Embedded finance:

Gestão de riscos na transição para serviços financeiros integrados

pwc

Conteúdo

Introdução

O *embedded finance* apresenta possibilidades atraentes para as empresas alcançarem clientes de novas maneiras, criar escala operacional e repensar como os produtos e serviços são entregues. No entanto, como de costume, essas oportunidades vêm acompanhadas de riscos.

O sucesso em todo o espectro do *embedded finance* – desde tecnologia única no ponto de venda (*Point of Sale*, na sigla em inglês) até soluções para integração total com vários terceiros – requer uma grande mudança de mentalidade e desenvolvimento de capacidades.

Nossa estrutura proprietária de risco define cinco áreas emergentes a serem consideradas pelos participantes dos ecossistemas financeiros, estendendo-se além das ameaças inerentes aos produtos financeiros. Elas incluem: interoperabilidade, administração de dados, parcerias complexas, clientes vulneráveis e riscos distribuídos. A compreensão de cada uma delas é fundamental para gerenciar esses riscos de maneira prudente e colaborativa.

Confrontando o risco existente

Apesar da necessidade de monitorar os riscos emergentes descritos em nossa estrutura, tanto as instituições financeiras tradicionais quanto as novas devem continuar atentas aos cenários de ameaças que já existem. Os riscos tradicionais decorrentes de crédito, liquidez, taxas de juros e operações continuam relevantes, conforme destacado pelo recente estresse nos mercados bancários dos EUA e da Europa.

À medida que os líderes se preparam para operacionalizar o *embedded finance*, eles precisam reconhecer e enfrentar esses riscos de mercado de frente, se quiserem competir em um cenário econômico em constante mudança. Por exemplo, bancos que ocupam um papel de utilidade dentro dos ecossistemas – como um parceiro licenciado ou um provedor de liquidez – podem ficar com atividades altamente regulamentadas e caras, que rendem pouco em termos de dados e retornos aos clientes.

Bancos e varejistas menores podem ter dificuldades para se estabelecer no mercado à medida que a consolidação se torna mais abrangente diante dos ventos contrários do setor. Já a consolidação dos maiores *players* – incluindo bancos "grandes demais para falir" e *big-techs* – poderia criar uma vantagem competitiva intransponível em ecossistemas que prendem os clientes aos provedores de *embedded finance*.

Para os CEOs de serviços financeiros no mundo, os principais riscos nos próximos cinco anos são volatilidade econômica (34%), riscos cibernéticos (33%) e inflação (30%).

Já para os CEOs de serviços financeiros brasileiros, são instabilidade macroeconômica (46%), riscos cibernéticos (39%) e inflação (32%).

26ª Pesquisa Anual Global de CEOs da PwC (Global e Brasil)

Gestão de riscos e integração tecnológica

A entrega de soluções de *embedded finance* começa com uma tecnologia bem integrada. Além dos riscos de mercado, as instituições financeiras e os novos *players* estão enfrentando um conjunto crescente de ameaças vinculadas à atualização de *stacks* tecnológicos e integração simplificada de APIs. Essas novas tecnologias financeiras devem proteger a integridade das transações e os dados dos clientes, fornecer autenticação e autorização contínuas e permitir a criação de trilhas de auditoria visíveis.

No entanto, garantir que as *embedded applications* sejam alavancadas pela tecnologia que atente às regras regulatórias e de conformidade, preservando o propósito de integração e facilidade, representa um desafio significativo para as instituições financeiras estabelecidas em que a tecnologia antiga ainda é comum. Também é difícil para as fintechs competirem pelo acesso ao mercado sem os recursos adequados de gerenciamento de riscos, o que pode resultar na perda da confiança do consumidor devido a vazamentos e violações de dados, além de atividades fraudulentas e produtos inoperáveis.

APIs: oferecendo experiências sem atrito para o cliente

A solução técnica de APIs permite a comunicação completa entre entidades financeiras e não financeiras em ofertas de serviços bancários como serviço (*banking-as-a-service*, na sigla em inglês), pagamentos como serviço (*payment-as-a-service*, na sigla em inglês) e seguros como serviço (*insurance-as-a-service*, na sigla em inglês). Eles facilitam uma gama cada vez maior de plataformas e soluções digitais, desde sites de comércio eletrônico até carteiras digitais. Essas e outras tecnologias permitem que os clientes acessem os serviços de forma rápida e contínua, seja comprando bens e serviços, garantindo um empréstimo ou gerenciando um portfólio financeiro.

