

# POLÍTICA DE GESTÃO DE FORNECEDORES E TERCEIROS

---



## **Diretrizes de Compliance, Anticorrupção, Integridade, Proteção de Dados Pessoais e Monitoramento de Terceiros**

Esta Política estabelece princípios, regras, responsabilidades e controles aplicáveis à seleção, homologação, contratação, gestão, monitoramento e desligamento de fornecedores, prestadores de serviços, representantes, consultores, intermediários, parceiros de negócio e quaisquer terceiros que atuem em nome, interesse ou benefício da Empresa.

Seu propósito é prevenir, detectar e remediar riscos de fraude, corrupção, conflito de interesses, lavagem de dinheiro, violações trabalhistas, ambientais e concorrenciais, falhas de segurança da informação e incidentes envolvendo dados pessoais, assegurando conformidade com a legislação aplicável, com o Código de Conduta e com as normas internas da Empresa.

## 1. Abrangência

---

Esta Política aplica-se a todos os administradores, sócios, diretores, empregados, estagiários e terceiros da Empresa envolvidos em solicitações de contratação, processos de compras, validação documental, negociação, gestão contratual, pagamentos, monitoramento, auditoria ou avaliação de fornecedores.

## 2. Fundamentos Normativos

---

- Lei nº 12.846/2013 (Lei Anticorrupção) e regulamentação aplicável;
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Legislação civil, societária, tributária, trabalhista, ambiental e concorrencial aplicável;
- Código de Conduta, Política Anticorrupção, Política de Privacidade e Segurança da Informação, Política de Conflito de Interesses e demais normas internas da Empresa.

## 3. Definições

---

Termo	Definição
Fornecedor ou terceiro	Pessoa física ou jurídica que fornece bens, executa serviços, representa interesses, intermedeia negócios ou apoia atividades da Empresa.
Due diligence	Procedimento de diligência prévia e periódica destinado a conhecer o terceiro, validar sua regularidade e avaliar riscos legais, reputacionais, de integridade, privacidade, segurança e sustentabilidade.
Red flags	Sinais de alerta que indiquem maior probabilidade de irregularidade, como estruturas societárias opacas, pagamentos atípicos, histórico sancionador, recusa em cooperar, interação sensível com agentes públicos ou incidentes de dados.
Dados pessoais	Informações relacionadas a pessoa natural identificada ou identificável, nos termos da LGPD.

## 4. Princípios gerais

---

- Legalidade, integridade, impessoalidade e transparência nos processos de contratação;
- Segregação de funções entre solicitação, validação, aprovação, contratação e pagamento;
- Proporcionalidade dos controles ao nível de risco do terceiro;
- Rastreabilidade documental, comprovação das decisões e preservação de evidências;
- Tolerância zero a corrupção, fraude, represálias, lavagem de dinheiro e uso indevido de dados pessoais..

## 5. Diretrizes de classificação de risco

---

Todo terceiro deverá ser classificado, no mínimo, em risco baixo, médio ou alto, considerando critérios objetivos e evidências documentais.

<b>Critério</b>	<b>Baixo</b>	<b>Médio</b>	<b>Alto / Crítico</b>
Interação com agentes públicos	Inexistente	Eventual e indireta	Frequente, estratégica ou em nome da Empresa
Tratamento de dados pessoais	Nenhum ou residual	Dados comuns e acesso limitado	Dados em volume relevante, sensíveis ou operações críticas
Natureza do serviço	Bem padronizado / serviço simples	Serviço técnico ou recorrente	Intermediação, representação, consultoria sensível, TI crítica
Estrutura e reputação	Regularidade comprovada	Algumas pendências saneáveis	Estrutura opaca, mídia negativa, sanções, PEP ou investigações
Valor e dependência	Baixo impacto	Impacto moderado	Contrato relevante ou alta dependência operacional

## 6. Processo de homologação e onboarding

### 6.1 Solicitação e justificativa

Toda contratação deverá ser precedida de solicitação formal pela área demandante, contendo escopo, justificativa comercial, valor estimado, prazo, descrição da criticidade do serviço e indicação de eventual tratamento de dados pessoais, uso de subcontratados ou interação com agentes públicos.

### 6.2 Cadastro mínimo

O fornecedor deverá apresentar, conforme aplicável, documentos societários, comprovante de inscrição fiscal, dados bancários em nome próprio, documentos de representação, licenças, certidões, referências, apólices, comprovação técnica, formulários de integridade e privacidade.

### 6.3 Due diligence proporcional

A diligência de integridade e de privacidade deverá ser compatível com o risco classificado, podendo incluir consultas a listas restritivas, sanções, pesquisa reputacional, beneficiário final, PEP, capacidade econômico-financeira, segurança da informação, histórico de incidentes e estrutura de compliance.

### 6.4 Aprovação em alçadas

Nenhum fornecedor poderá ser contratado ou pago sem que tenha sido devidamente aprovado nas alçadas definidas em norma interna, com participação obrigatória de Compliance e/ou Jurídico nos casos de risco médio ou alto.

## 7. Cláusulas contratuais obrigatórias

Os instrumentos contratuais deverão conter, no mínimo, cláusulas compatíveis com a natureza da contratação e com o nível de risco do terceiro.

