Pesquisa de Maturidade dos programas de PLD/FTP

The better the question. The better the answer.
The better the world works.

Shape the future
with confidence

Índice

01 Visão geral dos participantes

02 *Framework* de PLD-FTP

03 *Framework* Prevenção a Fraudes

04 Visão integrada - Fraude, PLDFTP e *Cyber*

05 Governança e qualidade dos dados

06 INR - Investidor não Residente

07 Aposta de quota fixa

08 eFX (*Electronic Foreign Exchange*)

09 Ativos Virtuais

10 *Trust*

11 BaaS (*Banking as a Service*)

Conclusão
O caminho a percorrer

Contatos

Introdução

A EY conduziu **a 2ª edição da Pesquisa de Maturidade dos Programas de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD-FTP).** A pesquisa foi desenvolvida após cinco anos do início da entrada em vigor das novas regulamentações junto às instituições financeiras reguladas pelos órgãos BCB, CVM, SUSEP e PREVIC.

O estudo foi realizado durante os meses de julho e agosto de 2025, por meio de formulário eletrônico respondido pelos participantes.

Esta iniciativa teve como objetivo construir uma visão ampla da situação atual do mercado em relação às atividades de PLD-FTP e obter *insights* relevantes com foco em *compliance* regulatório, efetividade dos programas e uso de novas tecnologias.

Nesta edição, o questionário foi ampliado para incorporar temas de destaque junto a reguladores locais e internacionais, como prevenção a fraudes, apostas de quota fixa, ativos virtuais, eFX (*Electronic Foreign Exchange*) e BaaS (*Banking as a Service*).

Além disso, a pesquisa passou a abranger outros países da América Latina, como Colômbia, Chile, Peru, Argentina, México, Panamá e outros. Os resultados específicos de cada país e o comparativo entre a maturidade geral dos países serão apresentados em um estudo separado. Neste relatório, foram considerados apenas os resultados de respondentes que atuam principalmente no Brasil.

Temas-chave

Os temas a seguir representam os principais focos de atenção no cenário atual de PLD/FTP. Eles refletem tanto as prioridades regulatórias quanto os desafios emergentes enfrentados por instituições financeiras. A pesquisa de maturidade busca entender como o mercado está respondendo a essas frentes críticas, revelando o grau de preparo, os riscos percebidos e as estratégias adotadas para lidar com um ambiente regulatório em constante evolução.

PLD/FTP

Completando **cinco anos da regulamentação atual**, este tema central da pesquisa permite avaliar a evolução da maturidade do setor, os avanços conquistados e os desafios que ainda persistem.

Prevenção a Fraudes

Com a crescente **convergência entre PLD/FTP e prevenção a fraudes**, a pesquisa busca entender como o mercado está estruturando essa integração e quais tecnologias estão sendo priorizadas para mitigar riscos emergentes.

Apostas de Quota Fixa

Com novas regulamentações, **IFs passaram a ter novas responsabilidades** na verificação da autorização das operadoras de apostas, no bloqueio de transações irregulares e na identificação de intermediários não autorizados. A pesquisa investiga como essas exigências estão sendo operacionalizadas.

Ativos Virtuais

A pesquisa explora como o mercado está **se preparando para lidar com as exigências regulatórias para criptoativos**, com foco na adoção de sistemas de KYT, na maturidade das equipes de PLD/FTP e nos procedimentos específicos para lidar com os riscos associados a esse tipo de operação.

efx (CÂMBIO ELETRÔNICO)

A pesquisa explora como instituições que atuam como **facilitadoras de pagamentos internacionais** estão estruturando seus controles de PLD/FTP, especialmente no bloqueio de transações com entidades sancionadas e na execução de processos específicos de verificação.

Baas (*BANKING AS A SERVICE*)

A pesquisa detalha como instituições estão se preparando para oferecer **serviços BaaS** diante dos desafios regulatórios em discussão, da demanda crescente do mercado e dos riscos ampliados relacionados à segurança de dados e conformidade.

1 Visão geral dos participantes

Shape the future with confidence

Visão Geral dos participantes

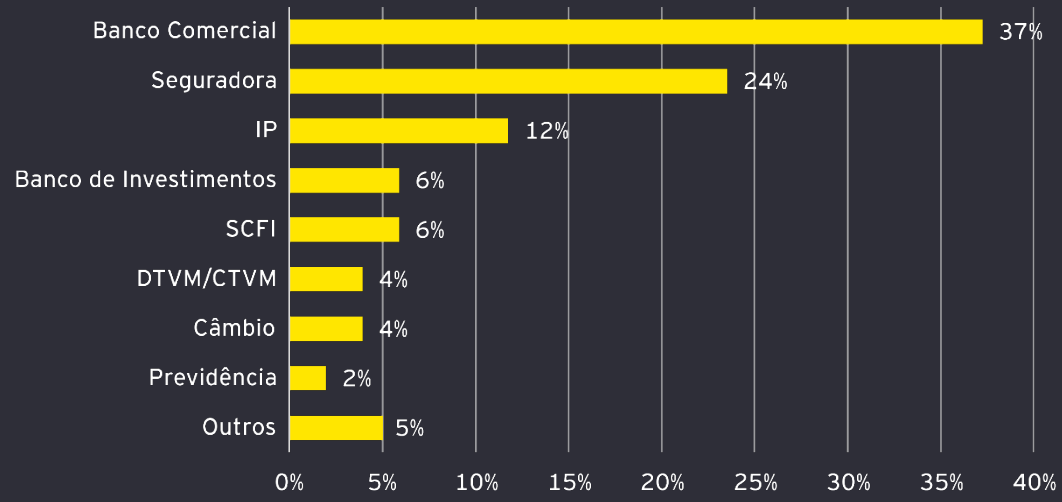
Perfil das Instituições Respondentes

A edição de 2025 da pesquisa contou com a participação de 51 instituições distribuídas entre diferentes setores e portes institucionais. A análise cruzada entre setor de atuação e segmento revela uma amostra bastante diversa, com presença significativa tanto de grandes grupos quanto de instituições menores.

No recorte por setor de atuação, os Bancos Comerciais lideram a amostra, com 19 instituições respondentes, representando 37% do total de respondentes. Em seguida, aparecem as Seguradoras, com 12 instituições (24%), e as Instituições de Pagamento, com 6 respondentes (12%). Esses três setores concentram a maior parte da amostra e refletem a diversidade de modelos de negócio presentes na pesquisa.

Além deles, também participaram Bancos de Investimento e SCFI (cada um com 6%), DTVMs/CTVMs e Câmbio (cada um com 4%), além de Previdência (2%) e instituições classificadas como "Outras" (6%), composto por uma *exchange* de ativos virtuais, uma cooperativa de crédito e uma ressegurada. Essa composição setorial amplia o escopo da análise e contribui para uma compreensão mais rica das práticas adotadas em diferentes tipos de instituições.

Atividade econômica principal das instituições respondentes

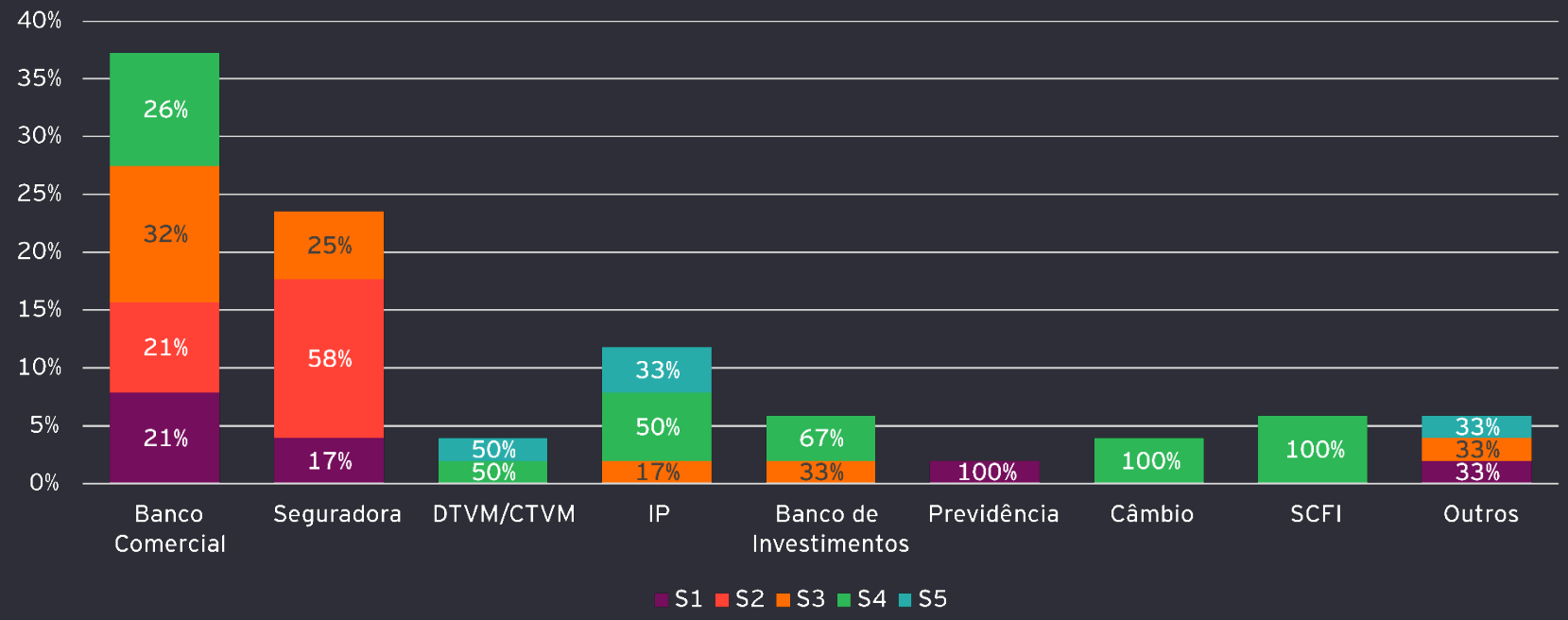


Visão Geral dos participantes

O Banco Central classifica as instituições financeiras em segmentos S1 a S5 com base no porte e relevância, considerando o conglomerado prudencial. Essa segmentação define a proporcionalidade regulatória, aplicando regras mais rigorosas para instituições maiores ou com atuação internacional. Instituições menores (S4 e S5) seguem exigências simplificadas. Essa classificação será utilizada como referência ao longo deste relatório.*

Os bancos comerciais estão distribuídos principalmente entre os segmentos S3 (32%) e S4 (26%), com presença também nos segmentos S1 (21%) e S2 (21%). As seguradoras concentram-se nos segmentos S2 (58%) e S3 (25%), enquanto as instituições de pagamento estão majoritariamente nos segmentos S4 (50%) e S5 (33%). Essa distribuição reforça a diversidade da amostra e permite uma leitura mais precisa dos desafios e práticas de PLD/FTP em diferentes contextos operacionais, respeitando as especificidades de cada setor.

Distribuição dos respondentes por setor e porte da empresa



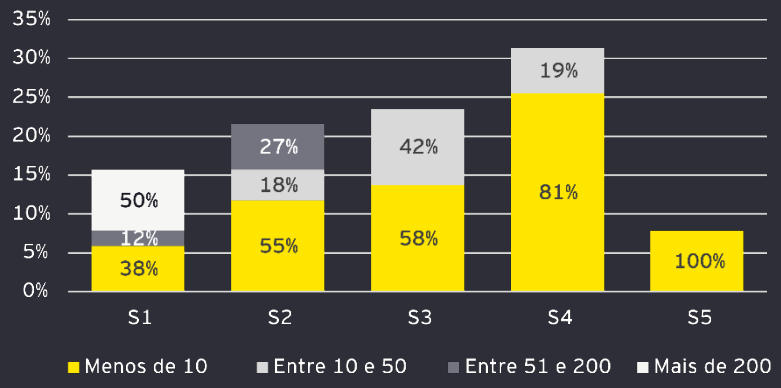
*Nota: Instituições sem classificação no site do BCB foram classificadas no segmento S5

Estrutura das Instituições Respondentes

A estrutura dedicada à PLD/FTP nas instituições participantes apresenta grande variação conforme o porte institucional. No segmento S1, que reúne as instituições de maior porte, 50% contam com mais de 200 profissionais dedicados ao tema, enquanto 38% possuem menos de 10 profissionais. Já no segmento S2, 55% das instituições têm equipes enxutas com menos de 10 profissionais, e 27% contam com estruturas entre 51 e 200 profissionais, evidenciando uma distribuição mais heterogênea. Nos segmentos S3 a S5, que representam instituições de menor porte, a predominância é clara: 58% a 100% das instituições possuem menos de 10 profissionais dedicados à PLD/FTP, com destaque para o segmento S5, em que todas as instituições se enquadram nessa faixa.

Esses dados revelam uma correlação esperada entre o porte da instituição e o tamanho da equipe dedicada ao tema, refletindo diferentes níveis de capacidade operacional e alocação de recursos. A presença de estruturas mais robustas nos segmentos superiores e mais enxutas nos segmentos inferiores reforça a importância de considerar o contexto institucional na análise das práticas de PLD/FTP.

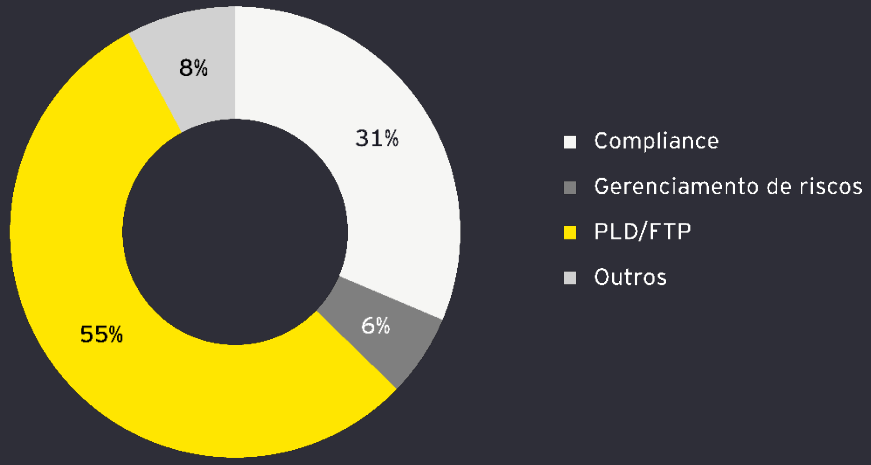
Profissionais de PLD nas empresas respondentes



Quanto à área de atuação dos respondentes, observa-se uma predominância de profissionais diretamente ligados à PLD/FTP, que representam 53% da amostra. Em seguida, aparecem os profissionais de *Compliance*, com 33%, e de Gerenciamento de Riscos, com 6%. Há ainda 8% de respondentes que atuam em outras áreas (normalmente áreas que combinam todos esses temas).

Essa diversidade de áreas de atuação entre os respondentes contribui para uma visão mais ampla sobre como o tema é tratado internamente, permitindo que a pesquisa capture diferentes perspectivas e níveis de envolvimento com as práticas de prevenção à lavagem de dinheiro e financiamento ao terrorismo.

Área de atuação do respondente



2 *Framework* de PLD-FTP

Shape the future with confidence

Framework de PLD-FTP

I. Avaliação Interna de Riscos

II. Processos de Conhecimento

III. Monitoramento de Transações

Nesta seção, buscamos compreender o grau de maturidade dos *frameworks* de PLD/FTP adotados pelas instituições financeiras, considerando aspectos estruturais, operacionais e tecnológicos dos programas de prevenção. A análise ganha relevância especial neste ano, que marca o quinto aniversário das normas atualmente vigentes no Brasil (Circular BCB nº 3.978/2020, a Resolução CVM nº 50/2021, a Resoluções PREVIC 25/2025 e PREVIC 23/2023 e a Circular SUSEP nº 612/2020), permitindo observar como o setor evoluiu desde sua implementação.

Comparamos também os resultados com a edição inaugural da pesquisa publicada em 2023, trazendo uma perspectiva mais aprofundada sobre os avanços e desafios enfrentados ao longo do tempo.

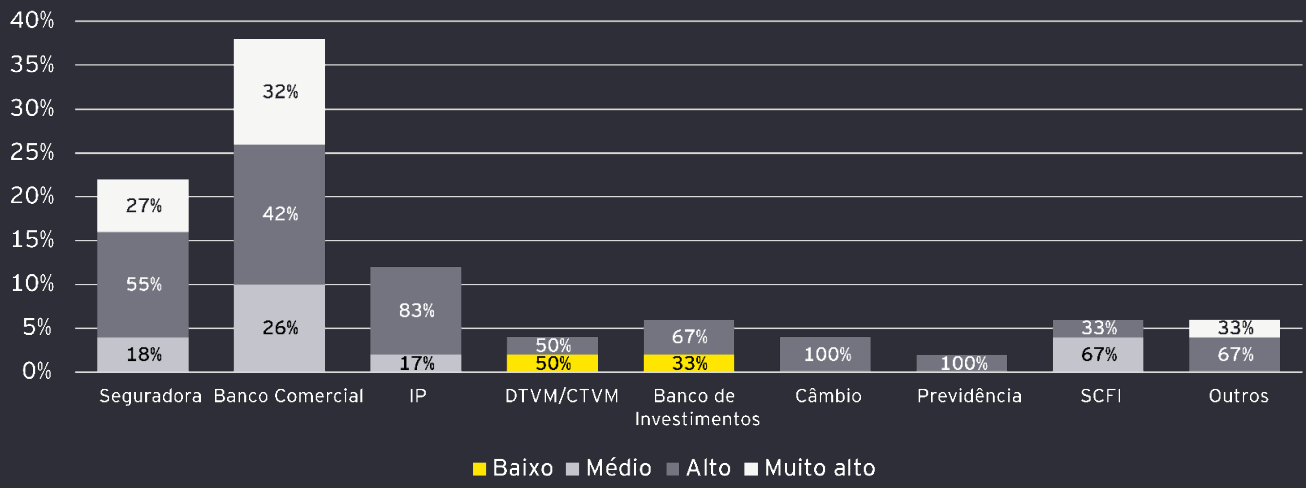
Iniciamos esta jornada avaliando a percepção de maturidade em três pilares fundamentais: a Avaliação Interna de Risco (AIR), os processos de conhecimento (KYC, KYE, KYP etc.) e o monitoramento de transações e situações suspeitas. Esses temas são apresentados com cortes por setor, permitindo identificar padrões e diferenças relevantes entre os segmentos do mercado.

Avaliação Interna de Riscos

A análise da maturidade da Avaliação Interna de Riscos revela diferenças relevantes entre setores, indicando padrões distintos de evolução. No recorte por setor, os bancos comerciais apresentam uma distribuição entre os níveis Alto (42%) e Muito alto (32%), com 26% ainda posicionados em Médio. As instituições de pagamento concentram-se na faixa Alto (83%). Os setores de Câmbio e Previdência apresentam 100% das respostas em Alto, enquanto DTVMs/CTVMs se dividem entre Alto (50%) e Baixo (50%). A diversidade de respostas entre os setores reforça a necessidade de abordagens adaptadas às características de cada modelo de negócio.

Em comparação com a edição de 2023, observa-se uma evolução positiva na maturidade da AIR. Naquele ano, 70% dos respondentes estavam nas faixas Alto ou Muito alto, enquanto 30% estavam em Médio. Em 2025, as faixas superiores somam 80% e as faixas inferiores caíram para 20%. Embora o avanço seja perceptível, os dados mostram que ainda há espaço para melhorias, especialmente em segmentos que apresentam maior concentração de maturidade em níveis intermediários.

Maturidade *Framework* PLD/FTP: AIR

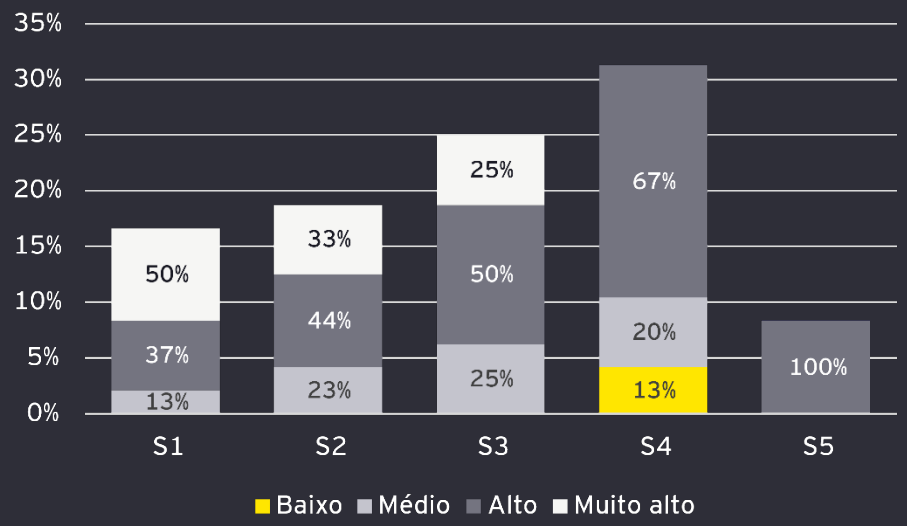


Avaliação Interna de Riscos

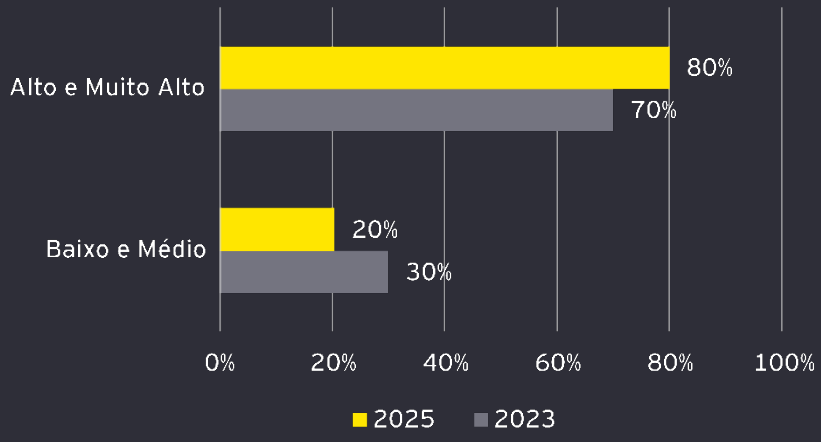
Uma análise focada apenas nos bancos comerciais revela diferenças relevantes entre os segmentos institucionais: o segmento S1 apresenta um cenário mais consolidado, com 75% das instituições posicionadas em Muito alto e 25% em Alto, sem nenhuma resposta em Médio – o que sugere uma estrutura de AIR mais pacificada entre as instituições de maior porte. Já os segmentos S2, S3 e S4 mostram uma presença expressiva de instituições ainda posicionadas em Médio, com destaque para o S2, em que 50% das instituições estão nessa faixa intermediária.

Essa leitura mostra que a maturidade da AIR é um ponto de atenção independente do porte institucional. A concentração de respostas em níveis intermediários nos segmentos S2, S3 e S4 indica que ainda existem lacunas na consolidação de metodologias mais estruturadas. O contraste com o desempenho do segmento S1 reforça a importância de iniciativas voltadas ao fortalecimento da AIR, mesmo em instituições com capacidade técnica e regulatória já estabelecida.

Maturidade *Framework* PLD/FTP: AIR



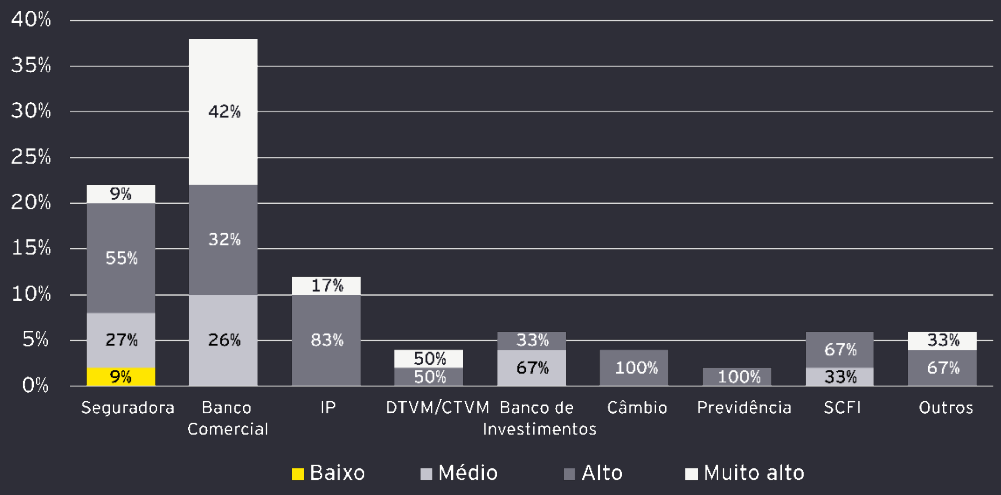
Maturidade AIR: 2023 vs 2025



Processos de Conheça (KYC, KYE, KYP, KYS)

A maturidade dos processos de *identificação* – que englobam KYC, KYE, KYP e KYS – apresenta avanços em relação à edição anterior da pesquisa, mas ainda revela pontos de atenção importantes. No recorte setorial, chama atenção o fato de 9% das seguradoras ainda se classificarem na faixa Baixo, além de 27% em Médio, indicando que uma parcela relevante do setor ainda não atingiu níveis mais altos de maturidade. Já os bancos comerciais apresentam uma distribuição mais equilibrada, com 32% em Alto e 42% em Muito alto.

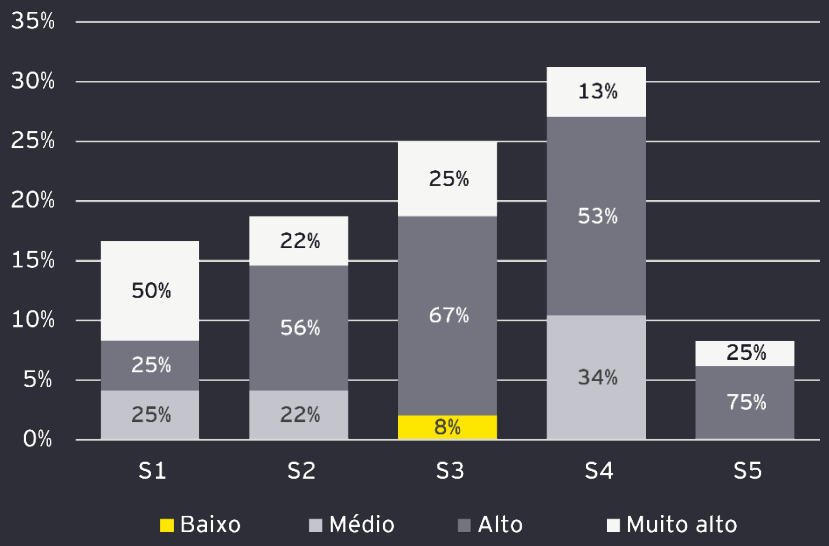
Maturidade *Framework* PLD/FTP: KYC/KYE/KYS/KYP, por setor



No recorte por segmento, os dados reforçam preocupações semelhantes às observadas na análise de AIR. 25% das instituições do segmento S1 e 22% do S2 se posicionaram na faixa Médio, o que é significativo considerando o porte dessas instituições. Além disso, 8% do segmento S3 ainda se classificam como Baixo, e 34% do S4 como Médio – o que reforça que ainda existem desafios significativos independente do segmento. Por outro lado, conforme o esperado, o segmento S1 apresenta o maior grau de maturidade, com 50% das instituições se classificando como Muito alto.

Em comparação com a edição de 2023, os dados de 2025 mostram uma melhora. Naquele ano, 70% das instituições se posicionavam nas faixas Alto ou Muito alto, enquanto 30% estavam em Baixo ou Médio. Em 2025, esse número caiu para 20%, com 80% das instituições agora se classificando nas faixas superiores – um avanço relevante, ainda que com desafios persistentes em segmentos estratégicos.

