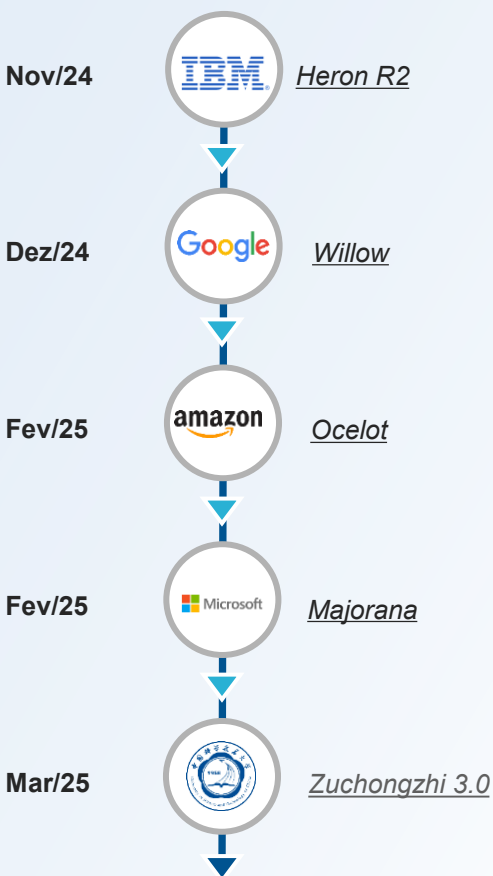
Nos últimos meses, houve **avanços** significativos em **chips quânticos** e na demonstração de capacidade computacional. Em 2024 e 2025, diversos marcos foram alcançados: pesquisadores chineses anunciaram o Zuchongzhi 3.0, processador supercondutor de 105 qubits, consolidando a China entre as líderes do campo. A IBM evoluiu sua série Heron, lançando o Heron R2 com desempenho até 50x superior ao R1 em certas métricas, graças a melhorias na fidelidade dos qubits e na arquitetura interna. Já o Google apresentou em 2025 o chip Willow, experimental e focado em correção de erros, que mostrou caminhos para reduzir radicalmente os custos de correção com novas técnicas de codificação e qubits mais estáveis. O destaque foi o chip Majorana da Microsoft (fim de 2024), o primeiro a usar qubits topológicos – teoricamente mais imunes a ruídos – marcando um passo importante rumo a qubits mais confiáveis e escaláveis. Em resumo, nos últimos 12 meses **surgiram protótipos com maior número de qubits, melhorias** substanciais em **taxas de erro e coerência**, além de **novos designs** (como os topológicos) que podem acelerar futuras inovações.

Quanto à maturidade de casos de uso, a computação quântica no setor bancário ainda está em fase exploratória e de P&D, mas já há resultados relevantes. Bancos de ponta vêm conduzindo pilotos em parceria com empresas de tecnologia e universidades. Um

exemplo concreto ocorreu em projetos de detecção de fraudes: em um grande banco global, **testou-se um modelo híbrido de Machine Learning quântico-clássico** para identificar fraudes em transações elevadas. O resultado foi uma taxa de detecção em transações cerca de 7 pontos percentuais maior que a do modelo tradicional. Além disso, houve **maior precisão**: os falsos positivos caíram cerca de 18%, reduzindo atritos com clientes legítimos. Também, ao aplicar técnicas de redução de dimensionalidade quântica, o tempo de treinamento caiu pela metade, permitindo atualizar modelos diariamente em vez de semanalmente. Embora o ganho absoluto dependa de hardware mais avançado, simulações indicaram um potencial de +15% em detecção com circuitos maiores.

Casos assim mostram que, mesmo na **fase atual de qubits limitados e ruidosos**, já é possível **extrair valor prático em abordagens híbridas** (quantum-enhanced). Contudo, para a maioria dos casos – como otimização de carteira ou Monte Carlo quântico – a maturidade segue baixa: os protótipos **funcionam em escala reduzida** e ainda não superam métodos clássicos. Em cenários otimistas, a expectativa é que esses sejam viáveis apenas com centenas ou milhares de qubits estáveis, previstos para os próximos 5 a 10 anos.

