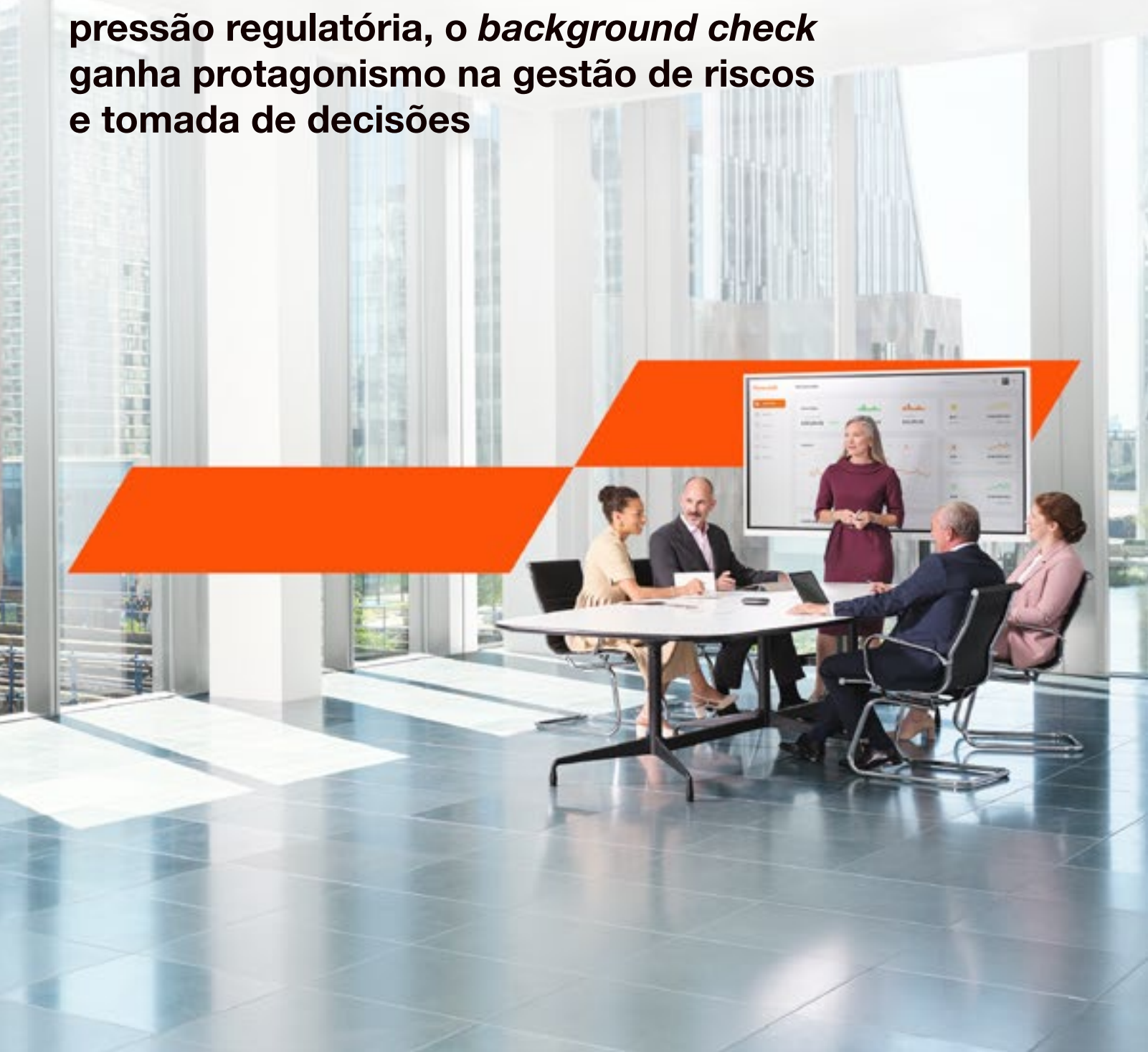
Como o *background check* protege operações, reputação e ajuda a evitar fraudes

Em um cenário de fraudes crescentes e maior pressão regulatória, o *background check* ganha protagonismo na gestão de riscos e tomada de decisões



Conteúdo

Apresentação **03**

01 Prevenção de riscos e proteção da marca **10**

02 Contexto legislativo **13**

03 Em diferentes setores, checagens internas e externas **20**

04 Personalização e segurança nas operações **25**

Considerações finais **29**

Contatos **33**

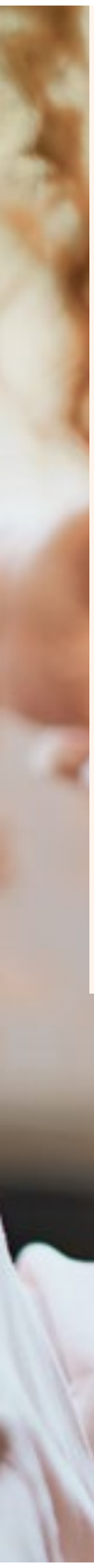
Apresentação

Em um ambiente de negócios cada vez mais complexo e digital, quem toma decisões já percebeu que verificar informações sobre clientes, fornecedores, parceiros e colaboradores deixou de ser apenas uma boa prática.

O *background check* – processo de análise reputacional e de dados relevantes sobre pessoas físicas ou jurídicas – tem ganhado protagonismo em diferentes setores da economia, impulsionado pelo aumento de fraudes, crescimento da procura por crédito, fortalecimento das exigências regulatórias no Brasil e nos Estados Unidos e pela necessidade de zelar pela reputação das empresas, executivos, diretores, fornecedores e demais envolvidos.

A preocupação ultrapassa fronteiras. A Pesquisa Global sobre Fraudes e Crimes Econômicos 2024, realizada pela PwC, ouviu aproximadamente 2.500 pessoas nas Américas, Europa, Oriente Médio e Ásia Pacífico – dois terços eram executivos de alto escalão e 40% eram de empresas com receita acima de US$ 1 bilhão.

As respostas mostram algo que muitas lideranças já sentem na prática: a fraude, em todas as suas formas, é um desafio constante. Uma das formas mais antigas, a fraude em *procurement* – conluio, superfaturamento, notas fiscais falsas e produtos de qualidade inferior com objetivos ilícitos –, que acontece em contratos de compra, foi citada entre os três crimes econômicos mais disruptivos enfrentados pelas organizações em todo o mundo (atrás do crime cibernético e da corrupção).



55%

dos entrevistados afirmaram que fraudes em *procurement* são uma preocupação em seus países, mas apenas uma minoria adota as ferramentas disponíveis no mercado para identificá-las ou combatê-las.

45%

disseram que não têm programas de gestão de riscos de terceiros ou não realizam nenhuma forma de pontuação de risco (*risk scoring*) como parte deles.