A estrutura de risco de *embedded finance*

Identificamos cinco elementos que influenciam a jornada do *embedded finance:* interoperabilidade, administração de dados, parcerias complexas, clientes vulneráveis e risco distribuído. Novas áreas de foco dentro desses tópicos apontam para importantes consequências de riscos para todos os *players*, mas particularmente para os bancos, que devem ampliar suas prioridades em: transformação tecnológica, foco em *data-enabled customer* e uma abordagem empreendedora para construção de relacionamento.

Os cinco elementos da estrutura de risco do *embedded finance*

Interoperabilidade: riscos associados à conexão e comunicação entre componentes fundamentais que permitem o *embedded finance:* tecnologia como APIs, microsserviços, nuvem privada e resiliência operacional, em resposta a incidentes e recuperação de desastres.

Administração de dados: questões de segurança, privacidade e controle de dados em relação ao uso e propriedade de informações fracionadas que geralmente estão em desacordo com as expectativas de excelência dos consumidores e clientes em suas interações e transações.

Parcerias complexas: riscos decorrentes da natureza única da complexidade de parcerias do *embedded finance,* como "um para muitos" (*one to many*), responsabilidade compartilhada e relacionamentos de terceiros, quartos e quintos com provedores, vendedores e instituições financeiras.

Clientes vulneráveis: preocupações específicas do cliente relacionadas a parcerias entre instituições financeiramente regulamentadas e não regulamentadas, incluindo: aumento da coleta de dados, criação de perfis e monetização, senso de cuidado com o cliente, marketing, venda cruzada e retenção e fidelidade do cliente.

Risco distribuído: o aumento exponencial na transferência de risco dentro de ecossistemas de *embedded finance* complexos – reforçando a necessidade de desenvolver uma abordagem eficaz de gerenciamento para riscos distribuídos e mudança de responsabilidade.

Interoperabilidade

Por natureza, o *embedded finance* depende da interoperabilidade, que é ter a arquitetura de nuvem, serviços de autenticação e tecnologia API adequados para facilitar transações entre organizações. No entanto, como os ecossistemas que o sustentam envolvem necessariamente vários parceiros intermediários – como fintechs, provedores de infraestrutura, de plataforma e bancos – eles devem ser gerenciados com cuidado.

Para fazer isso, as empresas exigem novos recursos tecnológicos e uma estratégia consistente que inclua maior consideração de responsabilidade e os riscos relacionados à interoperabilidade de componentes entre tecnologias, experiência do usuário e do cliente (UX e CX) e parceiros do ecossistema. Também deve definir abordagens para arquitetura aberta baseada em nuvem, uma vez que as empresas estão sendo observadas pelos reguladores e algumas multas significativas estão sendo aplicadas para restringir o acesso de desenvolvedores terceirizados a suas plataformas.

As instituições financeiras precisam atualizar seu *stack* tecnológico e tomar medidas em direção à arquitetura aberta, desenvolvendo recursos e talentos digitais, ao mesmo tempo em que aprimoram o gerenciamento de riscos. O mesmo vale para fintechs orientadas a produtos, que não estão acostumadas a incorporar práticas de risco na medida necessária para a governança e entrega de *embedded finance*. Quem demonstrar uma função de gerenciamento de risco confiável, adaptada para lidar com ameaças operacionais e de conformidade únicas e emergentes, será o vencedor neste mercado competitivo.

Uma estratégia de interoperabilidade articulada também pode reduzir custos e aumentar a receita e as oportunidades de negócios. A arquitetura aberta é a base para os bancos desenvolverem suas capacidades tecnológicas e oferecerem serviços e soluções financeiras inovadoras, que sejam compatíveis e personalizáveis em todas as plataformas. Isso pode levar a uma vantagem competitiva se os bancos forem reconhecidos pelo seu software e sua tecnologia – em vez de apenas fornecedores de serviços financeiros tradicionais e regulamentados.

Esses recursos também aumentam o escopo de serviços que os bancos e outras instituições financeiras podem fornecer às plataformas voltadas para o cliente, incluindo a integração de produtos e serviços existentes em ecossistemas de *embedded finance.*

Administração de dados

Os dados permitem que as empresas mantenham a fidelidade do cliente em ecossistemas específicos e sustentam o fornecimento de experiências contínuas — sem interromper as compras. No entanto, a complexidade das arquiteturas abertas aumenta a propriedade parcial e o uso de dados. As informações normalmente são trocadas entre vários *players* de um ecossistema, desde a formulação de contratos de privacidade e compartilhamento de dados até a obtenção de consentimento.