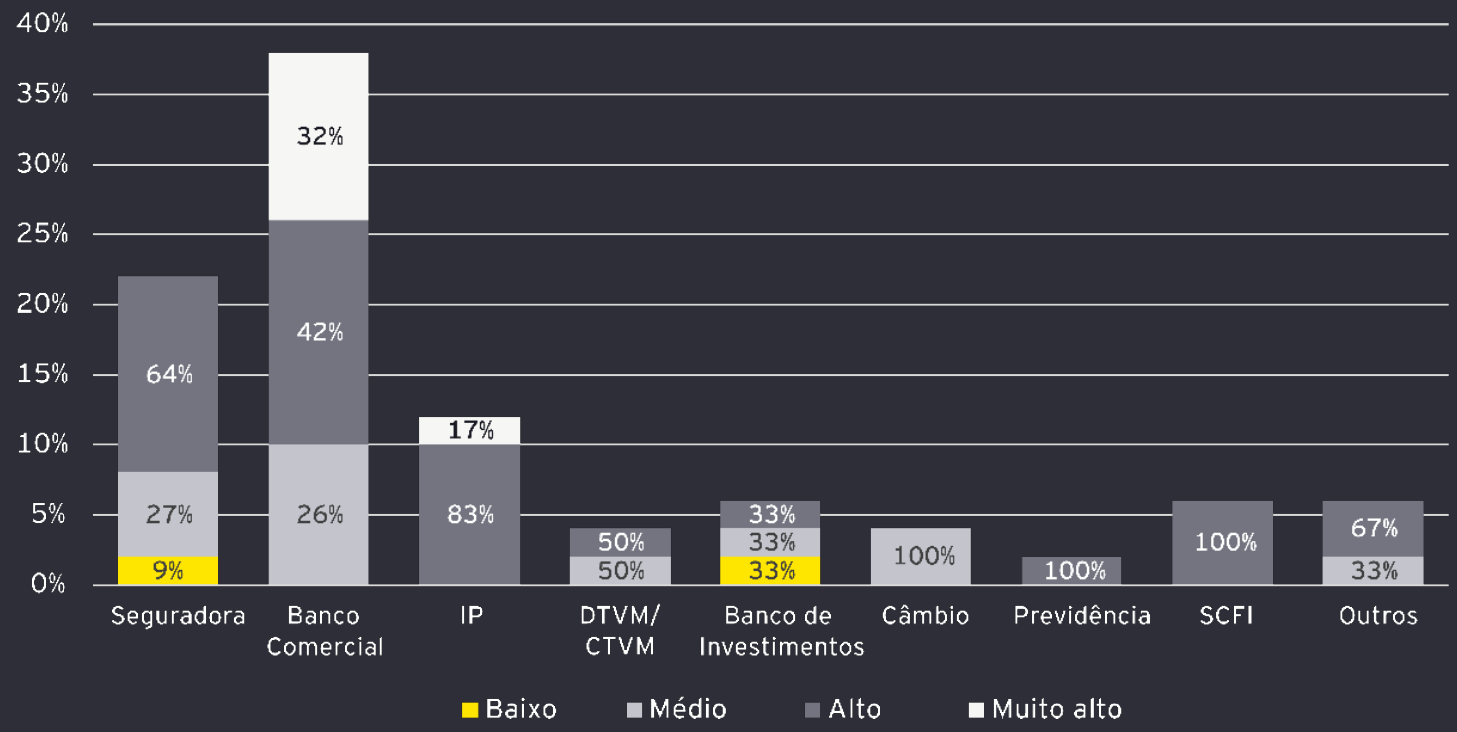
Maturidade *Framework* PLD/FTP: KYC/KYE/KYS/KYP, por segmento



Monitoramento de Transações

A maturidade dos mecanismos de monitoramento segue como um dos pilares mais desafiadores dos programas de PLD/FTP. No recorte por setor, os bancos comerciais apresentam uma distribuição relativamente equilibrada: 32% das instituições se posicionam em Muito alto, 42% em Alto e 26% ainda em Médio. Embora a maioria esteja nas faixas superiores, o percentual em Médio indica que ainda há espaço para evolução, especialmente considerando o papel central que o monitoramento ocupa nos *frameworks* de PLD/FTP.

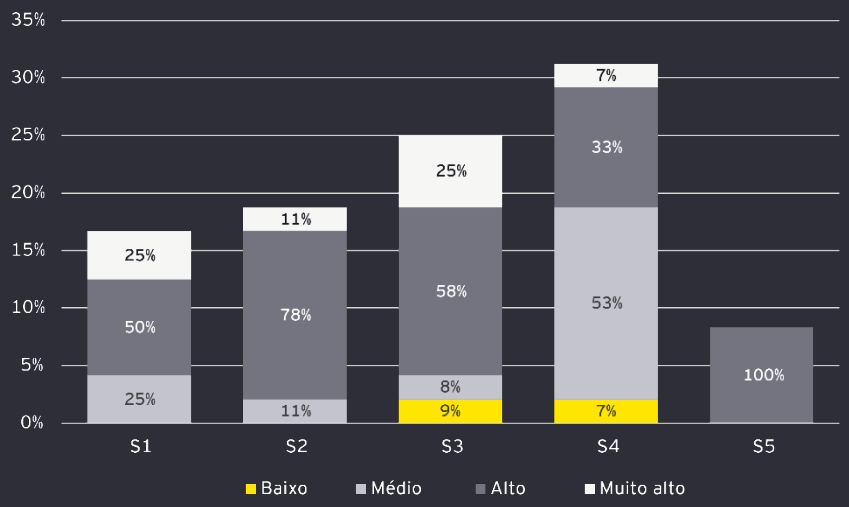
Maturidade *Framework* PLD/FTP: monitoramento de transações, por setor



Monitoramento de Transações

No recorte por segmento, os dados reforçam a necessidade de atenção entre instituições de diferentes portes. O segmento S4 apresenta um cenário preocupante, com 60% das instituições posicionadas nas faixas inferiores – 7% em baixo e 53% em médio – o que sugere uma maturidade ainda em consolidação. O segmento S1, por outro lado, concentra 25% das instituições em Muito alto, mas ainda mantém 25% em Médio, o que reforça que o desafio não está restrito às instituições de menor porte. Já o segmento S2 apresenta 11% em médio.

Maturidade *Framework* PLD/FTP: monitoramento de transações, por segmento



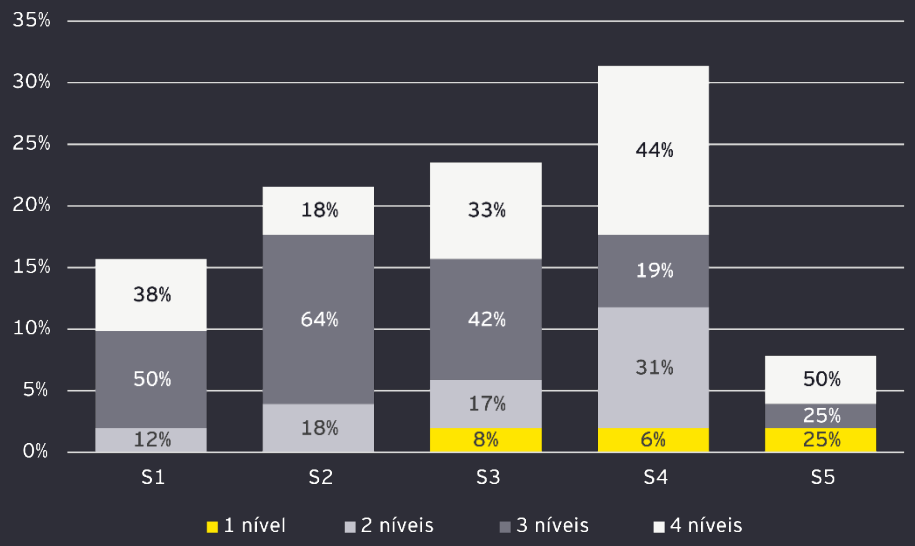
No caso do segmento S5, chama atenção o fato de 100% das instituições se posicionarem na faixa Alto. Embora esse dado possa refletir uma percepção positiva sobre os mecanismos adotados, é importante considerar que instituições de menor porte podem enfrentar limitações na mensuração objetiva da maturidade de seus processos. A ausência de respostas em faixas inferiores pode indicar uma avaliação otimista, que merece ser analisada com cautela à luz da complexidade envolvida no monitoramento de transações.

Em comparação com a edição de 2023, os dados de 2025 mostram um avanço moderado. Na edição anterior, 65% das instituições estavam nas faixas Alto ou Muito alto, enquanto 35% se posicionavam em Baixo ou Médio. Em 2025, esse número caiu para 29%, com 71% agora nas faixas superiores. O progresso é relevante, mas ainda há margem para evolução, especialmente entre os segmentos que concentram maior número de instituições em níveis intermediários.

Monitoramento de Transações:
Estrutura e Capacidade de Análise

A estrutura de tratamento dos alertas de monitoramento mostra evolução relevante em 2025. A proporção de instituições com quatro níveis de análise subiu de 15% em 2023 para 35% em 2025, indicando maior robustez nos processos de validação e decisão. Esse avanço pode estar relacionado ao aumento da complexidade das operações e à busca por maior rigor na triagem de alertas, refletindo uma tendência de amadurecimento dos *frameworks* de monitoramento.

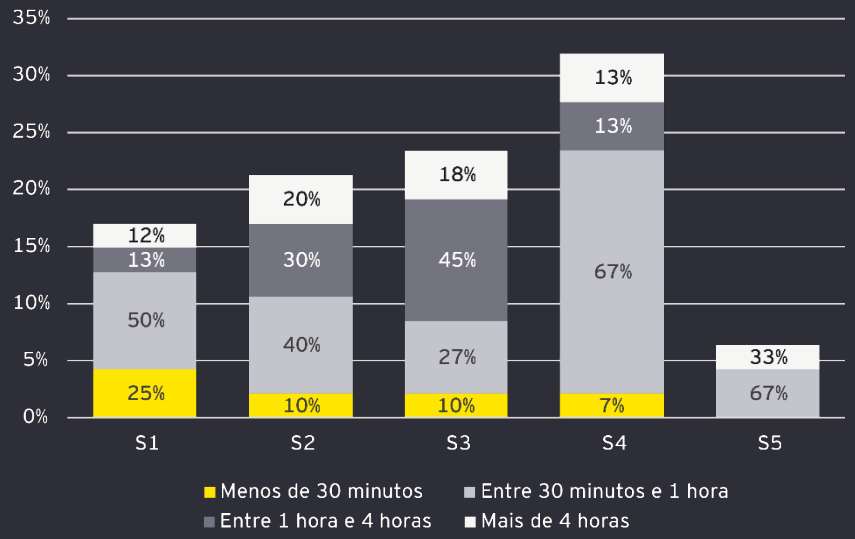
Níveis de análise para tratamento de alertas de monitoramento, por segmento



O tempo dedicado à análise e desenvolvimento de narrativas de casos nível II também passou por mudanças importantes. A proporção de instituições que levam menos de 30 minutos caiu de 24% em 2023 para 11% em 2025, enquanto os casos que levam mais de uma hora subiram de 20% para 38%. Esse movimento pode estar associado à maior sofisticação dos processos investigativos, com os analistas dedicando mais tempo à construção de narrativas detalhadas e bem fundamentadas. Em outra seção da pesquisa, foi identificado o uso de *machine learning* como apoio à análise de operações suspeitas, o que pode ter contribuido para que os analistas recebam casos mais refinados e direcionem seus esforços à tomada de decisão – em vez de à triagem inicial.

Monitoramento de Transações:
Estrutura e Capacidade de Análise

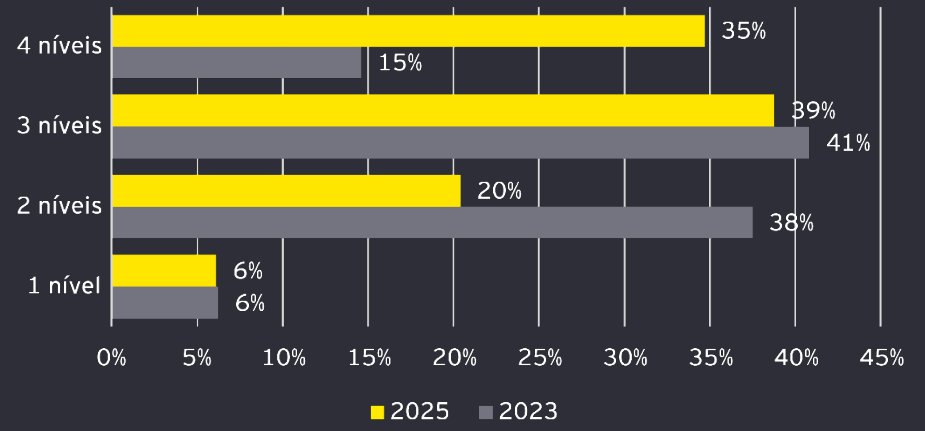
Tempo médio de análise e desenvolvimento de narrativa de casos nível II de investigação, por segmento



No recorte por segmento, o S4 apresenta 67% das instituições com tempo médio entre 30 minutos e 1 hora, superando inclusive o S2, que tem 40% nessa faixa. Já o segmento S5 se destaca com 33% das instituições levando mais de 4 horas para concluir a análise – o maior percentual entre todos os segmentos. Esse dado pode refletir limitações operacionais ou menor maturidade nos processos de investigação, especialmente em instituições com estruturas mais enxutas.

De forma geral, os dois indicadores se complementam ao revelar uma tendência de maior estruturação e aprofundamento nos processos de monitoramento. O aumento no número de níveis de análise sugere uma busca por maior rigor, enquanto o crescimento no tempo de investigação pode indicar que as instituições estão dedicando mais atenção à qualidade das narrativas – especialmente quando contam com ferramentas que ajudam a direcionar os esforços para os casos mais críticos.

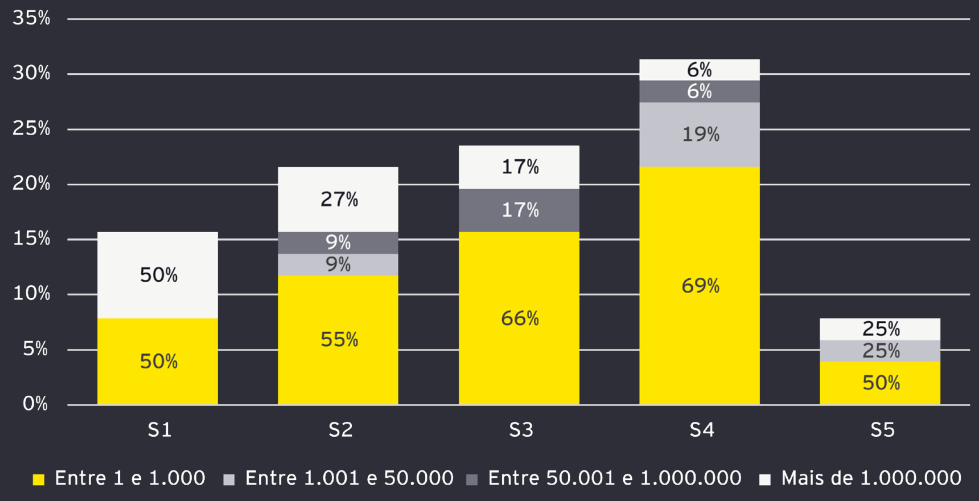
Nível de análise para tratamento de alertas de movimento



Monitoramento de Transações: Volume e *Backlog*

A distribuição do volume de transações processadas por dia varia significativamente conforme o setor de atuação das instituições. Seguradoras, por exemplo, concentram 92% das respostas na faixa de até 1.000 transações por dia, o que é compatível com a natureza do negócio. Já as instituições de pagamento apresentam 50% das respostas na faixa de mais de 1 milhão de transações por dia, refletindo o alto volume operacional característico do setor. Esse contraste reforça que o recorte por setor é mais adequado para interpretar os dados de volume, uma vez que o porte institucional (segmento) nem sempre está diretamente relacionado à quantidade de transações processadas.

Volume de transações processadas por sistemas de monitoramento de operações suspeitas por dia, por segmento

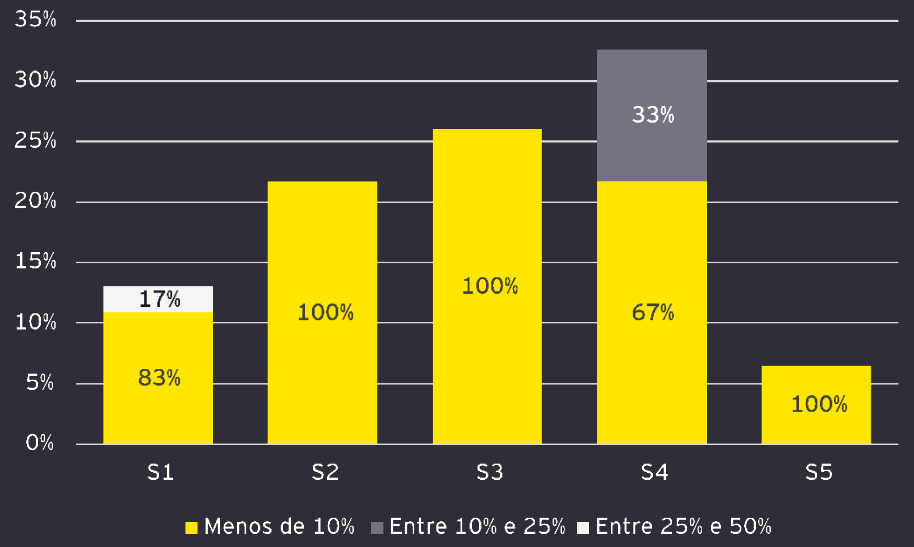


Monitoramento de Transações: Volume e *Backlog*

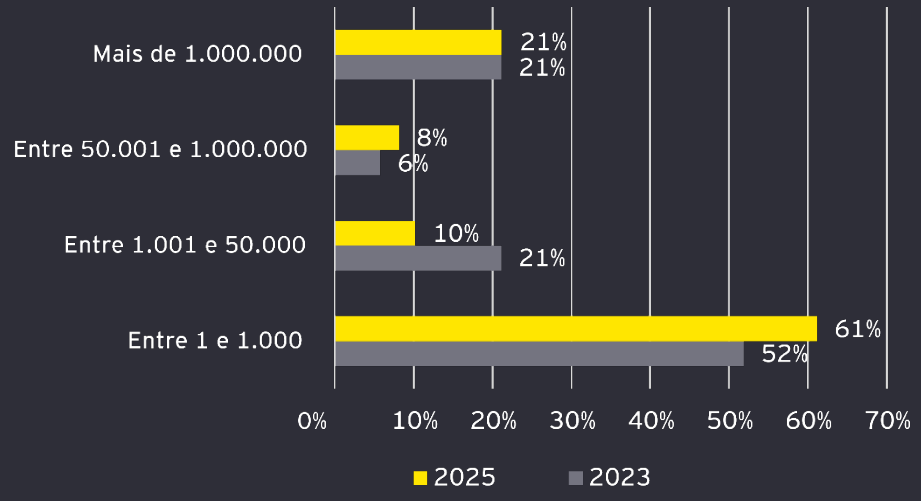
O monitoramento do *backlog* mensal de casos suspeitos é um indicador direto da capacidade de resposta das instituições. Em 2025, os segmentos S2 e S3 se destacam positivamente, com 100% das instituições mantendo menos de 10% de *backlog*, o que sugere alta eficiência no tratamento dos alertas. Já o segmento S1 apresenta 17% das instituições com *backlog* entre 25% e 50%. A evolução entre 2023 e 2025 é positiva: em 2023, 14% das instituições tinham *backlog* acima de 50%, enquanto em 2025 nenhuma instituição se posicionou nessa faixa. Além disso, a proporção de instituições com menos de 10% de *backlog* subiu de 75% para 87%.

Uma possível explicação para essa melhora está no aumento do uso de inteligência artificial nos processos de PLD/FTP, conforme apontado em outra seção da pesquisa. Segmentos como S1 e S2 têm adotado com mais frequência modelos de IA voltados para o monitoramento de transações suspeitas, classificação de risco e apoio à análise de operações. Essas ferramentas ajudam a identificar com mais precisão os casos relevantes, permitindo que os analistas priorizem os alertas com maior potencial de risco. Por outro lado, os segmentos S4 e S5, que apresentam menor adoção de IA – com 67% e 100% das instituições, respectivamente, declarando não utilizar esse tipo de tecnologia – podem enfrentar limitações na triagem automatizada, o que impacta diretamente a eficiência operacional.

% Média mensal de casos suspeitos em *backlog* para análise, por segmento



Volume de transações processadas - 2023 vs 2025



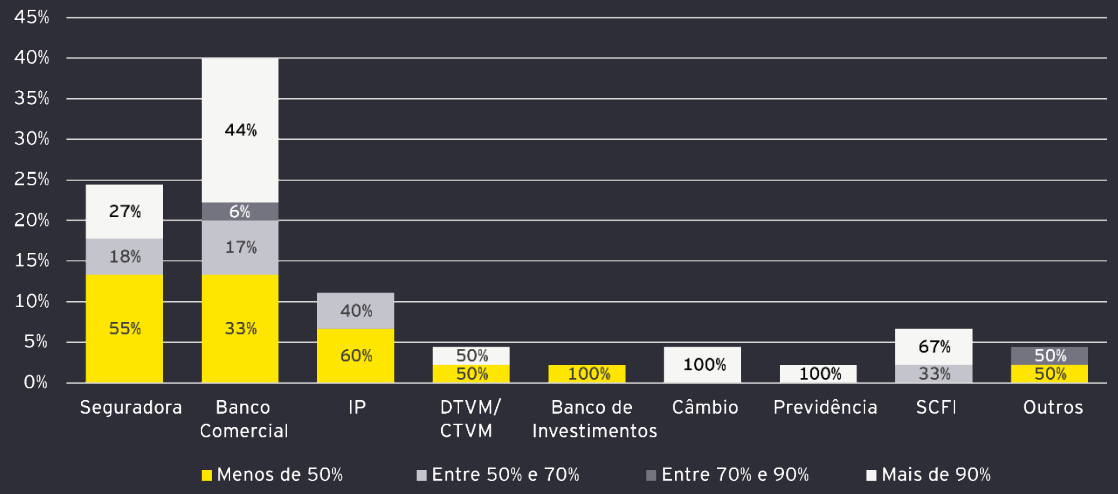
Monitoramento de Transações

Qualidade dos Alertas e Reportes

A eficiência dos sistemas de monitoramento continua sendo impactada por altos índices de falsos positivos, que permanecem como um dos principais desafios enfrentados pelas instituições. Em 2025, 44% dos bancos comerciais indicaram que mais de 90% dos alertas gerados **não** resultam em investigações relevantes. Esse dado reforça a dificuldade persistente na parametrização e calibração das regras de monitoramento, que, quando mal desenvolvidas, geram ruído excessivo e sobrecarregam as equipes de análise. Setores como câmbio e previdência também apresentaram 100% das respostas na faixa acima de 90%, o que pode indicar necessidade de revisão dos parâmetros adotados.

A comparação com 2023 mostra variações relevantes, especialmente no grupo de instituições com mais de 90% de falsos positivos, que subiu de 20% para 37% em 2025. Embora a soma das faixas superiores e inferiores tenha se mantido relativamente estável, o crescimento na faixa mais crítica reforça que os desafios relacionados à qualidade dos alertas continuam presentes. A manutenção de altos índices de falsos positivos ao longo dos anos indica que, apesar dos avanços tecnológicos, ainda há dificuldades em traduzir esses recursos em parametrizações mais eficazes. A leitura dos dados reforça que o problema não está necessariamente no volume de transações ou na natureza do setor, mas sim na forma como os sistemas são configurados para identificar comportamentos suspeitos.

Percentual de falsos positivos, por setor



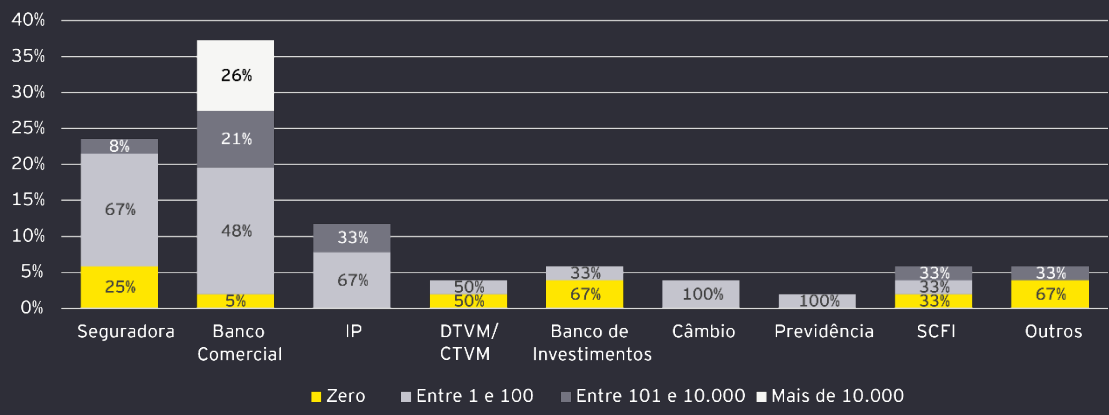
Monitoramento de Transações

Qualidade dos Alertas e Reportes

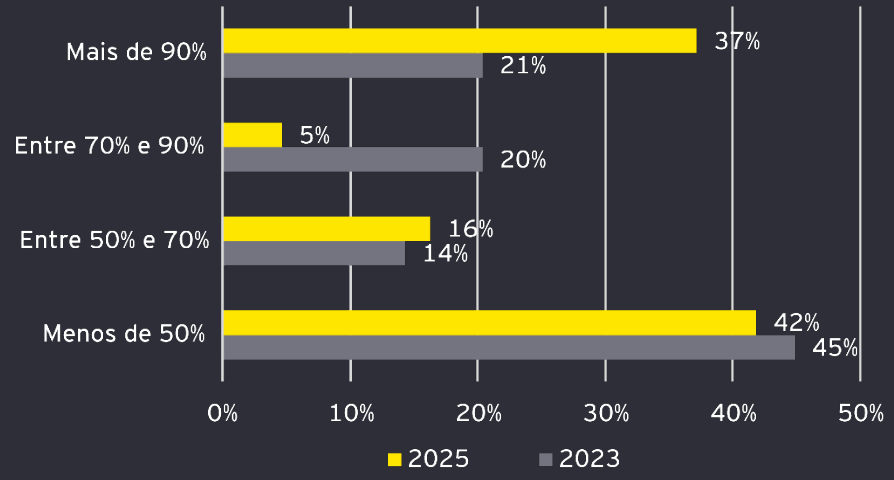
O volume de reportes ao COAF também traz *insights* relevantes. Como esperado, os bancos comerciais concentram os maiores volumes – 26% dos respondentes indicaram mais de 10 mil comunicações no ano de 2024. Por outro lado, chama atenção o fato de que pelo menos 50% das DTVMs e bancos de investimento não realizaram nenhum reporte ao longo do ano. O recorte sobre instituições de pagamento também merece destaque: 67% delas realizaram entre 1 e 100 reportes no ano, o que é um número relativamente baixo considerando a volumetria expressiva de transações que esse tipo de instituição costuma processar, – reforçando novamente a importância de calibrar adequadamente os sistemas de monitoramento.

A leitura conjunta dos dois indicadores – falsos positivos e volume de reportes – sugere que ainda há espaço para evolução na calibragem dos sistemas e na efetividade dos processos investigativos. A persistência de altos índices de falsos positivos, combinada com a ausência de reportes em alguns setores relevantes, aponta para a necessidade de revisão contínua dos parâmetros e maior integração entre tecnologia e análise humana.

Quantidade de Reportes ao COAF em 2024, por setor



Percentual de falsos positivos - 2023 vs 2025

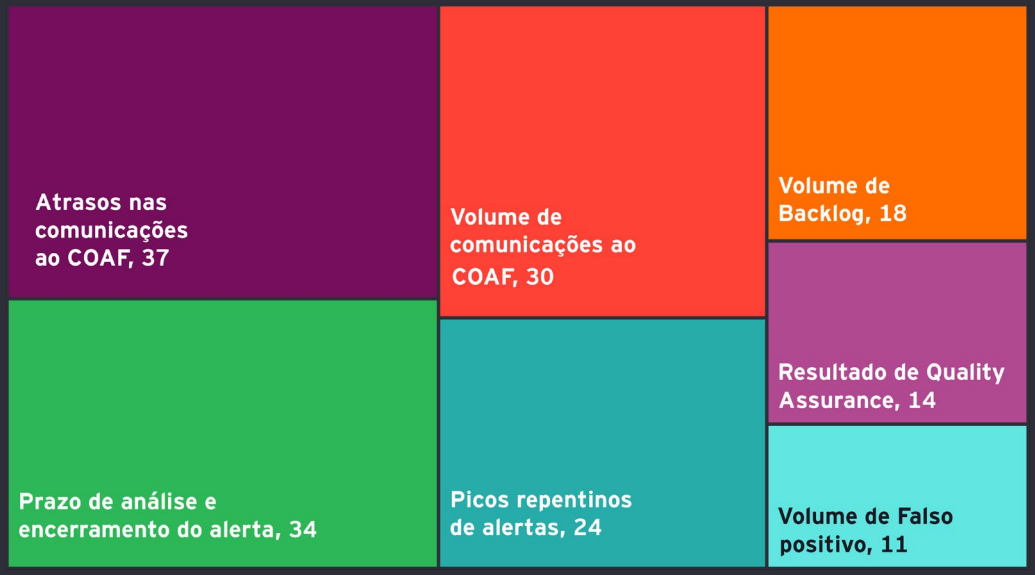


Monitoramento de Transações:
Efetividade e Ferramentas

As métricas utilizadas para acompanhar a eficácia dos *frameworks* de monitoramento apresentaram mudanças relevantes entre 2023 e 2025. O destaque vai para o crescimento na adoção da métrica de atrasos nas comunicações ao COAF, que passou de 8% para 22% – um aumento de 14 pontos percentuais. Por outro lado, o uso de resultado de *Quality Assurance* caiu de 19% para 8%, uma redução de 11 pontos percentuais.

Esse último dado levanta uma questão interessante. Em outro ponto da pesquisa, observamos que a proporção de instituições com quatro níveis de análise – justamente onde o *Quality Assurance* costuma estar inserido como etapa final de validação – subiu de 15% para 35%. A queda na adoção da métrica de QA, portanto, contrasta com esse avanço estrutural. É possível que haja alguma inconsistência na forma como os respondentes interpretam ou reportam essa informação, o que merece atenção na leitura dos dados.