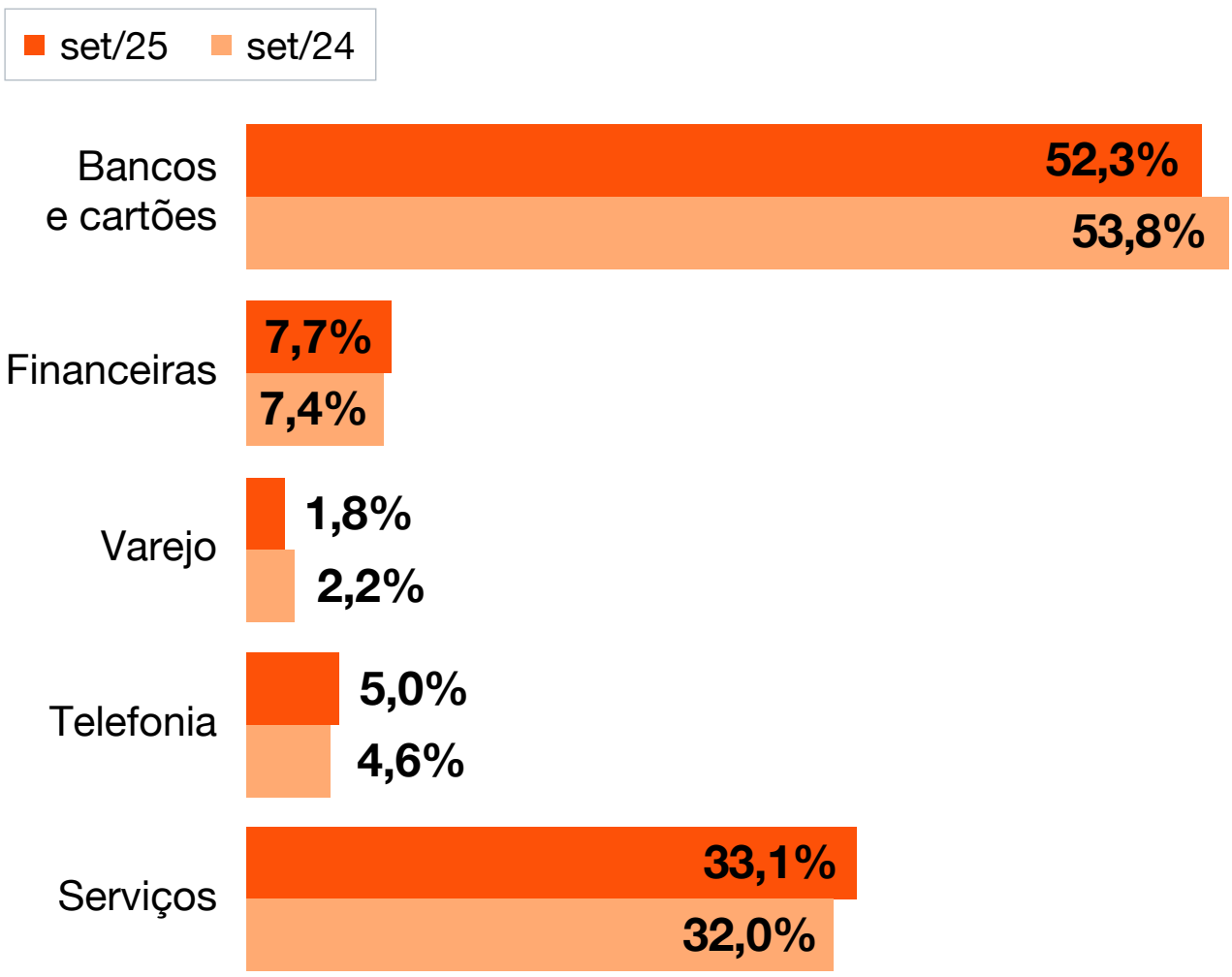
No mundo, o mercado de detecção e prevenção a fraudes deve crescer 16,98% ao ano até 2030, segundo estimativa da Verified Market Research (VMR), divulgada via PRNewswire. No Brasil, seis em cada dez empresas consideram a prevenção a fraudes como prioridade estratégica.

Dados do Indicador de Tentativas de Fraude da Serasa Experian mostram que o país registrou 10.886.982 tentativas de fraude de janeiro a setembro de 2025 – um aumento de 28,6% em relação ao mesmo período de 2024. Isso significa que houve uma ocorrência a cada dois segundos.

Além disso, o levantamento aponta que bancos, emissores de cartões e instituições financeiras somaram 60% das tentativas de fraude em nove meses. As inconsistências cadastrais foram a principal modalidade (51,4%), seguidas por autenticidade de documentos e biometria (33%) e comportamentos suspeitos em dispositivos (15,6%).

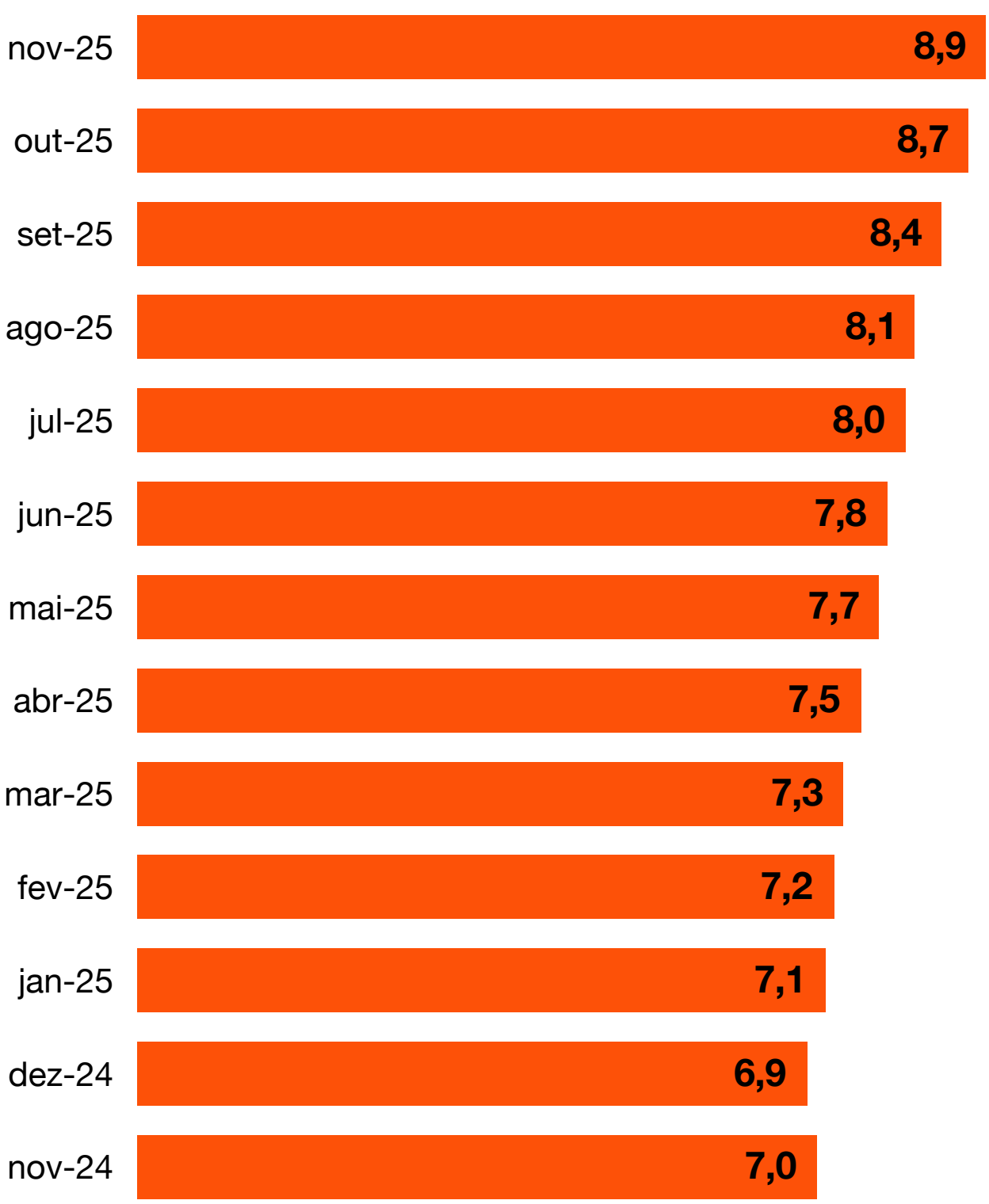
Indicador de tentativas de fraude – Por setor (%)