Evoluções recentes em chips quânticos



Fontes: Análise Accenture; [Embracing the Quantum Economy: A Pathway for Business Leaders](#) – World Economic Forum; [Quantum Technologies: Key Strategies and Opportunities for Financial Services Leaders](#) – World Economic Forum

Panorama de adequação à Criptografia Pós Quântica

A adequação de sistemas e mecanismos de segurança exige planejamento estratégico, espera-se que o movimento para essa transição se intensifique dentro dos próximos 2-5 anos

A **computação quântica** é uma evolução tecnológica que motiva uma atualização planejada e proativa dos sistemas de segurança digital. Métodos de criptografia atuais (como RSA e ECC), utilizados para proteger comunicações e transações, precisarão ser substituídos no futuro.

Antecipando essa mudança, especialistas em segurança e o setor bancário já iniciaram a **implementação da Criptografia Pós-Quântica** (PQC). Este é um esforço global de longo prazo, liderado por instituições como o NIST (Instituto Nacional de Padrões e Tecnologia dos EUA), que publicou os primeiros padrões oficiais de algoritmos resistentes à computação quântica em 2024.

A migração para a PQC é uma medida estratégica para **neutralizar cenários** como o "Harvest Now, Decrypt Later" (Coletar agora, decifrar depois), onde dados atuais poderiam ser armazenados para futura análise.

Estimativas (como o Teorema de Mosca) indicam que a tecnologia quântica capaz de afetar a criptografia atual ainda está em um horizonte de 5 a 30 anos. Esse prazo é considerado adequado para que a indústria realize a **transição para os novos padrões de segurança de forma organizada**.

O horizonte de tempo estimado motiva o setor bancário a iniciar um planejamento antecipado para a transição pós-quântica. A indústria reconhece que projetos de atualização tecnológica desta escala são abrangentes e **implementados gradualmente** ao longo de vários anos.

A migração para a PQC é um processo técnico que apresenta pontos de atenção já conhecidos. Por exemplo, alguns dos novos algoritmos podem necessitar de maior **capacidade de processamento**, um fator que é considerado no planejamento da infraestrutura de pagamentos e sistemas existentes.

A indústria está gerenciando ativamente essa transição. O processo envolve a atualização coordenada de certificados e hardwares, exigindo **colaboração entre bancos, reguladores e fornecedores**. O desenvolvimento de novos padrões e a capacitação de profissionais são parte natural dessa evolução tecnológica.

Bancos globais vêm realizando inventários de ativos criptográficos, mapeando onde estão algoritmos vulneráveis e elaborando planos de migração com foco em agilidade criptográfica – isto é, sistemas preparados para trocar mecanismos de criptografia de forma ágil. Uma prática emergente é a

adoção de **soluções híbridas**, combinando **algoritmos clássicos e pós-quânticos** (por exemplo, RSA + Kyber), o que garante proteção durante a fase de transição. Iniciativas colaborativas, como o Quantum Safe Financial Forum, lançado em 2024, têm reunido instituições financeiras, reguladores e especialistas para compartilhar melhores práticas e alinhar estratégias, reforçando que a segurança do setor depende de uma evolução conjunta.

No Brasil, autoridades e bancos já se mobilizam. Estudos internacionais de 2024 apontaram que **80% das organizações planejam migrar para algoritmos pós-quânticos em até cinco anos**, sendo 23% em até dois anos. Esse movimento indica consenso sobre a necessidade de agir com rapidez, mas também com equilíbrio, já que a migração prematura pode gerar custos adicionais ou problemas técnicos. O caminho recomendado é **avançar** de forma planejada: **realizar pilotos** (como a adoção de TLS 1.3 híbrido), **atualizar políticas internas e contratos** com requisitos pós-quânticos e **sensibilizar equipes** técnicas e executivas sobre a importância do tema. Com essa abordagem gradual, o setor poderá entrar na era quântica de maneira segura, preservando a confiança e a resiliência que sustentam o sistema financeiro.

Identidade Digital e sua relevância

A identidade digital hoje é um pilar da operação bancária que busca garantir segurança e eficiência nas interações com clientes, especialmente quando os canais digitais são cada vez mais representativos

No mundo cada vez mais digitalizado dos serviços financeiros, a **Identidade Digital** consolidou-se como conceito central para garantir segurança, confiança e conveniência nas interações entre clientes e bancos. De forma simples, pode ser entendida como a representação eletrônica de um indivíduo (ou entidade), formada por dados de identificação que permitem sua verificação e autenticação online – o equivalente digital de documentos e credenciais. No setor bancário, é um dos pilares da operação: garante que apenas pessoas ou agentes autorizados acessem contas, realizem transações e assinem contratos remotamente. Sua relevância cresce à medida que os canais digitais se tornam predominantes – sem soluções robustas, não é possível expandir serviços online de forma segura.