Métricas utilizadas para acompanhamento de monitoramento, por número de respondentes

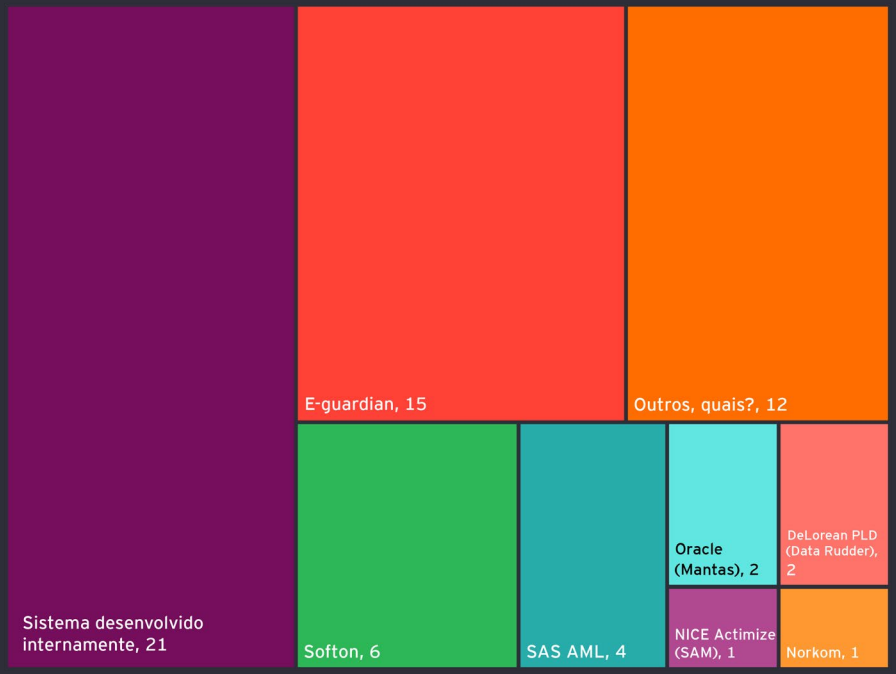


Monitoramento de Transações:
Efetividade e Ferramentas

Em relação aos sistemas utilizados para monitoramento de transações, os dados de 2025 mostram uma predominância de soluções desenvolvidas internamente (33% das respostas recebidas), seguidas por E-guardian (23%) e Softon (9%). A comparação com 2023 revela uma estabilidade na liderança das soluções internas e do E-guardian, embora com leve queda percentual. Sistemas como SAS AML, Oracle Mantas e DeLorean PLD mantêm presença marginal, enquanto ferramentas como Feedzai e Fico não foram mencionadas em 2025. É importante lembrar que os respondentes puderam selecionar múltiplas opções, portanto os percentuais representam a distribuição das respostas, e não o número de instituições.

A leitura conjunta dos dados sugere que, embora haja uma diversificação nas ferramentas utilizadas, a efetividade dos processos ainda depende fortemente da forma como essas soluções são parametrizadas e integradas aos fluxos operacionais. A mudança nas métricas de acompanhamento indica uma atenção crescente à conformidade e à agilidade, mas também levanta a necessidade de reequilibrar o foco entre eficiência regulatória e qualidade técnica — especialmente em um cenário onde o uso de tecnologia tem se expandido, mas os desafios de calibragem permanecem.

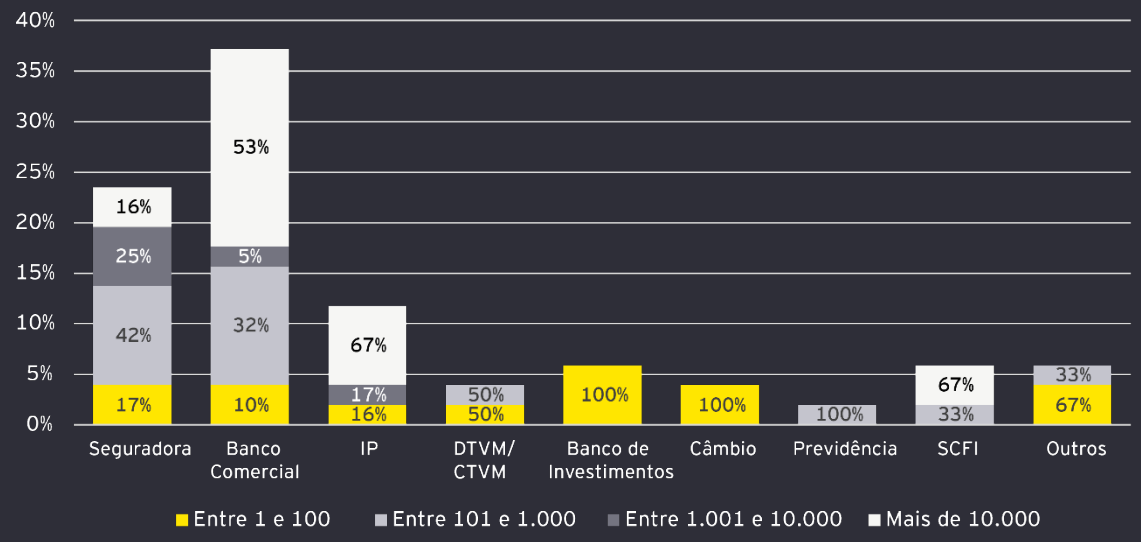
Sistema de monitoramento das instituições, por número de respondentes



KYC Volume e *Backlog*

O volume de KYC processado mensalmente pelas instituições varia significativamente conforme o setor de atuação. Em 2025, bancos comerciais e instituições de pagamento concentram os maiores volumes: 53% dos bancos e 67% das instituições de pagamento indicaram processar mais de 10.000 KYC por mês. Esse dado é compatível com a natureza operacional desses setores, que lidam com grandes bases de clientes e alta rotatividade. Por outro lado, setores como banco de investimento, câmbio e DTVMs/CTVMs apresentam predominância nas faixas mais baixas – com até 100 KYC mensais – o que está alinhado com seus modelos de negócio mais especializados e de menor escala.

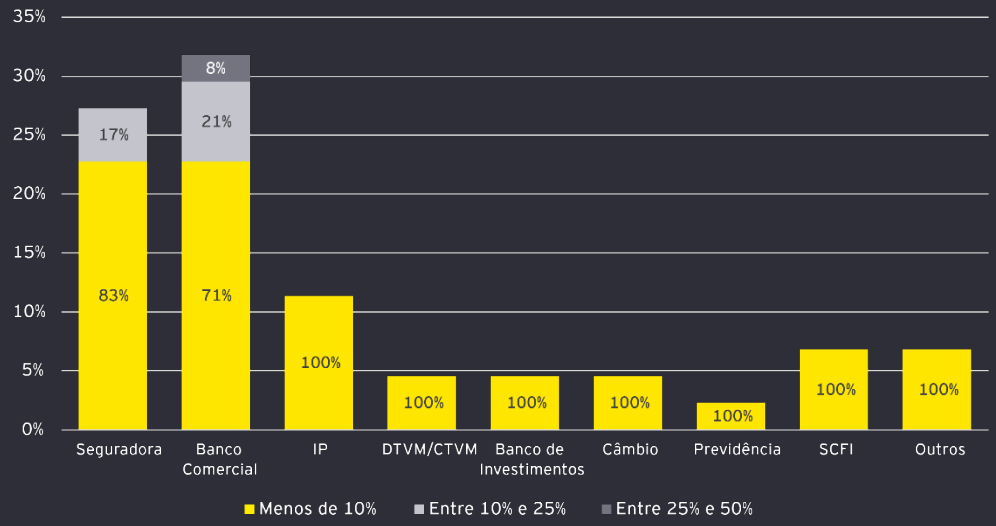
Volume de KYCs processados por mês, por setor



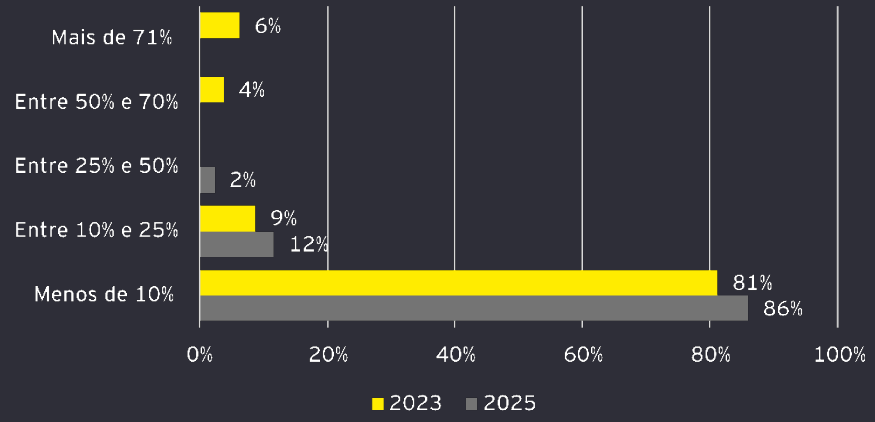
Setores como seguradoras e bancos comerciais concentram os principais pontos de atenção em relação ao *backlog*. Em 2025, 17% das seguradoras e 29% dos bancos comerciais indicaram manter níveis entre 10% e 50% de *backlog* – faixas que, embora não sejam majoritárias, ainda representam uma carga relevante de casos pendentes. No total, 14% dos respondentes se posicionam nessas faixas superiores, o que reforça a importância de revisar fluxos operacionais e estratégias de automação para mitigar gargalos no processamento de KYC, especialmente em setores com maior complexidade cadastral e exigência regulatória.

KYC Volume e *Backlog*

Volume de *Backlogs* de KYC por mês, por setor



Backlog de KYC - 2023 vs 2025



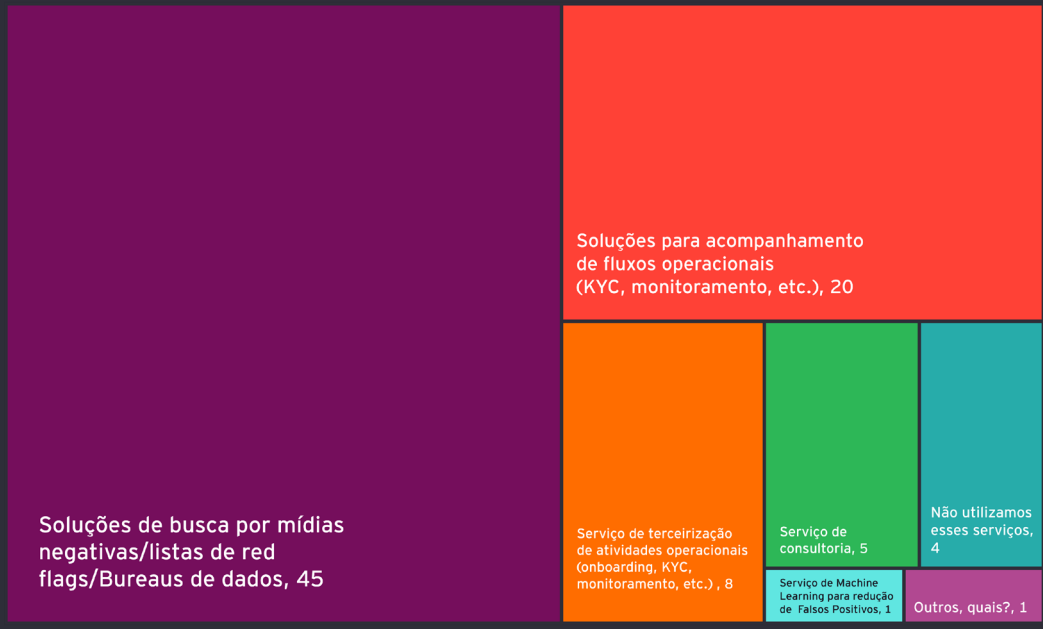
Na comparação entre 2023 e 2025, os dados de *backlog* de KYC mostram uma evolução positiva. A proporção de instituições com menos de 10% de *backlog* subiu de 81% para 86%, enquanto os percentuais nas faixas superiores caíram significativamente. Em 2023, 10% das instituições estavam nas faixas de 50% ou mais de *backlog* – sendo 4% entre 50% e 70% e 6% acima de 71%. Em 2025, nenhuma instituição se posicionou nessas faixas. Essa melhora é relevante e pode estar associada à adoção de tecnologias que aceleram o processamento de KYC.

Em outra seção da pesquisa, os respondentes indicaram o uso de inteligência artificial em processos de PLD/FTP, com destaque para ferramentas como IA generativa como agente de captura de mídias e aprendizado de máquina na classificação de risco / escore de risco. Tais tecnologias têm potencial direto para reduzir o tempo de coleta e análise de dados cadastrais, contribuindo para a diminuição do *backlog*. A correlação entre o avanço tecnológico e a melhora nos indicadores operacionais de KYC reforça a importância de investir em soluções que integrem automação e inteligência analítica aos processos de *onboarding* e atualização cadastral.

Uso de soluções de terceiros

A adoção de serviços e plataformas de terceiros para suporte aos programas de PLD/FTP apresentou crescimento relevante entre 2023 e 2025. O dado mais expressivo é a redução na proporção de respostas que indicam ausência total de uso desses serviços: em 2023, 23% das respostas apontavam que a instituição não utilizava nenhuma solução de terceiro, enquanto em 2025 esse número caiu para apenas 5%. Essa mudança sugere uma maior abertura do mercado à terceirização e ao uso de ferramentas especializadas, possivelmente impulsionada por pressões regulatórias, aumento de complexidade operacional ou busca por maior eficiência.

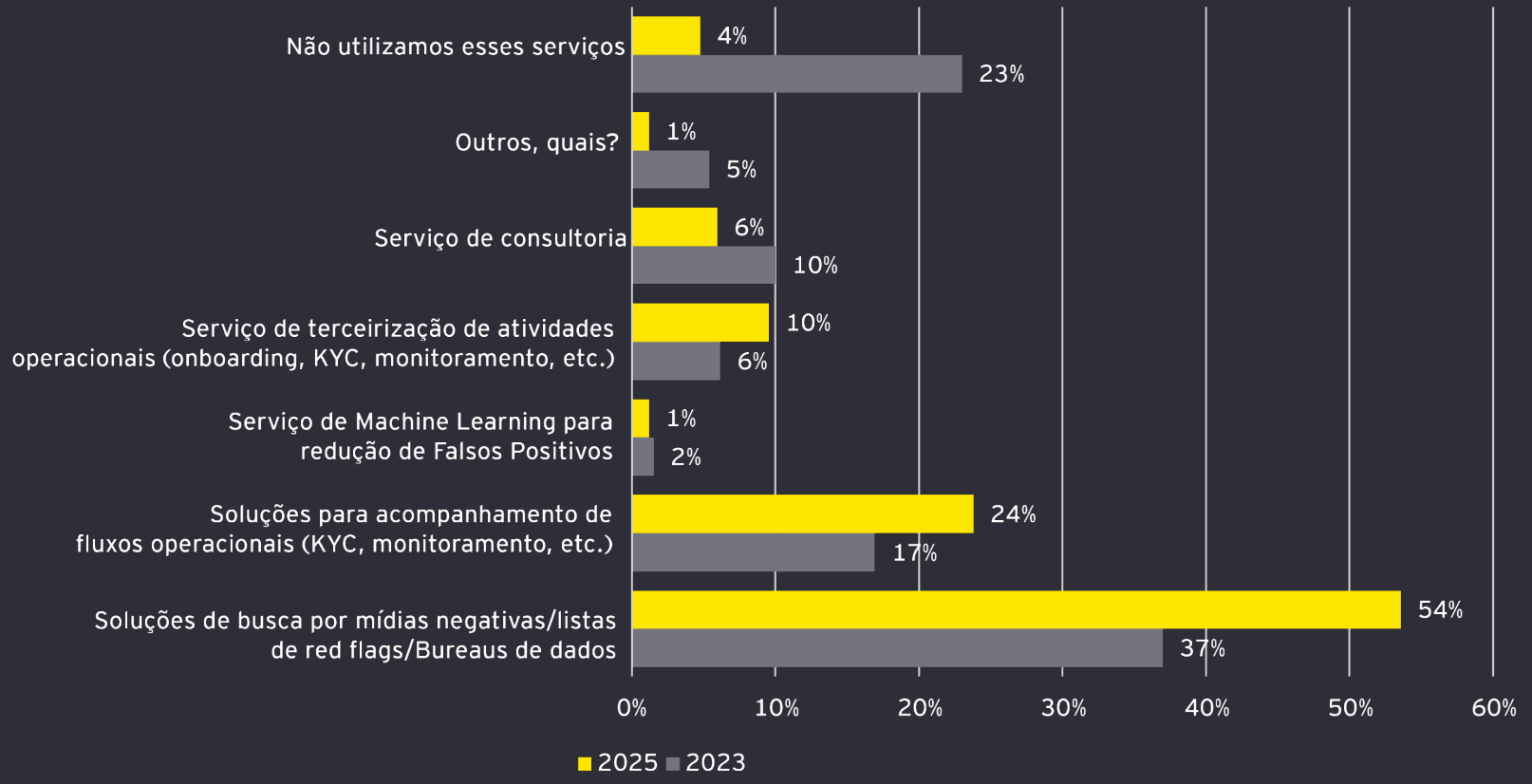
Uso de soluções de terceiros em PLD/FTP



Entre os serviços com maior crescimento percentual, destacam-se as soluções voltadas à busca por mídias negativas, listas de *red flags* e *bureaus* de dados, que passaram de 37% para 54% das respostas. Esse avanço pode refletir uma maior preocupação das instituições com o monitoramento reputacional e com a identificação de riscos externos, especialmente em um cenário de maior exposição pública e exigência de diligência ampliada.

Uso de soluções de terceiros

Uso de soluções de terceiros em PLD/FTP: 2023 vs 2025



Outro destaque é o crescimento das soluções para administração e acompanhamento de fluxos operacionais – como KYC e monitoramento – que subiram de 17% para 24% das respostas. Embora o crescimento seja mais moderado, ele indica uma tendência de apoio tecnológico às atividades de linha de frente, com potencial para reduzir gargalos operacionais e melhorar a rastreabilidade dos processos.

A leitura dos dados reforça que o uso de terceiros está se consolidando como parte integrante dos programas de PLD/FTP, com destaque para ferramentas que ampliam a capacidade de análise e monitoramento. A queda na proporção de instituições que não utilizam nenhum serviço externo é um indicativo claro dessa mudança de postura, ainda que a adoção não seja uniforme entre os diferentes tipos de soluções disponíveis.

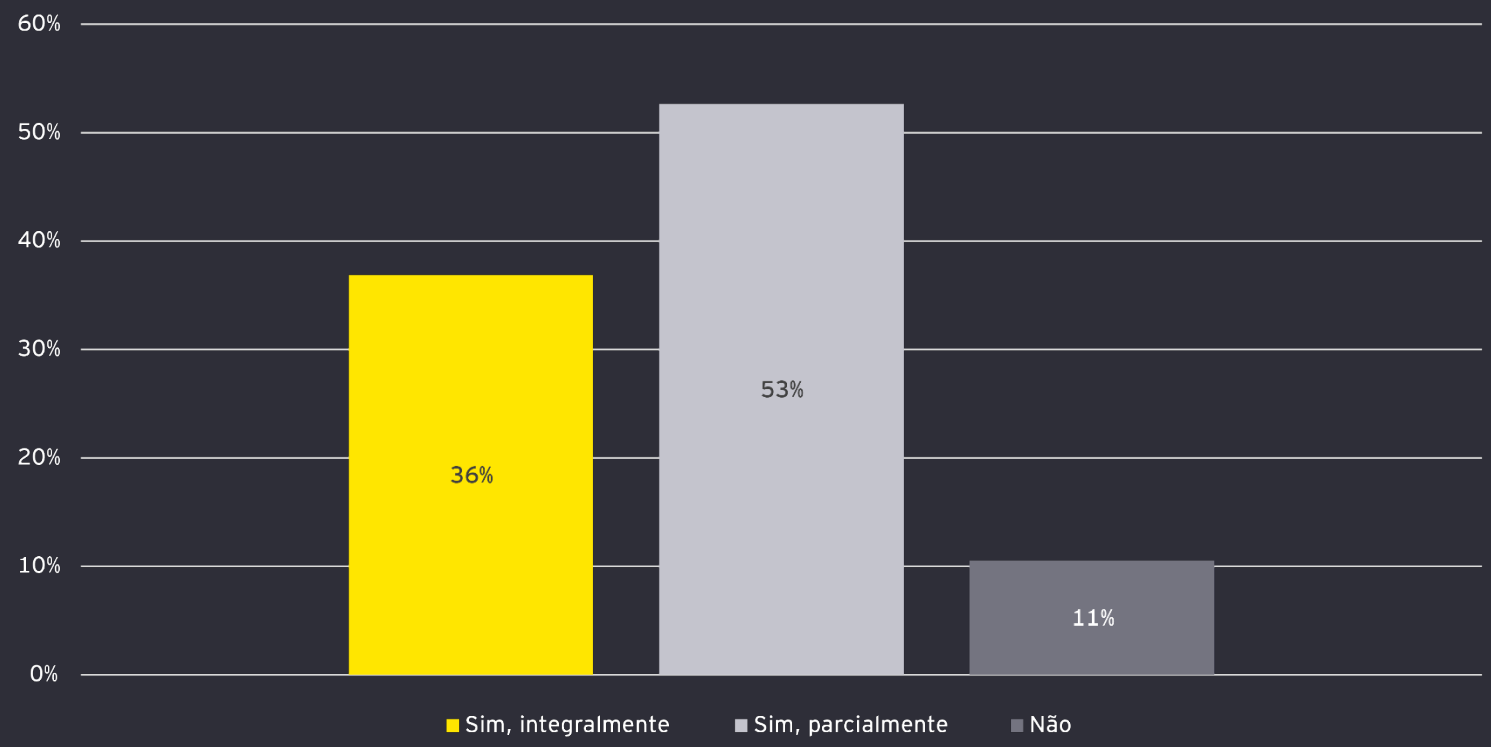
Aderência aos Guias de Práticas de Supervisão (GPS)

Os Guias de Práticas de Supervisão (GPS) do Banco Central são manuais de boas práticas com caráter educativo e de orientação, que buscam apoiar as instituições na correta interpretação e implementação da regulamentação vigente. No contexto de PLD/FTP, os guias têm especial relevância por esclarecer expectativas de supervisão quanto à estruturação de controles internos, governança, monitoramento de operações e comunicação de situações atípicas. Mais do que criar novas obrigações, o GPS oferece transparência sobre como o BCB avalia a efetividade dos programas de prevenção, funcionando como referência prática para elevar o nível de maturidade das instituições e reduzir assimetrias no mercado.

Apesar da disponibilidade e clareza dos materiais, os dados da pesquisa indicam que a adoção ainda está em estágio intermediário para boa parte das instituições. Apenas 36% dos respondentes afirmaram ter aderido integralmente ao GPS, enquanto 53% indicaram adesão parcial e 11% ainda não iniciaram o processo. Considerando que o "**Guia 7.30.01 – Conduta – Lavagem de Dinheiro (LD) e Financiamento do Terrorismo (FT)"** foi atualizado pela última vez em 26/06/2024, há mais de um ano, o cenário atual sugere que ainda há espaço relevante para avanço.

Aderência aos Guias de Práticas de Supervisão (GPS)

Quantidade de instituições que aderiram ao Guia de Práticas de Supervisão (GPS)



Embora o GPS não represente novas exigências regulatórias, ele consolida as expectativas da supervisão com base nas melhores práticas do setor. Nesse sentido, a aderência aos guias é um indicativo de maturidade institucional e alinhamento com os padrões esperados. Desde a última atualização do Guia 7.30.01, em junho de 2024, as instituições tiveram tempo para iniciar ou aprofundar seus processos de adaptação. Ainda que esse tempo não esteja formalmente delimitado, os dados sugerem que é necessário acelerar o ritmo de alinhamento para evitar que os *gaps* se perpetuem.

A leitura dos dados reforça que o GPS deve ser tratado como um instrumento de apoio estratégico, capaz de orientar melhorias estruturais e operacionais nos programas de PLD/FTP. A expectativa é que as instituições avancem de forma consistente, reduzindo gradualmente os *gaps* identificados e promovendo maior uniformidade na aplicação das boas práticas.

3 *Framework* de Prevenção à Fraude

EY
Shape the future with confidence

Framework de Prevenção à Fraude

I. Estrutura e Investimentos

II. Tecnologias e Processos

III. Cultura e Resposta a Incidentes

A prevenção à fraude tem ganhado protagonismo nas agendas de risco das instituições financeiras, impulsionada pelo aumento da digitalização, pela sofisticação dos ataques e pela crescente expectativa de resposta rápida e eficaz por parte do mercado e dos reguladores.

Nesta seção, buscamos mapear o grau de maturidade das práticas adotadas pelas instituições para mitigar riscos de fraude, considerando aspectos organizacionais, tecnológicos e operacionais.

Embora esta seja a primeira edição da pesquisa com foco específico em prevenção à fraude, os dados coletados oferecem uma visão abrangente sobre os principais desafios enfrentados, os investimentos realizados e as estratégias adotadas para proteger clientes, processos e ativos.

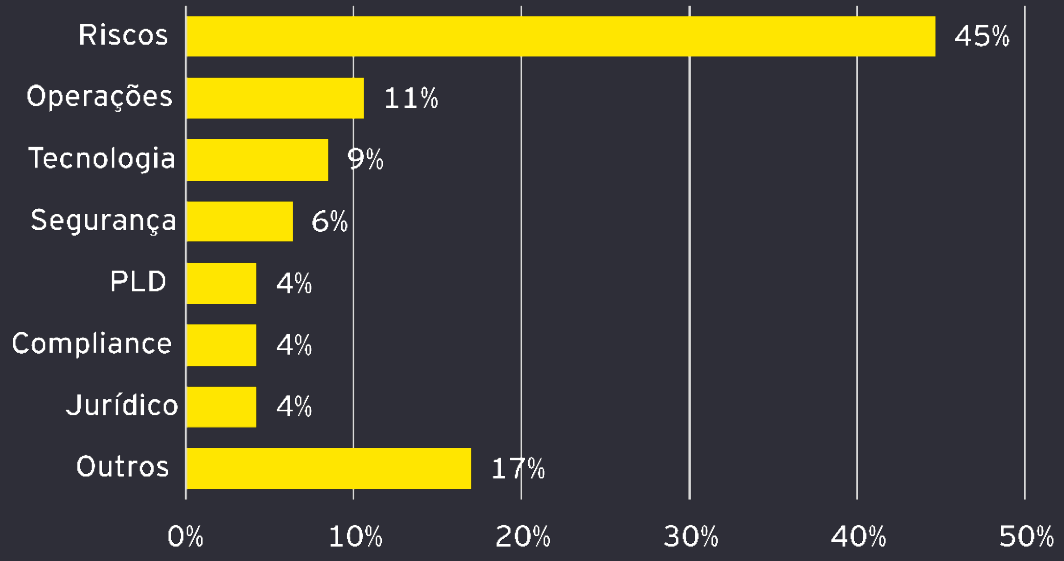
A análise também permite identificar tendências emergentes e oportunidades de aprimoramento, especialmente em temas como integração de áreas, uso de tecnologia e tempo de resposta a incidentes.

Prevenção à Fraude

Estrutura Organizacional e Investimentos

A pesquisa indica que a governança da área de prevenção a fraudes é heterogênea entre as instituições. A maior parte dos respondentes vincula a função à diretoria de Riscos (45%), reforçando a tendência de tratar a fraude como parte da gestão integrada de riscos. Ainda assim, uma parcela significativa posiciona a área em Operações (11%) ou Tecnologia (9%), sugerindo que em muitos casos o tema é abordado sob um viés mais técnico-operacional. Outras instituições a alocam em Segurança ou Jurídico, reforçando a falta de uniformidade de mercado quanto ao enquadramento da função. O cenário sugere que o mercado ainda se encontra em processo de consolidação de boas práticas quanto ao posicionamento organizacional.