Janeiro a setembro 2024 x 2025



Outro fator que entra diretamente na mesa de decisão é o cenário econômico, que aumenta os riscos em relações comerciais, concessões de crédito e contratos de fornecimento. O Serasa Experian apontou que a inadimplência bateu recorde histórico em novembro de 2025, quando alcançou 8,9 milhões de empresas brasileiras com R$ 210 bilhões em dívidas.

Quantidade de empresas inadimplentes (milhões)



Fonte: Serasa Experian

As micro, pequenas e médias empresas representam a maior parte das inadimplentes. São 57,7 milhões de dívidas negativadas. Para analistas, as companhias de menor porte são mais vulneráveis a ciclos de crédito mais restritivos.

Com menor acesso a crédito, menor poder de negociação com fornecedores e margens mais apertadas, essas empresas tendem a sentir de forma mais intensa os efeitos de ciclos econômicos restritivos, como juros elevados, inflação persistente e retração do consumo.



Quando passam a operar no limite do fluxo de caixa, recorrem a prazos mais longos com fornecedores ou assumem dívidas com custos mais elevados. Esse cenário aumenta o risco de inadimplência não apenas dessas organizações, mas também de toda a cadeia com a qual se relacionam, gerando um efeito cascata.

Entre as principais estratégias para evitar prejuízo estão a revisão de custos operacionais, a renegociação de dívidas, a diversificação de fontes de receita e, sobretudo, o aumento do rigor na concessão de crédito a clientes e parceiros. Há também um movimento crescente de profissionalização da gestão financeira, com maior uso de dados para tomada de decisão.

É nesse ponto que o *background check* ganha relevância estratégica. Ao permitir uma análise mais aprofundada do histórico financeiro, jurídico e reputacional de clientes, fornecedores e parceiros, ele ajuda empresas a tomar decisões mais seguras, reduzindo a exposição a inadimplência e fraudes.



Já existem formas de automatizar esse processo com ferramentas que possibilitam, por exemplo, identificar sinais de alerta como histórico de atrasos, envolvimento em litígios ou inconsistências cadastrais, permitindo que as companhias ajustem limites de crédito, negociem garantias ou até evitem determinadas relações comerciais.

Assim, em um cenário de maior pressão financeira, o uso inteligente de dados – especialmente por meio de soluções de *background check* – é um aliado importante para a sustentabilidade e o crescimento do negócio, em especial das empresas de menor porte, que precisam equilibrar expansão e controle de riscos com ainda mais precisão.



“Em um ambiente de negócios pressionado por fraudes, inadimplência e exigências regulatórias, o desafio passou a ser tomar decisões mais complexas com base em volumes crescentes de informação. O ponto central está em transformar dados dispersos em inteligência capaz de reduzir incertezas, antecipar riscos e sustentar decisões mais seguras ao longo de toda a cadeia de relacionamento, sempre respeitando os limites legais, éticos e regulatórios do uso de dados.”

Elisa Mayor,
sócia de Serviços Forenses da PwC Brasil

01

Prevenção de riscos e proteção da marca

Neste contexto, conhecer com profundidade quem está do outro lado de uma negociação se torna essencial para evitar prejuízos financeiros, danos reputacionais e, em alguns casos, até sanções. O *background check* é um processo estruturado de coleta, validação e análise de informações sobre indivíduos ou organizações antes do estabelecimento de qualquer relação comercial ou contratual, contribuindo para decisões mais seguras e alinhadas à estratégia da empresa.

No Brasil, há ampla disponibilidade de dados públicos e oficiais, como registros da Receita Federal, informações judiciais, cadastros societários e listas restritivas.
O principal desafio, no entanto, não é a falta de dados, mas a fragmentação dessas informações em centenas de fontes distintas. Quando analisados de forma isolada, esses dados oferecem apenas visões parciais do risco.

Ao integrar diferentes camadas de informações – como dados cadastrais, histórico financeiro, processos judiciais, participação societária, sanções e exposição negativa na mídia – o resultado é um *score* de risco mais robusto e contextualizado, capaz de apoiar decisões com mais velocidade, precisão e segurança ao longo de toda a relação comercial.

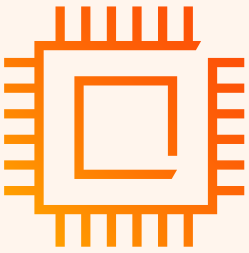
Segundo André Nigro, Chief Revenue Officer (CRO) da Zoox Smart Data, a integração dessas informações representa um avanço relevante na forma como empresas lidam com risco. Quando diferentes bases passam a ser analisadas de forma integrada, o *background check* deixa de ser um processo operacional e passa a apoiar decisões estratégicas, com impactos diretos na concessão de crédito, na escolha de parceiros e na gestão de riscos ao longo do tempo.



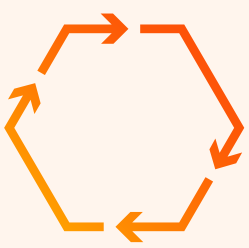
Esse avanço tecnológico também amplia o escopo da análise. Para Elisa Mayor, sócia de Serviços Forenses da PwC Brasil, o uso de dados não estruturados e contextuais tem ganhado relevância nas avaliações de risco. Informações como menções em mídia, padrões de geolocalização, redes de relacionamento e recorrência de contatos não oferecem respostas binárias, já que não indicam isoladamente se há ou não risco. No entanto, quando analisadas em conjunto, ajudam a revelar padrões e conexões que dificilmente seriam identificados por métodos tradicionais.

O objetivo é simples: reduzir incertezas. Ao consolidar informações provenientes de diversas bases públicas e privadas, é possível tomar decisões mais seguras sobre contratação de colaboradores, escolha de fornecedores, abertura de crédito ou formação de alianças estratégicas. Esse tipo de diligência também se tornou uma peça-chave nos programas de *compliance*, especialmente em setores que lidam com grandes volumes de dados e transações financeiras.

Como funciona o *background check* da Zoox



Tecnologia de ponta: ferramentas de IA e *machine learning* reúnem e analisam grandes volumes de dados em tempo real. Em segundos, podem detectar padrões suspeitos, informações desconectadas e indícios de fraude com precisão.



Análise 360°: ao realizar uma varredura completa de CPF ou CNPJ, é possível indicar riscos a curto, médio e longo prazo.