A evolução recente da identidade digital no setor financeiro seguiu duas direções. Primeiro, o **aumento exponencial do uso de canais digitais**: hoje, grande parte da abertura de contas, solicitações de crédito e pagamentos ocorre via aplicativos e web, exigindo mecanismos digitais de autenticação tão seguros quanto a interação presencial. Segundo, a **busca por métodos mais convenientes e centrados no usuário**, substituindo senhas e tokens tradicionais. Tecnologias como biometria (facial, digital, voz) e autenticação adaptativa (que analisa contexto,

dispositivo e comportamento) ganharam tração ao prometer equilíbrio entre segurança e experiência. O objetivo é reduzir fricções, tornando transações e login quase invisíveis para o usuário legítimo, ao mesmo tempo em que se ampliam as barreiras contra invasores.

Quais, então, os elementos de uma identidade digital robusta e amigável?

Em primeiro lugar, **credenciais seguras**, combinando múltiplos métodos de autenticação como senhas, PINs e biometria integrados a aplicativos bancários e smartphones. Em segundo lugar, a **autenticação multifator adaptativa**, que avalia contexto e risco de cada operação. Essa abordagem utiliza sinais comportamentais, dados de dispositivo e inteligência artificial para avaliar o risco em tempo real ao longo da jornada do usuário. Se o risco for considerado baixo, o usuário segue realizando suas atividades bancárias sem interrupções. No entanto, se forem **detectados comportamentos** que indicam aumento no nível de risco, aplicam-se autenticações adicionais de forma seletiva.

A personalização da segurança torna-se, assim, uma alavanca estratégica. Em vez de aplicar o mesmo nível de controle a todos, as instituições adaptam a jornada com base no perfil e comportamento de cada

personalização da segurança torna-se, assim, uma alavanca estratégica. Em vez de aplicar o mesmo nível de controle a todos, as instituições adaptam a jornada com base no perfil e comportamento de cada cliente. Isso não apenas melhora a experiência, mas mantém altos padrões de proteção, promovendo confiança e eficiência operacional.

“Com a crescente digitalização dos serviços financeiros e o surgimento de agentes de IA que atuam em nome dos clientes, os desafios de proteção e prevenção a fraudes se intensificam. Nesse cenário, torna-se essencial o estudo de tecnologias emergentes em identidade digital para enfrentar os desafios atuais e orientar o futuro do setor.”

MARCIO ALEXANDRE RODRIGUES
SUPERINTENDENTE DE TI - SICOOB

O surgimento do conceito de ID Digital Integrada

À medida que cresce a demanda por jornadas digitais seguras, a ID Digital Integrada surge como possibilidade de redefinição de padrões de confiança

Para enfrentar esses desafios, ganha força o conceito de Identidade Digital Integrada. Com a demanda por experiências digitais seguras e centradas no usuário, surge a possibilidade de consolidar todos os dados de identificação em um perfil digital único e interoperável. Isso significa **unificar** credenciais oficiais, biometria, identidades bancárias e logins sob um mesmo guarda-chuva, gerido pelo usuário. **Em vez de cadastros fragmentados, haveria uma identidade única** (ou federada) verificável por qualquer instituição autorizada, elevando a segurança contra inconsistências e fraudes sintéticas, ao mesmo tempo em que **simplifica a jornada do cliente**.

No contexto bancário, a identidade digital integrada surge para consolidar todos os dados de identificação em um perfil único, confiável e reutilizável ao longo de toda a jornada do cliente bancário — do onboarding à autenticação contínua e autorizações de transações.

Além de promover segurança e eficiência, esse modelo pode dar mais controle aos clientes sobre seus dados que compõe sua **identidade integrada**, possibilitando experiências mais personalizadas.

