# Compliance Data Driven – Investigações Inteligentes com um Background Check e Due Diligence Digital

**Sumário**


**Módulo 1: Introdução**

- **Capítulo 1:** Introdução

**Módulo 2: Conceitos Fundamentais**

- **Capítulo 1:** O que é Background Check
- **Capítulo 2:** O que é Due Diligence?

**Módulo 3: Objetivos do Due Diligence**

- **Capítulo 1:** Como fazer uma boa Due Diligence?
- **Capítulo 2:** Quais são as boas práticas de uma boa Due Diligence?

**Módulo 4: Do Presencial ao Digital**

- **Capítulo 1:** O eKYC (Electronic Know Your Customer) e o eKYB (Electronic Know Your Business)
- **Capítulo 2:** A Lei Geral de Proteção de Dados – Princípios e exceções para coleta de dados

**Módulo 5: Metodologia aplicada**

- **Capítulo 1:** O ciclo PDCA

**Módulo 6: Tipos de Due Diligence**

- **Capítulo 1:** Customer Due Diligence (CDD)

- **Capítulo 2:** Due Diligence de Fornecedores, Prestadores de Serviço e Parceiros
- **Capítulo 3:** Due Diligence Operacional
- **Capítulo 4:** Due Diligence Jurídico
- **Capítulo 5:** Due Diligence Financeira
- **Capítulo 6:** Due Diligence Reputacional
- **Capítulo 7:** Due Diligence Tecnológica
- **Capítulo 8:** ESG Due Diligence
- **Capítulo 9:** Enhanced Due Diligence (EDD)

**Módulo 7: Análises que compõem uma boa Enhanced Due Diligence**

- **Capítulo 1:** Beneficiário final (UBO) e Estruturas Societárias
- **Capítulo 2:** Listas Restritivas Internacionais
- **Capítulo 3:** Lista de Sanções do Conselho de Segurança da ONU (CSNU)
- **Capítulo 4:** Lista de Sanções da União Europeia (UE)
- **Capítulo 5:** Lista da OFAC (EUA)
- **Capítulo 6:** Lista de Entidades Bloqueadas da OFAC
- **Capítulo 7:** Lista da Interpol
- **Capítulo 8:** Lista de Procurados pelo FBI
- **Capítulo 9:** Lista de HMT (Reino Unido)
- **Capítulo 10:** Lista de PEPs
- **Capítulo 11:** Mídia adversa e reputação
- **Capítulo 12:** OSINT – Open Source Intelligence

**Módulo 8: Gestão de Riscos em Due Diligence e Compliance**

- **Capítulo 1:** Risco cibernético de terceiros (Third Party Risk Management - TPRM) na due diligence
- **Capítulo 2:** Avaliação de Riscos e Red Flags
- **Capítulo 3:** Governança e abordagem baseada em risco

**Módulo 9: Etapas práticas da Due Diligence**

- **Capítulo 1:** Planejamento e Definição de Escopo
- **Capítulo 2:** Coleta de Informações
- **Capítulo 3:** Verificação em Listas Restritivas e Sanções
- **Capítulo 4:** Análise de Mídia Adversa e Reputação
- **Capítulo 5:** Avaliação de Aspectos Financeiros e Operacionais
- **Capítulo 6:** Avaliação de Segurança da Informação (Quando aplicável)
- **Capítulo 7:** Entrevistas e Esclarecimentos
- **Capítulo 8:** Relatório e Classificação Final
- **Capítulo 9:** Monitoramento Contínuo

**Módulo 10:** Conclusão

**Módulo 11:** Referências Bibliográficas

## 1. Introdução

No contexto corporativo contemporâneo, marcado por um ambiente de negócios cada vez mais globalizado e digitalizado, a gestão de riscos tornou-se elemento central para a sustentabilidade das organizações. Nesse cenário, Background Check e Due Diligence Digital emergem como ferramentas estratégicas para todas as instituições que compõem o Sistema Financeiro Nacional (SFN), capazes de oferecer visibilidade

aprofundada sobre contrapartes, parceiros comerciais, fornecedores e até mesmo colaboradores internos.

Essas práticas não apenas auxiliam na prevenção de fraudes, corrupção e lavagem de dinheiro, mas também fortalecem a reputação institucional e asseguram conformidade com exigências regulatórias nacionais e internacionais.

Bancos, corretoras, seguradoras, fundos de pensão e instituições de pagamento lidam diariamente com grandes volumes de dados sensíveis, operações financeiras complexas e interações com clientes, fornecedores e parceiros. O uso estratégico de dados permite identificar padrões de risco, antecipar fraudes, prevenir lavagem de dinheiro e garantir que todas as transações estejam em conformidade com normas regulatórias.

Para instituições que compõem o SFN, essas práticas são estratégicas, pois fortalecem a cultura de conformidade e o monitoramento contínuo, oferecendo relatórios detalhados que atendem às exigências regulatórias e permitem que os órgãos fiscalizadores do SFN, avaliem a solidez dos processos de governança e mitigação de riscos.

Por outro lado, a transformação digital elevou os níveis de segurança em contraponto às exigências de diminuição de prazos para garantir a aderência dos clientes. E isso já não é mais uma tendência, mas sim a realidade diária de empresas, governos e cidadãos. A forma como fazemos negócios, contratamos parceiros e nos relacionamos com clientes foi radicalmente alterada pela tecnologia.

Nesse cenário, o Background Check automatizado e a Due Diligence digital ganharam novas formas de execução e, com elas, novas responsabilidades e desafios.

O Background Check consiste em um processo estruturado de verificação voltado a indivíduos, em especial dirigentes-chave e profissionais em posições sensíveis. Ele contempla a análise de identidade, histórico profissional, formação acadêmica, eventual envolvimento em litígios e a identificação de menções negativas na mídia.

Se antes a verificação de parceiros, fornecedores e clientes dependia de visitas presenciais, entrevistas e análise física de documentos, hoje esse processo é feito com base em dados digitais, muitas vezes obtidos em tempo real e analisados por sistemas inteligentes.

No passado, conduzir uma due diligence significava alocar equipes inteiras para visitar fisicamente empresas, entrevistar funcionários, solicitar cópias físicas de documentos e esperar semanas até que todos os dados fossem analisados. Hoje, em um mundo globalizado e interconectado, empresas conseguem levantar informações de um potencial parceiro em pouco tempo, usando bases públicas, tecnologia de análise de dados e inteligência artificial.

Já a Due Diligence Digital adota um escopo mais abrangente, utilizando metodologias de inteligência de fontes abertas e bases restritivas para investigar tanto indivíduos quanto organizações. Essa abordagem combina dados de registros públicos, listas de sanções, informações corporativas, monitoramento de mídia adversa[1] e análises de risco cibernético.

A integração dessas duas práticas potencializa significativamente a capacidade de prevenção e detecção de riscos. Enquanto o Background Check garante a confiança nas pessoas que ocupam posições estratégicas, a Due Diligence Digital expande o olhar para todo o ambiente que envolve a relação comercial ou societária. Essa complementaridade é particularmente relevante para empresas que atuam em setores de alto risco, lidam com transações internacionais ou estão sujeitas a regulamentações rigorosas, como instituições do Sistema Financeiro Nacional, empresas de tecnologia e multinacionais.

Em um mundo onde a informação circula em alta velocidade e a tolerância a falhas de integridade é cada vez menor, investir nessas ferramentas significa proteger não só o presente, mas também a perenidade do negócio.

## 2. Conceitos Fundamentais

### 2.1 O que é Background Check

O Background Check é uma vertente específica dentro do universo mais amplo da due diligence, direcionada à análise de pessoas físicas e dirigentes-chave de uma organização.

Seu objetivo é validar informações de identidade, formação acadêmica, histórico profissional e eventuais registros em ações judiciais, além de examinar a presença de cobertura midiática adversa que possa impactar a reputação ou a integridade da empresa.

No contexto de compliance, esse processo exige rigor metodológico e atenção especial às exigências legais aplicáveis, como a Lei Geral de Proteção de Dados[2] (LGPD) no Brasil, que define limites claros para a coleta, tratamento e armazenamento de dados pessoais.

[1] Mídia adversa: qualquer conteúdo publicado em fontes públicas — como jornais, portais de notícias, blogs, redes sociais oficiais, registros públicos ou relatórios especializados — que aponte informações negativas, suspeitas ou prejudiciais sobre uma pessoa física, pessoa jurídica ou entidade.
[2] Lei nº 13.709/2018.

A due diligence digital, por sua vez, abrange um escopo mais amplo e tecnológico, aplicando metodologias e ferramentas de inteligência de fontes abertas (OSINT - Open Source Intelligence[3]) para analisar tanto pessoas quanto empresas.

Ela inclui pesquisas em bases públicas, listas restritivas, sanções, dados corporativos, registros setoriais e monitoramento de mídia em múltiplos idiomas. Enquanto o background check costuma se concentrar na trajetória e integridade de indivíduos, a due diligence digital examina todo o ecossistema do relacionamento, considerando redes de conexões, riscos de terceiros e aspectos cibernéticos, o que amplia a capacidade de identificar ameaças ocultas.

As diferenças entre os dois processos também se refletem na profundidade e abrangência das análises. No background check, a ênfase está na verificação de informações fornecidas e na identificação de inconsistências que possam indicar riscos éticos ou legais.

Já na due diligence digital, o objetivo é criar um panorama completo de riscos, combinando dados reputacionais, financeiros, regulatórios e operacionais. Assim, o background check pode ser visto como uma parte essencial da due diligence digital, mas não cobre todos os ângulos necessários para uma visão holística do risco.

Tanto no background check quanto na due diligence digital, aplica-se o princípio do risk-based approach — a abordagem baseada em risco. Esse conceito estabelece que a profundidade e o escopo das verificações devem ser proporcionais ao risco potencial do relacionamento, levando em consideração o setor de atuação, a geografia, o histórico de conformidade e a exposição do indivíduo ou da empresa a riscos regulatórios ou reputacionais. Isso garante eficiência na alocação de recursos e evita investigações desnecessariamente invasivas.

No contexto prático, um background check pode incluir consultas a bases de dados de tribunais, verificação de diplomas acadêmicos, análise de registros profissionais e busca por menções em fontes jornalísticas relevantes. Já a due diligence digital utiliza ferramentas mais sofisticadas, como cruzamento automatizado de informações, análise de redes corporativas, identificação de beneficiários finais, verificação de presença em listas internacionais de sanções e até monitoramento contínuo para detecção de mudanças no perfil de risco.

Por fim, a integração entre due diligence digital e background check é o que fortalece a efetividade do programa de compliance. Ao unir a profundidade das investigações

[3] É o trabalho de coletar informações que já estão disponíveis publicamente — na internet, jornais, redes sociais, registros públicos — e usar essas informações para montar um “quebra-cabeça” sobre uma pessoa, empresa ou situação. É como fazer uma investigação usando só “pistas abertas”, sem precisar invadir nada. Exemplo: se alguém vê seu perfil no LinkedIn, cruza com fotos no Instagram e dados que você publicou em fóruns, já está fazendo OSINT — e pode usar isso para conhecer seus hábitos, onde você trabalha, horários, gostos e até prever seu comportamento.

sobre indivíduos com a amplitude das análises corporativas e setoriais, a organização cria uma barreira mais sólida contra riscos de fraude, corrupção, lavagem de dinheiro e danos reputacionais.