Fácil integração: para agilizar o trabalho, vale integrar a solução a sistemas existentes e já usados pela empresa e pelos seus colaboradores-chave.

02

Contexto legislativo

Além dos processos internos, há um ponto que não pode ser ignorado: o arcabouço regulatório brasileiro voltado ao combate a crimes financeiros. As empresas têm obrigação legal de evitar fraudes e lavagem de dinheiro, entre outras ações, já que isso é fundamental para preservação da integridade do sistema financeiro, mitigação de riscos legais e reputacionais e fortalecimento da confiança nos mercados e nas relações de negócio.

O Decreto nº **11.129/22** regulamenta a Lei Anticorrupção (nº **12.846/13**) e traz diretrizes claras sobre Programas de Integridade. Entre elas, destaca-se o uso de diligências apropriadas, com base em riscos, na contratação e na supervisão de terceiros – como fornecedores, prestadores de serviço, intermediários, despachantes, consultores, representantes comerciais e associados – além de Pessoas Politicamente Expostas (PEPs).

Isso acontece porque a Lei Anticorrupção estabelece a responsabilidade objetiva da pessoa jurídica. Na prática, a organização pode ser responsabilizada por atos lesivos praticados por terceiros que venham a beneficiá-la, mesmo sem seu conhecimento. Esse cenário amplia os riscos nas contratações e reforça a importância de conduzir diligências adequadas e proporcionais ao risco envolvido.

A **Lei nº 9.613/1998**, com as alterações promovidas pela Lei nº 12.683/2012, conhecida como Lei de Lavagem de Dinheiro, instituiu o sistema nacional de prevenção e combate a esse tipo de crime. A legislação determina, entre outros pontos, que empresas e instituições mantenham cadastro atualizado de clientes, registrem operações e comuniquem atividades suspeitas às autoridades competentes.



A estrutura regulatória foi posteriormente ampliada por normas de supervisão e por diretrizes de órgãos como o Conselho de Controle de Atividades Financeiras (Coaf), o Banco Central do Brasil (BC) e a Comissão de Valores Mobiliários (CVM).



Além do arcabouço regulatório formal, o próprio mercado tem avançado em iniciativas de autorregulação voltadas à prevenção de crimes financeiros. Um exemplo disso é o lançamento de selos de conformidade em PLD/FTP por entidades representativas dos setores financeiro e de tecnologia. A proposta é clara: estabelecer parâmetros mínimos de boas práticas, incentivar a transparência e reforçar a responsabilidade das empresas na gestão de riscos.

Esse movimento sinaliza o amadurecimento do ecossistema e reforça uma expectativa cada vez mais presente: diligências estruturadas deixam de ser um diferencial competitivo e passam a integrar o padrão operacional das organizações.

As regras exigem que as organizações implementem políticas, procedimentos e controles internos capazes de identificar riscos e prevenir irregularidades, incluindo possíveis tentativas de lavagem de dinheiro ou financiamento ilícito. Dessa forma, as organizações são obrigadas a reportar problemas, sob risco de sofrerem sanções por envolvimento em crimes.

Ferramentas tecnológicas de *background check* ajudam a transformar uma obrigação regulatória em um processo eficiente e escalável, pois facilitam a checagem de dados, com agilidade e precisão.

Uma plataforma de *background check* pode realizar consultas automatizadas em centenas de fontes de informação, cruzando dados e apontando eventuais inconsistências ou sinais de alerta em poucos segundos. Isso permite que empresas mantenham processos de *Know Your Partner* (KYP)*, Know Your Employee* (KYE) e outras práticas de diligência exigidas por reguladores e programas de integridade.

A possibilidade de personalização é mais um aspecto fundamental. Cada organização enfrenta riscos específicos – que variam conforme setor, porte, modelo de negócios e perfil de clientes. Por isso, é possível configurar aspectos diferentes de análise, desde verificações cadastrais básicas até investigações sobre reputação, estrutura societária ou exposição a sanções e listas restritivas.

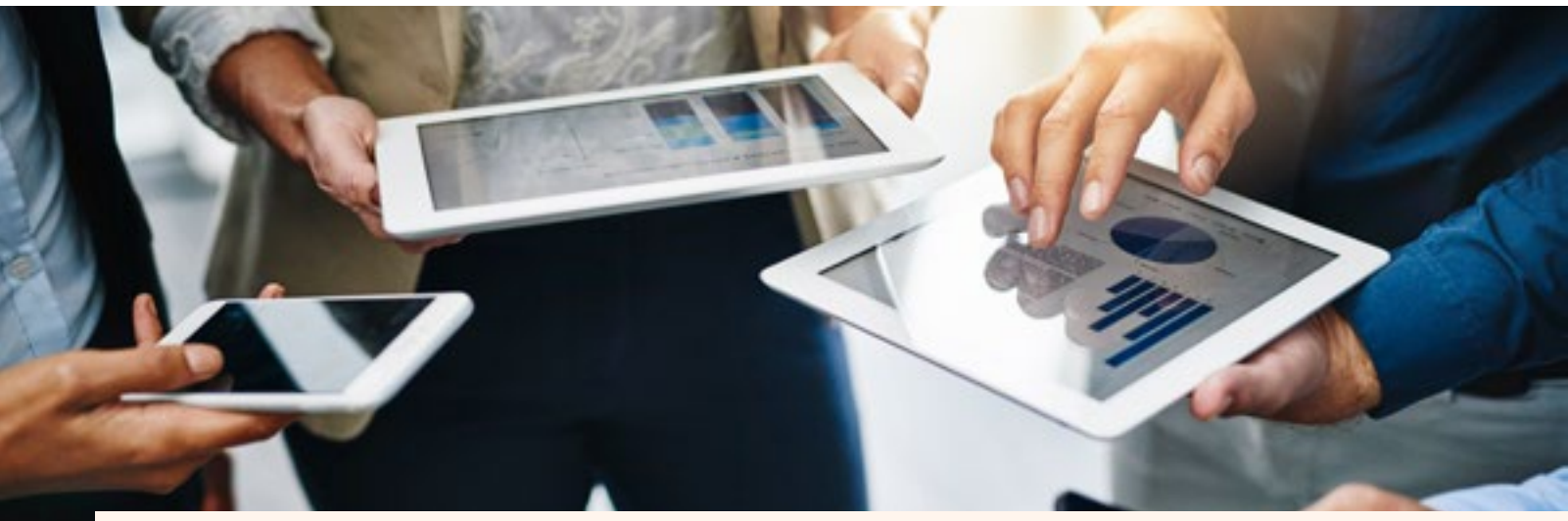
Com relação à Lei Geral de Proteção de Dados (LGPD), a Zoox Smart Data esclarece que o serviço de verificação deve ter uma finalidade específica e o uso da ferramenta deve ser limitado à coleta de dados estritamente necessários. O *background check* é uma prática ética e alinhada à legislação brasileira, que deve ser realizado com informações públicas e legítimas para apoiar decisões e tornar relações e operações mais seguras.



Esse entendimento é reforçado pelo Tribunal Superior do Trabalho (TST), que considera legal a exigência de antecedentes criminais em processos seletivos, desde que haja justificativa relacionada à natureza da função. Isso se aplica ao *background check*, uma vez que a análise deve ser pertinente e não excessiva.