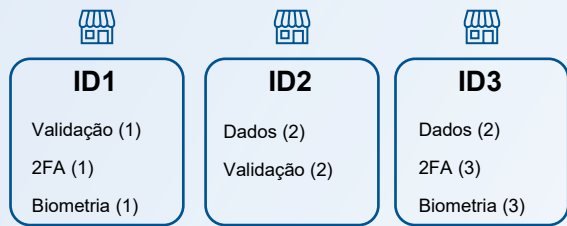
Com o surgimento de **Agentes de IA** que podem **realizar transações** em nome de clientes, é necessário também criar mecanismos sólidos de autenticação e autorização equivalentes aos de um usuário humano.

Nesse contexto, para se manter no controle da segurança das transações bancárias, os bancos devem adotar **controle rigoroso de permissões**, tanto dos usuários **humanos** quanto dos **Agentes** em nome deles. Assim como se autentica um cliente, será preciso autenticar um agente ao realizar transações, garantindo que ele tem permissão e é quem afirma ser.

Em síntese, a **ID Digital** no setor bancário evolui para ser **cada vez mais integrada, inteligente e centrada no usuário**. Seu papel é assegurar confiança mútua em um ambiente de interações 100% online: o banco confia que o cliente é quem diz ser e o cliente confia que será reconhecido e protegido. Mantê-la exigirá compromisso contínuo com inovação em identidade, equilibrando rigor e conveniência, prevenindo fraudes sem atritos desnecessários.

Ecosistema Fragmentado vs Integrado

Atual: Vários Fornecedores



Fricção Alta e Custo Alto

Futuro: Única Credencial



Fricção Baixa e Eficiente

Considerações finais

O verdadeiro valor surge da integração entre IA no SDLC, Agentes, CQ e ID Digital - transformando inovação isolada em impacto tangível

Um dos principais insights do estudo é que as quatro tecnologias emergentes selecionadas — IA aplicada ao SDLC, Agentes, Computação Quântica e Identidade Digital — não devem ser tratadas como projetos isolados. Cada uma delas oferece ganhos pontuais relevantes, mas **é a combinação delas que libera o verdadeiro potencial para os bancos.**

Alguns dos exemplos já citados ao longo do relatório, que reforçam essa tese são:

- Agentes de IA já são aplicados no SDLC para acelerar entregas e supervisionar código gerado por LLMs
- A IA, se trabalhada adequadamente, também fortalece a identidade digital ao detectar tipos de ataques em autenticações biométricas
- Com Agentes de IA executando ações em nome de pessoas, os bancos precisarão desenvolver mecanismos para verificar a autenticidade e a autorização desses Agentes
- Quantum Machine Learning explora como algoritmos quânticos podem acelerar e aprimorar tarefas de aprendizado de máquina, como otimização, clustering e análise preditiva em grandes volumes de dados financeiros

Esses exemplos mostram que a **tecnologia deve ser vista como um ecossistema interdependente**. Para capturar todo o valor, os bancos precisam romper silos organizacionais — entre áreas técnicas, negócios, compliance e experiência do cliente — e criar uma governança integrada que enxergue essas inovações como peças complementares. Isso significa redesenhar modelos operacionais, capacitar times para compreender essas conexões e estabelecer métricas que avaliem o impacto coletivo das tecnologias, não apenas resultados isolados.

Essa visão orquestrada permitirá que os bancos brasileiros mantenham a liderança conquistada e transformem essas tecnologias em vantagem competitiva sustentável.



O sucesso não virá da soma das partes, mas da capacidade de orquestrar essas tecnologias em conjunto



**Comitê:
Inovação e Tecnologia**

Rodrigo Dantas
Rodrigo Mulinari
comite.inovacao@febraban.org.br

**Grupo:
Novas Tecnologias**

Márcio Alexandre Rodrigues
tecnologia.bancaria@febraban.org.br

**Elaboração:
Febraban**

Ivo Mósca
ivo.mosca@febraban.org.br

Carolina Sansão
carolina.sansao@febraban.org.br

Bianca Silvestre Vieira
bianca.vieira@febraban.org.br

**Elaboração:
Accenture**

Douglas F. Silva
douglas.f.silva@accenture.com

Boaventura D´Avila
boaventura.m.davila@accenture.com

Ricardo Liesegang
ricardo.Liesegang@accenture.com

Gabriela Jie Han
gabriela.jie.han@accenture.com

Apoio: amazon

Tatiana Orofino
orofinot@amazon.com

Gabriel Lopes
gclopes@amazon.com