Essa visão complementar, sustentada por políticas claras e conformidade legal, especialmente em relação à LGPD, assegura decisões mais embasadas e defensáveis perante órgãos reguladores e parceiros de negócios.

### 2.2 O que é Due Diligence?

A Due Diligence (diligência prévia, em português), conduzida pela área de Compliance é um processo que requer conhecimento em diferentes áreas, com o objetivo de averiguar a integridade, a capacidade e a conformidade de terceiros — clientes, parceiros, fornecedores e investidores — antes e durante um relacionamento comercial.

No contexto de Integridade e Prevenção à Lavagem e ao Financiamento do Terrorismo, ela se materializa em conhecer quem é a contraparte, quem a controla, de onde vêm seus recursos e como se comporta no mercado.

Na prática, trata-se de um conjunto de procedimentos para investigar e verificar informações antes de uma tomada de decisão importante.

A ideia é levantar uma série de informações que sirva de suporte para a tomada de decisão. É um processo sistemático de investigação e análise de informações sobre um indivíduo ou empresa antes de firmar uma relação comercial, contratual ou financeira.

Requer um estudo e investigação de diferentes fatores de uma empresa ou pessoa, tendo como objetivo analisar possíveis riscos que ela possa trazer de modo assertivo. É necessário realizar uma busca por informações em diversas fontes, visando avaliar o grau de risco.

Esse processo detalhado minucioso desempenha um papel crucial na identificação e mitigação de riscos, permitindo que as empresas operem dentro da legalidade e evitem possíveis repercussões negativas no futuro.

Conforme veremos, a Due Diligence é aplicada em diversas áreas. A ideia é levantar uma série de informações que sirva de suporte para a tomada de decisão, no sentido de avaliar não só o passado de uma empresa, mas também ser uma projeção fidedigna sobre o futuro.

A due diligence é essencial para garantir que a empresa não se envolva com partes que possam comprometer sua integridade ou expô-la a riscos legais, regulatórios e reputacionais.

➢ Exemplo:

Imagine que uma fintech brasileira pretenda firmar parceria com uma empresa estrangeira para processar pagamentos internacionais. Antes de assinar o contrato, o time de compliance deve investigar se essa empresa cumpre as leis do seu país, se não está envolvida em processos judiciais relevantes, se os seus beneficiários finais (UBOs[4]) não estão em listas de sanções, e se a reputação da empresa é sólida no mercado.

## 3. Objetivos do Due Diligence

Nas instituições do Sistema Financeiro Nacional, essa prática é aplicada especialmente durante o processo de onboarding de clientes, com o propósito de conhecer o cliente (KYC – Know Your Customer) e prevenir fraude de identidades, lavagem de dinheiro e outros tipos de crimes financeiros.

Em geral, a due diligence inclui a verificação da origem dos recursos, a sua capacidade econômico-financeira, a avaliação de sua idoneidade, a identificação de riscos reputacionais, legais, financeiros ou regulatórios.

Existem obrigações regulatórias na realização da due diligence, tais como o cumprimento de normas do BACEN (Banco Central do Brasil), do COAF (Conselho de Controle de Atividades Financeiras), da CVM (Comissão de Valores Mobiliários) e padrões de organizações internacionais, como por exemplo: FATF (Financial Action Task Force), conhecido em português como GAFI (Grupo de Ação Financeira Internacional).

Isso tudo, com o intuito de analisar o grau de risco que essa relação pode trazer à Instituição — especialmente riscos de:

- Lavagem de dinheiro;
- Corrupção;
- Fraude;

[4] Ultimate Beneficial Owner. É a pessoa natural que, em última instância, possui, controla ou influencia, de forma significativa, uma entidade, direta ou indiretamente, de acordo com a Receita Federal.

- Financiamento ao terrorismo;
- Sanções internacionais;
- Conflitos de interesse;
- Reputação negativa.

➢ Exemplo prático:

Um banco digital que realiza onboarding rápido de clientes precisa, em segundos, validar se a pessoa não está em listas de sanções ou não apresenta histórico de crimes financeiros.

### 3.1 Como fazer uma boa Due Diligence?

Uma boa Due Diligence começa pelo planejamento e definição do escopo, etapa em que a organização identifica com clareza quais informações precisa levantar e para qual finalidade.

Isso envolve entender o contexto da relação comercial ou parceria, o grau de criticidade do negócio e os riscos potenciais envolvidos. É nessa fase que se definem critérios de pesquisa tais como: situação jurídica, reputação, histórico financeiro, vínculos societários e aspectos regulatórios — além de estabelecer quais fontes serão utilizadas: registros públicos, bases privadas, entrevistas e análises de campo, quando necessário.

O segundo passo é a coleta de informações de forma estruturada e confiável, priorizando dados oficiais e fontes verificáveis. Em uma Due Diligence digital, entram nesse processo ferramentas de OSINT, pesquisas em mídias abertas e redes sociais, consulta a listas de sanções e restrições, e análise de bases governamentais. Aqui, a qualidade é mais importante do que a quantidade: informações desencontradas ou sem verificação podem gerar conclusões equivocadas e comprometer a tomada de decisão.

O terceiro elemento é a análise crítica e contextualização dos dados coletados. Não basta listar fatos — é preciso interpretá-los à luz do negócio e dos padrões de risco definidos pela empresa.

Um simples registro de processo judicial ou menção negativa na mídia não significa necessariamente um impedimento, é preciso avaliar a gravidade, a recorrência e o potencial impacto para a organização. Essa etapa também demanda profissionais

capacitados, que unam conhecimento jurídico, experiência em investigação e habilidades analíticas.

- ➢ Exemplo:

  Uma ação judicial pode não representar um risco relevante se estiver relacionado a uma disputa trabalhista pontual, mas pode ser crítico se indicar padrões repetitivos de conduta ilegal. É nessa etapa que se avalia o nível de exposição e classificação de risco.

Por fim, uma boa Due Diligence exige documentação clara e recomendações objetivas. A rastreabilidade do processo é essencial: manter registros do que foi pesquisado, onde e quando, protege a empresa em auditorias e eventuais questionamentos legais. Uma Due Diligence eficaz é, portanto, mais do que um levantamento de dados — é um instrumento estratégico de gestão de riscos e tomada de decisão segura.

O relatório de *due diligence* deve apresentar de forma clara e objetiva as descobertas, classificando os riscos identificados e oferecendo recomendações práticas. Além disso, a implementação de ferramentas de acompanhamento contínuo é uma boa prática para prevenir surpresas futuras, garantindo que as informações sejam atualizadas e que mudanças no perfil de risco sejam rapidamente detectadas.

Ferramentas tecnológicas especializadas são essenciais para dar agilidade e profundidade ao processo. Plataformas de *screening* de listas restritivas (OFAC, ONU, UE), sistemas de monitoramento de mídia e *social listening*, além de softwares de análise forense digital, podem fornecer uma visão mais completa do histórico e das conexões de uma pessoa ou empresa. Ferramentas de *OSINT* são especialmente úteis, pois permitem cruzar dados de fontes abertas para identificar vínculos ocultos, inconsistências ou padrões suspeitos.

**Checklist Prático — Como Fazer uma Boa Due Diligence**

| **Etapa** | **Objetivo** | **Ações Recomendadas** | **Ferramentas/Sugestões** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **1. Planejamento e escopo** | Definir foco e profundidade da análise | - Identificar objetivos da due diligence<br>- Determinar áreas de investigação (jurídica, financeira, reputacional, regulatória)<br>- Definir critérios de risco | • Questionário<br>• Matriz de Risco<br>• Reunião com áreas-chave |
| **2. Coleta de informações** | Obter dados relevantes e confiáveis | - Consultar registros públicos e governamentais<br>- Pesquisar em bases privadas e listas de sanções<br>- Utilizar técnicas OSINT para análise de fontes abertas | • Juntas Comerciais<br>• LinkedIn<br>• Bases governamentais (CVM, Bacen, Receita Federal)<br>• Tribunais de Justiça |
| **3. Análise crítica** | Interpretar dados à luz do negócio | - Avaliar relevância de cada informação<br>- Classificar riscos (baixo, médio, alto)<br>- Identificar padrões e tendências | • Matriz de Probabilidade e Impacto<br>• Ferramentas de BI |
| **4. Relatório e recomendações** | Apresentar conclusões e orientações | - Estruturar relatório com evidências documentadas | • Modelos de relatório<br>• Checklists internos |

| | | | |
|---|---|---|---|
| | | - Apontar riscos e sugestões de mitigação<br><br>- Incluir decisão recomendada (seguir, renegociar, encerrar) | |
| **5. Arquivamento e rastreabilidade** | Garantir histórico e conformidade | - Guardar registros e fontes<br><br>- Manter evidências disponíveis para auditorias | • Sistema de Gestão Documental<br><br>• Pasta digital criptografada |

### 3.2 Quais são as boas práticas de uma boa Due Diligence?

Uma vez iniciado, não é recomendado que acabe. Além disso, não basta aprovar um fornecedor, por exemplo, e, em seguida, deixar de monitorar a atividade dessa empresa. Tal atitude aumenta os riscos de ocorrer algum problema de passivo.

Uma boa prática de Due Diligence começa pela integração com a estratégia corporativa. Isso significa que a análise de parceiros, fornecedores ou clientes não deve ser feita como um procedimento isolado, mas conectada ao planejamento de negócios e à política de risco da empresa.

➢ Exemplos:

- uma organização com apetite de risco baixo deve adotar protocolos de verificação mais rigorosos, enquanto que;
- empresas que atuam em mercados de maior volatilidade podem priorizar a agilidade, sem abrir mão de controles essenciais.

Esse alinhamento garante que a Due Diligence não seja apenas burocrática, mas efetivamente estratégica.

Outro ponto-chave é o mapeamento aprofundado de stakeholders, que vai além das informações básicas. Em boas práticas, investiga-se a estrutura societária completa, beneficiários finais, histórico de litígios, passivos ocultos e até relações indiretas com terceiros de risco.

Essa visão ampliada é especialmente importante no ambiente digital, onde dados podem ser fragmentados ou manipulados. Por isso, o uso combinado de bases oficiais, relatórios de mercado e ferramentas de OSINT é essencial para formar um retrato fiel do investigado.

A análise contextual é igualmente relevante. Uma boa Due Diligence não se limita a constatar fatos, mas interpreta esses fatos à luz do setor, do país e do momento econômico em que o investigado atua. Por exemplo, estar presente em um país com alta classificação no índice de percepção de corrupção já aumenta o grau de atenção, mesmo que não haja incidentes registrados contra a empresa. Esse tipo de leitura evita conclusões precipitadas e ajuda a dimensionar riscos com mais precisão.

Por fim, as boas práticas exigem feedback e atualização contínua. Não basta entregar um relatório final; é necessário criar mecanismos para monitorar alterações relevantes, como mudanças societárias, novas sanções ou envolvimento em investigações.

Empresas que mantêm esse monitoramento ativo conseguem reagir rapidamente a novos riscos e demonstrar diligência contínua perante reguladores e parceiros. Assim, a Due Diligence deixa de ser um evento pontual e passa a ser parte viva da gestão de riscos.