Tema	Conteúdo mínimo
Integridade	Obrigações de observar a legislação aplicável, o Código de Conduta da Empresa e a vedação expressa a fraude, corrupção, superfaturamento, pagamentos indevidos, facilitação e ocultação de beneficiários.
Direito de auditoria	Faculdade de a Empresa solicitar documentos, evidências, certificações e realizar auditoria, diretamente ou por terceiro independente, quando houver justificativa razoável ou previsão contratual específica.
Subcontratação	Vedação ou condicionamento da subcontratação à autorização prévia e escrita, com extensão das obrigações de integridade, confidencialidade e LGPD à cadeia de subcontratados.
Confidencialidade e segurança	Proteção de informações confidenciais, obrigação de controles mínimos de segurança da informação, notificação tempestiva de incidentes e devolução/eliminação segura de documentos e dados.
LGPD	Cláusulas sobre papéis das partes, finalidade, instruções documentadas, base legal, medidas técnicas e administrativas, compartilhamento, retenção, descarte, cooperação com titulares e autoridades.
Rescisão	Hipóteses de suspensão e rescisão imediata ou motivada por violação de integridade, privacidade, segurança, sanções legais, negativa de cooperação ou omissão de informações relevantes.

## 8. Monitoramento contínuo e reavaliação

---

- Revalidação cadastral periódica e atualização de documentos críticos;
- Reanálise de integridade e privacidade em periodicidade compatível com o risco;
- Monitoramento de notícias adversas, sanções, incidentes de dados, mudanças societárias e uso de subcontratados;
- Avaliação de desempenho técnico, financeiro, comportamental e aderência contratual;
- Gatilhos de revisão extraordinária em caso de red flags, incidentes, investigações ou alteração relevante do escopo..

## 9. Red Flags

---

<b>Categoria</b>	<b>Exemplos de red flags</b>	<b>Resposta mínima esperada</b>
Integridade	Pedidos de pagamento em espécie, conta de terceiro, comissão excessiva, nota fiscal incompatível, recusa em informar sócios ou beneficiários finais	Suspender aprovação/pagamento até esclarecimento e documentação satisfatória
Poder público	Promessa de facilitação, alegação de relacionamento privilegiado, atuação perante autoridade em nome da Empresa sem autorização	Escalonar imediatamente a Compliance e Jurídico; revisar contratação
LGPD e segurança	Incidente de segurança, ausência de controles mínimos, compartilhamento indevido, armazenamento sem base legal	Acionar DPO/TI/Jurídico, conter exposição e avaliar obrigação de notificação
Reputação	Mídia negativa grave, investigação, sanção, trabalho análogo ao escravo, corrupção, dano ambiental relevante	Abrir apuração, avaliar contingência e eventual suspensão/rescisão

## 10. Pagamentos e Controles Financeiros

- Pagamentos apenas mediante fornecedor homologado, instrumento contratual válido, comprovação de entrega/medição e documentação fiscal idônea.
- Vedação de pagamento em espécie, para conta de terceiros, em jurisdição incompatível ou com descrição financeira desconectada do objeto contratado, salvo justificativa formal e aprovação especial;
- Proibição de fracionamento indevido de contratação ou despesa para contornar alçadas, due diligence ou controles internos;
- Retenção cautelar de pagamentos quando houver indício razoável de irregularidade, até conclusão da análise competente.

## 11. Canal de denúncias, investigações e não retaliação

A Empresa disponibilizará canal de denúncia acessível e, sempre que possível, independente, para recebimento de relatos envolvendo fornecedores e terceiros. É vedada qualquer forma de retaliação a denunciante de boa-fé. As apurações observarão confidencialidade, preservação de evidências, imparcialidade, segregação de funções e registro adequado das conclusões e medidas adotadas.

## 12. Papéis e responsabilidades

Área	Responsabilidades essenciais
Área demandante	Justificar contratação, definir escopo, acompanhar execução, validar entrega e reportar red flags.
Compras Suprimentos	Conduzir cadastro, cotação, documentação, alçadas e manter trilha de aprovação.
Compliance	Definir critérios de risco, realizar ou supervisionar due diligence, orientar controles e apurar sinais de integridade.
Jurídico	Revisar instrumentos contratuais, cláusulas críticas, conflitos, responsabilização e medidas de remediação.
DPO Privacidade TI	Avaliar tratamento de dados pessoais, requisitos de segurança, incidentes e medidas corretivas.
Financeiro	Executar pagamentos somente mediante evidências mínimas e observar bloqueios, retenções e anomalias.
Diretoria Comitês	Deliberar casos críticos, exceções justificadas, fornecedores de alto risco e medidas sancionatórias relevantes.

### **13. Medidas disciplinares e consequências contratuais**

---

O descumprimento desta Política poderá ensejar, conforme a gravidade do caso e a legislação aplicável, suspensão de cadastro, bloqueio de acesso, retenção cautelar de pagamentos, exigência de plano corretivo, descredenciamento, rescisão contratual, aplicação de penalidades previstas em contrato, reparação de perdas e danos e comunicação às autoridades competentes.

### **14. Disposições gerais**

---

Exceções a esta Política somente poderão ser admitidas de forma motivada, extraordinária e previamente aprovadas na alçada competente, com registro documental dos fundamentos, riscos, medidas compensatórias e prazo de revisão. Esta Política entra em vigor na data de sua aprovação e deverá ser revisada periodicamente ou sempre que houver alteração normativa, mudança material de risco ou necessidade de aprimoramento de controles.