Questões mais amplas sobre práticas de aquisição, propriedade, uso, retenção e descarte de dados representam riscos significativos, juntamente com preocupações de segurança, como roubos, violações e ataques cibernéticos. Ações judiciais coletivas recentes foram movidas contra fintechs por práticas negligentes de segurança de dados e pela coleta e venda deles sem consentimento. Por sua vez, os bancos foram multados por vazamentos de dados em suas plataformas on-line e descarte indevido de hardware por meio de fornecedores terceirizados.

Os regulamentos de privacidade de dados e o escrutínio das agências de vigilância do consumidor aumentarão a pressão sobre as funções de risco. Os clientes se sentem ameaçados devido ao uso indevido de dados intencionalmente ou ao manuseio impróprio e não intencional. Reguladores como o *Consumer Financial Protection Bureau* nos EUA publicaram novas diretrizes que visam fornecer aos consumidores do *embedded finance*, como aqueles que usam aplicativos “Compre Agora, Pague Depois”, as mesmas proteções que os usuários de cartão de crédito.

Para combater esses riscos e garantir fortes controles sobre segurança de dados, privacidade e proteção do consumidor, as organizações em redes *embedded finance* exigem programas de governança de dados e gerenciamento de riscos tecnológicos mais sofisticados do que os existentes.

Compartilhar dados de clientes entre organizações financeiras, plataformas digitais e fintechs lideradas por produtos cria novas vulnerabilidades. *Players* menores ou mais novos muitas vezes carecem de conhecimento, eficácia operacional ou mesmo destreza organizacional para analisar riscos diligentes para dados. Bancos maiores e outras instituições financeiras, que construíram reputação como administradores de dados, agora precisam fazer mais por meio de esforços coletivos e coordenados para manter a segurança, a confiança e a lealdade do cliente.

As organizações também precisarão estar sintonizadas com os riscos emergentes de novos modelos e algoritmos que consomem e transformam dados alternativos. Isso pode levar a desafios como informações (e suas análises) sendo usadas de maneiras injustas, discriminatórias ou não transparentes.

A proliferação de APIs exige um forte inventário e gerenciamento de alterações, bem como controle de documentação para mitigar vazamentos de dados e riscos. Quando as proteções são bem feitas, as instituições financeiras podem acessar as informações dos clientes e seus dados financeiros, incluindo comportamentos e preferências de compra, que podem ser usados para adaptar novos produtos e serviços, além de promover oportunidades de vendas cruzadas entre os parceiros do ecossistema.

Parcerias complexas

Em *embedded finance,* os riscos de parceria são muito mais amplos, devido às complexidades da arquitetura aberta, das novas estratégias de monetização e da necessidade de mudar de uma mentalidade de gerenciamento da responsabilidade para uma abordagem mais empreendedora.

Veja o caso de um grande varejista que busca oferecer serviços bancários aos seus clientes. Ele utiliza a gestão de suas parcerias com distribuidores, fornecedores e transportadoras e é suscetível aos riscos operacionais, de produto e financeiros. No entanto, suas capacidades não se estendem a parcerias com bancos, fintechs e outros fornecedores financeiros.

Para seus gerentes de risco, trabalhar de forma eficaz com instituições financeiras envolverá a construção de um certo grau de conhecimento interno em áreas como novas taxonomias de risco, liquidez, escrutínio regulatório, “conheça seu cliente” (*Know Your Client*, na sigla em inglês), comunicações de termos e condições etc. Por outro lado, as instituições financeiras devem se aprimorar para entender e se integrar às práticas de empresas não financeiras.

Outro exemplo é a parceria bidirecional que precisa existir entre fintechs e organizações patrocinadoras, como um banco ou uma seguradora. É necessário que o banco entenda como as fintechs gerenciam riscos e obrigações de maneira eficaz, sem apenas transferir os subjacentes de volta para elas. As fintechs precisam acessar o *stack* tecnológico do banco e também devem entender como os serviços de suporte são executados, como subscrição de crédito, KYC e monitoramento de transações.

Com essa abordagem, as empresas não apenas diversificam sua exposição ao risco, mas também criam um processo de negócios resiliente e um ecossistema de TI que permite agilidade. Com as parcerias certas, as empresas podem entrar no mercado de *embedded finance*, criando produtos e serviços inovadores dentro do ambiente disruptivo das fintechs.