**Más Práticas x Boas Práticas em Due Diligence Digital**

| **Aspecto** | **Más Práticas** | **Boas Práticas** |
|---|---|---|
| **Integração com a estratégia** | Realizar a Due Diligence apenas como exigência burocrática, sem conexão com a política de risco da empresa. | Integrar o processo à estratégia corporativa, ajustando a profundidade da análise ao apetite de risco e aos objetivos de negócio. |
| **Fontes de informação** | Confiar apenas em informações enviadas pelo próprio investigado ou em uma única base de dados. | Combinar dados oficiais, relatórios de mercado, OSINT e fontes independentes para confirmar e enriquecer a análise. |

| | | |
|---|---|---|
| **Escopo da análise** | Limitar-se a verificar dados cadastrais básicos e documentos apresentados. | Investigar estrutura societária, beneficiários finais, histórico jurídico, reputação e conexões indiretas de risco. |
| **Contextualização** | Avaliar riscos de forma genérica, sem considerar setor, país ou contexto econômico. | Interpretar informações à luz do ambiente regulatório e geopolítico, identificando fatores externos que elevam o risco. |
| **Periodicidade** | Fazer a Due Diligence apenas na fase inicial de relacionamento. | Implementar monitoramento contínuo, atualizando informações e reagindo a mudanças relevantes. |
| **Documentação** | Relatórios superficiais, sem evidências ou referências claras. | Relatórios detalhados, com fontes citadas, evidências arquivadas e conclusões justificadas. |
| **Uso de tecnologia** | Processos manuais sem ferramentas de automação ou análise de dados. | Utilização de softwares especializados, IA e analytics para acelerar e aprofundar verificações. |
| **Tomada de decisão** | Conclusões baseadas apenas em “checklists” sem interpretação crítica. | Análise crítica dos achados, com recomendações práticas e cenários de mitigação de riscos. |

## 4. Do Presencial ao Digital

### 4.1 O eKYC (Electronic Know Your Customer) e do eKYB (Electronic Know Your Business)

O processo de diligência presencial tradicional depende da verificação manual de identidade em documento físico. Ou seja, os clientes são obrigados a fornecer documentos físicos como prova da sua identidade, normalmente visitando um escritório, agência ou filial presencialmente.

A diligência presencial tradicional enfatiza: inspeções in loco, conferência física de documentos, validação de instalações, conversas face a face com responsáveis e observação de sinais práticos (estrutura, atividade real, controles).

Durante a pandemia da COVID-19, as organizações passaram por um rápido fluxo de digitalização. Desde então, as pessoas se acostumaram à conectividade onipresente e à conveniência de uma experiência do cliente que prioriza o digital. As empresas, por sua vez, perceberam que muitos processos poderiam ser migrados para o ambiente online com eficiência e segurança.

E, com mais identidades digitais para gerenciar, as organizações exigem uma solução de comprovação de identidade que equilibre a experiência do cliente com segurança de alta garantia.

Hoje, é possível:

- Coletar documentos digitalizados e verificar sua autenticidade com OCR e blockchain.
- Usar biometria facial para confirmar identidade.
- Pesquisar antecedentes criminais e cíveis em bases públicas online.
- Integrar ferramentas de *screening* a listas de sanções globais em tempo real.

A Due diligence presencial, por vezes é necessária, quando a digital não supre toda a acuracidade necessária para dar à organização a completude de seus processos.

Por outro lado, a digitalização permite escala, velocidade e repetibilidade, essenciais para bancos digitais e marketplaces. Em compensação, introduz desafios como fraude sintética, deepfakes, homônimos e spoofing de websites, por meio de ferramentas on-line e inteligência artificial (IA).

Na prática madura, os dois mundos se complementam: processos digitais robustos são o padrão, com camadas presenciais ou síncronas acionadas por risco, valor ou exceções.

Esses processos se beneficiam da automação e da inteligência artificial para detectar padrões incomuns, como transações fracionadas para evitar reporte ou operações em horários e locais não habituais.

A era digital proporciona a realização do eKYC (Electronic Know Your Customer) e do eKYB (Electronic Know Your Business), verificação biométrica e de vivacidade, validações automatizadas em bases públicas, consultas a listas restritivas, análise de mídia e monitoramento contínuo por alertas.

Em pessoas físicas, a verificação envolve documento de identidade, prova de vida, conferência de autenticidade, confirmação de endereço e, quando aplicável, validação de vínculo empregatício e renda. Em pessoas jurídicas, começa pelo registro no órgão competente (CNPJ/Junta Comercial no Brasil), contrato social, alterações e quadro societário, identificação de administradores e procurações, e segue para demonstrações financeiras, licenças e certificações setoriais.

Em cenários digitais, o eKYC combina captura guiada de documento, OCR e verificação biométrica, com checagens contra bases governamentais e regras antifraude (documento vencido, selfie recortada, inconsistência de Zona de Leitura por Máquina - MRZ).

Ademais, é importante checar se o dispositivo em uso não foi roubado e não esteve envolvido em transações fraudulentas. Ele verifica os sinais passivos do dispositivo para determinar se o usuário está dizendo a verdade sobre quem ele é. Sinais passivos podem incluir: Endereço IP, Dados de localização, Impressão digital no dispositivo, Dados do navegador ou Metadados.

O objetivo é reduzir falsos positivos sem criar atrito excessivo e aumentar o nível de satisfação da jornada do cliente, sem abrir mão do apetite de risco definido pela empresa.

### 4.2 A Lei Geral de Proteção de Dados - Princípios e exceções para coleta de dados

A Lei Geral de Proteção de Dados (LGPD), é um marco regulatório fundamental para o setor financeiro. Ela estabelece regras claras sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, assegurando direitos aos titulares e impondo responsabilidades às instituições.

Para organizações financeiras, isso significa que qualquer investigação ou verificação de antecedentes deve ser conduzida dentro dos limites legais, equilibrando a necessidade de mitigação de riscos com a proteção da privacidade de indivíduos.

A LGPD baseia-se em princípios essenciais, incluindo:

- Finalidade – os dados devem ser coletados para propósitos legítimos, específicos e informados ao titular.

- Necessidade – apenas os dados estritamente necessários para atingir a finalidade devem ser tratados.

- Transparência – os titulares devem ser informados sobre o uso de seus dados de forma clara e acessível.

- Segurança – medidas técnicas e administrativas devem proteger os dados contra acessos não autorizados, vazamentos ou uso indevido.

- Livre acesso e qualidade – o titular tem direito a consultar e corrigir suas informações pessoais.

Mas existem também exceções legais que permitem o tratamento de dados sem consentimento[5], quando necessários para garantir a prevenção à fraude e a segurança do titular, especialmente em processos de identificação e autenticação em sistemas eletrônicos. Este dispositivo reflete a preocupação da LGPD com a proteção dos indivíduos contra fraudes, equilibrando a segurança e os direitos fundamentais dos titulares, tais como:

- Cumprimento de obrigação legal ou regulatória (ex.: registros obrigatórios de transações financeiras);

- Execução de políticas de prevenção à fraude, lavagem de dinheiro e financiamento ao terrorismo;

- Exercício regular de direitos em processos judiciais ou administrativos;

- Proteção do crédito e de interesses legítimos do controlador, desde que respeitados os direitos fundamentais do titular;

- Pesquisa e análise de mercado, quando conduzidas anonimamente ou agregadas.

[5] O artigo 11, inciso II, alínea "g", da LGPD estabelece uma importante uma exceção ao princípio do consentimento para o tratamento de dados pessoais sensíveis:
*"Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:*
*(...)*
*II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:*
*(...)*
*g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."*

Contudo, o tratamento de dados sensíveis sem o consentimento do titular só é permitido se forem respeitados os direitos previstos no artigo 9º da LGPD, que assegura a proteção da privacidade e a segurança dos dados pessoais. Além disso, caso prevaleçam direitos e liberdades fundamentais do titular, as medidas de prevenção à fraude devem ser adotadas de maneira equilibrada, sempre garantindo a proteção dos dados pessoais.

Exemplos práticos de aplicação dessa alínea incluem:

i. Autenticação em dois Fatores em Plataformas Bancárias: Sistemas de autenticação multifatorial, que combinam senha e um código enviado por SMS ou gerado por aplicativo, são utilizados para confirmar a identidade do usuário e evitar acessos não autorizados, prevenindo fraudes financeiras.

ii. Verificação de Identidade em Cadastros Online: Plataformas de e-commerce e serviços financeiros frequentemente solicitam documentos pessoais e até selfies para comparar com fotos do documento, visando evitar fraudes de identidade durante o cadastro ou transação.

iii. Detecção de Fraudes em Transações Eletrônicas: Em sistemas de pagamento online, tecnologias como análise comportamental e rastreamento de dispositivos são usadas para verificar a autenticidade de transações, solicitando uma verificação adicional em caso de atividades suspeitas.

iv. Monitoramento de Atividades Suspeitas em Plataformas Digitais: Sistemas que detectam comportamentos típicos de fraude, como tentativas de login com senhas incorretas, acionam verificações adicionais para garantir a segurança do processo de autenticação.

v. Prevenção de Fraudes em Empréstimos e Financiamentos: A análise de dados sensíveis, como informações de crédito e bancárias, é realizada para validar a identidade do solicitante e prevenir fraudes em processos de concessão de empréstimos e financiamentos.

Essas exceções permitem que instituições do Sistema Financeiro Nacional realizem verificações estratégicas sobre clientes, fornecedores ou terceiros, utilizando ferramentas de background check e due diligence digital, sem violar a legislação.

No entanto, é essencial documentar cada etapa, registrar bases legais e garantir que os dados coletados sejam restritos ao necessário, promovendo conformidade regulatória e mitigando riscos de responsabilidade civil ou administrativa.

Assim, a LGPD se torna um pilar do Compliance Data Driven, assegurando que decisões baseadas em dados sejam legítimas, transparentes e seguras, equilibrando eficácia investigativa com respeito à privacidade e proteção dos direitos individuais.

## 5. Metodologia aplicada

### 5.1 O ciclo PDCA

A metodologia para estabelecer um bom processo de due diligence é o ciclo PDCA[6] (Plan, Do, Check, Act), pois fornece uma abordagem estruturada para planejar, executar, monitorar e melhorar continuamente os processos de verificação e análise de riscos.

A primeira etapa, Plan (Planejar), consiste em definir claramente o objetivo da due diligence, o escopo da investigação, os critérios de risco e as fontes de informação a serem consultadas. Nesse momento, também se escolhem as ferramentas tecnológicas e se estabelecem os procedimentos que garantirão conformidade com leis como a LGPD e regulamentos setoriais.

A segunda etapa, Do (Fazer), envolve a execução prática do plano. Aqui, são realizadas as pesquisas em bases de dados públicas e privadas, listas de sanções (OFAC, ONU, UE), mídias e redes sociais, além do uso de ferramentas de *OSINT* e monitoramento de reputação. É nessa fase que a equipe coleta e organiza as evidências, documentando cada passo para garantir rastreabilidade e transparência do processo.

A terceira fase, Check (Checar), foca na análise crítica dos dados obtidos e na verificação se as informações coletadas atendem ao escopo e aos critérios definidos na etapa de planejamento. Isso inclui validar a confiabilidade das fontes, checar possíveis inconsistências e confirmar se os riscos identificados foram corretamente classificados. Nesta etapa, é essencial envolver especialistas multidisciplinares para garantir que as conclusões sejam sólidas e bem fundamentadas.

Na quarta etapa, Act (Agir), são implementadas as ações corretivas e preventivas com base nos achados da due diligence. Isso pode incluir recomendar o bloqueio de uma parceria de alto risco, exigir medidas adicionais de mitigação ou até mesmo aprimorar o processo para evitar falhas semelhantes no futuro. É também o momento de registrar as lições aprendidas e atualizar os procedimentos internos, fortalecendo a política de Compliance.