A legislação exige o consentimento livre, informado e inequívoco do titular dos dados, além de transparência sobre quais dados serão coletados, como serão utilizados, quem terá acesso e por quanto tempo serão armazenados. Cabe às empresas adotar medidas de segurança para proteger suas informações e garantir os direitos dos titulares, como acesso, correção e exclusão de dados.

Reclassificação de risco



O *background check* ganhou mais relevância em 2026 para empresas que atuam além das fronteiras brasileiras.

Recentemente, a decisão do governo dos Estados Unidos de designar o Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV) como organizações terroristas internacionais amplia a atenção necessária à gestão de riscos para empresas com operações, parceiros, fornecedores, clientes ou transações internacionais.

Em 28 de maio de 2026, o governo dos EUA designou o PCC e o CV como *Specially Designated Global Terrorists* (SDGT), e, em 5 de junho, também os incluiu na lista de *Foreign Terrorist Organizations* (FTO), ampliando os riscos relacionados a transações, relacionamentos comerciais e potenciais exposições regulatórias envolvendo pessoas e entidades associadas a essas organizações.

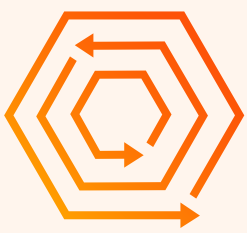
Enquanto a designação SDGT está associada, entre outros efeitos, a bloqueios de bens e restrições envolvendo pessoas e entidades designadas, a classificação como FTO pode ampliar riscos regulatórios e legais relacionados a determinadas formas de suporte, financiamento ou relacionamento com organizações designadas de acordo com a legislação aplicável.

No cenário corporativo, o tema de crime organizado passa do risco de lavagem de dinheiro e integridade para um contexto mais amplo de exposição regulatória e gestão de riscos, com possíveis implicações legais extraterritoriais.

Nesse contexto, processos estruturados de *background check, due diligence* de terceiros e monitoramento contínuo se tornam mecanismos relevantes para identificar potenciais vínculos diretos ou indiretos com pessoas, empresas ou redes de relacionamento associadas a indivíduos e entidades expostos aos referidos FTOs, permitindo decisões mais informadas e proporcionais ao risco.

Os principais impactos para empresas no Brasil são:

maior exposição a restrições e medidas internacionais, incluindo sanções internacionais, bloqueio de ativos e potencial responsabilização criminal para empresas com conexão com os EUA;



aumento da necessidade de diligência sobre fornecedores, clientes, parceiros e colaboradores;



riscos regulatórios, financeiros e reputacionais, decorrentes de potenciais vínculos diretos ou indiretos com os designados;



maior expectativa de monitoramento e *due diligence* contínua, incluindo processos de *background check*, avaliação de integridade e identificação de beneficiários finais e partes relacionadas.

Elisa Mayor, sócia de Serviços Forenses da PwC Brasil, destaca que os impactos dessas designações não se limitam a empresas com operações nos Estados Unidos. “Muitas organizações brasileiras podem estar expostas a esse tema pelo simples fato de participarem do sistema financeiro internacional. Em operações em dólar, a passagem da transação pelo sistema financeiro norte-americano pode tornar aplicáveis as regras daquele mercado, ainda que as partes envolvidas estejam fora do território norte-americano.”

O cenário se torna ainda mais desafiador diante da crescente sofisticação das estruturas utilizadas por organizações criminosas, que frequentemente buscam se inserir na economia formal por meio de empresas, intermediários, estruturas societárias complexas e mecanismos destinados a ocultar a origem e a movimentação de recursos. Esse contexto amplia os desafios relacionados à identificação de beneficiários finais, ao monitoramento de terceiros e à rastreabilidade de relações comerciais.

Em agosto de 2025, a operação “Carbono Oculto”, conduzida pelo Ministério Público de São Paulo, pela Receita Federal e pela Polícia Federal, divulgou alegações de vínculos entre integrantes do PCC e empresas ligadas a setores como combustíveis, serviços financeiros e investimentos. Posteriormente, outras investigações revelaram indícios de estruturas empresariais utilizadas para movimentação de recursos e potenciais conexões com diferentes segmentos econômicos.

Nesse contexto, o *background check*, a *due diligence* e o monitoramento contínuo se tornam ferramentas estratégicas para identificar potenciais vínculos com pessoas e empresas expostas a restrições internacionais, contribuindo para a mitigação de riscos regulatórios, financeiros e reputacionais.

03

Em diferentes setores, checagens internas e externas

Embora bancos, emissores de cartões e instituições financeiras registrem mais tentativas de fraude e estejam mais expostos a crimes financeiros e fiscais, empresas de outros setores também podem se beneficiar de ferramentas de *background check* para reduzir riscos e tomar decisões mais seguras.

Nos processos internos, por exemplo, a checagem ajuda o departamento de RH a verificar antecedentes profissionais, histórico de vínculos e possíveis inconsistências nas informações apresentadas por candidatos.

Em relação a parceiros externos, as áreas financeira e de *compliance* podem usar a análise automatizada para identificar riscos regulatórios, fraudes, conflitos de interesse ou vínculos de clientes com empresas problemáticas.

No desenvolvimento de negócios, a verificação é essencial para avaliar parceiros e fornecedores, garantindo relações comerciais mais transparentes e confiáveis, além de identificar como as empresas podem lidar melhor com as necessidades dos clientes.

Em um exemplo do setor de seguros, o uso combinado pela Zoox de *background check* e modelos preditivos se mostrou decisivo para fortalecer a saúde financeira da operação e aprimorar a tomada de decisão.

O desafio inicial da seguradora era a dificuldade em entender o comportamento do cliente e então gerar cotações precisas e competitivas. Havia ainda o desafio de fazer *cross sell* e *up sell* de seguros, além da falta de um banco de dados estruturado que ajudasse a definir a melhor abordagem de comunicação para diferentes grupos de clientes e *prospects*.