Estrutura organizacional da prevenção a fraudes

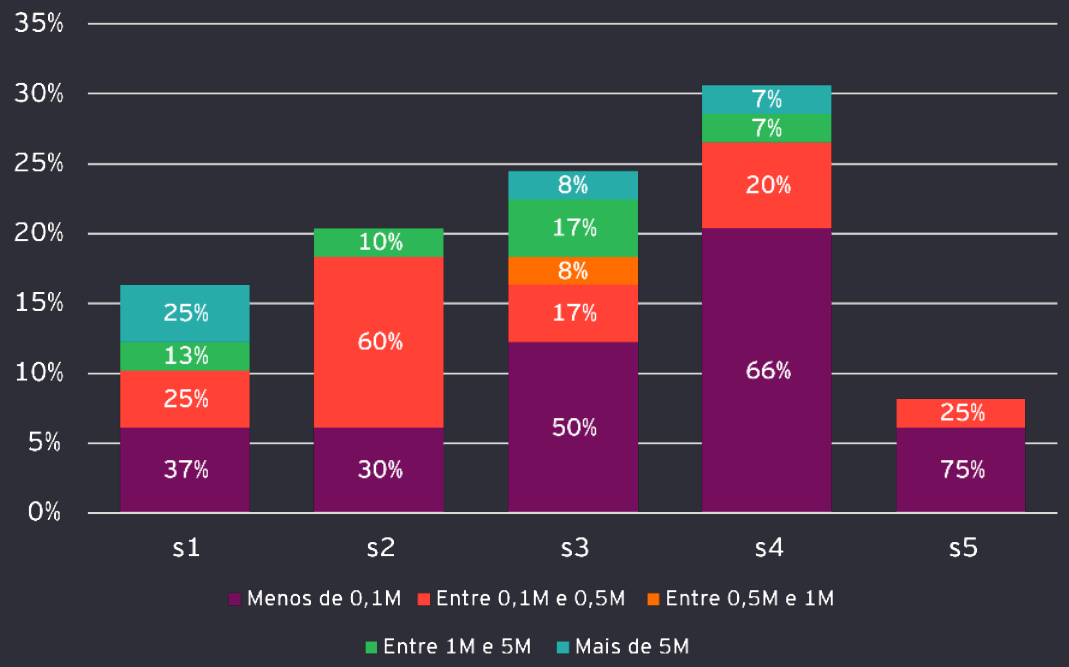


Prevenção à Fraude

Estrutura Organizacional e Investimentos

Em relação aos investimentos, os dados revelam uma correlação clara entre porte e gastos, mas também expõem disparidades importantes. Entre as instituições de maior porte (S1), 25% reportaram gastos superiores a USD 5 milhões em 2024, enquanto 37% declararam valores abaixo de USD 100 mil. Essa disparidade dentro do mesmo grupo evidencia que, mesmo entre *players* de escala similar, os níveis de maturidade e priorização do risco de fraude variam substancialmente.

Nível de gastos em prevenção a fraudes 2025 (USD), por segmento



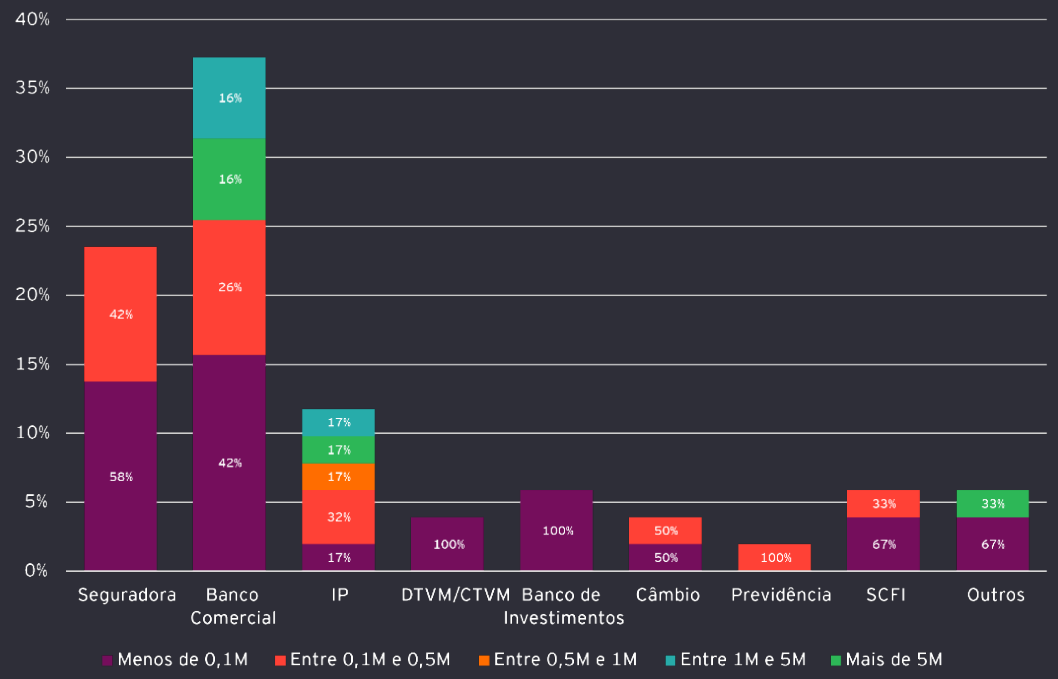
Nas instituições S2, observa-se maior concentração de respostas na faixa entre USD 100 mil e 500 mil (60%), refletindo um patamar de investimento mais moderado, mas ainda relevante frente à exposição do segmento. Casos pontuais acima de USD 1 milhão (10%) mostram, por outro lado, que parte das instituições de médio porte já começa a escalar seus gastos, sinalizando sensibilidade crescente ao tema e possivelmente respostas a pressões regulatórias ou ao aumento de incidentes recentes.

Nos segmentos S3, S4 e S5, a fotografia é ainda mais concentrada em gastos reduzidos. Pelo menos metade dessas instituições reportou desembolsos inferiores a USD 100 mil em 2024, o que sugere que ainda estão em estágios iniciais de estruturação da função. Apesar disso, há sinais isolados de movimentação: 8% das S3 e 7% das S4 indicaram gastos no patamar máximo da pesquisa, acima de USD 5 milhões, o que demonstra que, mesmo em segmentos intermediários, algumas instituições já começam a investir de forma mais robusta no enfrentamento à fraude. Ainda assim, o panorama geral evidencia que os investimentos permanecem, em grande parte, limitados frente à dimensão do risco.

Prevenção à Fraude

Estrutura Organizacional e Investimentos

Nível de gastos em prevenção a fraudes 2025 (USD), por setor



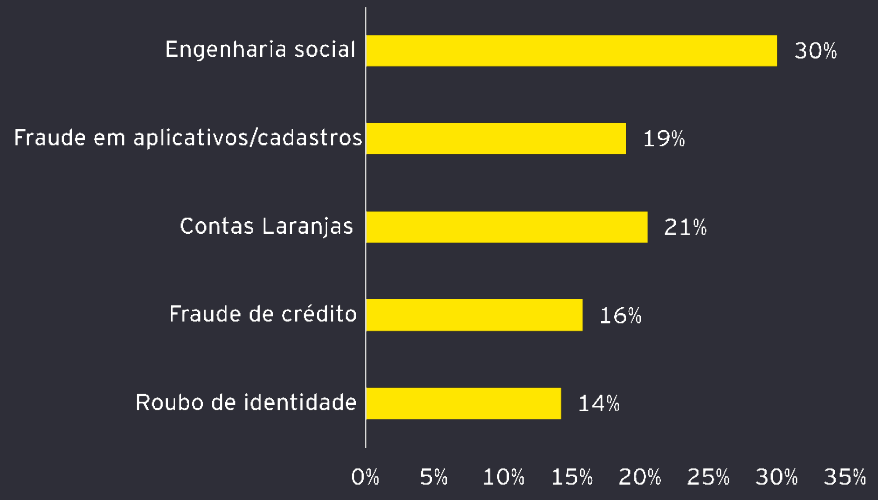
Por fim, a análise setorial confirma que bancos comerciais e instituições de pagamento estão entre os grupos que mais investem, o que é coerente com o fato de concentrarem a maior incidência de tentativas de fraude, especialmente no âmbito transacional. O padrão reforça que os investimentos acompanham a criticidade da exposição de cada setor, mas a persistência de grandes instituições com gastos reduzidos indica que parte do mercado pode estar subestimando o risco ou adotando estratégias de resposta mais reativas do que preventivas. Esse quadro aponta para a necessidade de maior alinhamento nos padrões de governança e nos critérios de alocação de recursos, de forma a reduzir assimetrias e fortalecer a resiliência do sistema.

Prevenção à Fraude

Tipologia de Fraudes

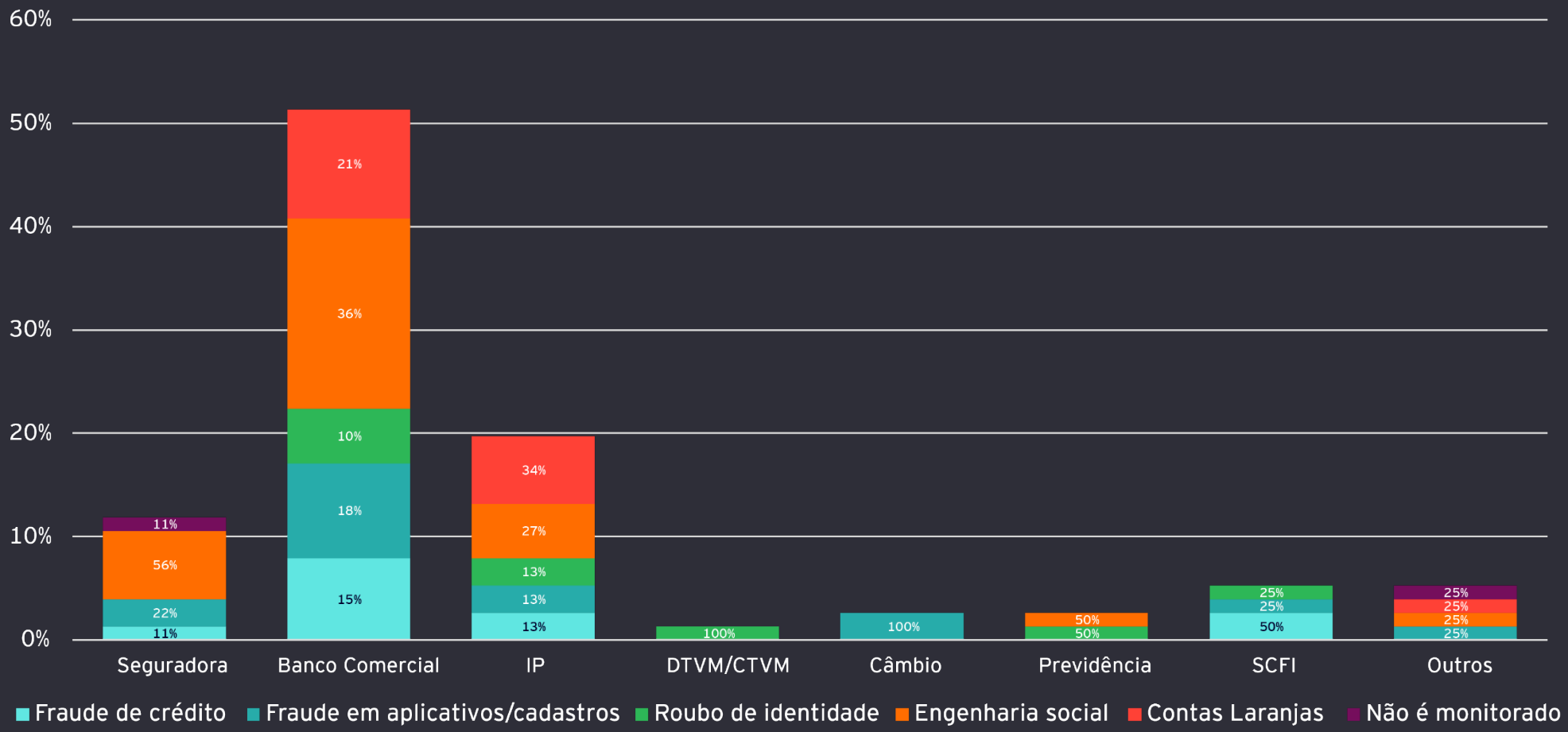
A análise das respostas evidencia que determinados tipos de fraude se destacam de forma recorrente no mercado. Engenharia social aparece como a tipologia mais citada, reportada por 30% das instituições, seguida por contas laranjas (21%) e fraudes em aplicativos/cadastros (19%). Em menor escala, surgem fraude de crédito (16%) e roubo de identidade ou tomada de conta (14%). O resultado confirma que ataques baseados na exploração do fator humano e na manipulação de cadastros digitais se consolidam como as principais frentes de preocupação para o sistema financeiro.

Tipologia da fraude 2025



Quando analisado por setor, o cenário revela variações significativas entre segmentos de mercado. Nos bancos comerciais, a tipologia mais frequente é a engenharia social (36%), seguida por contas laranjas (21%), refletindo tanto o alto volume transacional quanto a utilização de intermediários em esquemas ilícitos. Já nas instituições de pagamento, o padrão é mais distribuído, com destaque para engenharia social (27%), aplicativos/cadastros (13%) e fraude de crédito (13%), indicando vulnerabilidades no *onboarding* digital e em concessões de crédito de menor valor. As seguradoras, por sua vez, destoam do restante do mercado: 56% indicaram engenharia social como a principal tipologia e, de forma preocupante, 11% declararam não monitorar fraudes – um dado alarmante considerando que, ao contrário do risco de PLD, o risco de fraude nesse setor é elevado e de impacto direto nas operações.

Tipologia da fraude 2025 – por setor



Esse conjunto de resultados reforça a percepção de que o combate à fraude demanda abordagens diferenciadas conforme o setor. A predominância da engenharia social evidencia a necessidade de ampliar investimentos em educação do cliente, autenticação reforçada e mecanismos de verificação em tempo real. O peso relativo de fraudes em aplicativos e cadastros entre IPs e instituições menores destaca a importância de evoluir controles de *onboarding* digital e fortalecer processos de validação de identidade. Já nos bancos, a relevância das contas laranjas como segunda tipologia mais frequente confirma a urgência de estratégias integradas de monitoramento transacional e colaboração interbancária, essenciais para desarticular redes ilícitas e reduzir riscos sistêmicos.

No conjunto, a tipologia de fraudes reportada em 2025 ilustra tanto a resiliência de métodos tradicionais quanto a rápida adaptação dos fraudadores a novos canais digitais. A heterogeneidade dos resultados entre setores indica que não há um único vetor de risco dominante para todo o sistema, mas sim um mosaico de ameaças que se distribuem de acordo com as características de cada instituição. A leitura desse cenário reforça a importância de estratégias de prevenção sob medida alinhadas ao perfil de negócios e à realidade operacional de cada organização.

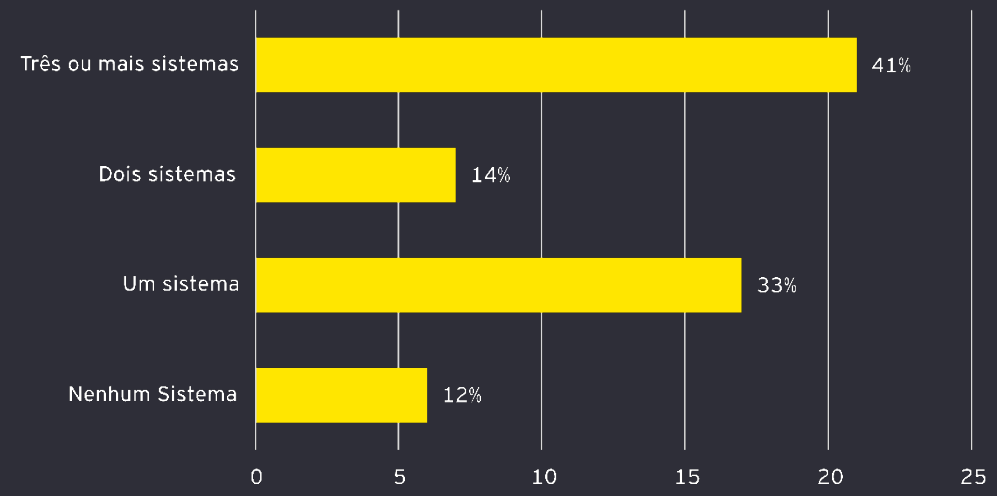
Prevenção à Fraude

Infraestrutura Tecnológica

A infraestrutura tecnológica é peça central no combate à fraude, definindo a capacidade das instituições de identificar, bloquear e responder a tentativas de ataque em tempo real. Os dados da pesquisa revelam que não há um modelo único consolidado no mercado: a maioria das instituições combina diferentes ferramentas, como sistemas de monitoramento de transações, acesso a bases compartilhadas, históricos internos de fraudes e mecanismos de bloqueio de abertura de contas. Essa diversidade mostra um esforço para construir defesas em camadas, ainda que a difusão dos sistemas varie de forma significativa entre os participantes.

A análise sobre a quantidade de sistemas utilizados por instituição reforça a leitura de que maturidade varia amplamente no mercado. Uma parte relevante das instituições ainda depende de apenas um ou dois sistemas, mas cresce o grupo que já utiliza três ou mais soluções de forma combinada. Apesar desse avanço, é preocupante que 12% das instituições reportem não utilizar nenhum dos sistemas listados, sinalizando fragilidades significativas em sua infraestrutura de combate à fraude. Essa diferença traduz o quanto algumas instituições permanecem em um estágio básico de estruturação, enquanto outras buscam maior robustez tecnológica para lidar com a diversidade de tipologias de fraude identificadas.

Quantidade de sistemas de prevenção à fraude

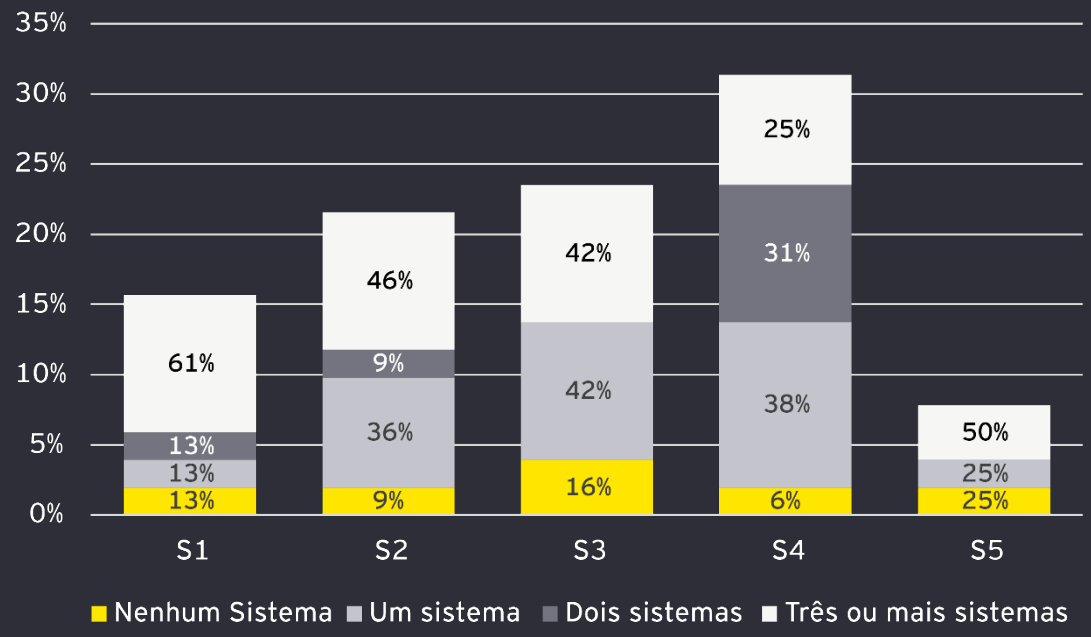


Prevenção à Fraude

Infraestrutura Tecnológica

Nos recortes por setor, destaca-se o desempenho das instituições de pagamento, que aparecem como o grupo mais avançado: nenhuma declarou operar sem sistemas de prevenção, e pelo menos 83% reportaram utilizar cada uma das principais categorias de ferramentas. Os bancos comerciais também apresentam alta presença de monitoramento e bloqueio de contas, embora de forma menos homogênea que as IPs. No recorte por segmento regulatório, observa-se que instituições de maior porte tendem a adotar mais sistemas combinados: entre as S1, 61% declararam utilizar três ou mais, contra apenas 25% entre as S4, reforçando que porte ainda é um fator determinante para a amplitude da infraestrutura tecnológica.

Quantidade de sistemas de prevenção à fraude, por segmento



No conjunto, os resultados reforçam que a infraestrutura tecnológica de prevenção à fraude no mercado brasileiro está em evolução, mas ainda desigual. A pluralidade de sistemas adotados mostra uma busca por defesas mais completas, mas a baixa adoção em algumas categorias e a existência de instituições sem sistemas básicos ativos revelam que ainda há fragilidades relevantes.

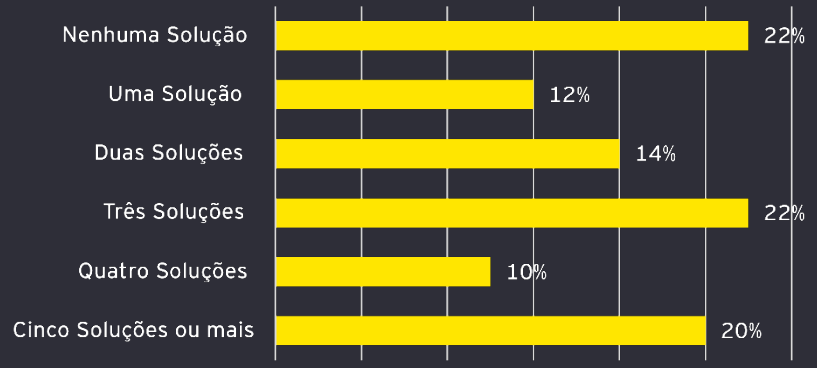
Cruzando esses resultados com a seção de interação entre áreas, observamos que 86% das instituições que declararam utilizar três ou mais sistemas também reportaram algum nível de integração entre áreas – um sinal de que maior complexidade tecnológica tende a estar associada a estágios mais maduros de governança. A consolidação de práticas de mercado e a maior integração entre soluções devem ser elementos-chave para elevar o nível de resiliência do sistema como um todo.

Prevenção à Fraude

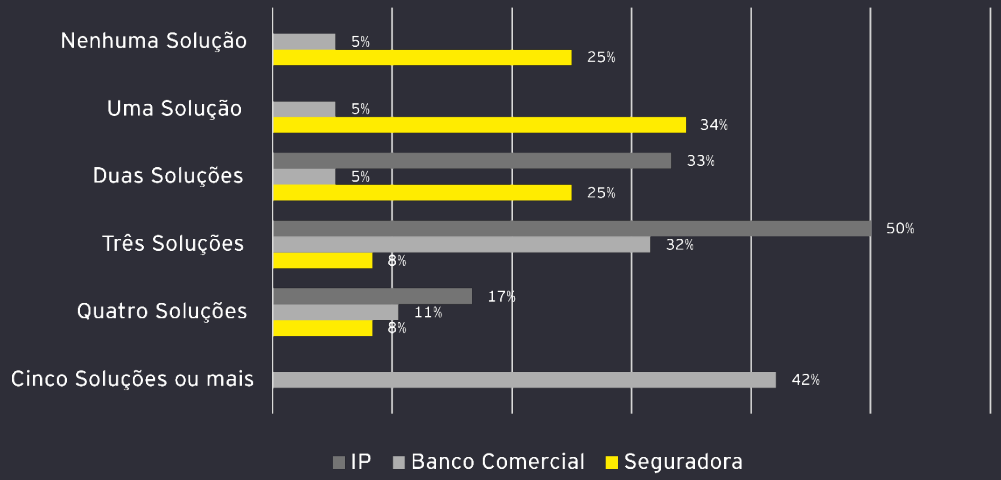
Onboarding e Verificação de Identidade

A etapa de abertura de contas é um dos pontos mais sensíveis para a prevenção a fraudes, já que concentra o risco de entrada de clientes maliciosos no sistema financeiro. Quando observada a quantidade de soluções utilizadas, apenas 20% das instituições declaram operar com cinco ou mais ferramentas, mas os bancos comerciais se destacam positivamente, com 42% nesse patamar e apenas 15% restritos a duas ou menos soluções. As instituições de pagamento também aparecem bem posicionadas: 67% afirmam utilizar três ou mais soluções, embora nenhuma tenha atingido a marca de cinco ou mais. O contraste com o setor segurador reforça a existência de diferentes estágios de maturidade entre segmentos, sugerindo que ainda há fragilidades relevantes em áreas específicas do mercado.

Número de soluções: validação no *onboarding*



Número de soluções: validação no *onboarding*, por setor

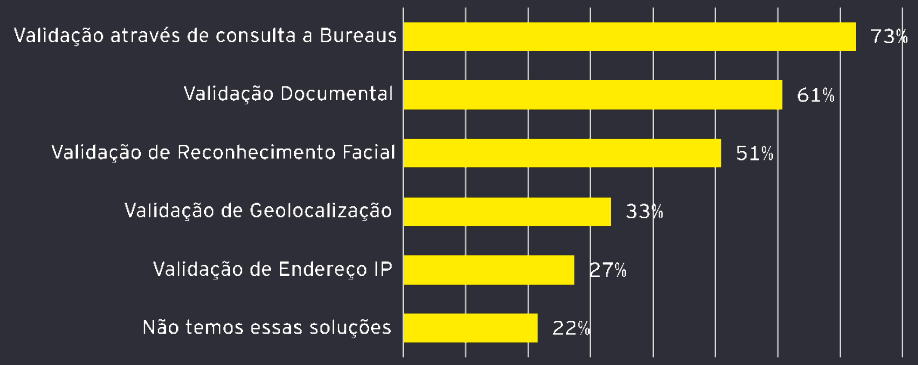


Prevenção à Fraude

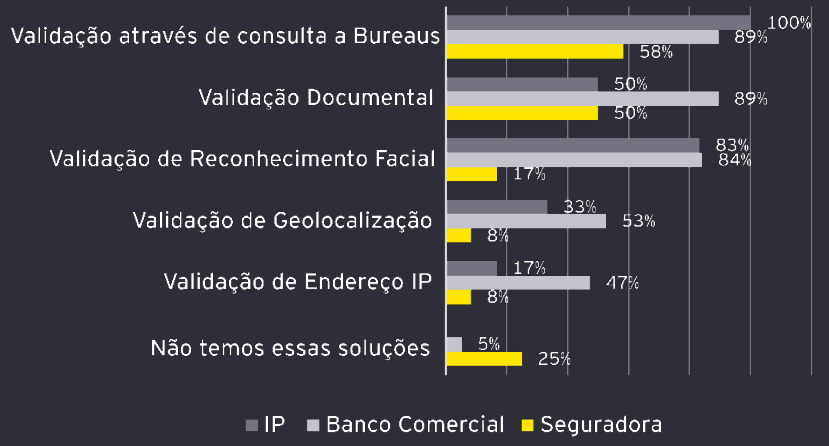
Onboarding e Verificação de Identidade

No que diz respeito às soluções mais comuns, prevalece a adoção de tecnologias mais tradicionais. Consulta a *bureaus* (73%) é a prática mais disseminada, seguida por validação documental (61%) e reconhecimento facial (51%), que já começam a se consolidar como padrão no mercado. Ainda assim, recursos de maior sofisticação permanecem subutilizados: validação de geolocalização está presente em apenas 33% das instituições, incluindo apenas um terço das IPs, apesar de sua importância para identificar transações em padrões atípicos. Ao observar especificamente quem **não adota tecnologias mais modernas** – como geolocalização, validação de endereço IP e reconhecimento facial –, nota-se que **80% pertencem às categorias S3, S4 ou S5**, reforçando que porte continua sendo determinante para a velocidade de adoção.

Soluções mais comuns: validação no *onboarding*



Soluções mais comuns: validação no *onboarding*, por setor



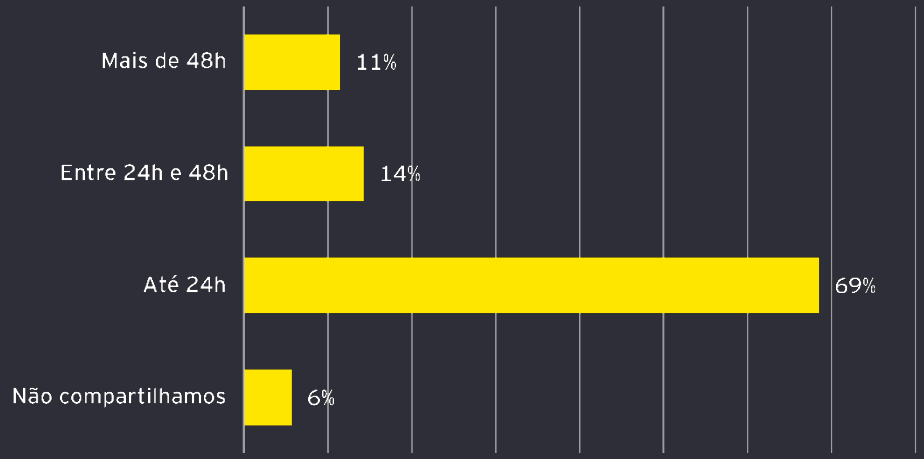
Bancos comerciais lideram a adoção das soluções mais avançadas, com mais de 80% reportando uso de reconhecimento facial, validação documental e consulta a *bureaus*, o que reforça seu papel de vanguarda em práticas de *onboarding* seguro. Já as instituições de pagamento, embora sem atingir o mesmo patamar em todas as frentes, apresentam índices elevados e consistentes, sem casos de ausência total de soluções, diferentemente de outros segmentos.

Prevenção à Fraude

Tempo de Resposta e Compartilhamento de Dados

A Resolução Conjunta nº 6/2023 e a Resolução BCB nº 343/2023, em vigor desde novembro de 2023, determinam que indícios de fraude devem ser registrados e compartilhados pelas instituições autorizadas a operar pelo Banco Central do Brasil em até 24 horas a partir de sua identificação. Este requisito normativo representa um marco fundamental na agenda regulatória de prevenção a fraudes e orienta a análise apresentada nesta seção, que considera exclusivamente instituições enquadradas sob a supervisão do BCB, excluindo seguradoras e entidades de previdência.