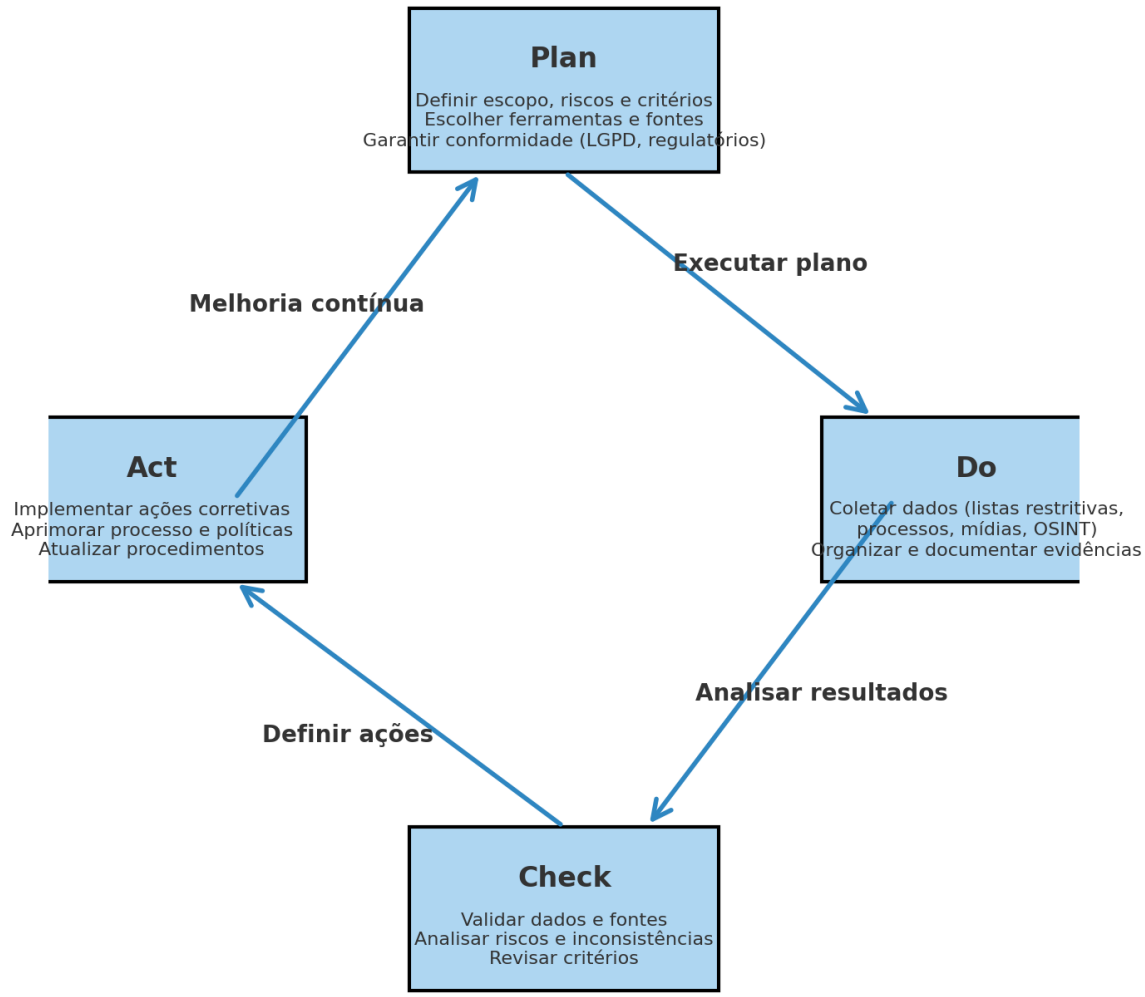
Assim, ao aplicar o ciclo PDCA no processo de due diligence, a organização não apenas assegura uma análise estruturada e consistente dos riscos, mas também

[6] DEMINING, W. Edwards. Out of the Crisis. Cambridge: MIT Press, 1986.

estabelece uma cultura de melhoria contínua que fortalece a governança e a tomada de decisão. Esse modelo permite que cada verificação vá além de um procedimento pontual, transformando-se em um mecanismo dinâmico de prevenção, alinhado às exigências regulatórias e às melhores práticas de Compliance.

Dessa forma, a due diligence deixa de ser apenas um requisito formal e passa a ser um diferencial estratégico, capaz de proteger a reputação, reduzir vulnerabilidades e garantir relacionamentos comerciais mais seguros e sustentáveis.

**Ciclo PDCA aplicado à Due Diligence Digital e Background Check**




## 6. Tipos de Due Diligence

Antes de iniciar qualquer processo de Due Diligence, é fundamental que a organização defina com clareza o escopo de atuação. Isso significa determinar quais riscos se pretende avaliar, quais partes interessadas serão analisadas, quais fontes de dados serão utilizadas e qual será o nível de profundidade da investigação.

Sem essa definição prévia, o processo pode se tornar excessivamente amplo, custoso e pouco eficiente, ou, ao contrário, superficial e incapaz de identificar riscos

relevantes. Um escopo bem estruturado garante que cada tipo de due diligence seja aplicado de forma direcionada, maximizando a eficácia e a relação custo-benefício.

Essa definição também deve estar alinhada ao apetite de risco da organização e às exigências regulatórias aplicáveis. Empresas de setores altamente regulados, como o financeiro ou o farmacêutico, tendem a adotar critérios mais rigorosos, realizando análises aprofundadas mesmo para parceiros e clientes de baixo valor financeiro. Já organizações com apetite de risco mais elevado podem optar por verificações mais enxutas, desde que cumpram as exigências legais. Essa escolha estratégica deve considerar não apenas o cumprimento de normas, mas também a proteção da reputação e a sustentabilidade do negócio.

Por fim, é importante que a organização estabeleça procedimentos, ferramentas e responsabilidades claras antes de iniciar o processo. Isso inclui definir quem conduz cada etapa da análise, quais plataformas e bases de dados serão usadas, como será feita a documentação e quais critérios serão utilizados para aprovar, condicionar ou reprovar um relacionamento comercial.

Com essa base bem definida, torna-se possível aplicar, de forma estratégica, os diferentes tipos de due diligence — desde a verificação de clientes (Customer Due Diligence) até análises mais específicas como IT Due Diligence ou ESG Due Diligence. Vamos a eles:

### i. Customer Due Diligence (CDD) - Due Diligence do Cliente

O Customer Due Diligence (CDD) é o processo de identificar, verificar e avaliar o risco de clientes antes e durante o relacionamento comercial. É parte essencial do programa de Know Your Customer (KYC) e tem como objetivo prevenir crimes como lavagem de dinheiro, financiamento ao terrorismo, fraude e corrupção. No contexto digital, o CDD envolve o uso de bases de dados públicas e privadas, listas de sanções, verificações de beneficiários finais (UBOs) e pesquisas em mídias abertas (OSINT), garantindo que a organização saiba exatamente com quem está se relacionando.

Além da verificação inicial, o CDD também exige monitoramento contínuo. Um cliente que, no momento da abertura de conta ou contratação, apresentava baixo risco, pode mudar de perfil ao longo do tempo, seja por envolvimento em investigações, mudanças societárias ou atuação em países com alto índice de corrupção. Por isso, ferramentas de monitoramento contínuo são fundamentais para alertar sobre alterações no perfil de risco e permitir que a empresa tome medidas preventivas.

- ➢ Exemplo: Um banco, ao abrir conta para um novo cliente corporativo, solicita documentos societários, cadastro na Receita Federal, endereço do

escritório, os beneficiários finais (UBOs), documentos que comprovam a sua capacidade financeira.

### ii. Vendor Due Diligence - Due Diligence de Fornecedores, Prestadores de Serviço e Parceiros

O Vendor Due Diligence consiste na avaliação criteriosa de fornecedores, prestadores de serviço e parceiros comerciais. O objetivo é prevenir riscos como corrupção, fraude, uso de trabalho escravo, não conformidade ambiental ou reputacional, que podem afetar a empresa contratante.

- ➢ Exemplo: Uma multinacional de alimentos contrata um fornecedor de matéria-prima e, antes de assinar o contrato, verifica se a empresa cumpre legislações ambientais, possui certificações válidas, não figura em listas de embargo do governo e não está envolvida em ações trabalhistas graves.

### iii. Operational Due Diligence - Due Diligence Operacional

O Operational Due Diligence foca na avaliação das práticas, controles e processos operacionais de uma organização. É muito aplicado em fusões e aquisições (M&A), fundos de investimento e parcerias estratégicas, para verificar se a operação é eficiente, segura e sustentável.

- ➢ Exemplo: Antes de adquirir uma startup de tecnologia, uma empresa realiza due diligence operacional para avaliar a maturidade dos processos internos, a segurança da infraestrutura de TI, a capacidade de entrega e a dependência de fornecedores críticos.

### iv. Legal Due Diligence - Due Diligence Jurídico

A Legal Due Diligence é voltada para identificar e avaliar riscos jurídicos que possam impactar a viabilidade de uma operação ou a relação com uma contraparte. Isso inclui revisar contratos vigentes, examinar disputas judiciais, avaliar licenças e autorizações, verificar a titularidade de ativos e analisar a conformidade com leis e regulamentos setoriais. No Compliance, ela é essencial para prevenir que a empresa se envolva em litígios ou herde passivos legais ocultos.

O processo envolve tanto consultas a bancos de dados oficiais — como tribunais, juntas comerciais e órgãos reguladores — quanto entrevistas e análises internas,

especialmente em operações de fusão e aquisição. Também é comum incluir a verificação de propriedade intelectual, cláusulas contratuais que possam representar riscos e obrigações trabalhistas ou ambientais.

➢ Exemplo: Em uma negociação de compra de uma rede de clínicas, o comprador contrata advogados para revisar contratos com operadoras de saúde, verificar ações trabalhistas e cíveis em andamento, confirmar se todas as licenças sanitárias estão em dia e se não há riscos de multas regulatórias.

### v. Financial Due Diligence - Due Diligence Financeira

A due diligence financeira é um pilar essencial na avaliação de empresas, projetos e parcerias, servindo como instrumento para identificar riscos ocultos e validar a saúde econômica de uma organização.

A Financial Due Diligence consiste na avaliação da saúde financeira de uma empresa, visando confirmar a exatidão das demonstrações contábeis e identificar passivos ocultos que possam afetar sua viabilidade. É amplamente utilizada em fusões, aquisições, captação de investimentos e análise de fornecedores ou parceiros estratégicos.

Essa análise vai além de revisar balanços e demonstrações de resultados. Inclui examinar fluxo de caixa, dívidas, obrigações fiscais, estrutura de capital, margem de lucro, variações financeiras, relatórios de auditoria e indicadores operacionais, possibilitando detectar inconsistências, distorções e sinais de estresse que, se ignorados, podem comprometer o sucesso de um investimento ou relacionamento comercial.

Essa etapa exige a interpretação dos dados dentro do contexto operacional, setorial e histórico da empresa. Ferramentas digitais podem ser usadas para cruzar dados contábeis com registros públicos, detectar inconsistências e analisar tendências de mercado.

➢ Exemplo: Antes de investir em uma empresa de logística, um fundo de private equity contrata auditores para revisar balanços, fluxo de caixa, passivos ocultos, dívidas fiscais e histórico de pagamentos, usando ferramentas que cruzam dados públicos e registros contábeis.