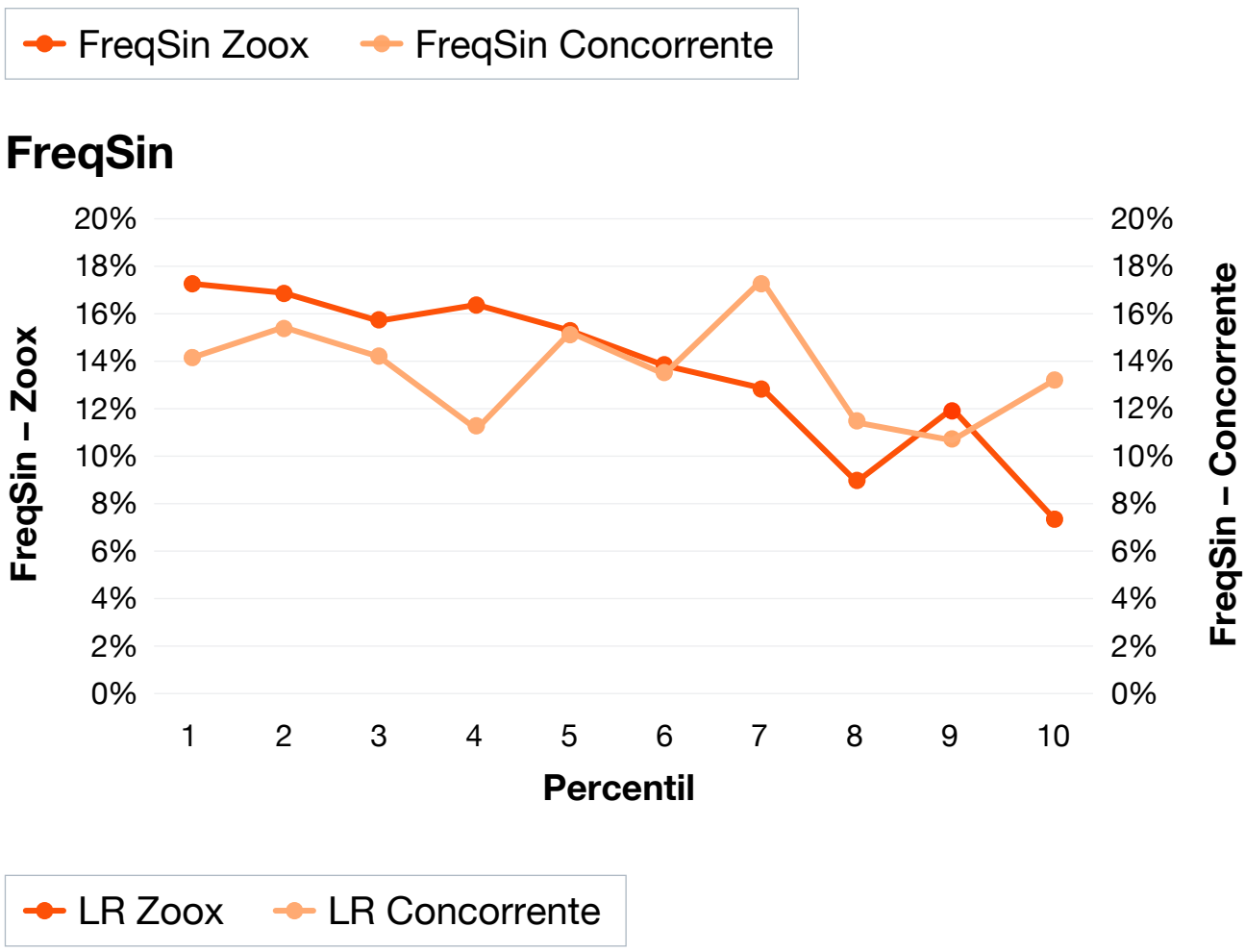
Por meio de modelos de *machine learning*, a solução permitiu uma visão unificada de clientes e *prospects*, resultando em uma precificação mais segura e segmentada. Foram desenvolvidos três modelos específicos para colisão, roubo e furto, que superaram as opções vigentes no mercado.

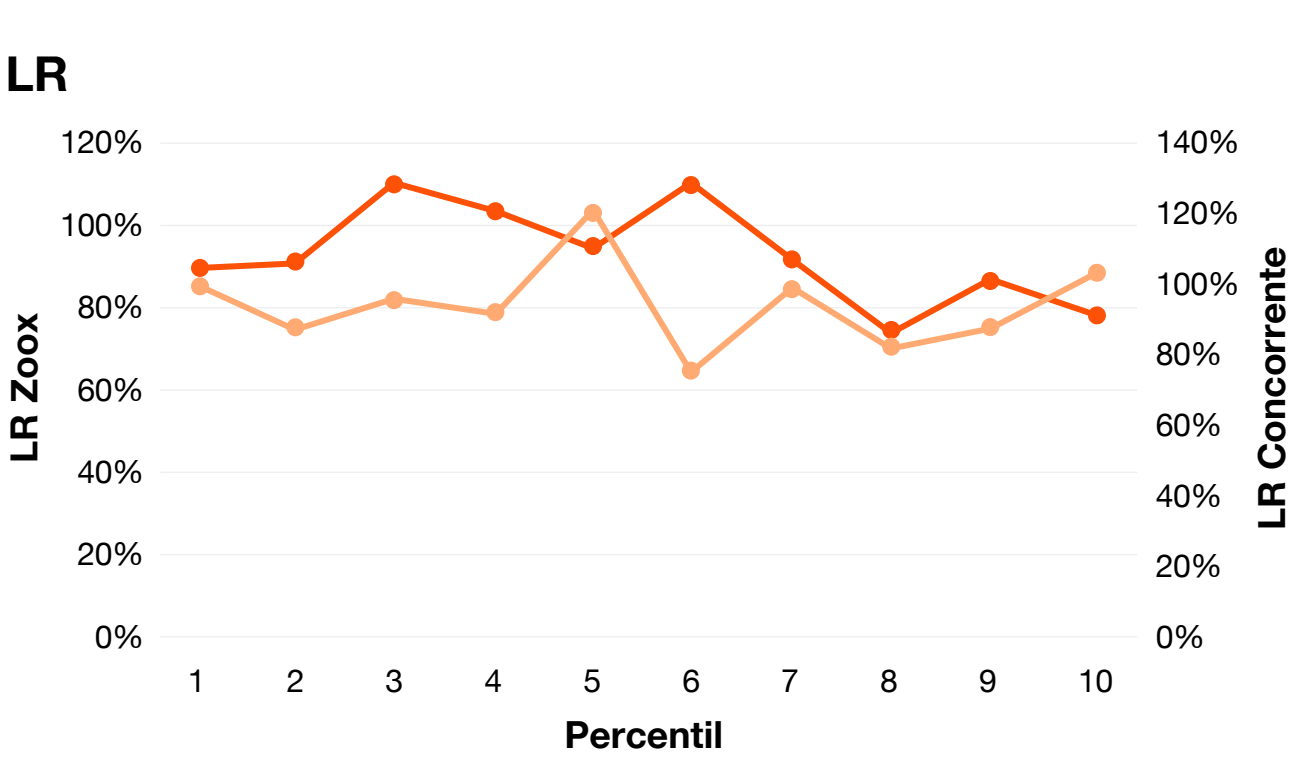


Entre os diferenciais adotados nesse tipo de iniciativa está o uso de sistemas avançados de *geoanalytics*, que permitem mapear áreas de sinistro, identificar zonas de maior risco e realizar análises georreferenciadas com maior precisão.

Como resultado prático, a eficácia da checagem estruturada projeta um retorno estimado de R$ 7,3 milhões por ano em receitas de prêmios, ao ajustar preços em riscos elevados e reduzir perdas com sinistros.

Riscos Seguro Auto Frota – Sinistro Global – Resultados





Retorno estimado*

R$ **7,3m** **por ano,** em receitas oriundas de recebimento de prêmio.

*A partir da análise de frequência x *score* Zoox, foi feita uma sugestão nos riscos mais elevados onde poderia ser aplicado um ajuste de agravo no preço da cobertura, diminuindo assim as perdas com sinistros.

Tipos de *background check*

Existem diferentes tipos de verificação – cada um com foco em dimensões específicas de risco. Esses dados podem ser cruzados, de acordo com a estratégia e o objetivo definidos pela empresa.