Tempo de resposta: compartilhamento de informações de fraudes

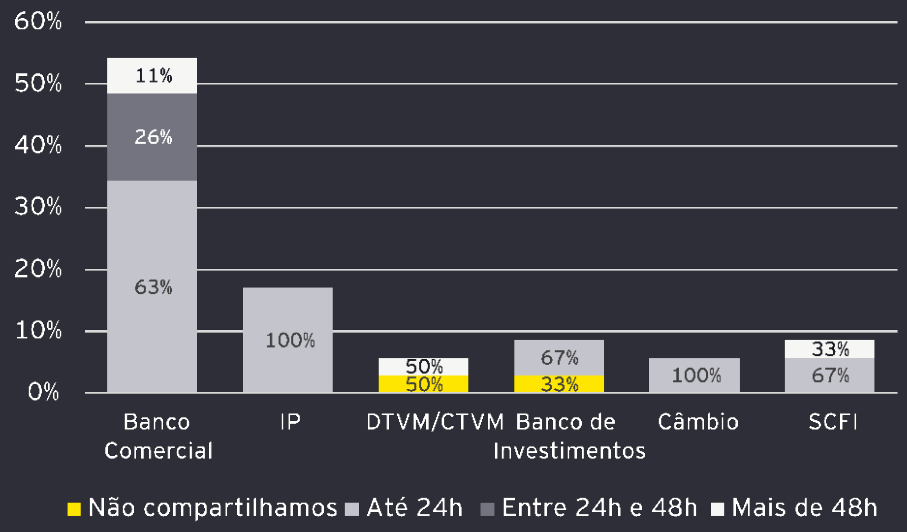


Prevenção à Fraude

Tempo de Resposta e Compartilhamento de Dados

Os resultados revelam um desalinhamento relevante com a norma. Aproximadamente 31% dos respondentes não cumprem o prazo regulatório, seja por não realizarem qualquer compartilhamento de informações ou por o fazerem além do limite de 24 horas. Entre os bancos comerciais, 37% ainda não atende o prazo de 24 horas para o compartilhamento de informações, apesar da relevância do setor. Situação ainda mais crítica é observada nas DTVMs, em que 100% dos respondentes não realizam o compartilhamento no prazo, divididos entre aqueles que não reportam e aqueles que o fazem apenas após 48 horas. Nos bancos de investimento, 33% declararam não realizar qualquer reporte, e nas SCFIs, 33% ainda reportam apenas após 48 horas.

Tempo de resposta: compartilhamento de informações de fraudes, por setor



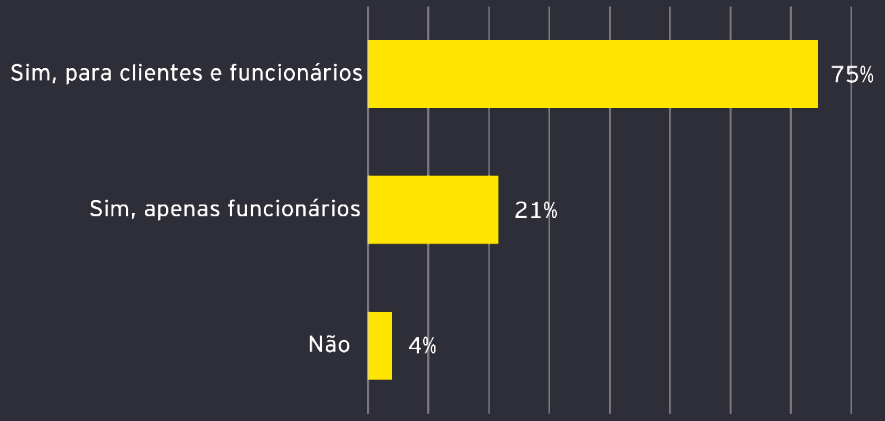
De forma geral, a fotografia não é favorável. Mais de um ano e meio após a entrada em vigor da Resolução 343, uma parcela significativa das instituições autorizadas a operar pelo BCB ainda não reporta as informações no prazo regulatório. Embora IPs e câmbio mostrem boa performance, segmentos como DTVMs, bancos de investimento e parte dos bancos comerciais permanecem com lacunas. O cenário aponta para a necessidade de ajustes estruturais por parte das instituições, a fim de assegurar a efetividade do arcabouço de prevenção a fraudes.

Prevenção à fraude

Conscientização e cultura organizacional

O fortalecimento da cultura organizacional e a conscientização sobre riscos de fraude são pilares centrais de qualquer programa de prevenção. Nesse sentido, os resultados da pesquisa indicam uma ampla maturidade no mercado: 96% das instituições afirmam possuir campanhas estruturadas de conscientização, com apenas 4% ainda sem iniciativas formais nesse campo. A relevância desse tema ganha ainda mais peso diante do fato de que, conforme identificado na seção sobre tipologias de fraude, a engenharia social foi a modalidade mais recorrente no último ano, reforçando que a conscientização de funcionários e clientes é uma das defesas mais eficazes contra esse tipo de ataque.

Campanhas de conscientização - prevenção à fraude



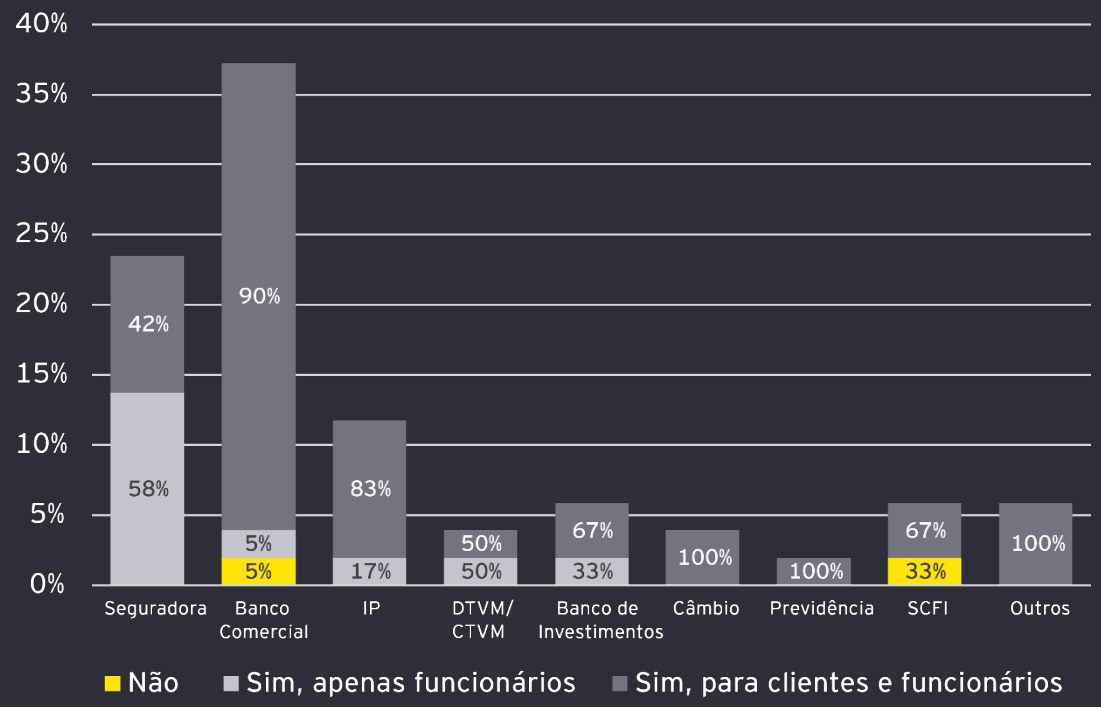
A maior parte das instituições adota uma abordagem mais abrangente, estendendo suas campanhas tanto a funcionários quanto a clientes. Esse grupo representa 75% da amostra total, evidenciando um entendimento consolidado de que a prevenção à fraude exige engajamento de toda a cadeia. Por outro lado, 21% limitam suas ações apenas ao público interno, restringindo o alcance e o potencial preventivo das iniciativas.

Prevenção à fraude

Conscientização e cultura organizacional

No recorte setorial, os bancos comerciais aparecem como líderes na adoção das campanhas mais completas, com 90% declarando realizar ações voltadas a funcionários e clientes. O dado de 5% de bancos que reportaram não possuir programas de conscientização refere-se exclusivamente a instituições voltadas ao segmento de pessoa jurídica, o que atenua parte da preocupação, dado o menor contato direto com clientes de varejo. Entre as instituições de pagamento, 17% limitam suas campanhas exclusivamente ao público interno, o que pode representar uma lacuna relevante em um segmento caracterizado por alto volume de fraudes envolvendo diretamente o cliente final.

Campanhas de conscientização - prevenção à fraude, por setor



De forma geral, os resultados demonstram avanços expressivos na consolidação da cultura de prevenção, com forte presença de campanhas abrangentes em diferentes setores. Além dos esforços institucionais, iniciativas coletivas lideradas por associações também contribuem para disseminar conhecimento e reforçar a cultura preventiva, como a campanha "Tem Cara de Golpe" da ABBC e a campanha antifraudes da FEBRABAN, que ampliam o alcance das mensagens de conscientização em toda a sociedade.

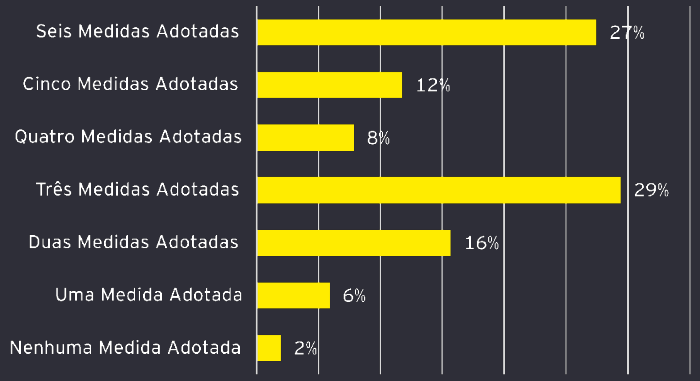
Prevenção à Fraude

Medidas Adotadas para Prevenção à Fraude

A análise das medidas de prevenção à fraude adotadas pelas instituições revela um cenário de relativa maturidade, ainda que marcado por diferenças importantes entre setores. Em linhas gerais, observa-se que a maior parte das organizações já estruturou um conjunto consistente de controles, com avanços mais expressivos em segmentos naturalmente mais expostos ao risco.

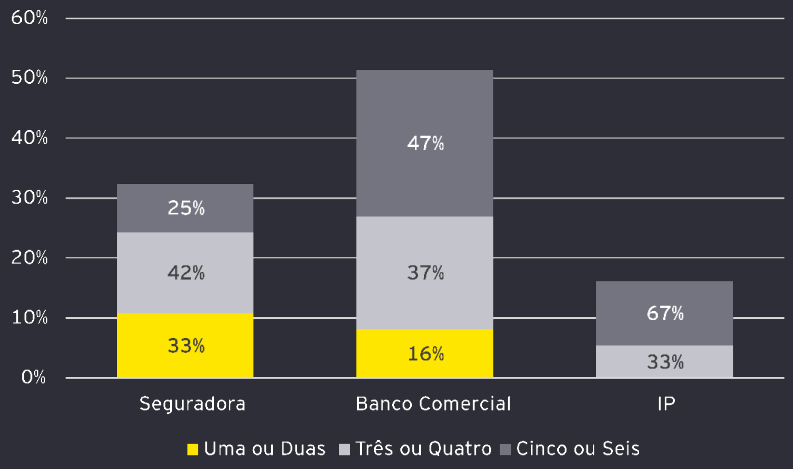
Do ponto de vista quantitativo, 39% das empresas declararam adotar cinco ou mais medidas de prevenção, indicador que demonstra um nível robusto de proteção. Destaca-se especialmente o desempenho de bancos e instituições de pagamento, em que 47% e 67%, respectivamente, afirmam operar com cinco ou seis medidas, além de nenhuma instituição de pagamento reportar menos de três iniciativas. Esse resultado reforça a maior maturidade desses segmentos frente à sua exposição ao risco.

Quantidade de medidas adotadas - prevenção à fraude



No recorte setorial, chama atenção o fato de nenhum banco comercial, instituição de pagamento ou seguradora ter reportado ausência total de medidas, o que representa um piso mínimo de proteção. Por outro lado, há sinais de fragilidade: 16% dos bancos ainda afirmam contar apenas com uma ou duas medidas. Esse grupo é composto exclusivamente por instituições S3 e S4, enquanto todos os bancos de maior porte (S1 e S2) declararam adotar conjuntos mais amplos de controles – evidência de que, mesmo quando há baixa cobertura, a limitação se concentra nos segmentos menores.

Quantidade de medidas adotadas - prevenção à fraude, por setor

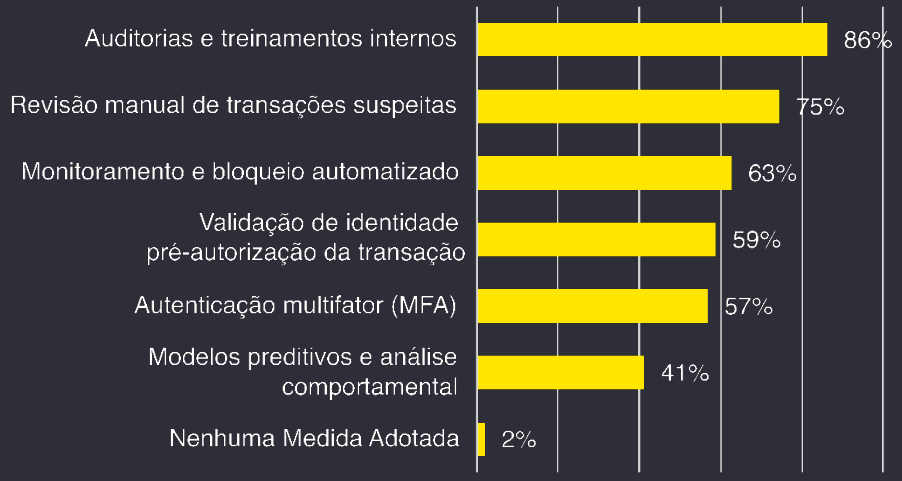


Prevenção à Fraude

Medidas Adotadas para Prevenção à Fraude

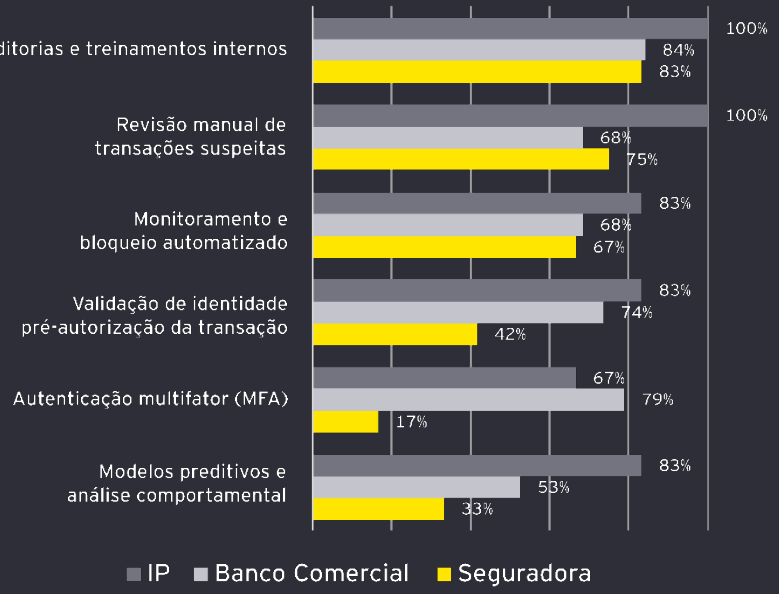
Em relação às medidas específicas, a pesquisa mostra que o mercado segue priorizando mecanismos mais tradicionais: "auditorias e treinamentos internos" e "revisão manual de transações suspeitas" aparecem como as mais adotadas, enquanto "modelos preditivos e análise comportamental" ocupa a última posição. Esse padrão sugere que o mercado ainda depende fortemente de práticas consolidadas e menos sofisticadas, com espaço significativo para evolução em soluções mais tecnológicas e adaptativas nos segmentos S3 e S4.

Medidas adotadas mais utilizadas - prevenção à fraude



O recorte por setor reforça esse diagnóstico, ao mesmo tempo em que evidencia avanços relevantes. Nas instituições de pagamento, mesmo a medida menos adotada — autenticação multifator — atinge 67% de adesão, enquanto 83% já utilizam modelos preditivos e análise comportamental, destacando-se como líderes em inovação. Entre as seguradoras, a adesão às soluções mais tecnológicas ainda é limitada, com menos de 50% de adoção nos pilares tecnológicos mais modernos.

Medidas adotadas mais utilizadas - prevenção à fraude, por setor



Em conjunto, os dados demonstram que, embora haja um núcleo robusto de medidas implementadas, o mercado ainda opera com forte dependência de controles tradicionais e a evolução rumo a soluções mais sofisticadas será determinante para o fortalecimento da resiliência no médio prazo.

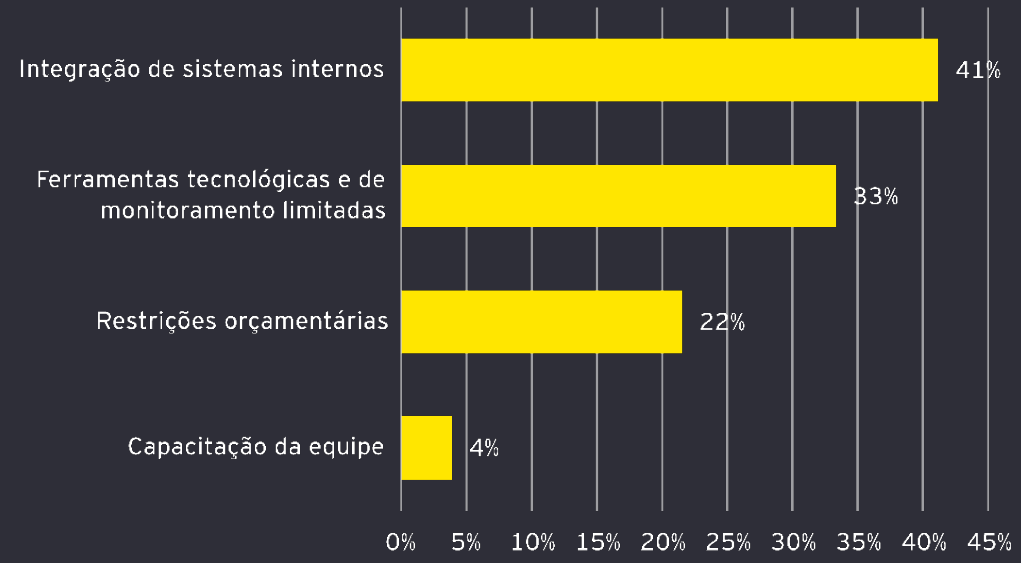
Prevenção à Fraude

Principais Desafios

Atualmente, o maior desafio apontado pelas instituições no combate à fraude é a integração de sistemas internos, destacada por 41% dos respondentes. O resultado chama atenção especialmente quando comparado com os achados da seção "Infraestrutura tecnológica", em que 65% das instituições afirmaram já ter acesso a bases compartilhadas. Esse contraste sugere que o gargalo não está na disponibilidade de ferramentas, mas sim na capacidade de integrar e orquestrar de forma eficiente os recursos tecnológicos existentes.

Em contraposição, apenas 4% das instituições indicaram capacitação da equipe como o principal desafio. Esse dado reforça a percepção de que as barreiras atuais são predominantemente tecnológicas e ligadas à integração, e não relacionadas à preparação dos profissionais. Ou seja, a questão central parece residir mais no solidez e conexão dos sistemas do que na competência dos times responsáveis pela prevenção a fraudes.

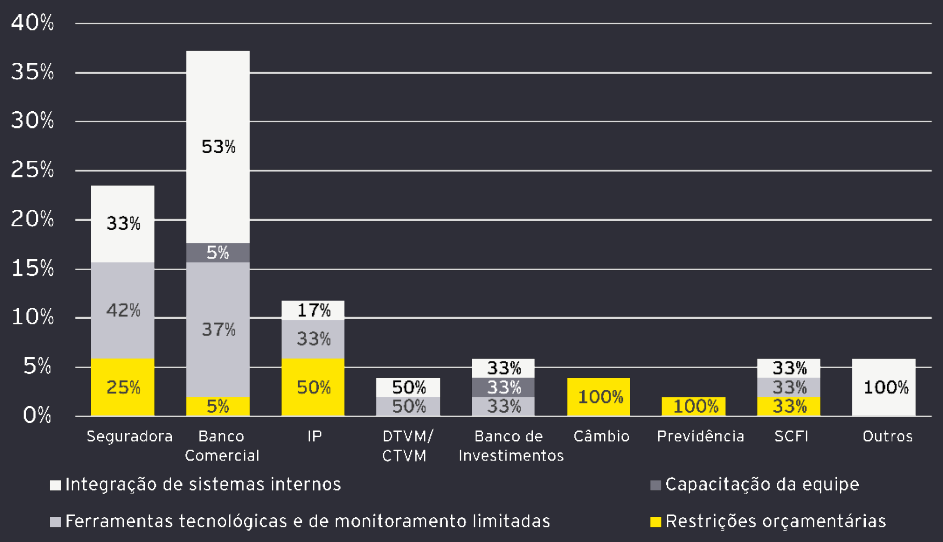
Principais desafios no combate à fraude



Prevenção à Fraude

Principais Desafios

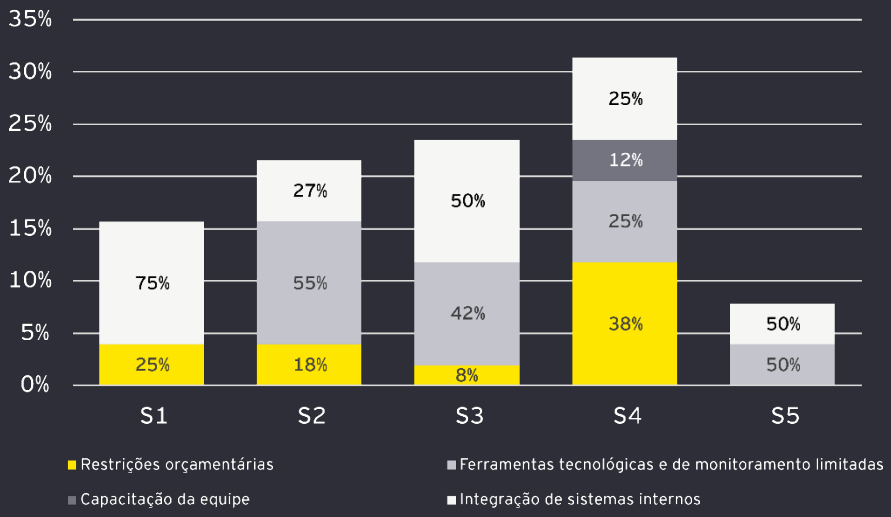
Principais desafios no combate à fraude, por setor



O recorte setorial evidencia como esses desafios se distribuem de maneira diferenciada. Nos bancos comerciais, por exemplo, 53% dos respondentes mencionaram integração de sistemas internos como o maior obstáculo, reforçando a complexidade das operações nesse setor. Já entre as instituições de pagamento (IPs), metade dos respondentes destacou restrições orçamentárias como o maior entrave, refletindo a dificuldade em equilibrar custos elevados de tecnologia com a necessidade crescente de proteção contra fraudes.

Sob a ótica de segmentação de porte, emergem achados ainda mais curiosos. No segmento S1, composto pelas maiores instituições do mercado, 75% das empresas apontaram integração de sistemas internos como principal desafio, sinalizando que mesmo as organizações mais robustas enfrentam dificuldades estruturais para consolidar suas tecnologias. Mais surpreendente ainda, 25% dessas instituições também citaram restrições orçamentárias — uma das maiores concentrações desse tipo de resposta em toda a pesquisa. O dado sugere que os segmentos menores podem estar subdimensionando a real dimensão financeira envolvida na construção de *frameworks* robustos de prevenção a fraudes.

Principais desafios no combate à fraude, por segmento



Em conjunto, os achados reforçam que, embora as necessidades variem conforme o porte e o setor, a integração tecnológica permanece como fator-chave e recorrente para toda a indústria.

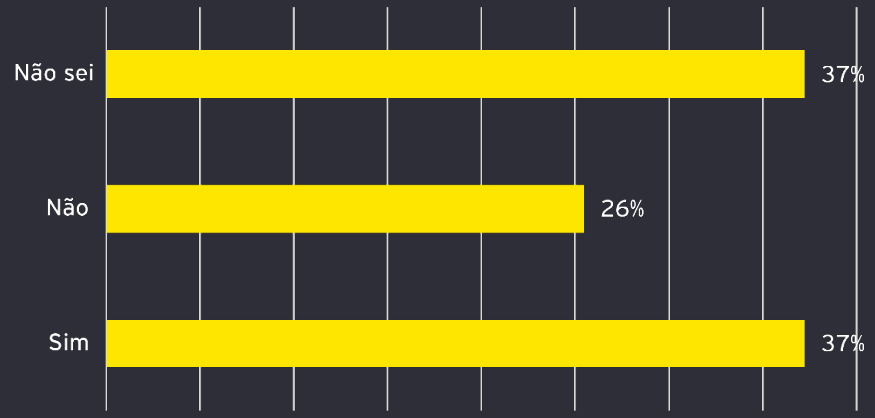
Prevenção à Fraude

Monitoramento Avançado

O monitoramento de dados na *dark web* tem se consolidado como um componente crítico dos *frameworks* modernos de prevenção a fraudes. Esses ambientes são utilizados para a comercialização de credenciais roubadas, dados de clientes, números de cartões e tutoriais de fraude, além de abrigarem discussões sobre novos esquemas ilícitos. Identificar essas movimentações de forma ágil permite ações preventivas — como bloqueio de contas, redefinição de senhas ou ajustes de controles internos — além de enriquecer investigações e fortalecer a postura de cibersegurança das instituições.

Ainda assim, a pesquisa mostra que esse é um campo onde existe espaço relevante para evolução. Quando consideradas todas as respostas, 37% dos participantes afirmaram "não saber" se sua instituição realiza esse tipo de monitoramento.

Monitoramento de dados na *dark web*

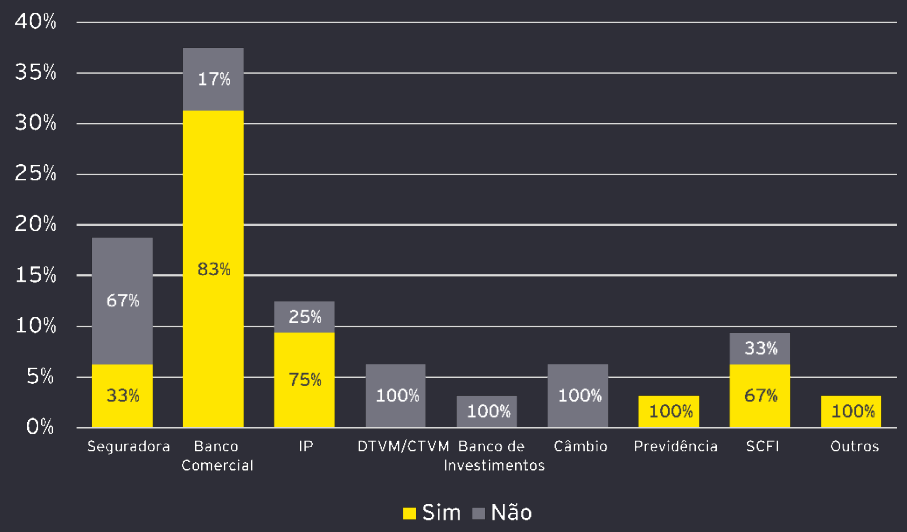


Ao restringir a análise apenas às instituições que responderam de forma categórica — "Sim" ou "Não" —, observa-se que 60% afirmaram monitorar a *dark web*, enquanto 40% indicaram não realizar essa atividade. Isso reforça a percepção de que, apesar do avanço, o monitoramento ainda não é plenamente difundido, permanecendo uma prática parcial e mais comum entre instituições de maior porte ou mais expostas a riscos complexos.