Entre os sinais clássicos de alerta, destacam-se variações abruptas de receita que não encontram respaldo na estrutura ou na capacidade produtiva da organização, margens de lucro irrealisticamente elevadas, dependência excessiva de um único

cliente ou fornecedor, saldos de caixa incompatíveis com o porte e a operação do negócio, além de notas explicativas incompletas ou vagas nos demonstrativos.

Esses indícios, conhecidos como red flags, podem apontar para riscos de má gestão, manipulação contábil, fraude ou até mesmo para problemas de liquidez iminentes.

No universo de fintechs e bancos digitais, a análise deve incluir fatores específicos, dada a natureza e velocidade desse mercado. É fundamental examinar a qualidade e a solidez da base de clientes, o custo de aquisição de usuários, os índices de inadimplência, a concentração de receitas em poucos parceiros estratégicos e as práticas adotadas para reconhecimento de receita.

A superficialidade nessa análise pode levar a decisões equivocadas, especialmente em setores onde o crescimento acelerado pode mascarar fragilidades estruturais.

Quando não houver demonstrações auditadas disponíveis, é necessário recorrer a fontes alternativas para validar as informações financeiras. Entre essas alternativas estão extratos de faturamento emitidos para fins tributários, contratos relevantes que comprovem receita recorrente, cartas de referência de clientes e fornecedores estratégicos, além de comprovantes de licenças e autorizações de operação.

A confiabilidade dessas fontes deve ser verificada com igual rigor, garantindo que os dados utilizados sejam legítimos e atualizados.

Por fim, a combinação de evidências financeiras e reputacionais aumenta significativamente a robustez da decisão final. Integrar dados quantitativos, como indicadores contábeis e operacionais, com informações qualitativas obtidas por meio de pesquisas de mercado, mídias e referências, cria uma visão holística do risco.

Assim, a due diligence financeira deixa de ser apenas um exercício contábil para se tornar um processo estratégico, capaz de proteger ativos, evitar perdas e sustentar decisões alinhadas aos princípios de compliance e governança corporativa.

➢ **Indicadores de alerta financeiro**

Indicadores Contábeis e de Receita

- Crescimento abrupto ou queda acentuada na receita sem justificativa operacional plausível.
- Margens de lucro significativamente acima da média setorial sem explicação convincente.
- Alto percentual de receita concentrado em um único cliente ou contrato.
- Reconhecimento de receitas de forma antecipada ou agressiva, incompatível com normas contábeis.
- Receitas inconsistentes com a estrutura de custos e capacidade operacional.

Caixa, Liquidez e Endividamento

- Saldos de caixa incompatíveis com o porte e o histórico do negócio.
- Endividamento crescente sem contrapartida em investimentos produtivos.
- Uso recorrente de linhas de crédito emergenciais para cobrir operações.
- Fluxo de caixa operacional negativo por períodos prolongados.
- Falta de clareza na origem de entradas financeiras relevantes.

Documentação e Transparência

- Ausência de demonstrações financeiras auditadas sem justificativa.
- Notas explicativas genéricas, incompletas ou inconsistentes.
- Alterações frequentes no auditor independente.
- Negativa ou demora excessiva em fornecer documentos solicitados durante a due diligence.
- Uso de práticas contábeis não padronizadas ou pouco transparentes.

Operações e Estrutura

- Estrutura societária complexa ou opaca, com empresas de fachada ou offshores não justificadas.
- Falta de segregação entre contas pessoais e contas corporativas.
- Operações recorrentes com partes relacionadas sem documentação formal.
- Mudanças frequentes e inexplicáveis na diretoria ou nos controladores.
- Alta rotatividade de executivos-chave do setor financeiro.

Sinais Externos e Reputacionais

- Litígios judiciais relevantes envolvendo questões financeiras, tributárias ou societárias.
- Envolvimento em investigações de fraude, corrupção ou lavagem de dinheiro.
- Reportagens ou menções em mídia adversa sobre má gestão ou práticas contábeis duvidosas.
- Divergências entre dados financeiros divulgados a diferentes stakeholders.
- Presença em listas restritivas, como sanções econômicas ou bloqueios regulatórios.

### vi. Due Diligence Reputacional

O Reputational Due Diligence busca avaliar a imagem e reputação de indivíduos ou empresas no mercado, usando tanto fontes abertas (OSINT) quanto dados proprietários. Esse tipo de análise identifica riscos que podem não aparecer em documentos formais, mas que podem impactar a confiança e a marca.

- ➢ Exemplo: Uma empresa farmacêutica, antes de fechar contrato com um distribuidor estrangeiro, realiza pesquisa aprofundada em mídias, redes sociais e notícias internacionais para verificar se o parceiro já esteve envolvido em escândalos, denúncias ou controvérsias públicas.

### vii. IT Due Diligence - Due Diligence Tecnológica

A IT Due Diligence é voltada para avaliar a infraestrutura tecnológica, sistemas de informação, cibersegurança e conformidade com leis de proteção de dados, como a LGPD e o GDPR. É especialmente relevante para empresas que dependem fortemente de tecnologia, tratam dados sensíveis ou estão em setores críticos como financeiro, saúde e e-commerce.

O processo envolve identificar vulnerabilidades em redes, servidores, aplicações e integrações com terceiros, além de avaliar práticas de backup, continuidade de negócios e governança de TI. Também é analisada a maturidade dos processos de segurança, políticas de acesso, gerenciamento de incidentes e aderência a padrões como ISO 27001 ou NIST.

- ➢ Exemplo: Uma fintech brasileira que vai receber aporte de um investidor estrangeiro passa por uma avaliação de segurança cibernética para confirmar se suas APIs, servidores e processos de criptografia estão protegidos contra ataques e se cumpre as exigências da LGPD.

### viii. ESG Due Diligence

A ESG Due Diligence avalia práticas ambientais, sociais e de governança (Environmental, Social and Governance) para garantir que parceiros e fornecedores estejam alinhados às políticas de sustentabilidade e ética da empresa.

- ➢ Exemplo: Uma rede de moda, antes de contratar fornecedores internacionais, verifica se estes não utilizam trabalho infantil, cumprem padrões ambientais e têm governança corporativa transparente, utilizando plataformas de monitoramento global de sustentabilidade.

### ixi. Enhanced Due Diligence (EDD)

Por último, mas não menos importante, o Enhanced Due Diligence é a diligência reforçada para situações de maior risco e é aplicado quando o relacionamento ou transação apresenta maior risco, risco elevado nas operações ou sinais de alerta.

Envolve coleta de dados mais extensa, entrevistas, visitas presenciais e cruzamento de múltiplas fontes para confirmar a integridade da contraparte.

Isso pode ser devido ao país de origem da contraparte, ao setor de atuação ou ao perfil dos beneficiários finais.

Ela se aplica a contrapartes com red flags relevantes, enquadradas em um risco alto, como por exemplo, presença em listas sancionatórias, pessoas com exposição política (PEP), estruturas societárias opacas, atuação em setores sensíveis ou em jurisdições de alto risco segundo o GAFI/FATF, volumes financeiros elevados, operações atípicas ou produtos com maior suscetibilidade a abuso (bens de luxo, criptoativos, remessas internacionais, jogos). É importante ainda cruzar informações com listas de sanções (OFAC, ONU, UE) e analisar o histórico de mídia negativa para detectar envolvimento prévio em esquemas ilícitos.

O EDD normalmente inclui validação independente do beneficiário final (UBO), evidências sobre a origem de recursos, entrevistas de compliance, coleta de declarações formais, verificação aprofundada de mídia adversa, eventual visita (presencial ou virtual) e aprovações escalonadas.

O objetivo não é “eliminar todo risco”, mas torná-lo conhecido, mitigado e aceitável dentro do apetite de risco da organização.

A grande diferença entre o CDD e o EDD é que o primeiro busca confirmar dados básicos e o segundo aprofunda a investigação.

- ➢ Exemplo: Um banco digital brasileiro detecta que um novo cliente corporativo tem como sócio majoritário um cidadão de país classificado pela FATF/GAFI como de alto risco para lavagem de dinheiro. Nesse caso, o banco fará um EDD, coletando informações adicionais, verificando a origem dos fundos e monitorando a conta de forma contínua.

## 7. Análises que compõe uma boa enhanced due diligence

### 7.1 Beneficiário final (UBO) e Estruturas Societárias

Identificar o beneficiário final é central para avaliar riscos de corrupção, lavagem e evasão. Estruturas com múltiplas camadas, holdings em jurisdições opacas e uso de trusts exigem diligência redobrada.

Na prática, mapeia-se a cadeia societária até chegar a pessoas físicas com percentual de controle ou influência significativa (limiares variam por regulação; adote critérios conservadores quando não houver norma específica). Defina o percentual mínimo de participação societária que a sua entidade vai adotar.

Quando a documentação é limitada, combine múltiplas fontes: registros mercantis, atas, divulgações regulatórias (como CVM/SEC), bases de beneficiários onde existirem, notícias e até declarações da própria contraparte com atestação.

Falhas em declarar UBO, resistência em compartilhar documentos e discrepâncias entre fontes são sinais que normalmente levam a EDD ou recusa no prosseguimento da relação.

A obrigação de identificar o beneficiário final recai sobre instituições sujeitas à prevenção à lavagem de dinheiro (PLD/FT), incluindo instituições que compõe o Sistema Financeiro Nacional[7].

### b. Listas Restritivas Internacionais

Sanções internacionais impõem proibições e restrições que podem atingir pessoas, empresas, estados e setores. O monitoramento de sanções deve ser diária ou em tempo real, com listas atualizadas e desambiguação de homônimos.

As listas restritivas e sancionatórias internacionais são bases de dados que reúnem nomes de indivíduos, empresas, organizações e até países que estão sujeitos a sanções impostas por governos, blocos econômicos ou organismos multilaterais. Essas sanções podem incluir bloqueio de ativos, restrições comerciais, proibição de viagens e limitações em transações financeiras.

Os principais sancionadores internacionais, definem listas e medidas restritivas que impactam diretamente a avaliação de contrapartes e a tomada de decisão em negócios transnacionais. São eles os principais:

- A Organização das Nações Unidas (ONU), por meio do seu Conselho de Segurança, pode aplicar sanções com caráter obrigatório para todos os Estados-membros. Essas medidas podem incluir embargos de armas, restrições econômicas, bloqueio de ativos e proibições de viagem, sendo geralmente adotadas para prevenir ou conter ameaças à paz e à segurança internacionais.

- O Escritório de Controle de Ativos Estrangeiros (OFAC), vinculado ao Departamento do Tesouro dos Estados Unidos, administra listas como a Specially Designated Nationals List (SDN), que identifica indivíduos e

[7] Circular 3978/2020: (...)
*"Art. 25. As instituições mencionadas no art. 1º devem estabelecer valor mínimo de referência de participação societária para a identificação de beneficiário final.*
*§ 1º O valor mínimo de referência de participação societária de que trata o caput deve ser estabelecido com base no risco e não pode ser superior a 25% (vinte e cinco por cento), considerada, em qualquer caso, a participação direta e a indireta."*

entidades com restrições de negócios. Essas sanções abrangem crimes como terrorismo, tráfico internacional de drogas, corrupção e proliferação de armas de destruição em massa, possuindo alcance extraterritorial e afetando empresas que utilizam o sistema financeiro norte-americano.