Entre os modelos mais utilizados, destacam-se:



***Background check* de contratação:** utilizado em processos seletivos para validar informações fornecidas por candidatos (como histórico acadêmico e profissional), além de eventuais antecedentes relevantes e até registros de trânsito.



***Background check* financeiro e de crédito:** avalia riscos em operações que envolvem concessão de crédito e parcerias comerciais, integrando práticas de *Know Your Costumer* (KYC) com a análise do histórico financeiro, comportamento de pagamento, endividamento, vínculos societários e eventuais litígios. O objetivo é identificar padrões de risco, antecipar inadimplência e apoiar decisões mais seguras sobre limites, garantias e condições comerciais.



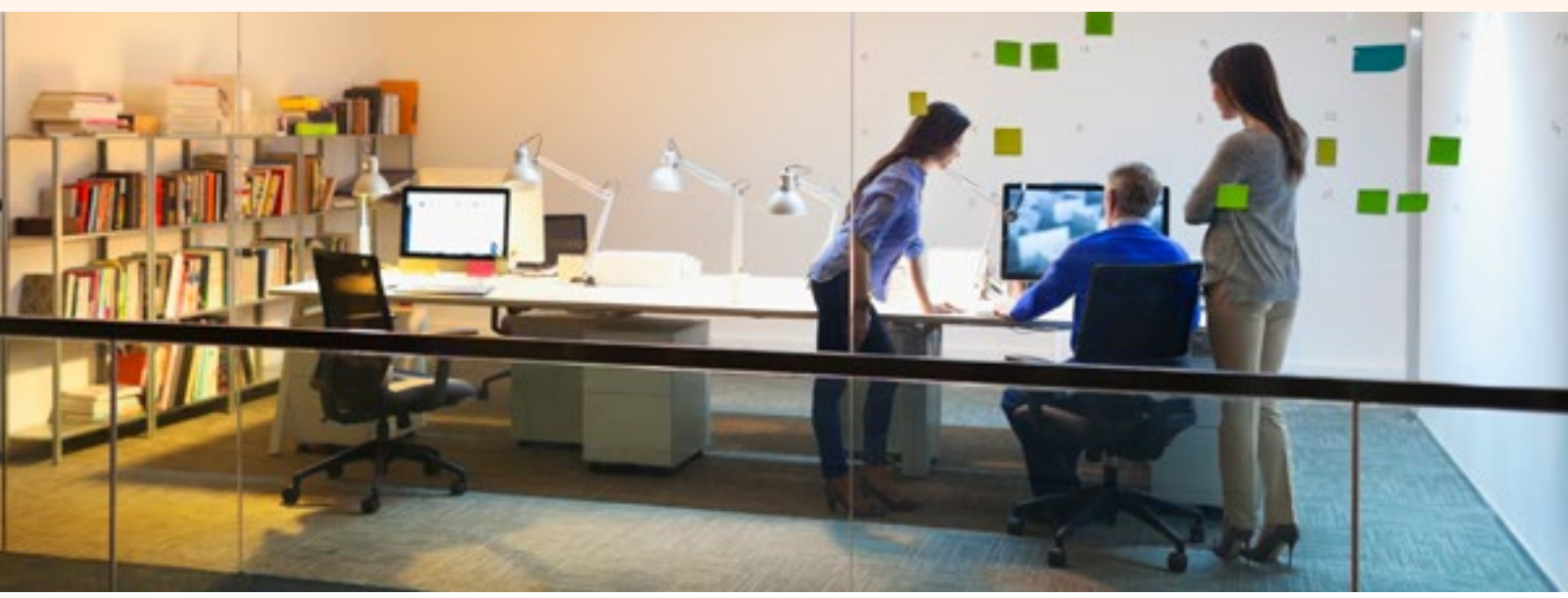
***Background check* criminal:** é aplicado em situações específicas e deve respeitar critérios legais e de proporcionalidade, conforme entendimento do Tribunal Superior do Trabalho (TST).

***Background check* de redes sociais:** analisa a presença digital e o comportamento em plataformas como Instagram, X (antigo Twitter) e LinkedIn. Ajuda a identificar possíveis riscos reputacionais, alinhamento de valores e exposição pública negativa.

***Background check* de integridade:** avalia riscos reputacionais e de *compliance* por meio da análise de informações profissionais, exposição negativa na mídia, processos judiciais, listas restritivas e de sanções, potenciais conflitos de interesse e outros sinais de alerta relacionados a indivíduos e empresas.

***Background check* de identidade:** é uma base essencial de qualquer processo, passa pela confirmação de dados pessoais, como CPF, RG, endereço e situação cadastral, garantindo que a pessoa ou empresa existe e é quem declara ser.

Quando integrados, esses diferentes tipos de *background check* oferecem uma visão ampla e estratégica de riscos.



04

Personalização e segurança nas operações

Um levantamento da Fortinet mostrou que, no primeiro semestre de 2025, o Brasil registrou 314,8 bilhões tentativas de fraude em meios digitais – um número expressivo e que representa mais de oito em cada dez casos na América Latina.

A Aliança Nacional de Combate a Fraudes Bancárias Digitais identificou ao menos 41 tipos de delitos praticados via tecnologia, que incluem autofraude – quando realizam transação e depois contestam os valores – até extorsões e golpes sentimentais. Não se trata apenas da multiplicação dos golpes, mas da criatividade. Assim, estar atualizado e antecipar os riscos é mandatório.

O cenário ainda conta com a maior complexidade das relações comerciais e a crescente regulamentação do mercado, fazendo com que conhecer de forma detalhada clientes, fornecedores e parceiros seja uma condição essencial para operar com segurança.

Esse processo vai muito além da checagem cadastral pontual. É possível usar o *background check* para analisar múltiplas camadas de risco, como histórico financeiro, envolvimento em processos judiciais, exposição em listas restritivas, reputação em fontes abertas e até comportamento digital, além de acompanhar os movimentos de todos os envolvidos nos negócios.



Um modelo de análise de risco eficiente não serve apenas para identificar relações que devem ser evitadas, mas também para acelerar decisões positivas. Quanto maior a confiança no processo de verificação, mais rápido as empresas conseguem aprovar crédito, integrar fornecedores, firmar parcerias e avançar em novos negócios. Neste contexto, o *background check* deixa de ser apenas uma etapa de controle e passa a atuar como um habilitador da operação, equilibrando crescimento, segurança e agilidade em ambientes cada vez mais competitivos.

Um aspecto relevante, especialmente na proximidade de eleições, é o monitoramento de pessoas politicamente expostas (PEPs) ou de indivíduos que passam a ter projeção pública. A entrada de um cliente ou parceiro na esfera pública – como ao se candidatar a um cargo político – pode trazer riscos reputacionais, regulatórios e de imagem que impactam diretamente o negócio.

Neste contexto, o acompanhamento contínuo é tão importante quanto a análise inicial. Um cliente considerado de baixo risco no momento do *onboarding* pode, ao longo do tempo, mudar significativamente seu perfil, seja por aumento do endividamento, envolvimento em disputas judiciais, alteração no padrão de transações ou exposição pública relevante. Sem monitoramento, essas mudanças passam despercebidas e ampliam a vulnerabilidade da empresa.