Prevenção à Fraude

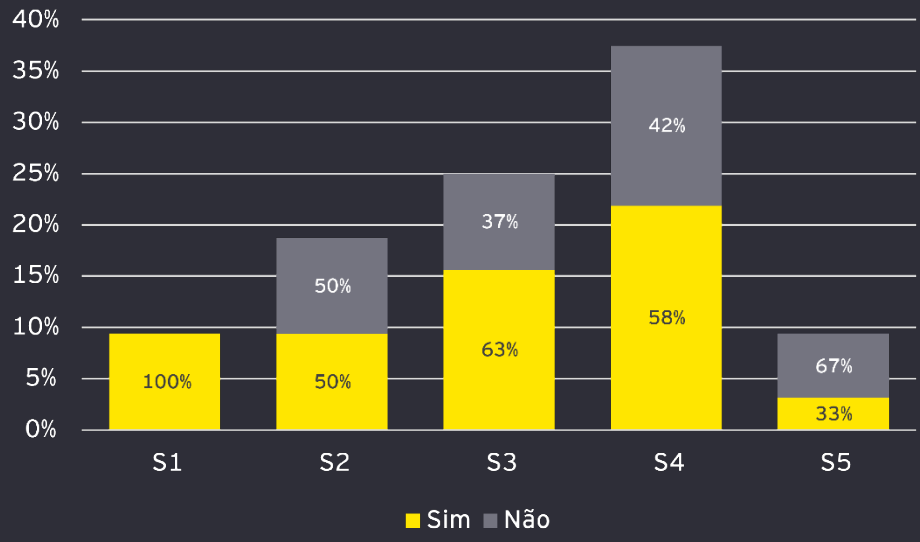
Monitoramento Avançado

Monitoramento de dados na *dark web*, por setor



O recorte setorial evidencia um padrão claro: bancos lideram a adoção, com 83% afirmando realizar monitoramento, seguidos pelas instituições de pagamento (75%). Esse resultado está em linha com outros achados da pesquisa, que mostram esses setores na vanguarda das medidas de combate a fraudes, dado seu perfil de maior risco. Em contrapartida, setores como DTVM/CTVM, Bancos de Investimento e Corretoras de Câmbio registraram 0% de monitoramento, o que as expõe a vulnerabilidades significativas.

Monitoramento de dados na *dark web*, por segmento



A análise por segmento de porte das instituições confirma a tendência: 100% das empresas S1 (as maiores do mercado) realizam monitoramento, enquanto no extremo oposto, entre as S5, apenas 33% adotam a prática. Apesar de pequenas variações entre os segmentos intermediários, a curva geral é clara: quanto maior a instituição, maior o nível de maturidade no acompanhamento de riscos oriundos da *dark web*.

Em síntese, os resultados apontam para uma implementação ainda parcial do monitoramento da *dark web* no setor financeiro brasileiro. Grandes instituições vêm incorporando a prática de forma consistente, mas empresas de menor porte e alguns segmentos específicos permanecem desprotegidos frente a um vetor de risco cada vez mais relevante. Reforçar essa capacidade, especialmente fora do núcleo bancário e das maiores organizações, é fundamental para fortalecer a resiliência do ecossistema como um todo.

4 Visão integrada | Fraude, PLDFTP e *Cyber*

Shape the future with confidence

Integração entre Áreas

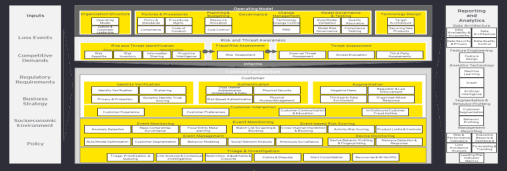
Introdução à Integração entre Áreas

As instituições financeiras enfrentam um cenário em constante transformação, impulsionado por inovações tecnológicas como inteligência artificial, automação e pagamentos instantâneos. Essas mudanças trazem tanto oportunidades quanto riscos, especialmente no combate a fraudes, lavagem de dinheiro e crimes cibernéticos. A Inteligência Artificial (IA), por exemplo, pode ser usada para detectar padrões suspeitos, mas também é explorada por criminosos para criar ameaças sofisticadas, como identidades sintéticas e *deepfakes*. Em 2020, o *Federal Bureau of Investigation* (FBI) apontou a fraude de identidade sintética como o crime financeiro que mais crescia nos Estados Unidos, causando perdas anuais de 20 bilhões de dólares – e isso antes mesmo da popularização das IAs que vimos no último ano.

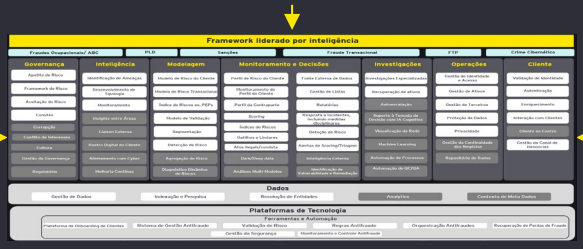
Para lidar com esses desafios, a colaboração entre equipes de PLD/FTP, cibersegurança e prevenção a fraudes é essencial, a fim de fortalecer a resiliência das instituições, permitindo respostas rápidas e coordenadas frente a ataques e vulnerabilidades emergentes. O combate a crimes financeiros deve evoluir para um ecossistema conectado, em que governança, inteligência e operações trabalham de forma coordenada, apoiadas por tecnologia e dados centralizados.

Prevenção a crimes financeiros

Fraude



Cibersegurança



***Framework* liderado por inteligência**

Integração entre Áreas

Resultados da pesquisa – Níveis de integração

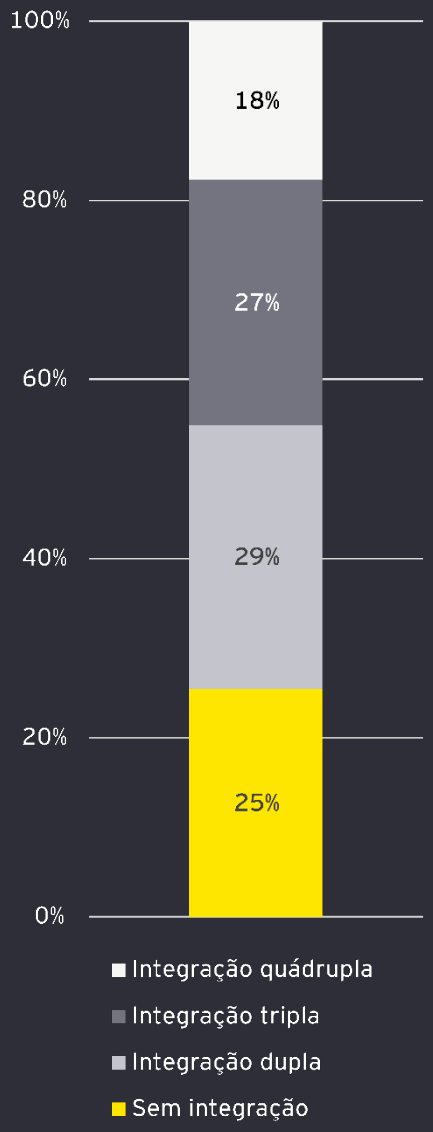
Como parte da pesquisa, tivemos como objetivo analisar o nível de integração entre as áreas de Prevenção a Fraudes, PLD/FTP, *Cyber* e Risco de Crédito das instituições participantes. Para isso, inicialmente avaliamos se as organizações possuem algum grau de integração entre essas funções e, em caso afirmativo, quais áreas estão integradas e qual a profundidade dessa integração.

A análise mostra que 75% das instituições respondentes já possuem algum grau de integração entre as áreas avaliadas, enquanto 25% ainda não apresentam nenhuma integração. Na pesquisa publicada em 2023, apenas 34% dos respondentes declarou possuir integração entre áreas.

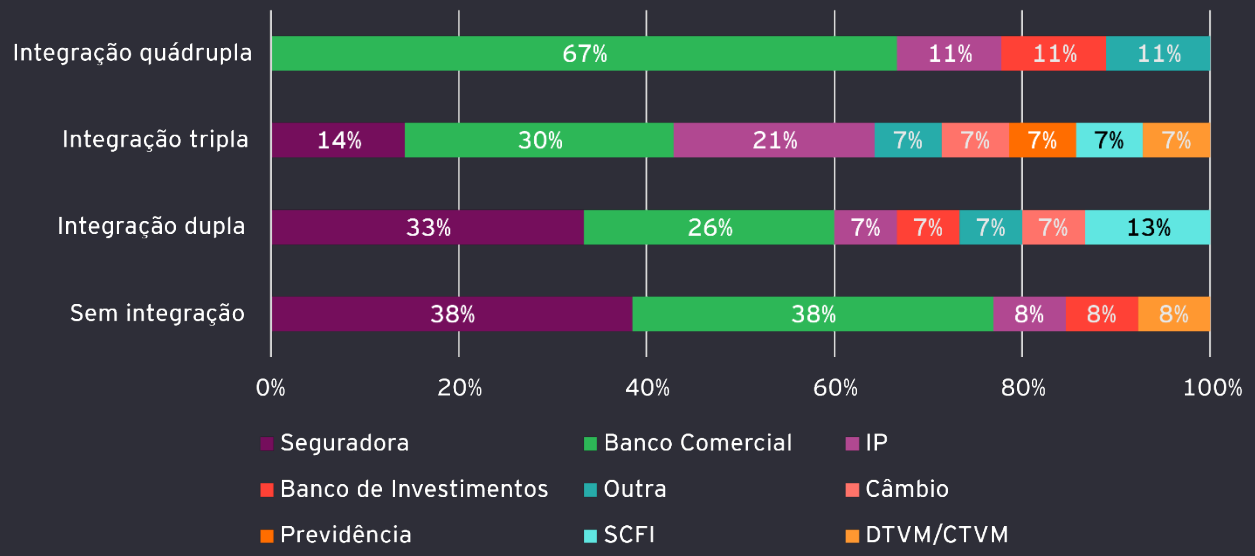
Entre aquelas que possuem integração, a maioria concentra-se em níveis intermediários, envolvendo duas ou três áreas. Observa-se, portanto, um movimento relevante em direção à colaboração entre funções, embora ainda exista espaço para evolução.

Integração entre Áreas

Nível de integração



Níveis de integração entre Áreas, for setor



A distribuição da integração entre os diferentes setores revela padrões distintos de integração.

Observa-se que os **bancos comerciais** concentram a maior parte das instituições com integração quádrupla, enquanto também apresentam casos sem integração (instituições estas distribuídas nos segmentos S1 e S4).

As instituições de pagamento (IPs) destacam-se por uma presença relevante nos níveis mais avançados (tripla e quádrupla), enquanto as seguradoras permanecem predominantemente em níveis intermediários ou sem integração, indicando maior necessidade de evolução.

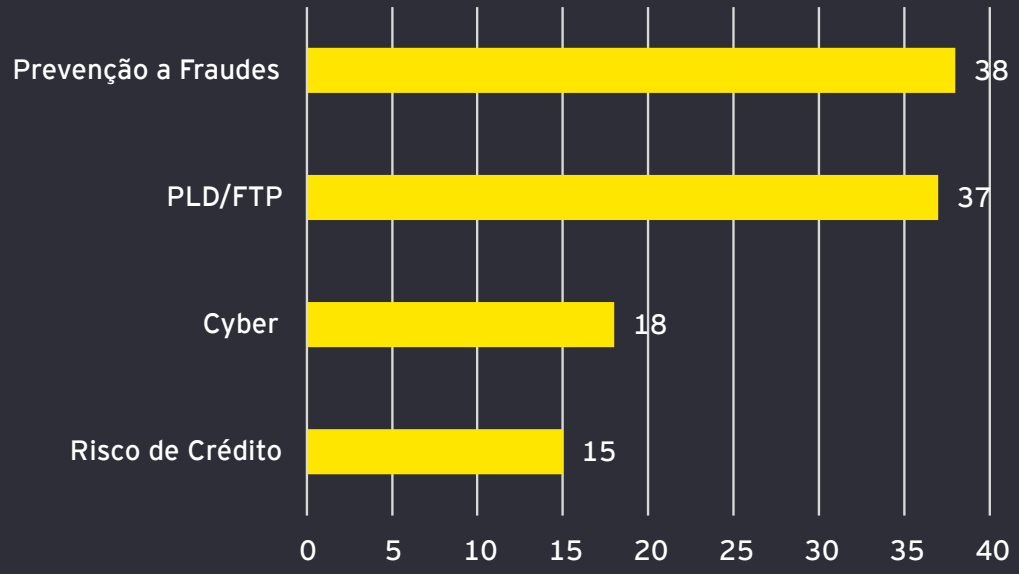
Outros segmentos, como bancos de investimento, SCFI e DTVM/CTVM, aparecem de forma pontual, mas com indícios de integração parcial.

Integração entre Áreas

Áreas integradas: onde a integração acontece

Para analisar em quais áreas a integração ocorre, consideramos apenas as instituições que reportaram algum nível de integração. Inicialmente, avaliamos a frequência por área (Prevenção a Fraudes, PLD/FTP, *Cyber* e Risco de Crédito).

Áreas com integração
(apenas instituições com integração)



A análise evidencia que a integração entre áreas é fortemente concentrada em Prevenção a Fraudes e PLD/FTP, que aparecem como os principais pontos de conexão entre as funções avaliadas.

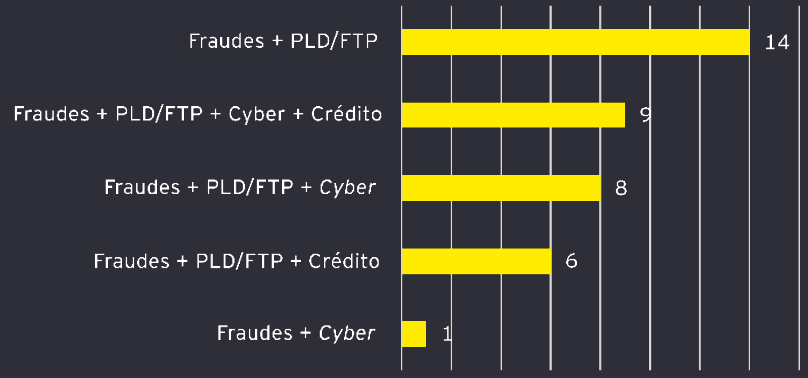
Esse padrão sugere que, embora exista um núcleo de integração bem estabelecido, há espaço relevante para ampliar a colaboração com funções tecnológicas e de risco de crédito, de forma a alcançar uma abordagem mais abrangente e robusta.

Integração entre Áreas

Como a integração acontece: combinações mais recorrentes de áreas

Também foram analisadas as combinações mais frequentes entre as áreas analisadas.

Combinação mais comum de áreas integradas
(apenas instituições com integração)



O *ranking* das combinações evidencia que a integração se estrutura a partir do núcleo Prevenção a Fraudes + PLD/FTP, que concentra a maior parte dos casos e atua como ponto de ancoragem para arranjos mais amplos. A partir desse núcleo, observa-se a evolução para tríades que incorporam *Cyber* e/ou Risco de Crédito, culminando na integração completa das quatro áreas, o que sugere um processo gradual de ampliação da colaboração.

A análise por setor confirma que a combinação entre Prevenção a Fraudes e PLD/FTP é transversal, presente em praticamente todos os segmentos, enquanto as integrações mais amplas (tríades e quádrupla) concentram-se em bancos comerciais e, em menor escala, em instituições de pagamento. Seguradoras permanecem restritas a arranjos mais simples.

Esses resultados consolidam a importância do eixo Fraudes–PLD/FTP e indicam que a próxima fronteira de evolução está na integração sistemática de *Cyber* e Risco de Crédito, por meio de casos de uso transversais, como modelos analíticos compartilhados, gestão unificada de alertas e processos orquestrados entre as áreas.

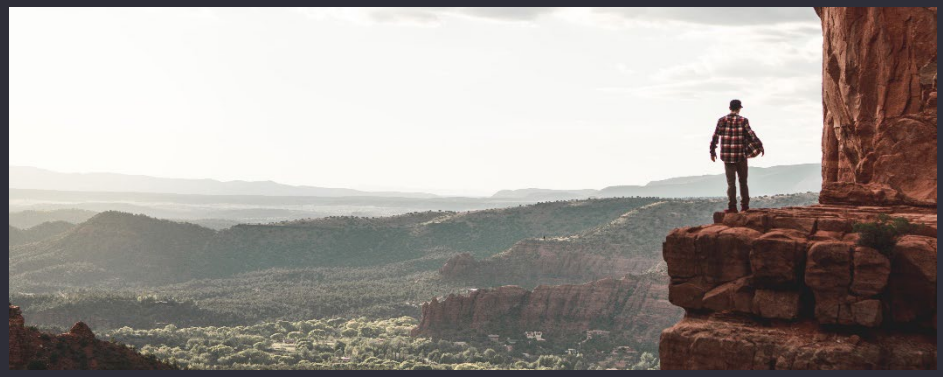
Integração entre Áreas

Tipo de Integração entre Áreas

Também foi analisada como a integração se concretiza na prática, considerando diferentes graus de profundidade:

- **Áreas integradas**, sugerindo uma coordenação mais limitada, sem suporte sistêmico.
- **Áreas e sistemas integrados**, indicando uma conexão operacional e tecnológica.
- **Áreas, sistemas e informações compartilhadas** para melhoria do monitoramento, refletindo um modelo mais avançado e colaborativo.

Entre as instituições que possuem algum nível de integração, 61% afirmaram contar com áreas, sistemas e informações compartilhadas para melhoria do monitoramento, caracterizando o modelo mais completo e colaborativo. Em seguida, 10% indicaram possuir áreas e sistemas integrados, com foco mais técnico e voltado à infraestrutura. Por fim, 29% relataram ter apenas áreas integradas, sem suporte sistêmico robusto, representando um estágio inicial de coordenação. Essa distribuição de respostas foi muito similar aos da pesquisa publicada em 2023.



Os resultados evidenciam uma tendência clara em direção a modelos mais completos, que combinam integração organizacional, tecnológica e informacional. O compartilhamento de dados surge como elemento central para fortalecer a capacidade de monitoramento e resposta a riscos interconectados. No entanto, a presença significativa de integrações limitadas (apenas áreas) indicam que ainda há desafios para consolidar uma governança verdadeiramente integrada e orientada por inteligência.

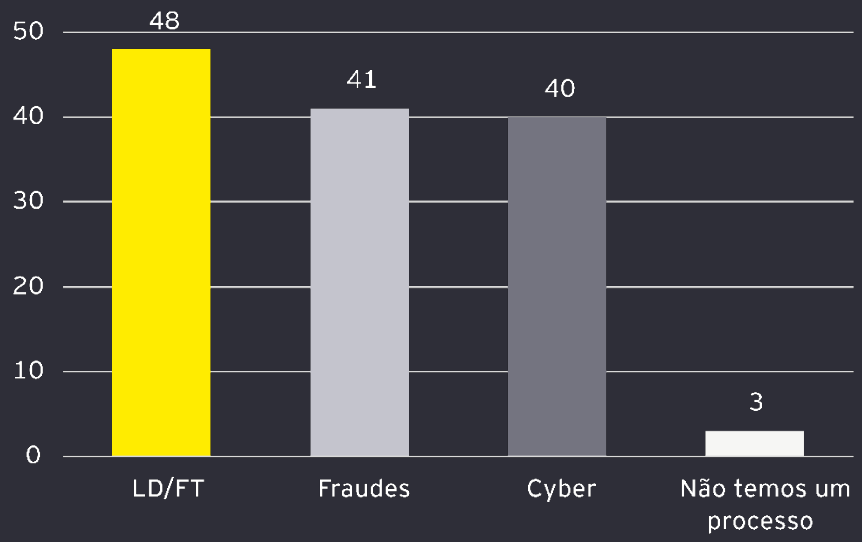
A análise permite avaliar a maturidade funcional da integração, revelando se ela está restrita à estrutura organizacional ou se já envolve tecnologia e compartilhamento de dados, elementos essenciais para uma atuação coordenada frente a riscos interconectados.

Integração entre Áreas

Gestão de riscos no desenvolvimento de novos produtos

Além da integração entre áreas críticas, foram analisados quais riscos são considerados pelas instituições no processo de desenvolvimento de novos produtos e serviços. Essa análise é relevante para avaliar o grau de maturidade na gestão preventiva e a capacidade de antecipar vulnerabilidades antes da entrada de novas ofertas no mercado. O gráfico a seguir apresenta a distribuição das respostas, destacando os riscos mais frequentemente incorporados a esse processo.

Riscos considerados no desenvolvimento de novos produtos e serviços



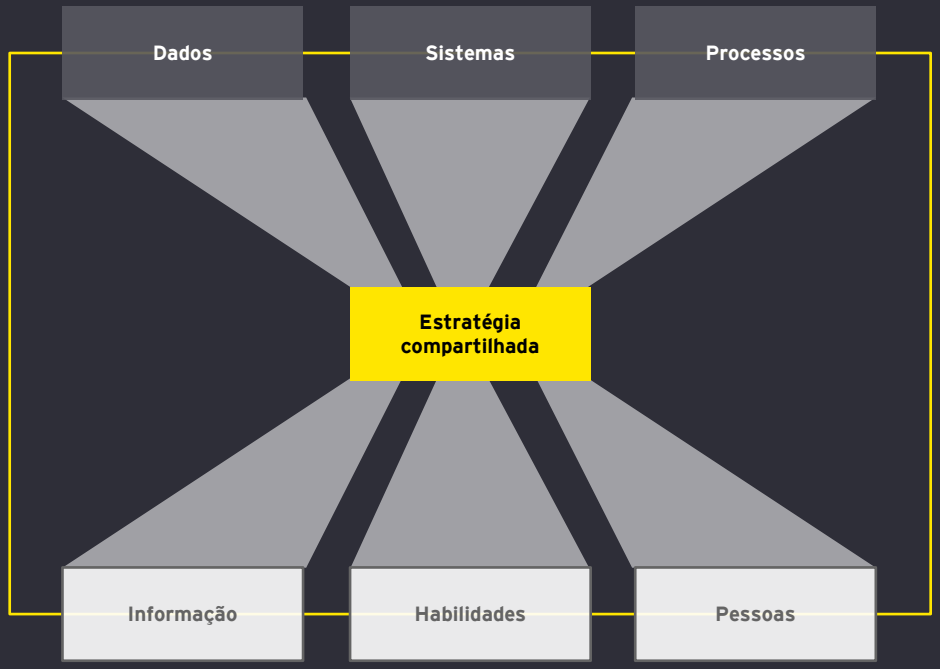
No processo de desenvolvimento de novos produtos e serviços, LD/FT é o risco mais considerado pelas instituições (48 menções), seguido por Fraudes (41) e *Cyber* (40), evidenciando uma abordagem cada vez mais multirriscos já na fase de concepção. A predominância de LD/FT é esperada, pois a avaliação desse risco é um requerimento regulatório. Apesar disso, chama atenção que 3 instituições declararam não possuir processo formal de avaliação, o que indica lacunas de governança e conformidade. Os resultados demonstram uma boa cobertura dos riscos críticos e apontam uma oportunidade relevante para evoluir rumo a um processo de avaliação que una PLD/FTP, Fraudes e *Cyber* de forma estruturada. Essa evolução para incluir novos riscos não deve representar um aprimoramento complexo, uma vez que a governança desse processo já está estabelecida e aplicada na maioria das instituições, e envolveria apenas a inclusão de áreas adicionais, novos requerimentos, análises e testes complementares.

Visão integrada - Fraude, PLD/FTP e Risco de Crédito

Como a EY vem apoiando as instituições?

A EY vê o **gerenciamento de crimes financeiros** como uma atividade de **equilíbrio contínuo**, que exige uma estratégia dinâmica.

A convergência bem sucedida para uma visão integrada requer que os seguintes componentes estejam no lugar...



Mentalidade: simplesmente compartilhar dados, tecnologia ou uma estrutura organizacional não é suficiente. A mentalidade e a cultura da organização devem ser convergentes com a estratégia definida.

Foco: a gestão executiva deve reconhecer os desafios existentes e fazer da mudança na abordagem da gestão de risco uma área de foco.

Paciência: qualquer transformação do modelo operacional leva tempo. É necessário ser paciente em processos de grande transformação.

Investimento: investimentos em pessoas, processos e tecnologia são necessários para permitir uma estratégia compartilhada eficaz.

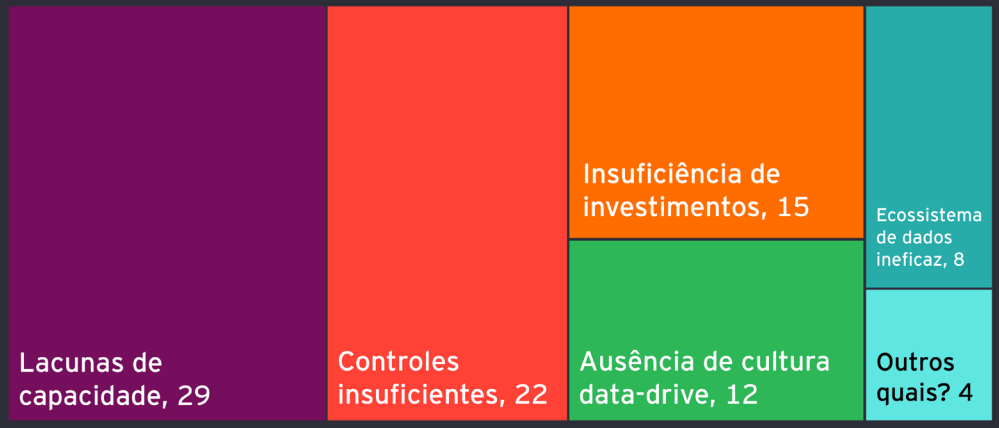
5 Governança e qualidade dos dados

EY
Shape the future with confidence

Governança e qualidade dos dados

Principais desafios para o devido tratamento de dados

As instituições também foram questionadas sobre os principais desafios para melhorar o tratamento de dados e a pesquisa revelou que o principal deles é a **Lacuna de capacidade**, relacionada principalmente à falta de profissionais qualificados. Em muitos casos, as equipes não dominam conceitos fundamentais de governança, análise avançada ou uso de ferramentas de Big Data e Inteligência Artificial (IA).



É importante destacar que um **ecossistema de dados eficaz** é a base para integração, consistência e escalabilidade, permitindo que informações fluam de forma segura e confiável. Por outro lado, **investimentos apropriados** são essenciais para modernização da infraestrutura, implementação de **controles compatíveis** e a adoção de soluções inovadoras, enquanto que uma **cultura data-driven** eficaz permite tomada de decisões mais assertivas.

Governança e qualidade dos dados

Uso de Inteligência Artificial (IA) nos processos de Prevenção a Crimes Financeiros

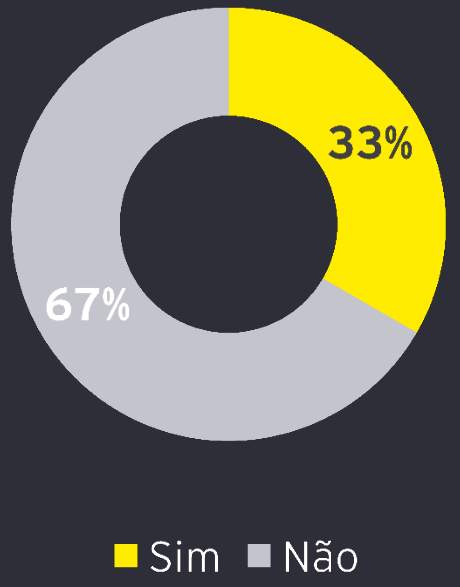
O uso de IA nos processos de Prevenção a Crimes Financeirostem se tornado cada vez mais estratégico para as instituições financeiras, porque **amplia a capacidade de detectar, analisar e agir** sobre operações e situações suspeitas de forma **muito mais rápida e precisa** comparada a métodos tradicionais.

Entretanto, nossa pesquisa revelou que modelos de IA disruptivos são utilizados **em apenas 33%** das instituições respondentes, sendo utilizados predominantemente em instituições S1.

Nossa pesquisa revelou ainda que:

- 14% da instituições já utilizam **Monitoramento de transações suspeitas baseados em aprendizagem de máquina**
- 11% utilizam **Aprendizado de máquina na classificação de risco / escore de risco**
- 9% utilizam **IA Generativa como assistente de análise de operações**
- Menos de 10% utilizam (i) **IA Generativa como assistente de análise de operações suspeitas**; (ii) **Redes Complexas e *Machine Learning* para identificação do caminho do dinheiro**; (iii) **IA Generativa como assistente das áreas de negócios com dúvidas de PLD/FTP** e (iv) **IA Generativa como agente de captura de mídias**

Quantidade de instituições que adota algum modelo de IA para prevenção a crimes financeiros



Em instituições S4 e S5, o desafio é ainda maior, nas quais a pesquisa revelou que mais de **76% delas ainda não utilizam nenhum modelo.**

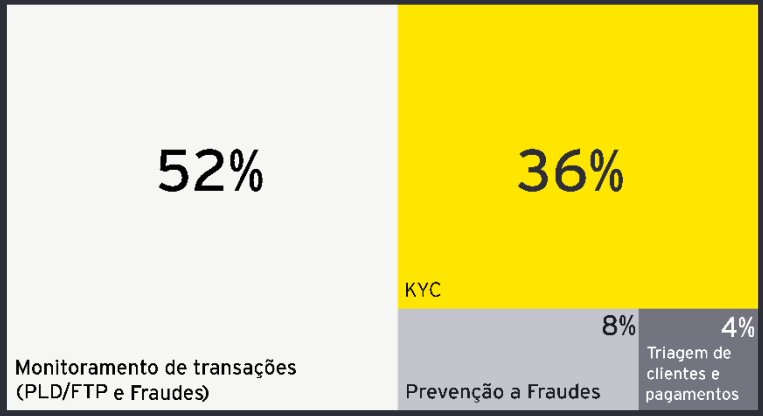
Governança e qualidade dos dados

Pilar mais impactado pela ausência da qualidade dos dados

Nossa pesquisa também revelou que não somente um, mas **dois pilares centrais**, são considerados pelas instituições respondentes como os mais **impactados negativamente pela ausência da qualidade dos dados, sendo:**

- **Monitoramento de transações:** no qual a qualidade dos dados é fundamental para detecção de operações e situações suspeitas de LD e fraude, além diminuição de falsos positivos; e
- **KYC:** no qual informações incompletas ou inconsistentes podem acarretar em falhas no processo de onboarding, dificultar a análise de risco e aumentar a exposição a crimes financeiros.