- A União Europeia (UE), através do Conselho da União Europeia, impõe sanções que podem abranger violações de direitos humanos, participação em conflitos armados e atividades que ameacem a paz regional ou global. Suas listas restritivas impactam não apenas empresas e cidadãos da UE, mas também organizações estrangeiras que realizem negócios com o bloco.

- Além desses, organizações regionais como a Organização dos Estados Americanos (OEA) também podem adotar sanções específicas para tratar de questões políticas, econômicas ou de segurança em suas áreas de atuação.

Para equipes de Compliance, monitorar essas fontes é uma etapa essencial na mitigação de riscos reputacionais, legais e financeiros.

Entre as mais conhecidas estão as listas da OFAC (EUA), ONU, União Europeia e HMT (Reino Unido). No contexto de due diligence digital, consultar essas listas é fundamental para evitar que a organização se envolva, direta ou indiretamente, com partes que representam riscos jurídicos e reputacionais elevados.

No processo de Customer Due Diligence (CDD) ou Vendor Due Diligence, a checagem contra listas restritivas serve como barreira inicial para identificar contrapartes que podem estar ligadas a crimes como lavagem de dinheiro, financiamento ao terrorismo, tráfico de drogas, corrupção ou violações de direitos humanos.

Por exemplo, um fornecedor pode estar operando legalmente em seu país, mas constar em uma lista internacional por envolvimento em comércio ilegal de armas — um risco que, se não detectado, pode expor a empresa contratante a sanções severas.

Além da consulta pontual no momento da contratação ou onboarding, boas práticas de due diligence incluem o monitoramento contínuo dessas listas. Isso porque elas são atualizadas com frequência, refletindo mudanças geopolíticas, decisões judiciais e investigações internacionais.

Ferramentas de *screening* automatizado permitem cruzar diariamente os dados de clientes, fornecedores e parceiros com listas restritivas globais, gerando alertas imediatos para que a área de Compliance adote medidas preventivas. Essa prática não apenas protege a organização de sanções, mas também reforça seu compromisso com a integridade e a conformidade regulatória.

Agora vamos às listas:

### i. Lista de Sanções do Conselho de Segurança da Organização das Nações Unidas (CSNU)

A ONU mantém um conjunto de listas de indivíduos, países, empresas e organizações que estão sujeitos a sanções impostas por decisão do Conselho de Segurança. Essas sanções podem incluir congelamento de ativos, proibição de viagens e embargos comerciais ou militares. A atualização dessas listas ocorre conforme resoluções aprovadas pelo Conselho de Segurança, geralmente em resposta a situações como terrorismo, proliferação nuclear, conflitos armados ou violações graves de direitos humanos.

No contexto de due diligence, a consulta a essa lista é obrigatória para todos os Estados-membros da ONU, o que significa que empresas que não a verificam podem acabar se envolvendo com contrapartes que são alvo de investigações internacionais e se expor a sanções legais e reputacionais.

O Conselho de Segurança das Nações Unidas possui autoridade para implementar medidas destinadas a preservar ou restabelecer a paz e a segurança internacionais, utilizando uma variedade de instrumentos que não envolvem o uso de força militar.

A Lista de Sanções da ONU é de acesso público, possibilitando que qualquer interessado verifique os registros e fundamentos das restrições impostas a indivíduos e entidades nela incluídos.

### ii. Lista de Sanções da União Europeia (UE)

A UE mantém a EU Consolidated List, uma base de dados de sanções que se aplica a todos os países-membros do bloco e inclui países, indivíduos, empresas e entidades sujeitas a medidas restritivas.

Essas sanções podem ser adotadas em alinhamento com as resoluções da ONU ou estabelecidas de forma independente pelo Conselho da União Europeia. Incluem medidas como congelamento de bens, restrições financeiras, proibição de fornecimento de determinados produtos e proibições de viagem.

Para empresas com operações, clientes ou fornecedores dentro do território europeu, o cumprimento dessa lista é essencial, pois as penalidades podem incluir multas pesadas e bloqueio de operações comerciais. Muitas multinacionais aplicam a verificação da lista da UE mesmo quando não estão legalmente obrigadas, como medida de proteção contra riscos reputacionais.

A verificação da Lista de Sanções da União Europeia pode ser feita diretamente nas fontes oficiais do bloco, que disponibilizam informações detalhadas sobre as medidas restritivas vigentes. Essa prática promove uma aplicação harmonizada das sanções entre os Estados-membros, fortalecendo a coerência das políticas de segurança e de cumprimento em toda a UE.

### iii. Lista da OFAC (EUA)

O Office of Foreign Assets Control (OFAC), órgão do Departamento do Tesouro dos Estados Unidos, administra e aplica sanções econômicas baseadas na política externa e segurança nacional dos EUA.

Sua lista mais conhecida é a SDN List (Specially Designated Nationals and Blocked Persons List), que reúne indivíduos, empresas, embarcações e aeronaves, com os quais cidadãos e empresas norte-americanas estão proibidos de manter relações comerciais.

Essas sanções possuem alcance extraterritorial, ou seja, podem afetar empresas fora dos EUA se houver uso do sistema financeiro americano ou transações em dólares. No *due diligence*, a checagem dessa lista é crítica, pois muitas instituições do Sistema Financeiro Nacional e corporações globais a utilizam como referência padrão.

A verificação na Lista de Sanções da OFAC que ameaçam as políticas de segurança nacional dos Estados Unidos, pode ser feita por meio da ferramenta de busca disponível no site oficial.

### iv. Lista de Entidades Bloqueadas da OFAC

Além da SDN List, a OFAC também mantém listas específicas de entidades bloqueadas por atividades como terrorismo, narcotráfico, tráfico de armas e proliferação de armas de destruição em massa. Essas listas adicionais podem incluir a Foreign Sanctions Evaders List (FSE), a Sectoral Sanctions Identifications List (SSI) e a Non-SDN Palestinian Legislative Council List (NS-PLC), entre outras.

Empresas que se relacionam com essas entidades podem sofrer penalidades mesmo que não haja uma proibição geral de comércio com o país onde elas atuam. Por isso, na due diligence, é fundamental não apenas verificar a SDN List, mas também todas as listas complementares administradas pela OFAC.

### v. Lista da Interpol

Fundada em 1923, a Interpol tem como objetivo integrar forças policiais de diferentes países para prevenir e combater a criminalidade transnacional. Sua Lista Internacional de Procurados reúne indivíduos com mandados de prisão em aberto, permitindo que as informações sejam compartilhadas de forma ágil entre os Estados-membros. No Brasil, essa função é coordenada pelo Escritório Central Nacional, operado pela Polícia Federal.

A consulta à Lista de Procurados da Interpol pode ser feita diretamente no site oficial da organização, onde é possível inserir dados como sobrenome, nome, nacionalidade, gênero, idade, país solicitante e até palavras-chave específicas.

### vi. Lista de Procurados pelo FBI

O Departamento Federal de Investigação dos Estados Unidos (FBI) mantém uma Lista de Procurados que reúne indivíduos foragidos ou com mandados de prisão ativos no país.

A consulta está disponível no site oficial do FBI, com opções de pesquisa por categorias como “10 fugitivos mais procurados”, “fugitivos”, “terrorismo”, “sequestro/pessoas desaparecidas” e “sequestro parental”. A busca pode ser aprimorada por meio de filtros como tipo de crime, nome do indivíduo ou ano de inclusão na lista.

### vii. Lista de HMT (Reino Unido)

No Reino Unido, o HM (His Majesty’s) Treasury, por meio do OFSI (Office of Financial Sanctions Implementation), é responsável pela aplicação de sanções financeiras. A UK (United Kingdom) Consolidated List of Sanctions reúne pessoas, empresas e embarcações sujeitas a congelamento de ativos e outras restrições.

Desde o Brexit, o país passou a gerenciar e atualizar suas próprias listas de forma independente, o que significa que elas podem divergir, total ou parcialmente, das listas da União Europeia. Empresas que atuam no Reino Unido ou mantêm relações comerciais com entidades britânicas devem seguir estritamente essas diretrizes, sob risco de multas elevadas e sanções criminais.

Essa política faz parte dos esforços do Reino Unido para contribuir com a paz e a estabilidade globais, mantendo alinhamento com metas e compromissos internacionais. A consulta à Lista de Sanções do Reino Unido é feita por meio das

plataformas oficiais do governo britânico, que disponibilizam informações atualizadas e detalhadas sobre as restrições vigentes.

### viii. Lista de PEPs

Pessoas Expostas politicamente (PEPs) estão sujeitas a medidas reforçadas de Due Diligence, que incluem verificações detalhadas sobre a origem dos recursos e o propósito das transações. Essa abordagem busca reduzir significativamente o risco de que pessoas com influência política usem o sistema financeiro para fins ilícitos.

É importante ressaltar que PEPs não são proibidas por si, mas exigem EDD, validação de origem de recursos e aprovações superiores. É uma checagem essencial, para identificar indivíduos que, devido a suas funções públicas ou relacionamento próximo com autoridades, apresentam maior risco de envolvimento em corrupção, lavagem de dinheiro ou outros ilícitos.

Essas listas incluem:

- Chefes de Estado e de Governo, ministros e vice-ministros;
- Membros do Congresso Nacional, Assembleias Legislativas e Câmaras Municipais;
- Governadores, prefeitos e seus vices;
- Altos dirigentes da administração pública, como presidentes e diretores de autarquias, fundações, empresas estatais e sociedades de economia mista;
- Membros do Poder Judiciário, do Ministério Público e dos Tribunais de Contas;
- Oficiais-generais das Forças Armadas.

A Resolução nº 40, publicada em 2021 pelo Conselho de Controle de Atividades Financeiras (COAF), define de forma clara e atualizada os cargos e funções que enquadram um indivíduo como Pessoa Exposta Politicamente (PEP) no Brasil. A identificação de PEPs não significa, por si só, que exista atividade ilícita, mas indica que a instituição deve aplicar procedimentos reforçados de verificação e monitoramento.

Essa classificação abrange diferentes níveis de poder, incluindo diversos escalões da União, e está alinhada a padrões internacionais de prevenção à lavagem de dinheiro e ao financiamento do terrorismo. A listagem contempla não apenas autoridades políticas, mas também outros agentes públicos com capacidade de influência em decisões administrativas, financeiras ou regulatórias.

No âmbito da identificação de PEPs, instituições financeiras, corretoras, seguradoras e demais entidades sujeitas à legislação de prevenção à lavagem de dinheiro são

obrigadas a verificar se seus clientes se enquadram nessa categoria. Essa análise não se restringe ao titular do cargo político ou público, mas se estende a familiares diretos e associados próximos, justamente para evitar que recursos ilícitos sejam movimentados por meio de terceiros (laranjas) ligados ao PEP.

Uma vez identificados, esses clientes passam a ter suas transações monitoradas com maior rigor. O objetivo desse acompanhamento contínuo é detectar movimentações atípicas ou suspeitas que possam indicar práticas como lavagem de dinheiro, ocultação de patrimônio ou financiamento do terrorismo. O monitoramento envolve desde a análise de grandes operações até a identificação de padrões irregulares de movimentação financeira.

Quando há indícios de atividades incomuns ou suspeitas, as instituições são legalmente obrigadas a reportar essas ocorrências ao órgão regulador. No Brasil, esse papel cabe ao próprio COAF, que centraliza, analisa e compartilha informações relevantes com autoridades competentes, podendo acionar investigações criminais, fiscais ou administrativas. O não cumprimento dessas obrigações pode acarretar penalidades severas às instituições envolvidas.