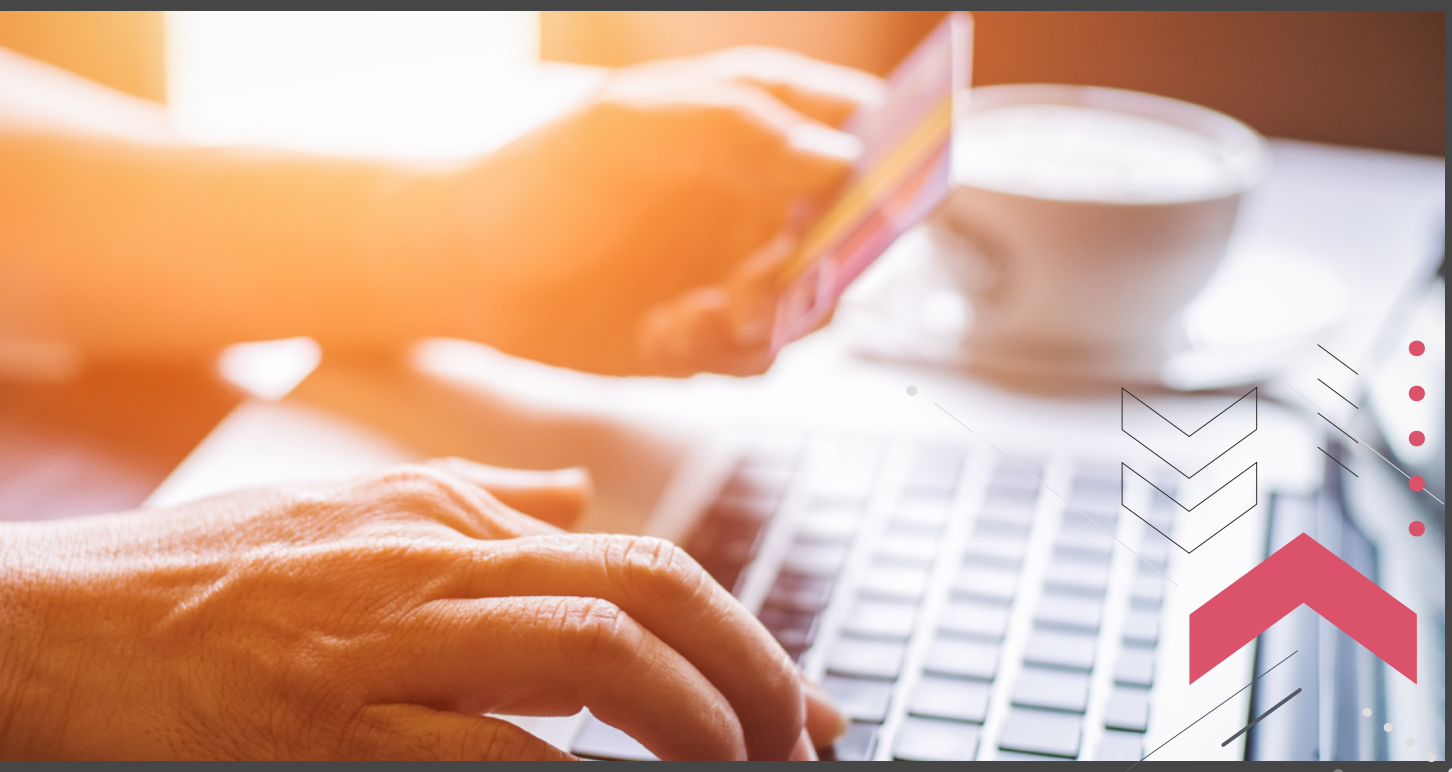
Clientes vulneráveis

As soluções de *embedded finance* permitem que organizações não bancárias forneçam serviços financeiros sem assumir uma significativa carga regulatória. Isso cria um risco único em relação à propriedade do cliente para todas as partes e para organizações financeiras.

Por exemplo, uma empresa de manufatura oferece aos clientes um cartão de crédito que permite acesso a um financiamento especial quando usado na organização. Para permitir que o fabricante reconheça a receita desses gastos, ele cria uma nova empresa para aproveitar uma instituição financeira como prestadora de serviço e financiadora das contas. Ele também se envolve com um processador de pagamento global como intermediário entre esse *servicer* e o banco do cliente para maximizar os *end-points* em que esses cartões podem ser usados.

Há muitas perguntas para cada parte desse ecossistema: quem é o responsável pelo relacionamento com o cliente? O banco pode fazer vendas cruzadas para esse cliente com empréstimos e outras oportunidades de crédito? Quem é responsável pelo dever de cuidar dos clientes que são incentivados a gastar – mesmo sem poder?