Pilares mais impactados



Governança e qualidade dos dados

Qualidade dos dados utilizados para Prevenção a Crimes Financeiros

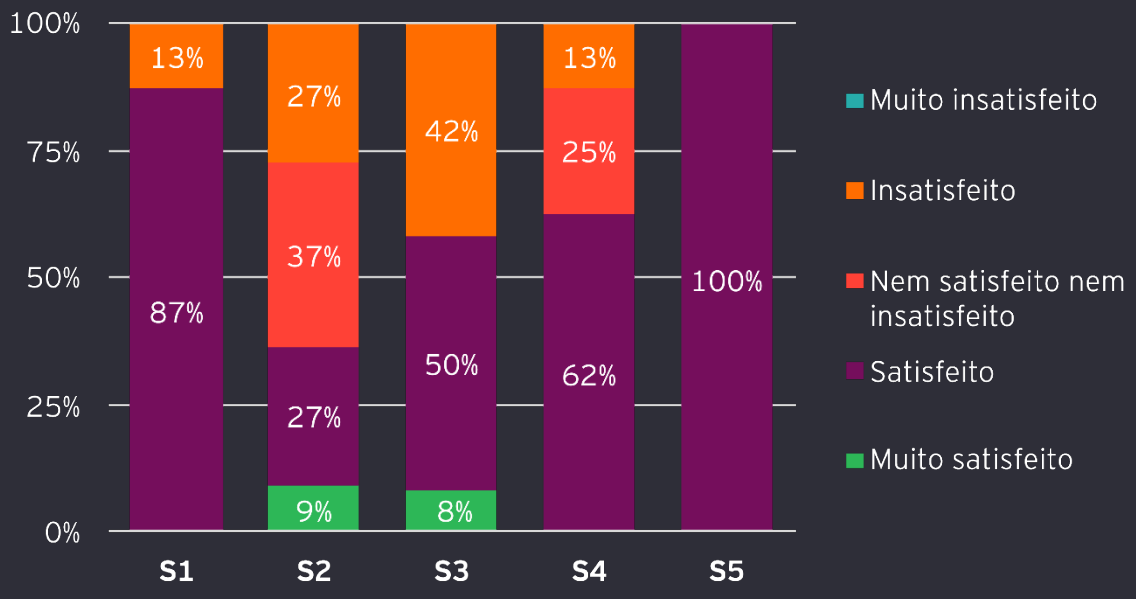
Em relação à qualidade dos dados utilizados na prevenção, as instituições se demonstraram **satisfeitas**, em sua maioria, de acordo com a pesquisa realizada.

Nesse contexto, é importante reforçar que a qualidade dos dados é fundamental, porque impacta diretamente a eficácia dos controles e a detecção de atividades suspeitas.

Dados incompletos, desatualizados ou inconsistentes dificultam a identificação correta de clientes (KYC), aumentam a ocorrência de falsos positivos e reduzem a capacidade de correlacionar informações para detectar padrões de risco.

Dados de alta qualidade permitem análises mais precisas, melhor monitoramento transacional e maior conformidade regulatória, fortalecendo a governança e reduzindo riscos de sanções e fraudes.

Nível de satisfação: qualidade dos dados, por segmento



Governança e qualidade dos dados

Integração e uso inteligente dos dados

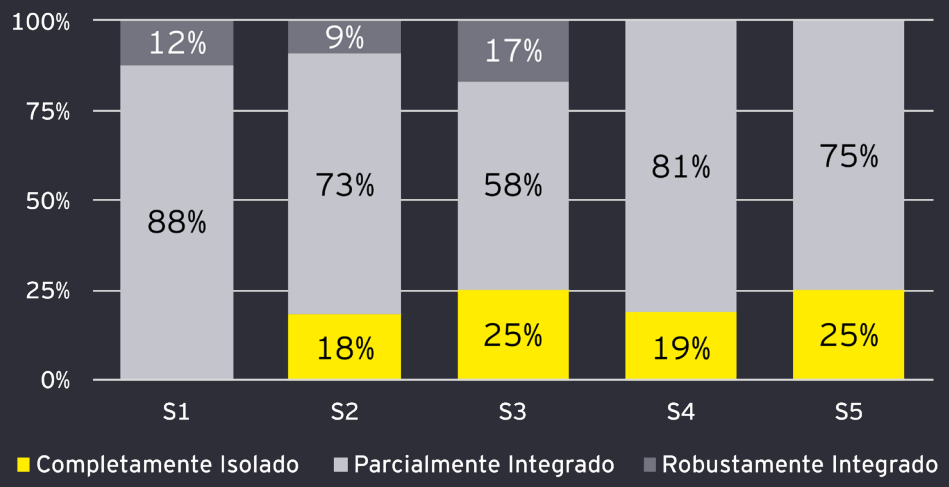
Por fim, os respondentes foram questionados sobre como os dados são usados para alimentar a estratégia de prevenção a crimes financeiros e gestão de clientes de forma integrada.

Quando os dados são tratados de forma centralizada e com qualidade, é possível:

- Identificar riscos com maior precisão;
- Reduzir inconsistências;
- Aprimorar a experiência do cliente;
- Atender às exigências regulatórias; e
- Potencializar análises preditivas.

Nossa pesquisa revelou que a maioria das instituições respondentes consideram que há uma **integração parcial** dos dados para a estratégia de prevenção e gestão de clientes.

Nível de integração dos dados, por segmento



Governança e qualidade dos dados

Iniciativas de dados de alta prioridade

Considerando a concentração dos respondentes em Bancos Comerciais, Seguradoras e IPs, os resultados demonstram que as iniciativas classificadas como de alta prioridade estão relacionadas à **Qualidade de dados**, **Controle e governança** e **Data science e analytics**, respectivamente.

Essas iniciativas **asseguram informações precisas, conformidade regulatória e reduzem riscos**. Ao mesmo tempo, prepara as instituições para temas emergentes, como uso ético de dados, big data e resiliência frente à transformação digital, assegurando vantagem competitiva e robustez nos programas de PLD/FTP.

Iniciativas de dados classificadas como de alta prioridade

Em contrapartida, **Estratégia de dados**, **Adoção de serviços de nuvem e migração** e **Democratização dos dados** apresentam espaço significativo para evolução. Essa síntese reforça a necessidade de fortalecer a abordagem estratégica para que as instituições avancem na maturidade de gestão de dados.

6 INR - Investidor não Residente

Shape the future with confidence

INR – Investidores Não-Residentes

Introdução a Investidores Não-Residentes

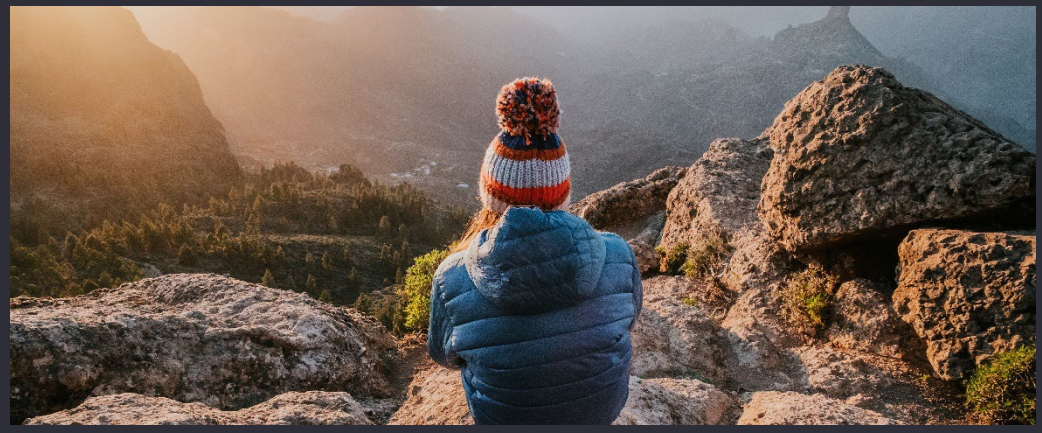
Esta seção trata dos investidores não residentes (INRs), com o objetivo de apresentar como as instituições financeiras brasileiras abordam esse perfil de cliente sob a ótica da PLD/FTP.

Os INRs são pessoas físicas ou jurídicas domiciliadas fora do Brasil que realizam investimentos nos mercados financeiro e de capitais nacionais. Por envolverem fluxos internacionais e estruturas jurídicas muitas vezes complexas, esses clientes demandam atenção especial por parte das instituições, sobretudo no que diz respeito à identificação e compreensão do perfil de risco.

O processo de identificação envolve a coleta e validação de informações relevantes, como dados cadastrais, estrutura societária, beneficiário final e jurisdição de origem. Essa etapa é essencial para que a instituição possa formar uma visão adequada sobre o cliente e sobre os riscos associados à relação comercial.

A avaliação de risco, nesse contexto, desempenha papel estratégico, permitindo que a instituição adote medidas proporcionais e compatíveis com o grau de exposição identificado. Mais do que seguir um modelo único, essa análise deve considerar as características específicas de cada cliente e operação, respeitando os princípios de proporcionalidade e efetividade.

Todo esse tratamento deve estar alinhado às exigências regulatórias estabelecidas pelos órgãos supervisores brasileiros – CVM e Banco Central do Brasil, baseando-se na Resolução Conjunta nº 13, de 3 de dezembro de 2024, e aos padrões internacionais definidos pelo GAFI.



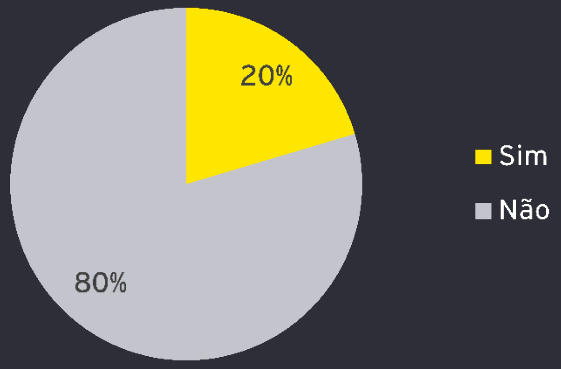
INR – Investidores Não-Residentes

Os dados coletados indicam que a presença de investidores não residentes (INRs) ainda é limitada entre as instituições financeiras brasileiras. Das instituições que participaram da pesquisa, **apenas 10 (cerca de 20%) declararam possuir esse tipo de cliente em sua base.**

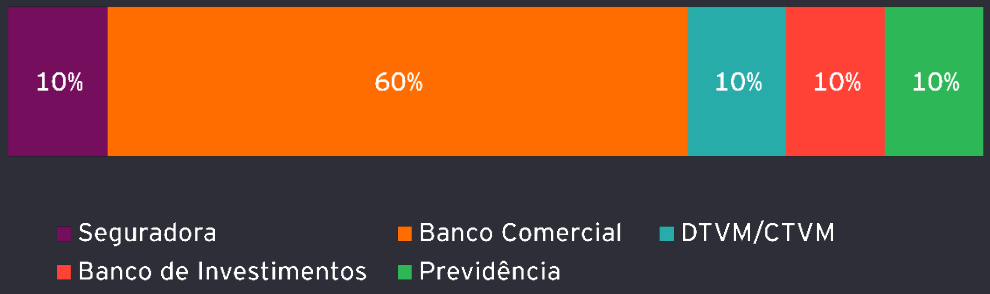
Entre essas 10 instituições, observa-se uma predominância dos bancos comerciais, que representam 60% do grupo. Esse dado sugere que, embora a atuação com INRs seja restrita, ela tende a se concentrar em instituições com maior capacidade operacional e estrutura voltada ao atendimento de clientes internacionais.

A distribuição observada destaca a importância de compreender os diferentes perfis institucionais no tratamento de clientes não residentes, especialmente em contextos que exigem maior robustez nos processos de identificação, monitoramento e gestão de riscos.

Respondentes com Investidores Não Residentes como Clientes



Setor das Instituições que possuem Investidores Não-Residentes



Entre as instituições que possuem investidores não residentes em sua base de clientes, 90% afirmaram considerar a Resolução Conjunta nº 13/2024, publicada pela CVM e pelo Banco Central, na adaptação de seus processos relacionados ao tratamento desse perfil. Essa norma estabelece diretrizes operacionais para o registro, representação e movimentação de recursos de não residentes no mercado financeiro e de capitais brasileiro.

Além disso, 70% das instituições indicaram que consideram os INRs como um perfil de risco específico em suas análises de PLD. Essa abordagem reforça a importância de se avaliar, de forma estruturada, os riscos associados à complexidade das operações, como a opacidade na estrutura de propriedade, o uso de veículos de investimento em jurisdições com baixa transparência e a dificuldade de acesso a informações confiáveis sobre o beneficiário final.

A identificação desses elementos permite que a instituição adote medidas proporcionais ao risco identificado, contribuindo para a efetividade dos mecanismos de prevenção e para a aderência às exigências regulatórias.

7 Relacionamento de IFs com operadores de aposta de quota fixa

EY
Shape the future with confidence

Aposta de quota fixa

Introdução às apostas de quota fixa

As apostas de quota fixa têm se consolidado como uma das modalidades mais populares no mercado brasileiro. Nesse formato, o valor do prêmio é conhecido no momento da aposta, definido com base nas probabilidades estabelecidas pela própria operadora. A simplicidade da mecânica e a presença crescente de plataformas digitais ajudaram a ampliar o alcance desse produto, tanto em eventos esportivos quanto em jogos virtuais.

As operações em plataformas de apostas de quota fixa costumam envolver valores baixos, alta frequência e canais digitais. Em muitos casos, observa-se a movimentação imediata dos recursos — com depósitos, apostas simbólicas e saques feitos em sequência. Esse tipo de comportamento dificulta a identificação de finalidade econômica legítima e pode indicar o uso do setor para dar aparência lícita a recursos de origem suspeita. A análise desses padrões é essencial para entender como o ambiente pode ser explorado para fins não compatíveis com sua proposta original.

A relação entre operadoras e instituições financeiras torna-se, nesse contexto, estratégica. Bancos, instituições de pagamento e outras entidades autorizadas pelo Banco Central são os principais intermediários dos fluxos financeiros entre apostadores e operadoras, mas sua atuação não se limita à execução de pagamentos. Compreender como esse mercado opera — e os riscos que ele representa — é um passo necessário para o setor financeiro. Esse entendimento permite calibrar estratégias de controle, adaptar processos e, principalmente, antecipar vulnerabilidades que podem comprometer a segurança das transações.

Resultados da pesquisa

A pesquisa contou com a participação de instituições financeiras que mantêm algum tipo de relacionamento com operadoras de loteria na modalidade de aposta de quota fixa. Dentre essas, quatro instituições possuem operadoras como clientes de conta bancária pessoa jurídica (PJ).

O número reduzido de participantes reflete uma tendência observada no mercado: **instituições financeiras tradicionais têm adotado uma postura cautelosa em relação a esse segmento**. Essa cautela está diretamente relacionada à percepção de risco, especialmente em um momento de estruturação e amadurecimento do setor, marcado pela implementação de novas regulamentações e exigências de conformidade.

Entre as instituições participantes, 17% afirmaram não ter procedimentos para verificar se as operadoras de apostas estão autorizadas pela SPA/MF (Secretaria de Prêmios e Apostas do Ministério da Fazenda), conforme exige a regulamentação. Em contrapartida, 67% dos respondentes indicaram possuir controles para bloquear transações com operadoras não autorizadas e o mesmo percentual afirma comunicar operações suspeitas ao COAF em até 24 horas, conforme regulamentação.

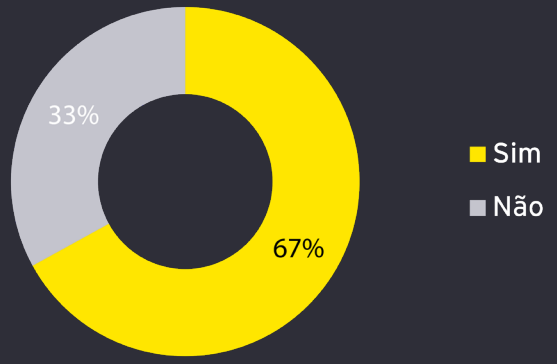
O desenvolvimento de regras de monitoramento para o segmento de apostas de quota fixa deve considerar a dinâmica operacional do setor, caracterizada por transações de baixo valor em volumes muito elevados. Nesses casos, a análise da capacidade financeira do apostador torna-se essencial para identificar operações atípicas. Ganha relevância, nesse contexto, a tipologia do "jogo mínimo", na qual os recursos são rapidamente sacados sem que haja atividade de jogo real — prática comum em esquemas de lavagem de dinheiro em cassinos físicos, agora adaptada ao ambiente digital. A proximidade com as operadoras é estratégica para que as instituições financeiras incorporem aprendizados práticos ao desenho das suas regras de monitoramento e prevenção.

As IFs têm um papel central, pois conseguem identificar padrões de comportamento que envolvem múltiplas plataformas de apostas — algo que as operadoras, isoladamente, não conseguem enxergar. Essa visão consolidada permite uma atuação mais eficaz na prevenção de abusos e movimentações atípicas.

Aposta de quota fixa

Tais fatos mostram que, embora a maioria das instituições esteja atenta à regularidade das operadoras com as quais se relaciona, nem todas possuem mecanismos para impedir que transações com empresas irregulares sejam concluídas. Essa diferença mostra que, para uma pequena parte das instituições, os controles internos ainda estão em processo de adaptação às exigências regulatórias do setor.

Instituições com monitoramento reforçado de PLD/FTP em relação às operadoras de apostas



67% das instituições participantes indicaram possuir procedimentos específicos de diligência e monitoramento reforçado de PLD/FTP voltados para operadoras de apostas de quota fixa. Esse resultado sugere que parte significativa do mercado já reconhece os riscos associados ao segmento e vem estruturando práticas voltadas à mitigação desses riscos.

Por outro lado, o fato de esse percentual não ser mais elevado pode estar relacionado ao processo de familiarização das instituições financeiras com o comportamento desse segmento, aos riscos a ele associados e à consequente dificuldade de desenvolver controles específicos.

8 eFX (*Electronic Foreign Exchange*)

EY
Shape the future with confidence

eFX (*Electronic Foreign Exchange*)

Introdução ao serviço eFX

O eFX é definido como o serviço de pagamento ou transferência internacional que viabiliza, por meio de operação de câmbio ou movimentação em conta em reais de não residente, nos termos da Resolução BCB nº 277/22:

- Aquisição de bens e serviços, no País ou no exterior, de forma presencial, ou mediante solução de pagamento digital;
- Transferência unilateral, limitada a US$10.000,00 (dez mil dólares dos Estados Unidos) ou o seu equivalente em outras moedas;

  Transferência de recursos entre contas no País e contas no exterior de mesma titularidade, limitada aUS$10.000,00 (dez mil dólares dos Estados Unidos) ou o seu equivalente em outras moedas, com características específicas determinadas na resolução;
- Saque no País ou no exterior.

O prestador de eFX atua como intermediário, coletando recursos em reais por meio de diversos meios de pagamento e, posteriormente, realizando a conversão cambial ou a transferência internacional, por meio de instituições autorizadas a operar no mercado de câmbio. Essas operações são registradas em lote, com *layouts* específicos (arquivo C220).

Transações realizadas digitalmente, com maior rapidez e eficiência

O serviço pode ser prestado por instituições financeiras e instituições de pagamento autorizadas pelo Banco Central, como bancos múltiplos, corretoras de câmbio, emissores de moeda eletrônica e credenciadores. Empresas que não possuem autorização direta para operar câmbio podem atuar como facilitadoras, desde que utilizem instituições autorizadas para a execução das operações.

Contudo, a instituição autorizada, no seu relacionamento com prestador de eFX não autorizado a funcionar pelo BCB, deve ser capaz de comprovar perante o BCB que se certificou de que esse prestador adota política, procedimentos e controles internos para cumprir os deveres e as obrigações previstos na resolução, exigindo, portanto, controles de gerenciamento e de mitigação de riscos reforçados para KYP (*Know Your Partner*).

Diante disso, destacam-se os seguintes aspectos que merecem atenção especial por parte das instituições financeiras:

- Prestador com práticas limitadas de KYC para cumprimento de leis e normas
- Prestador de fachada, sem estrutura e capacidade técnica e operacional
- A celebração da operação deve estar amparada no arquivo C220
- Vedada compensação em arquivo C220 (registro pelo valor líquido)
- Vedado fracionamento (C220)
- Defasagem temporal entre o negócio e o registro da operação
- Ausência de *screening* pré-fato
- Deficiência de procedimentos para certificar a legalidade das operações (inclui "boletagem")
- Ausência de diligências de KYP destinadas a averiguar alta incidência de CPFs "baixados" em arquivos C220, fracionamentos etc.

O serviço eFX representa uma inovação regulatória e tecnológica que moderniza o mercado de câmbio brasileiro, promovendo maior inclusão, agilidade e segurança nas transações internacionais.

eFX (*Electronic Foreign Exchange*)

Resultados da pesquisa

Contamos com a participação de 8 instituições que atuam com prestadores de eFX. Desses respondentes, **63%** são Bancos Comerciais, **25%**, Instituições de Câmbio, e **12%**, Instituições de Pagamento.

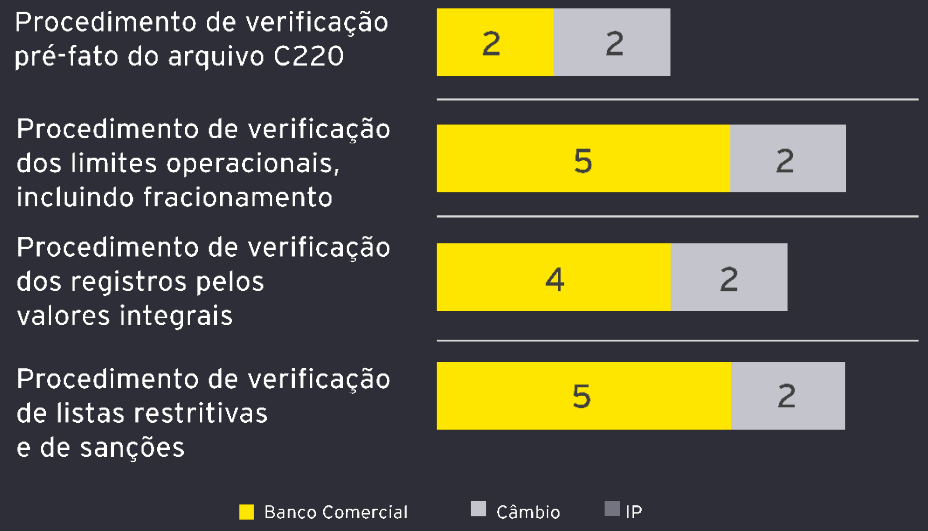
Dessas instituições, **7** informaram que possuem procedimentos para evitar que os usuários do serviço de eFX (como comerciantes, plataformas de *streaming* e *marketplaces*) realizem operações com **pessoas ou entidades com restrições ou sujeitas a sanções**.

Outros controles que chamaram atenção pela presença nas instituições respondentes foram a existência de procedimentos para **evitar que os limites operacionais sejam desrespeitados**, mitigando, inclusive, situações de fracionamento, e procedimentos para **mitigar situações de compensação envolvendo os pagamentos e os recebimentos**, presentes em **81%** dos respondentes.

No entanto, **procedimentos de verificação pré-fato do arquivo C220**, ou seja, anterior à efetivação das operações, estão presentes em apenas **25%** das instituições respondentes. Essas são deficiências recorrentemente identificadas em instituições financeiras, além da ausência da devida formalização dos critérios de verificação desse arquivo em manual interno.

No gráfico abaixo, apresentamos os resultados dos controles executados pelas instituições respondentes que atuam com prestadores eFX:

Controles implementados pelas instituições relacionados à eFX



Considerando os resultados obtidos, reforça-se a necessidade de fortalecer os procedimentos de KYP (*Know Your Partner*) e as verificações relacionadas às transações de eFX, garantindo maior aderência regulatória, mitigação de riscos e prevenção a crimes financeiros.

9 Ativos Virtuais

EY
Shape the future
with confidence

Ativos Virtuais

Introdução a Ativos Virtuais

A regulamentação de ativos digitais tem avançado globalmente, com diferentes jurisdições implementando medidas para mitigar riscos e promover maior transparência no setor. Entre os principais temas abordados pelos reguladores, estão regimes de licenciamento para prestadores de serviços, regras de PLD/FTP, diretrizes para intermediários e custodiantes, além de normas voltadas à cibersegurança. Outros pontos relevantes incluem a definição de regras tributárias, a aprovação de ETFs de criptomoedas, a tokenização de ativos e diretrizes para distribuição e *marketing*. Essas tendências foram identificadas no estudo da EY chamado "Global Wealth and Asset Management Regulatory Landscape", que analisou regulamentações recentes no setor de gestão de patrimônio e ativos em diferentes mercados do mundo.

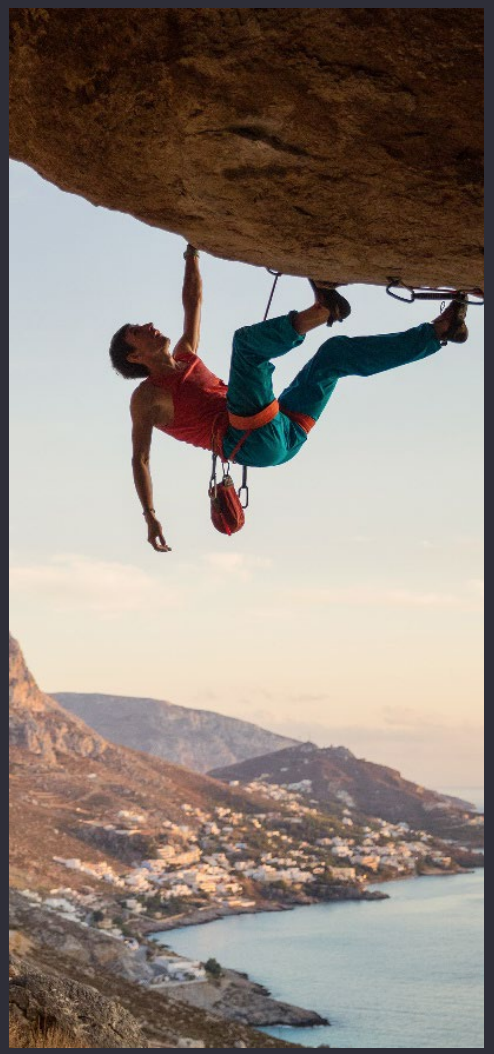
Esse panorama internacional evidencia a busca por um equilíbrio entre inovação e segurança, servindo como base para analisarmos a maturidade das instituições do Brasil.

Os ativos virtuais no Brasil são definidos pelo Marco Legal dos Ativos Virtuais (Lei nº 14.478/2022) como representações digitais de valor que podem ser negociadas ou transferidas por meios eletrônicos e utilizadas para pagamentos ou como forma de investimento.

Entre os exemplos mais conhecidos, estão as criptomoedas e os *tokens*, que vêm transformando a forma como transações financeiras e investimentos são realizados globalmente.

Nesse ecossistema, surgem os VASPs (*Virtual Asset Service Providers*) ou Prestadores de Serviços de Ativos Virtuais, que são entidades responsáveis por atividades como intermediação, custódia, câmbio, transferência e negociação de ativos digitais. Essas empresas desempenham um papel central na economia digital, garantindo a infraestrutura necessária para que ativos virtuais circulem de forma segura e regulamentada.

Com a promulgação da Lei nº 14.478/2022 e o Decreto nº 11.563/2023, o Banco Central do Brasil (BCB) foi designado como autoridade responsável por autorizar e supervisionar os VASPs. A regulamentação busca proteger investidores, aumentar a transparência e mitigar riscos de fraudes e crimes financeiros. Entre as exigências, destaca-se que nenhum VASP poderá operar sem autorização do BCB, e as regras incluem requisitos prudenciais, prestação de informações, governança, controles internos robustos, inclusive controles de PLD/FTP alinhados com os padrões internacionais.



Ativos Virtuais

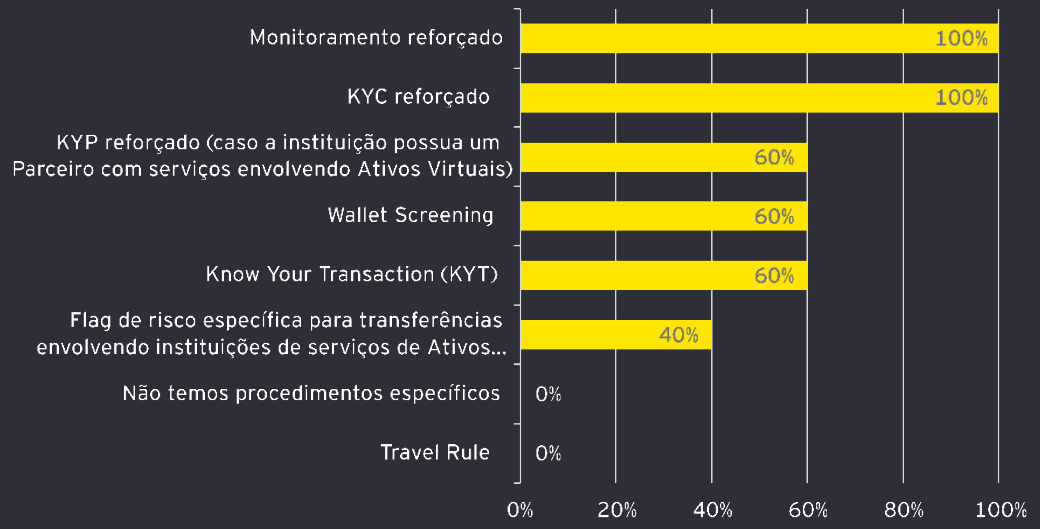
Resultados da pesquisa

A pesquisa contou com a participação de 5 instituições que já realizam operações envolvendo ativos virtuais no Brasil e 2 instituições que pretendem ingressar nesse setor no curto prazo. Entre os serviços envolvendo ativos virtuais realizados pelas instituições respondentes, há uma ampla gama, incluindo: Custódia de Ativos Virtuais (2 instituições), Portfólio de Investimentos (1 instituição), Conversão de Ativos Virtuais para Moedas Fiduciárias (1 instituição) e Pagamentos (1 instituição).