Por fim, as PEPs estão sujeitas a medidas reforçadas de Due Diligence, que incluem verificações detalhadas sobre a origem dos recursos e o propósito das transações. Essa abordagem busca reduzir significativamente o risco de que pessoas com influência política usem o sistema financeiro para fins ilícitos. Ao aplicar controles mais rígidos, as organizações contribuem para a integridade do sistema financeiro global, fortalecendo a confiança nos mercados e protegendo a sociedade contra crimes de alta complexidade e impacto.

Em uma boa prática de Due Diligence, a análise contra listas de PEPs e outras listas restritivas deve ser feita tanto no momento da entrada do cliente, fornecedor ou parceiro, quanto periodicamente durante o relacionamento comercial.

Isso se deve ao fato de que a condição de PEP ou a inclusão em listas sancionatórias pode ocorrer a qualquer momento, alterando significativamente o nível de risco associado. Para garantir efetividade, muitas empresas utilizam plataformas digitais de triagem (*screening*), que integram diversas bases nacionais e internacionais, permitindo consultas automatizadas, alertas em tempo real e relatórios detalhados para fins de Compliance.

### 7.9 Mídia adversa e reputação

A análise de mídia adversa é um componente estratégico que complementa as consultas a listas restritivas e sancionatórias no contexto de Due Diligence Digital e Background Check.

Essa abordagem vai além de bases oficiais e incorpora informações provenientes de investigações jornalísticas, registros de ações civis e criminais, sanções administrativas, litígios trabalhistas, infrações ambientais e falhas de governança corporativa.

➢ Exemplos:

- Reportagens sobre corrupção, fraude, lavagem de dinheiro ou cartel envolvendo a empresa ou seus dirigentes.
- Notícias de processos criminais, cíveis, ambientais ou trabalhistas.
- Sanções administrativas aplicadas por agências reguladoras.
- Investigações jornalísticas de fontes reconhecidas.
- Cobertura negativa de incidentes de governança ou gestão.

O grande desafio está em filtrar um volume cada vez maior de informações — frequentemente dispersas em múltiplos idiomas e publicadas em diferentes formatos — de modo a separar ruído informacional de sinais efetivos de risco reputacional e legal.

Uma boa prática para lidar com esse cenário é estabelecer taxonomias de risco claramente definidas, como corrupção, fraude contábil, formação de cartel, uso de trabalho análogo à escravidão, entre outros. Além disso, é fundamental delimitar janelas temporais adequadas para a análise, garantindo relevância e atualidade.

A seleção de fontes deve privilegiar veículos de comunicação de reconhecida credibilidade, publicações setoriais respeitadas e documentos oficiais, sempre ponderando o contexto e a confiabilidade da informação. Essa filtragem sistemática ajuda a reduzir vieses e a evitar a tomada de decisões baseadas em conteúdos frágeis ou não verificados.

No processo de uma due diligence digital, recomenda-se adotar uma metodologia robusta de captura e registro de evidências. Isso inclui armazenar links, realizar capturas de tela com data e hora, e documentar a origem da informação em relatórios de auditoria. Esses registros não apenas reforçam a transparência e a rastreabilidade do trabalho, mas também permitem avaliar a consistência das informações com a narrativa apresentada pela contraparte investigada.

Quando surgirem alegações ou reportagens negativas, o procedimento adequado envolve solicitar esclarecimentos formais à parte envolvida, possibilitando que apresente sua versão e documentação comprobatória.

Em situações nas quais existam ações judiciais em curso, é indispensável consultar diretamente os sites dos Tribunais de Justiça, verificar o estágio processual e identificar se há decisões relevantes já proferidas. Esse acompanhamento processual contribui para contextualizar os riscos e distinguir situações pontuais de padrões recorrentes de conduta. Sempre que possível, deve-se oferecer o direito de resposta,

garantindo imparcialidade na apuração e fortalecendo a integridade da avaliação de compliance.

### 7.10 OSINT – Open Source Intelligence

O uso de OSINT (Open Source Intelligence) como ferramenta no contexto de Due Diligence Digital e Background Check em Compliance oferece vantagens significativas, pois permite a coleta, análise e correlação de informações provenientes de fontes abertas e legalmente acessíveis.

Diferente de investigações clandestinas, o OSINT se baseia em dados públicos, disponíveis em meios digitais, impressos ou presenciais, disponíveis para análise e tomada de decisão, que podem incluir registros oficiais, mídias de comunicação, redes sociais e bancos de dados comerciais.

Essa abordagem proporciona às equipes de Compliance uma visão abrangente sobre a integridade, histórico e riscos potenciais associados a indivíduos ou empresas, auxiliando na tomada de decisões mais seguras e alinhadas com políticas internas e regulamentações externas.

Do ponto de vista ético e legal, o OSINT se diferencia por trabalhar apenas com informações obtidas de forma legítima, sem invasão de sistemas, violação de privacidade ou métodos ilegais de obtenção de dados.

As fontes oficiais e públicas no Brasil representam um dos pilares mais seguros para a aplicação de OSINT. Isso inclui, por exemplo:

- CPF/CNPJ na Receita Federal fornece os dados cadastrais;
- Juntas Comerciais disponibilizam contratos sociais e alterações;
- Tribunais (PJe e e-SAJ) permitem consulta a ações judiciais públicas;
- Conselho Nacional de Justiça (CNJ) e do Conselho Nacional do Ministério Público (CNMP) oferecem dados relevantes para verificação de processos e investigações em curso;
- Diário Oficial da União e diários estaduais/municipais divulgam atos oficiais, sanções administrativas e contratos;
- A CVM publica informações de companhias abertas e de participantes do mercado;
- O Banco Central divulga normativos e, em alguns casos, consultas a instituições autorizadas;
- Portais de transparência trazem despesas públicas e fornecedores;
- O TCU e CGU divulgam acórdãos, acordos de leniência e penalidades;
- Bases setoriais (ANVISA, ANTT, ANEEL, ANATEL) conforme o tipo de atividade.

Para contrapartes fora do Brasil, fontes internacionais e de mercado incluem por exemplo:

- Companies House no Reino Unido;
- Reguladores de valores mobiliários (SEC/EDGAR nos EUA, ESMA/AFM na UE);
- Listas de sanções (OFAC, UE, ONU, UK HMT https://www.gov.uk/government/organisations/hm-treasury);
- Bases de PEPs oficiais onde existentes, diários oficiais, além de listas de inidoneidade do Banco Mundial e outros bancos multilaterais;
- Bases abertas de organismos como a Interpol, Europol, Banco Mundial e FMI;
- Ferramentas abertas como a Wayback Machine, WHOIS e bases de patentes e marcas ajudam a confirmar histórico e propriedade intelectual;
- Pesquisas acadêmicas, relatórios de ONGs e investigações jornalísticas de veículos reputados complementam a visão.

Quando recorrer a provedores comerciais de screening e mídia adversa, valide cobertura, atualidade e qualidade dos dados, evitando dependência exclusiva de um único fornecedor para complementar a visão sobre riscos transnacionais e ajudar na identificação de ligações com atividades ilícitas ou jurisdições de alto risco.

As técnicas práticas de OSINT no Due Diligence Digital envolvem desde pesquisas avançadas em motores de busca até o uso de ferramentas especializadas para mineração de dados em redes sociais, agregadores de notícias e registros corporativos.

Além disso, é prática recomendada registrar todo o processo, com printscreens, URLs e datas de acesso, garantindo rastreabilidade e integridade das evidências coletadas.

Outro ponto relevante é que o OSINT possibilita detecção antecipada de riscos, uma vez que notícias, denúncias e registros podem surgir em fontes abertas muito antes de aparecerem em listas restritivas ou decisões judiciais definitivas. Essa capacidade proativa fortalece o papel do Compliance em prevenir relações comerciais com partes potencialmente envolvidas em corrupção, fraude, crimes ambientais ou violações de direitos humanos, evitando danos reputacionais e financeiros à organização.

Por fim, o uso de OSINT em Compliance exige uma abordagem responsável e contínua. Não basta realizar uma única investigação no momento da contratação; o monitoramento constante é essencial, especialmente em setores de alto risco ou em relações comerciais estratégicas.

Ao unir legalidade, rigor metodológico e uso inteligente de fontes abertas, esta ferramenta se consolida como indispensável para proteger a organização contra

riscos financeiros, regulatórios e reputacionais, ao mesmo tempo em que respeita a privacidade e os direitos fundamentais das pessoas investigadas.

Por fim, é essencial adotar uma abordagem ética, garantindo que o uso de dados em Compliance sirva unicamente para prevenir riscos, atender a obrigações regulatórias e preservar a integridade das operações, sem violar direitos fundamentais ou expor indevidamente os indivíduos analisados.

## 8. Gestão de Riscos em Due Diligence e Compliance

### 8.1 Risco cibernético de terceiros (Third Party Risk Management - TPRM) na due diligence

Com a crescente digitalização das cadeias de fornecimento, o risco cibernético associado a terceiros passou a ser um componente essencial nas análises de Due Diligence e Background Check corporativos.

Avaliar a postura de segurança da informação de um fornecedor vai muito além de verificar requisitos básicos de TI: é necessário compreender se ele possui um Sistema de Gestão de Segurança da Informação (SGSI) maduro, certificado por normas reconhecidas como a ISO 27001.

Essa avaliação deve considerar também a existência de relatórios de auditoria independentes, a realização periódica de testes de intrusão (pentests[8]), políticas claras de criptografia, gestão sistemática de vulnerabilidades, segregação adequada de ambientes e governança sólida de acesso.

Para tornar essa análise mais estruturada e comparável, organizações utilizam questionários padronizados. Esses instrumentos permitem levantar informações de forma consistente e facilitam a identificação de lacunas de segurança. Além dos questionários, a coleta de evidências documentais — como políticas internas, registros de auditorias e relatórios técnicos — é essencial.

O ideal é complementar essas informações com avaliações independentes conduzidas por especialistas, garantindo um panorama mais realista e menos suscetível a vieses de autoavaliação.

Quando o relacionamento envolve serviços críticos para a operação — por exemplo, provedores de nuvem, processamento de dados ou sistemas de missão crítica — é imprescindível estabelecer cláusulas contratuais específicas para proteção cibernética.

[8] Simulação controlada de um ataque cibernético com o objetivo de identificar e explorar vulnerabilidades em sistemas, redes, aplicativos ou infraestrutura de TI de uma organização.

Entre elas, podem constar obrigações de notificação imediata de incidentes, direitos de auditoria para o contratante, exigência de níveis mínimos de serviço (SLA - *Service Level Agreement*), bem como planos de continuidade de negócios e recuperação de desastres devidamente testados. Essas cláusulas devem ser redigidas de forma clara e objetiva, permitindo sua aplicação efetiva em caso de incidentes.

No cenário atual, em que ameaças cibernéticas evoluem rapidamente, contar apenas com avaliações pontuais não é suficiente. Por isso, empresas mais maduras adotam soluções de monitoramento contínuo da superfície de ataque de seus fornecedores, identificando em tempo real vulnerabilidades expostas, mudanças de configuração e indicadores de comprometimento.

Ferramentas capazes de rastrear vazamento de credenciais na dark web e redes clandestinas também oferecem uma camada extra de prevenção, permitindo ações proativas antes que um incidente se concretize.