Cada vez mais, ferramentas conseguem cruzar grandes volumes de dados em tempo real, identificar padrões de comportamento suspeitos e gerar alertas antes que o problema se concretize. Isso permite, por exemplo, ajustar limites de crédito, exigir garantias adicionais, revisar contratos ou até interromper relações comerciais de forma preventiva. Em setores regulados, como financeiro, imobiliário e tecnologia, essa prática já é parte integrante das políticas de *compliance* e governança.

Além disso, o *background check* tem sido amplamente utilizado em processos de contratação e seleção de parceiros estratégicos, ajudando a evitar vínculos com empresas ou indivíduos envolvidos fraudes, corrupção, FTOs ou práticas incompatíveis com os valores da organização.

Manter uma ferramenta adequada às suas necessidades e com suporte garantido é importante porque a análise de *background check* não é uma fotografia estanque e exige acompanhamento e evolução. Um cliente de baixo risco hoje pode se tornar um risco alto no futuro ao se candidatar a um cargo público ou mudar seu padrão transacional.

Na prática, a adoção de *background check* estruturado traz impactos diretos e mensuráveis para o negócio. É um investimento em segurança, eficiência e sustentabilidade.

Redução de perdas financeiras

Ao identificar riscos antes da concretização de uma relação comercial, o *background check* ajuda a evitar inadimplência, fraudes e prejuízos decorrentes de decisões mal-informadas. A análise prévia de clientes, fornecedores e parceiros permite estabelecer limites mais adequados, exigir garantias quando necessário e evitar vínculos com alto potencial de risco.

Conformidade regulatória

A ferramenta correta contribui para atender exigências legais e regulatórias, além de fortalecer políticas internas de governança e prevenção a ilícitos, reduzindo a exposição a sanções e penalidades.

Proteção da reputação

A reputação é um dos ativos mais valiosos – e mais sensíveis – de qualquer organização. Associar-se a indivíduos ou empresas com histórico negativo pode gerar impactos duradouros na imagem institucional.

Economia de tempo e recursos

Processos manuais de verificação tendem a ser mais lentos, fragmentados e sujeitos a falhas. A automação do *background check*, por sua vez, centraliza as análises em um único fluxo, reduz tempo e custo operacional e aumenta a padronização, a rastreabilidade e a confiabilidade das decisões – especialmente em operações de crédito, contratação de parceiros e gestão de terceiros.

Considerações finais

Quando dados passam a ser tratados como ativos estratégicos, o resultado é claro: menos perdas e operações mais sólidas, confiáveis e preparadas para crescer. Em um ambiente de negócios pressionado por restrições de crédito, aumento da inadimplência e cadeias de relacionamento mais complexas, crescer com segurança se torna uma condição para a sustentabilidade. Neste contexto, o *background check* proporciona decisões mais inteligentes, protege operações e fortalece relações comerciais.

Para além de gerenciar riscos, o uso estruturado de dados permite às empresas antecipar cenários, identificar padrões e construir uma cultura orientada à prevenção de fraudes, lavagem de dinheiro e outros problemas legais e corporativos.

Por isso, o *background check* não deve ser usado apenas de forma reativa, mas integrado aos seus processos de crédito, *compliance* e gestão de parceiros, transformando informação em vantagem competitiva.

A inteligência aplicada – contínua, conectada e confiável – permite reduzir incertezas, aumentar a resiliência e sustentar o crescimento, especialmente para micro, pequenas e médias empresas, que são mais expostas e vulneráveis às oscilações do ambiente econômico.

Na prática, os primeiros passos para incorporar o *background check* de forma estratégica são:

1. **Estruture uma política de análise de risco**

   Defina critérios claros para avaliação de clientes, fornecedores, colaboradores e parceiros. Estabeleça quais dados são essenciais nesta análise, quais níveis de risco são aceitáveis para a empresa e como essas informações impactam decisões de negócio a curto, médio e longo prazo.

2. **Centralize e qualifique os dados**

   Garanta que as informações utilizadas sejam confiáveis, atualizadas e integradas. Dados fragmentados ou desatualizados comprometem análises e aumentam a exposição a riscos. E são exatamente essas situações que você quer evitar.

3. **Incorpore o *background check* à rotina decisória**

   Mais do que uma checagem pontual, o processo deve estar integrado às etapas de *onboarding*, concessão de crédito, contratação de fornecedores e revisão de contratos.

4.

Utilize tecnologia para ganhar escala e precisão

Ferramentas automatizadas e inteligência analítica permitem cruzar grandes volumes de dados, identificar padrões e gerar insights mais rápidos e assertivos. O trabalho que antes demorava meses para ser finalizado pode ser concluído em segundos – e com precisão.

5.

Monitore continuamente e ajuste a estratégia

O risco não é estático. Acompanhar mudanças no comportamento financeiro e reputacional dos clientes, fornecedores, parceiros e colaboradores permite agir preventivamente, revisando limites, ajustando garantias ou reavaliando relações.



Fraude, inadimplência e danos reputacionais raramente são eventos isolados. Em geral, decorrem de processos pouco estruturados, decisões baseadas em informações incompletas e da ausência de monitoramento contínuo.

Em um ambiente de negócios cada vez mais dinâmico, operar com verificações lentas e desconectadas deixa de ser apenas uma limitação operacional e passa a representar um risco estratégico. A tecnologia e os dados necessários para mitigar esses riscos já existem. O desafio das lideranças está em incorporá-los de forma consistente à rotina de tomada de decisão.



“Quando o uso de dados deixa de ser pontual e passa a fazer parte da rotina decisória, o *background check* evolui de uma etapa operacional para um instrumento estratégico. Ele permite que as empresas tomem decisões com mais previsibilidade, reduzam incertezas e ajam de forma preventiva diante de mudanças no perfil de risco de clientes, parceiros e fornecedores. Em mercados cada vez mais pressionados por fraudes e exigências regulatórias, velocidade e precisão deixam de ser diferenciais e passam a ser condições para crescer com segurança.”

André Nigro,
Chief Revenue Officer (CRO) da Zoox Smart Data

Contatos



Luís Ruivo
Sócio e líder de Consultoria
da PwC Brasil
luis.ruivo@pwc.com



Elisa Mayor
Sócia de Serviços Forenses
da PwC Brasil
elisa.mayor@pwc.com



Yuri Hollerbach
Sócio de Front Office
Transformation da PwC Brasil
yuri.hollerbach@pwc.com



Alan Dias
Sócio e líder de Alianças & IA
da PwC Brasil
alan.dias@pwc.com



André Nigro
Chief Revenue Officer (CRO)
da Zoox Smart Data
andre.nigro@zooxsmart.com



Vinicius Mathias
Diretor de Marketing
da Zoox Smart Data
vinicius.mathias@zooxsmart.com

Siga a PwC nas redes sociais

Neste documento, “PwC” refere-se à PricewaterhouseCoopers Brasil Ltda., firma membro do network da PricewaterhouseCoopers, ou conforme o contexto sugerir, ao próprio network. Cada firma membro da rede PwC constitui uma pessoa jurídica separada e independente. Para mais detalhes acerca do network PwC, acesse: www.pwc.com/structure.

pwc.com.br

© 2026 PricewaterhouseCoopers Brasil Ltda. Todos os direitos reservados.