Controles

Para avaliar como as instituições estão mitigando riscos relacionados a ativos virtuais, avaliamos quais controles de PLD/FTP já foram implementados. O gráfico a seguir apresenta a distribuição desses controles entre os participantes.

Relação de procedimento específico de PLD/FTP relacionado a ativos virtuais implementados pelas instituições



Ativos Virtuais

Monitoramento reforçado e KYC reforçado foram os principais procedimentos implementados por essas instituições (que realizam ou pretendem realizar operações com ativos virtuais), a fim de identificar transações e situações suspeitas e reduzir o risco de serem utilizadas por criminosos.

Outros controles implementados incluem *Know Your Transaction* (KYT) e *Wallet Screening*. O KYT é composto por um conjunto de práticas e ferramentas para monitorar transações no ambiente cripto, analisando padrões, origem/destino e comportamento para identificar riscos de PLD-FTP em tempo real. *Wallet Screening* é um componente do KYT e consiste em verificar endereços de carteiras contra listas de sanções, listas negras e indicadores de risco (por exemplo, carteiras associadas a *ransomware*, *darknet*, *mixers*, entre outros).

Flag de risco para transferências a instituições de serviços de ativos virtuais também foi implementada por algumas instituições. Esse controle consiste em configurar alertas específicos para identificar quando clientes realizam transferências de recursos para instituições que operam ativos virtuais, como *exchanges* de criptomoedas.

Essa *flag* permite que a instituição identifique e realize análises manuais sobre a legitimidade da operação.

Também foi identificado um investimento significativo por parte das instituições no processo de *Know Your Partner* (KYP) reforçado. Esse processo é aplicável quando a instituição possui um parceiro que oferece serviços relacionados a ativos virtuais. Com o advento do mercado de BaaS/*Cripto as a Service*, esse processo de KYP é fundamental para que a instituição avalie se o parceiro que utilizará sua estrutura possui processos e controles adequados, evitando aumento da exposição ao risco.

Nenhuma instituição indicou possuir procedimentos relacionados à *Travel Rule*. A *Travel Rule* é uma exigência estabelecida pelo GAFI (Grupo de Ação Financeira) que determina que provedores de serviços de ativos virtuais e instituições financeiras compartilhem informações sobre o remetente e o destinatário em transferências de criptoativos acima de USD 1.000. Essa regra é fundamental para aumentar a transparência e a rastreabilidade das transações.

No Brasil, a Lei nº 14.478/2022, as consultas públicas realizadas pelo BCB e as normas que serão implementadas pelo regulador estão construindo a base para o futuro cumprimento dessa exigência.

Para saber mais sobre a *Travel Rule*, consulte o documento "Best Practices – Travel Rule Supervision", emitido pelo GAFI em junho de 2025 (LINK).

Dos respondentes, nenhuma instituição indicou **não** possuir procedimentos reforçados de PLD/FTP relacionados a ativos virtuais. Esse resultado demonstra a preocupação das instituições com esse tipo de ativo, uma vez que a grande maioria implementou controles específicos para mitigar os riscos elevados associados a ele decorrentes de sua maior atratividade para criminosos, tanto na movimentação de recursos ilícitos quanto no processo de lavagem.

Ativos Virtuais

O que vem pela frente

Com o aprimoramento do arcabouço regulatório brasileiro de ativos virtuais, é possível observar um comportamento semelhante ao observado nos Estados Unidos. Uma pesquisa realizada pela EY-Parthenon em parceria com a Coinbase, publicada em março de 2025, revela um forte entusiasmo dos investidores por ativos digitais, com 83% planejando aumentar suas alocações ainda neste ano. Esse otimismo é impulsionado principalmente pela expectativa de maior clareza regulatória, que deve fomentar o crescimento e estimular a inovação em produtos como DeFi, *stablecoins* e ativos *tokenizados*.

A eleição presidencial dos EUA em 2024 é apontada como um catalisador decisivo para a consolidação dos ativos digitais no sistema financeiro global, marcando uma virada após anos de ceticismo e regulamentações restritivas.

Para acessar o relatório completo da pesquisa – 2025 ***Institutional Investor Digital Assets Survey*** –, clique no LINK.

O processo regulatório no Brasil está sendo implementado em fases, com consultas públicas já realizadas para consolidar normas sobre autorização, governança, *stablecoins*, integração com o mercado de câmbio e regras prudenciais. A expectativa é que, até o final de 2025, o arcabouço regulatório esteja completo, alinhando o Brasil às melhores práticas internacionais e fortalecendo a prevenção à lavagem de dinheiro e ao financiamento do terrorismo no ecossistema de ativos virtuais.

As instituições que operam com ativos virtuais (e as que desejam entrar nesse segmento) devem se antecipar à publicação das novas regulamentações, tomando como base os requerimentos de PLD/FTP já previstos na legislação brasileira e normas existentes, como a Circular nº 3.978 do BCB, para desenvolver seus processos e controles. Essa abordagem proativa reduz riscos regulatórios e fortalece a governança, garantindo maior aderência às melhores práticas do mercado e preparando a instituição para o que está por vir.


10
Trust
EY
Shape the future
with confidence

Visão sobre *Trusts*

Introdução sobre *Trusts*

Trusts são estruturas jurídicas versáteis que oferecem a indivíduos e famílias uma ampla gama de opções para gerenciar seus ativos, proteger seu patrimônio e alcançar objetivos específicos.

No Brasil, não é possível abrir um *trust* típico como em outros países, porque ele não é regulamentado pelo Código Civil ou por outra legislação específica. O Brasil utiliza contratos e estruturas societárias para funções semelhantes, como *holdings* familiares, fundos patrimoniais e testamentos com cláusulas específicas.

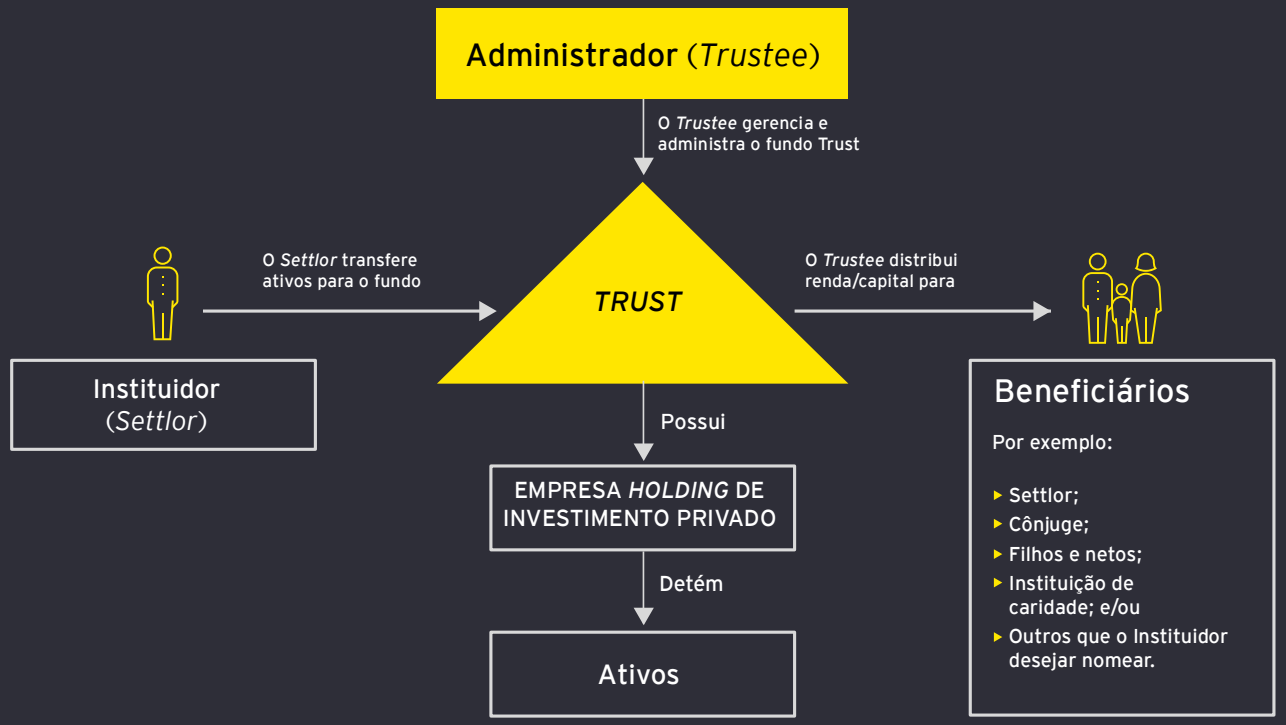
É frequente que *trusts* sejam administrados por entidades ligadas à gestão de patrimônio, como bancos privados e gestoras de investimentos. Nesses casos, uma instituição financeira pode ter um *trust* localizado no exterior, como cliente de uma de suas filiais. Outra opção é o cliente pessoa física, com o qual a instituição financeira possui relacionamento no Brasil, ser uma das partes de um *trust* e, consequentemente, devendo ser considerado no KYC e outros processos de PLD/FTP.

Visão sobre *Trusts*

Os principais componentes de um *trust*:
Ao realizar processos de KYC envolvendo *trusts*, é fundamental considerar a identificação de seus principais componentes:

1. Instituidor (*Settlor*): a pessoa física que cria o *trust* e transfere seus bens para ele. O instituidor define os termos e objetivos do *trust*.
2. Administrador (*Trustee*): a pessoa física ou jurídica responsável por administrar e proteger os bens do *trust*. O *trustee* tem o dever fiduciário de agir no melhor interesse dos beneficiários e seguir as instruções estabelecidas no documento do *trust*.
3. Beneficiário (*Beneficiary*): a pessoa ou organização que se beneficia dos bens mantidos no *trust*. Os beneficiários podem receber a renda gerada pelos ativos do *trust* ou ter acesso aos próprios bens, conforme os termos do *trust*.
4. Patrimônio do *Trust* (*Trust Property*): os bens ou ativos transferidos pelo instituidor para o *trust*. Isso pode incluir dinheiro, imóveis, investimentos, empresas ou outros ativos de valor.

Para identificação da estrutura e das partes envolvidas, assim como instituição e o funcionamento do *trust*, a escritura do *trust* (também chamada de *trust deed* ou *declaration of trust*) é o principal documento a ser utilizado pelas instituições financeiras.



Visão sobre *Trusts*

Resultado da pesquisa e maturidade dos controles

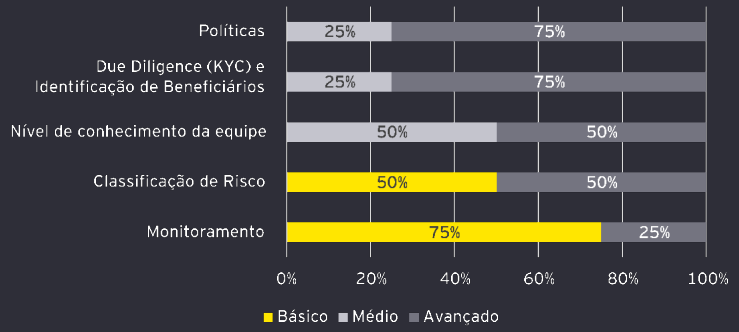
Dos respondentes da pesquisa, uma pequena quantidade de instituições se relacionam com *trusts* como clientes. Dos respondentes, 4 instituições reportaram ter *trust* como cliente final, sendo dois Bancos Comerciais, um Banco de Investimentos e uma Seguradora.

No entanto, com base em nossa experiência prévia, é possível que esse número esteja subestimado. Em interações anteriores, identificamos casos em que empresas inicialmente responderam negativamente a essa pergunta, mas posteriormente verificou-se que, de fato, possuíam clientes com essa estrutura (seja o próprio *trust* localizado fora do Brasil ou o cliente pessoa física como tendo alguma responsabilidade dentro de um *trust* e este fazendo parte de sua riqueza). Isso ocorre, possivelmente, por não reconhecerem o termo ou por esse tipo de cliente representar uma porcentagem muito pequena da base de clientes da instituição.

No que se refere à maturidade das instituições participantes, especialmente quanto aos controles implementados para *trusts*, a pesquisa analisou diferentes mecanismos de controle. A seguir, apresentamos a distribuição das instituições por nível de maturidade identificado em cada controle avaliado.

Visão sobre *Trusts*

Maturidade por controle



A análise da maturidade dos controles relacionados a *trusts* revela um cenário heterogêneo. Políticas aparecem como um dos pontos mais consolidados, com três das quatro instituições no nível Avançado de maturidade, ou seja, com documentos formalizando as particularidades, procedimentos e riscos associados especificamente a estruturas de *trust*. *Due Diligence* (KYC e Identificação de Beneficiários) apresenta padrão semelhante, também com predominância no nível Avançado. Nesse estágio, as práticas incluem identificação e qualificação dos beneficiários finais e de todas as partes envolvidas (incluindo classificação de PEP), verificação da origem de fundos e riqueza, definição do propósito do *trust* e coleta de documentação comprobatória (como instrumentos de constituição e estrutura legal).

Em relação ao nível de treinamento e conhecimento da equipe sobre as especificidades de *trusts*, os resultados se dividem entre Médio e Avançado. Um nível avançado pressupõe treinamentos regulares, abrangentes e com avaliação de conhecimento sobre estruturas complexas.

Em contrapartida, monitoramento surge como o maior desafio: três instituições ainda se encontram no nível Básico, enquanto apenas uma alcançou o estágio Avançado. O nível básico é caracterizado pela ausência de regras específicas para considerar essas estruturas, como limites e alertas para movimentações atípicas.

A classificação de risco apresenta maturidade polarizada, com metade das instituições em Básico e metade em Avançado. Um nível avançado significa considerar fatores como a jurisdição onde a estrutura está localizada e a complexidade do *trust* na definição do risco.

Vale destacar que a amostra é reduzida (N=4), o que limita generalizações, mas indica tendências relevantes. Esses resultados sugerem avanços significativos em políticas e processos de identificação, ao mesmo tempo em que reforçam a necessidade de fortalecer práticas de monitoramento e padronizar metodologias de classificação de risco para aumentar o nível de controle sobre estruturas complexas.

Visão EY

Pelo *trust* ser uma estrutura legal que possibilita que os ativos sejam geridos por um terceiro em favor de um ou mais beneficiários, essa e outras estruturas complexas podem ser consideradas como de maior risco pelas instituições e, consequentemente, demandar procedimentos específicos de controle no *onboarding*, identificação de beneficiários e monitoramento. Esse controle reforçado não é exclusivo de *trusts*, mas também deve ser realizado para estruturas como *holdings* familiares, fundos patrimoniais e testamentos com cláusulas específicas.


11
BaaS (*Banking as a Service*)
EY
Shape the future with confidence

Visão sobre *Banking as a Service*

Introdução sobre *Banking as a Service* (Baas)

Banking as a Service é um modelo no qual instituições financeiras (prestadoras do serviço) disponibilizam sua infraestrutura, licenças e serviços bancários para que empresas terceiras (tomadores de serviços), como *fintechs* ou plataformas digitais, possam oferecer produtos financeiros sob sua própria marca.

Na prática, a instituição fornece a base regulatória e operacional, enquanto o parceiro tomador de serviços cuida da experiência do cliente e da distribuição. Esse modelo tem ganhado força por permitir inovação e expansão de serviços financeiros de forma ágil, mas também traz desafios relevantes de governança e gestão de riscos. De acordo com a pesquisa, os respondentes avaliam a demanda do mercado por serviços de BaaS entre alta e moderada.

A principal diferença em uma relação BaaS é que a interação com o cliente e a entrega do serviço, que normalmente são realizadas pela linha de negócio da instituição financeira (a chamada "primeira linha de defesa"), passam a ser executadas por parceiros externos que não estão diretamente sob a supervisão da instituição financeira, exigindo controles adicionais para garantir conformidade e mitigação de riscos.

O Banco Central do Brasil lançou, em outubro de 2024, a Consulta Pública nº 108/2024, com o objetivo de estabelecer regras específicas para o modelo *Banking as a Service*. A proposta busca garantir maior transparência, segurança e governança nas parcerias entre instituições financeiras e empresas parceiras, definindo responsabilidades claras para cada parte. Entre as diretrizes apresentadas estão a definição dos papéis de prestadores e tomadores de serviços, regras para contratação, direito de auditoria e exigência de controles internos robustos.

Visão sobre BaaS

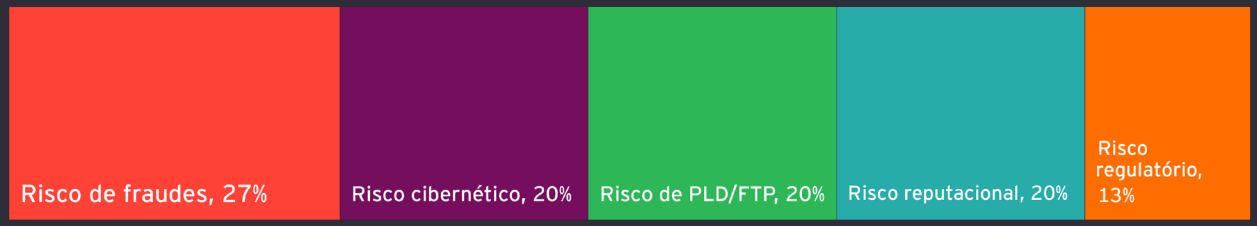
Resultado da pesquisa e maturidade dos controles

Entre as instituições respondentes da pesquisa, contamos com a participação de instituições que já prestam serviços de *Banking as a Service* e instituições que pretendem oferecer esse serviço no curto prazo. Os serviços oferecidos pelas instituições respondentes da pesquisa são: Pagamentos (4 instituições), PIX (4), Boletos (3), Cartão de crédito (3) e Cartão pré-pago (2).

Embora o modelo BaaS não crie riscos totalmente novos para a instituição prestadora de serviços – exceto aqueles relacionados aos novos produtos e serviços oferecidos por meio dessas parcerias –, ele amplia a exposição aos riscos tradicionais que toda instituição já precisa gerenciar, como *compliance*, riscos financeiros, riscos de terceiros e riscos reputacionais.

Isso fica claro quando analisamos as respostas dos participantes da pesquisa em relação aos riscos mais relevantes ampliados ao iniciar a oferta de *Banking as a Service*:

Riscos mais relevantes ampliados ao iniciar a oferta de BaaS



Quanto aos principais desafios enfrentados (ou esperados) na implementação de serviços BaaS, a gestão de riscos do parceiro foi unanimidade, sendo apontada por todas as instituições. Outros desafios citados foram: segurança de dados (3 instituições), conformidade regulatória (2) e integração de sistemas (1).

Esse último dado demonstra que a integração tecnológica deixou de ser um grande obstáculo para as instituições financeiras, tornando-se um processo mais consolidado e menos crítico em termos de risco.

Visão sobre BaaS

Esses desafios identificados pelas instituições respondentes podem ser enfrentados de forma eficaz. Alguns provedores de BaaS bem-sucedidos desenvolveram uma linha de negócios específica responsável por BaaS. Devido ao perfil de risco do BaaS, este exige uma gestão e governança dedicadas à linha de negócios, nas quais a responsabilidade pelo gerenciamento esteja incorporada. Dessa forma, cria-se uma nova linha de defesa, mais próxima das operações diárias do parceiro BaaS, fornecendo supervisão direta das suas atividades.

Das instituições respondentes, três indicaram já ter realizado ou planejam realizar alterações na estrutura corporativa, como a criação de equipes ou departamentos específicos para gestão de BaaS.

Antes de firmar uma parceria de BaaS, o prestador do serviço deve realizar uma *due diligence* para avaliar se o parceiro está alinhado aos padrões internos e às políticas da instituição (além, é claro, de requerimentos regulatórios). No caso de divergências entre as instituições, as políticas, procedimentos e padrões definidos pela prestadora do serviço devem ser compartilhados e seguidos pelo parceiro.

Também é essencial realizar auditorias e testes periódicos nas operações dos parceiros BaaS. Esses processos foram indicados como sendo realizados por todas as instituições respondentes que já operam BaaS.

Visão sobre BaaS

Adicionalmente, o contrato entre as partes deve definir claramente: o fluxo de dados e informações entre as partes; o direito do banco de auditar o parceiro BaaS; as responsabilidades e papéis de gestão de riscos e operações de cada parte; os acordos de nível de serviço (SLAs), prazos e as consequências caso o parceiro BaaS não cumpra as entregas ou as obrigações regulatórias do banco.

As instituições financeiras também devem monitorar indicadores-chave de risco e desempenho para identificar problemas emergentes, como reclamações de clientes recebidas pelo parceiro. Outro ponto importante é o aprimoramento do sistema de monitoramento de transações para considerar riscos de operações BaaS, implementado por todas as instituições respondentes que já operam nesse modelo.

Medidas adicionais implementadas pelas instituições participantes incluem capacitação da equipe (3 instituições) e implementação de tecnologias de segurança (3 instituições).

Para saber mais sobre a gestão de riscos de *Banking as a Service* e o programa regulatório do banco central dos Estados Unidos (Federal Reserve System), consulte o relatório da EY "***What banks need to know about the Fed's new Banking as a Service supervisory program***" (LINK).

O caminho a percorrer

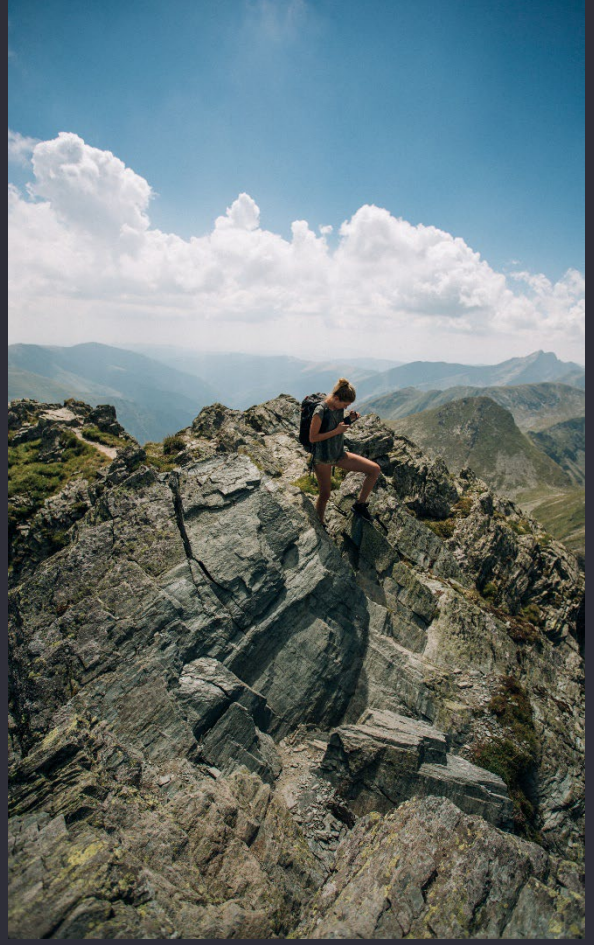
Shape the future
with confidence

Dados confiáveis e precisos são fundamentais para o sucesso do programa de Prevenção a Crimes Financeiros. Atualmente, as instituições de serviços financeiros enfrentam diversos desafios, como volume de dados cada vez maiores, sistemas legados, falta de controles sofisticados e baixos níveis de liderança.

Há quatro aspectos-chave para o sucesso do programa:

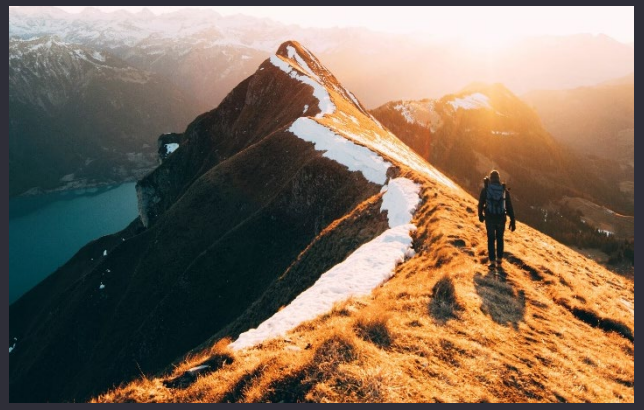
Para Capacidade e Criação de Valor: Um líder visionário promoverá a inovação e melhorará continuamente os recursos de gerenciamento de informações, por meio de análises para aumentar o compartilhamento, colaboração, compliance e segurança. A habilitação de tecnologias, como inteligência artificial, ajudará a lidar com o grande volume e variedade de conteúdos gerados por uma infinidade de soluções tecnológicas, aprimorando ainda mais os mecanismos de gestão. Há oportunidades também para redução do custo operacional, mas, mais significativamente, possibilidades de identificar formas baseadas em inteligência e evidências para combater o crime financeiro.

Para Base de Dados Sólida: fundamental a atribuição de um líder de dados, responsável por dados globais em toda instituição. A visão centralizada do cliente é um passo vital para garantir o bom funcionamento e escopo do programa de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo, independente do tamanho da organização. O líder de dados garantirá que os dados sejam vistos como centrais em toda a instituição e que estejam alinhados aos objetivos do negócio.



Para ecossistema e iniciativa: Atualmente, os ecossistemas de prevenção a crimes financeiros precisam responder às inovações tecnológicas e mudanças regulatórias que ocorrem frequentemente. Com isso, muitas vezes são consideradas parcerias de dados e provedores de dados externos. Neste cenário, hubs de serviços compartilhados, FinTechs e RegTechs também desempenharão um papel importante e as instituições precisarão abraçar essa disrupção para ganhar valor e melhorar a Prevenção a Crimes Financeiros.

Para Monitoramento Contínuo: O setor apresenta um alto nível de dinamismo por natureza. Este aspecto vem tomando maior importância nos últimos anos devido à rápida evolução do setor, novos canais, produtos e o volume transacional em si. Assim, as questões relacionadas à disponibilidade e qualidade de dados se tornam ainda mais importantes. Uma vez que os controles para detecção e prevenção são desenvolvidos e implementados, consideramos extremamente importante a definição de uma estratégia de monitoramento contínuo para garantir que os resultados esperados continuem a ser alcançados ou mesmo detectar a tempo possíveis falhas do processo (de dados ou sistêmico), além de possível identificação de tendências. Aspectos como estes devem servir como gatilhos para análise de impacto e possível tomada de ação para mitigação, remediação ou solução de problemas identificados.



Contatos

Natalia Grigolin
Sócia de Prevenção a Crimes Financeiros da EY Brasil

natalia.grigolin@br.ey.com

Roberto Millan de Almeida Falcão
Gerente Sênior em Prevenção a Crimes Financeiros da EY Brasil

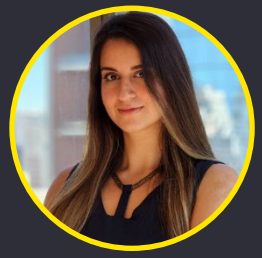
roberto.falcao@br.ey.com

Antônio Minhoto
Gerente de Projetos em Prevenção a Crimes Financeiros da EY Brasil

antonio.minhoto@br.ey.com

Junio Souza
Gerente de Projetos em Prevenção a Crimes Financeiros da EY Brasil

junio.souza@br.ey.com



Isabella Sorato Mendonça
Consultora Sênior em Prevenção a Crimes Financeiros da EY Brasil

isabella.mendonca @br.ey.com

EY | Building a better working world

Sobre a EY

A EY existe para construir um mundo de negócios melhor, ajudando a criar valor em longo prazo para seus clientes, pessoas e sociedade e gerando confiança nos mercados de capitais.

Utilizando dados, inteligência artificial e tecnologia como viabilizadores, equipes diversas da EY ajudam clientes a moldar o futuro com confiança e a solucionar as questões mais complexas do mundo atual.

As equipes da EY atuam em todo espectro de serviços em *assurance*, *consulting*, *tax* e *strategy and transactions*. Impulsionadas pela visão dos setores da indústria, parceiros de diversos ecossistemas e uma rede multidisciplinar e globalmente conectada, as equipes da EY podem fornecer serviços em mais de 150 países.

Todos juntos para moldar o futuro com confiança.

ey.com.br

Facebook | EYBrasil
Instagram | eybrasil
Linkedin | EY
Youtube | EYBrasil