Por fim, integrar a avaliação de risco cibernético de terceiros ao programa de Compliance e Due Diligence digital não apenas reduz a probabilidade de incidentes, mas também fortalece a resiliência operacional e a reputação corporativa. Empresas que tratam essa análise como parte central de sua estratégia de governança, risco e conformidade criam um ecossistema de fornecedores mais seguro, alinhado a padrões internacionais de proteção de dados e preparado para responder de forma ágil a ameaças emergentes.

### 8.2 Avaliação de Riscos e Red Flags

Toda due diligence, digital ou presencial, deve ter um componente de avaliação de risco. Isso envolve identificar e classificar red flags — sinais de alerta que indicam possíveis problemas.

A detecção precoce desses indicadores é fundamental para evitar que a organização se envolva com parceiros comerciais, fornecedores ou clientes que possam representar riscos financeiros, reputacionais ou legais. A abordagem deve ser sistemática, garantindo que nenhum ponto crítico seja negligenciado.

Red Flags comuns:

- Endereços de correspondência em paraísos fiscais, que podem sugerir práticas de evasão fiscal ou ocultação de patrimônio;
- Beneficiários finais não declarados ou ocultos, dificultando a identificação de quem realmente controla a operação;
- Histórico de processos trabalhistas e ambientais, que indicam fragilidades na gestão de conformidade;

- Mudanças frequentes na estrutura societária, que podem estar associadas a tentativas de diluir responsabilidades ou dificultar rastreamentos.

    ➢ Exemplo: Um fornecedor apresenta como endereço comercial um *coworking* que não possui atividades relacionadas ao produto ofertado. Esse é um red flag que exige investigação. Essa discrepância entre a estrutura declarada e a atividade real caracteriza um red flag claro. Nesses caso, é indispensável aprofundar a apuração, verificando se a empresa é genuinamente operacional ou apenas uma fachada para fins questionáveis, como triangulação comercial, ocultação de ativos ou fraude.

Outro aspecto essencial é o monitoramento contínuo. A due diligence não se encerra com a aprovação inicial de um parceiro. Mudanças societárias, inclusão em listas de sanções, abertura de novas investigações, alterações de beneficiários finais, notícias de fraudes, variações abruptas de volume de transações e comportamentos financeiros fora do perfil estabelecido são eventos que devem acionar uma reavaliação imediata. Esses “eventos gatilho” permitem que a instituição identifique e reaja rapidamente a riscos emergentes, evitando exposição prolongada.

Cada um desses pontos exige investigação detalhada para contextualizar e validar sua gravidade.

Por fim, a implementação de ferramentas de alerta automatizado, como monitoramento de mídia adversa e listas de sanções, associada a uma governança clara para tratamento de exceções, reduz significativamente a vulnerabilidade da organização.

É essencial documentar todas as decisões de manter, mitigar ou encerrar relacionamentos, justificando cada ação e assegurando aprovação hierárquica adequada.

### 8.3 Governança e abordagem baseada em risco

Um programa de governança eficaz deve iniciar-se a partir de políticas claras e formalmente aprovadas pela alta administração. Essas diretrizes devem estabelecer de forma precisa o escopo de aplicação, os papéis e responsabilidades de cada área envolvida, o apetite de risco institucional, os critérios para classificação das contrapartes e as obrigações relacionadas ao monitoramento contínuo.

Essa base normativa garante alinhamento entre as práticas operacionais e a estratégia corporativa, além de fornecer respaldo para decisões sensíveis.

A abordagem baseada em risco é o eixo central dessa estrutura, pois permite que a organização direcione seus recursos de forma proporcional à exposição potencial. Para isso, é essencial segmentar as contrapartes considerando variáveis críticas, como o setor de atuação, a jurisdição em que operam, o grau de exposição a transações em dinheiro, a utilização de intermediários, a complexidade da estrutura societária, a condição de Pessoa Exposta Politicamente (PEP), eventuais vínculos com listas de sanções e o histórico de menções na mídia, especialmente se negativas.

A partir dessa segmentação, cada faixa de risco deve ter níveis de diligência proporcionais, incluindo controles compensatórios como limites transacionais, exigência de dupla aprovação para determinadas operações e reforço de verificações documentais. Além disso, a periodicidade de revisão deve ser calibrada de acordo com o risco — por exemplo, revisões anuais para risco médio e semestrais para risco elevado. Esses ciclos de revalidação evitam que mudanças graduais passem despercebidas e protegem a organização contra riscos emergentes.

Por fim, é imprescindível prever gatilhos que determinem a reavaliação imediata de uma contraparte, como alterações no controle societário, variações abruptas de volume transacional, surgimento de notícias negativas ou mudanças significativas na legislação aplicável.

Todas as etapas do processo, incluindo decisões de aceitação condicionada ou recusa, devem ser registradas de forma auditável, com justificativas claras e documentação comprobatória. Esse registro robusto não apenas garante conformidade regulatória, mas também fortalece a capacidade de defesa da organização em caso de questionamentos internos ou externos.

## 9. Etapas práticas da Due Diligence

As etapas de uma boa due diligence podem ser organizadas em um fluxo claro, que integra planejamento, execução, análise e monitoramento.

### 9.1 Planejamento e Definição de Escopo

- Determinar o objetivo da due diligence (fornecedor, parceiro, cliente, investidor, funcionário-chave).

- Definir escopo (jurídico, financeiro, reputacional, operacional, cibernético, regulatório).

- Estabelecer abordagem baseada em risco (risk-based approach).
- Definir papéis e responsabilidades.

### 9.2 Coleta de Informações

- Solicitar documentos formais (contratos sociais, licenças, demonstrações financeiras, certidões).
- Utilizar fontes oficiais e registros públicos (Junta Comercial, Receita Federal, TSE, tribunais, diários oficiais).
- Empregar OSINT e pesquisa em fontes abertas confiáveis (mídia, bancos de dados, listas restritivas).
- No caso de Background Check, incluir verificação de identidade, histórico profissional e educacional, ações judiciais e mídia adversa.

### 9.3 Verificação em Listas Restritivas e Sanções

- Consultar listas de sanções (ONU, CSNU, OFAC, União Europeia, UK *Consolidated List*).
- Verificar listas nacionais (COAF, BACEN, CGU, CEIS/CNEP).
- Checar listas de Pessoas Expostas Politicamente (PEP).
- Registrar prints e evidências de todas as consultas.

### 9.4 Análise de Mídia Adversa e Reputação

- Buscar notícias, investigações, processos ou menções negativas.
- Separar fatos de rumores e identificar padrões.
- Priorizar veículos confiáveis e registros oficiais.
- Classificar riscos por gravidade (corrupção, fraude, crimes ambientais, etc.).

### 9.5 Avaliação de Aspectos Financeiros e Operacionais

- Analisar demonstrações financeiras e indicadores operacionais.
- Identificar red flags: margens irrealistas, caixa incompatível, dependência de um cliente, notas explicativas vagas.
- Verificar compliance fiscal e trabalhista.
- Validar certificações e licenças operacionais.

### 9.6 Avaliação de Segurança da Informação (Quando aplicável)

- Verificar maturidade em SGSI (ISO 27001, SOC 2).
- Checar políticas de segurança, criptografia, gestão de vulnerabilidades, segregação de ambientes.
- Confirmar existência de testes de intrusão e auditorias periódicas.

### 9.7 Entrevistas e Esclarecimentos

- Solicitar explicações formais sobre inconsistências ou red flags encontrados.
- Conceder direito de resposta e registrar todos os posicionamentos.

### 9.8 Relatório e Classificação Final

- Consolidar resultados em relatório claro e documentado.
- Classificar o risco (baixo, médio, alto).
- Recomendar manter, condicionar ou encerrar o relacionamento.
- Arquivar evidências e relatórios para auditoria.

### 9.9 Monitoramento Contínuo

- Definir periodicidade de revalidação por nível de risco.
- Configurar alertas de mídia adversa e listas restritivas.
- Estabelecer eventos gatilho para reavaliação (mudança societária, novas investigações, inclusão em sanções).

## 10. Conclusão

O avanço da tecnologia e a transformação digital alteraram profundamente a forma como empresas conduzem seus processos internos e externos. Entre essas mudanças, a due diligence digital se tornou um instrumento estratégico essencial para compliance, prevenção a ilícitos e tomada de decisão corporativa.

A due diligence digital é uma aliada indispensável para qualquer área de compliance. Ela reduz custos, acelera processos e amplia o alcance das investigações, mas deve ser combinada com análise humana crítica para evitar erros.

Boas práticas:

- Atualizar constantemente as fontes de dados;
- Capacitar equipes em ferramentas de OSINT;
- Documentar cada etapa do processo para fins de auditoria;
- Integrar due diligence ao monitoramento contínuo.

Em um cenário de crescente complexidade regulatória, transformação digital e exposição pública, conhecer profundamente contrapartes, fornecedores, clientes e parceiros não é apenas uma boa prática — é uma exigência estratégica e, muitas vezes, legal. A combinação de metodologias robustas, fontes confiáveis e abordagem baseada em risco permite que as organizações tomem decisões informadas e consistentes.

Ficou claro que, embora a Due Diligence Digital e o Background Check compartilhem fundamentos semelhantes, eles têm escopos e propósitos distintos. A primeira é mais ampla e multifacetada, voltada para empresas, cadeias de fornecimento e terceiros, enquanto o segundo é mais direcionado a indivíduos e dirigentes-chave, com foco em identidade, histórico e reputação. Em ambos, o uso inteligente de OSINT e de fontes oficiais é determinante para identificar riscos ocultos e evitar surpresas que possam gerar prejuízos financeiros, reputacionais ou jurídicos.

Também discutimos a importância da conformidade com normas como a LGPD, garantindo que a coleta, o tratamento e o armazenamento de dados pessoais sejam feitos dentro dos limites legais e éticos. A transparência, a rastreabilidade das evidências e o respeito aos direitos dos envolvidos fortalecem não apenas a conformidade regulatória, mas também a credibilidade e a reputação da organização.

Uma due diligence bem conduzida deve ser tanto rigorosa quanto justa, equilibrando a necessidade de proteção com o respeito à privacidade.

Outro ponto fundamental foi a percepção de que a due diligence não é um evento isolado, mas sim um processo contínuo. Monitoramento permanente, identificação de eventos gatilho e reavaliações periódicas são peças-chave para manter a proteção ativa e reduzir a janela de exposição a riscos. A governança, os critérios claros de classificação e a documentação cuidadosa de cada etapa garantem que o programa seja consistente, auditável e defensável perante órgãos reguladores e stakeholders.

Por fim, esperamos que este curso tenha fornecido não apenas conhecimento técnico, mas também a consciência de que diligências bem feitas são ferramentas de tomada de decisão estratégica. Implementados de forma consistente, eles permitem que a organização avance com segurança, preserve sua reputação, fortaleça relações comerciais e cumpra suas obrigações regulatórias. Mais do que cumprir requisitos, trata-se de cultivar uma cultura de integridade e vigilância que sustente o crescimento sustentável e a confiança no mercado.

---

## 11. Referências Bibliográficas


BANCO CENTRAL DO BRASIL. Circular nº 3.978, de 24 de junho de 2020. Disponível em: https://www.bcb.gov.br. Acesso em: 20 ago. 2025.

DEMINING, W. Edwards. *Out of the Crisis*. Cambridge: MIT Press, 1986.

Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 2018.