Uma empresa de manufatura geralmente não precisa considerar a posse do cliente quando seus produtos são comprados, mas um empreendimento *embedded finance* deve fazê-lo – dando aos parceiros direitos suficientes no relacionamento com o cliente para que seja favorável para eles também. Além disso, as organizações devem gerenciar os riscos associados à forma como eles e seus parceiros se comunicam com os consumidores e constroem fidelidade à marca de seus produtos e serviços.



Risco distribuído

O risco distribuído – o aumento na transferência entre ecossistemas complexos – é o ponto culminante de todas as ameaças que descrevemos até aqui. Ele é compartilhado por muitos *players* e existe há décadas nas relações financeiras, por exemplo, um banco pode usar um modelo "*white-label*" em seus serviços por meio de um provedor de cartão de crédito e um processador de pagamentos. No entanto, o risco se tornou maior em ecossistemas integrados que envolvem mais *players* tocando os mesmos dados e transações, muitas vezes ao mesmo tempo.

Bancos regulamentados e instituições financeiras, que são responsáveis por proteger os dados do cliente à medida que passam pelo ecossistema distribuído, assumem responsabilidades adicionais de proteção com relacionamentos bancários abertos. A falta de conscientização e conhecimento sobre as práticas de segurança e gerenciamento de riscos de fornecedores terceiros, quartos e quintos pode, rapidamente, sair do controle.

Riscos existem em diversos pontos de falha de segurança, privacidade de dados, lavagem de dinheiro e outras práticas e vulnerabilidades. Reguladores e entidades de vigilância estão aumentando seu escrutínio em relação a essas áreas. Um caso recente envolveu reguladores dos EUA ordenando um banco que melhorasse sua supervisão de parcerias com fintechs terceirizadas, depois que um grupo de advogados especialistas expressou preocupação com suas práticas.

Algumas complicações incluem maior ambiguidade em torno de insights e propriedade de risco, relacionamentos extensos e sem transparência com quarta e quinta partes e fluxos de transações complexos ou de "tipo misto", tanto nacional quanto internacionalmente. Olhando para o futuro, as tecnologias emergentes, incluindo Web 3.0, metaverso e finanças descentralizadas (*Decentralized finance* – DeFi, na sigla em inglês), provavelmente aumentarão os riscos distribuídos, ampliando ainda mais o número de *players* e parceiros nos ecossistemas *embedded finance*. Um fator agravante neste contexto é a falta de estruturas regulatórias para pagamentos alternativos, instrumentos financeiros ou ativos digitais como *stablecoins*, criptomoedas e *tokens* não fungíveis (NFTs).

Ao lidar com o risco distribuído, as práticas tradicionais de gerenciamento permanecem eficazes, mas as empresas devem reforçá-las com novas técnicas e abordagens para garantir supervisão e mitigação eficientes, quando apropriado. A implementação de estruturas de gerenciamento de riscos e a operacionalização de programas periódicos para avaliação de ameaças de terceiros podem ajudar a identificar os riscos distribuídos entre as várias partes do fornecedor.

A instituição de políticas de gerenciamento de identidade e acesso (*Identity Access Management*, na sigla em inglês), incluindo confiança zero e controle de acesso com privilégios mínimos, pode evitar consequências, como roubo de dados, ataques para recusa de serviço e de injeção de *malware*, para citar alguns. Práticas bem conhecidas, como transferência, prevenção e aprovação, ainda são apropriadas para ajudar a mitigar os riscos. Mas é crucial desafiar os vieses e as experiências organizacionais históricas – especialmente à medida que os riscos distribuídos evoluem com a adoção do *embedded finance.*

Conforme a conversa muda do risco puro e da resiliência para a preservação do valor – e, eventualmente, para o valor criado por meio das receitas do *embedded finance* – a complacência não é uma opção. Em todos esses ecossistemas, o crescimento das organizações dependerá da sua capacidade de reconhecer e adaptar seus modelos de negócios – e antecipar e gerenciar os riscos que estão por vir.

Sobre a publicação

Este conteúdo faz parte de uma série de três artigos, produzidos pela PwC Global em parceria com a PwC Brasil, que busca oferecer insights sobre casos de uso de *embedded finance,* incluindo ecossistemas de negócios emergentes.

Contatos

Lindomar Schmoller

Sócio e líder de Serviços Financeiros
da PwC Brasil

lindomar.schmoller@pwc.com

Willer Marcondes

Sócio Strategy& Brasil e líder de estratégia
para Serviços Financeiros

willer.marcondes@pwc.com

Catarina Lyra

Diretora na Prática de Transformação em
Serviços Financeiros da PwC Brasil

catarina.lyra@pwc.com

pwc

www.pwc.com.br

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil