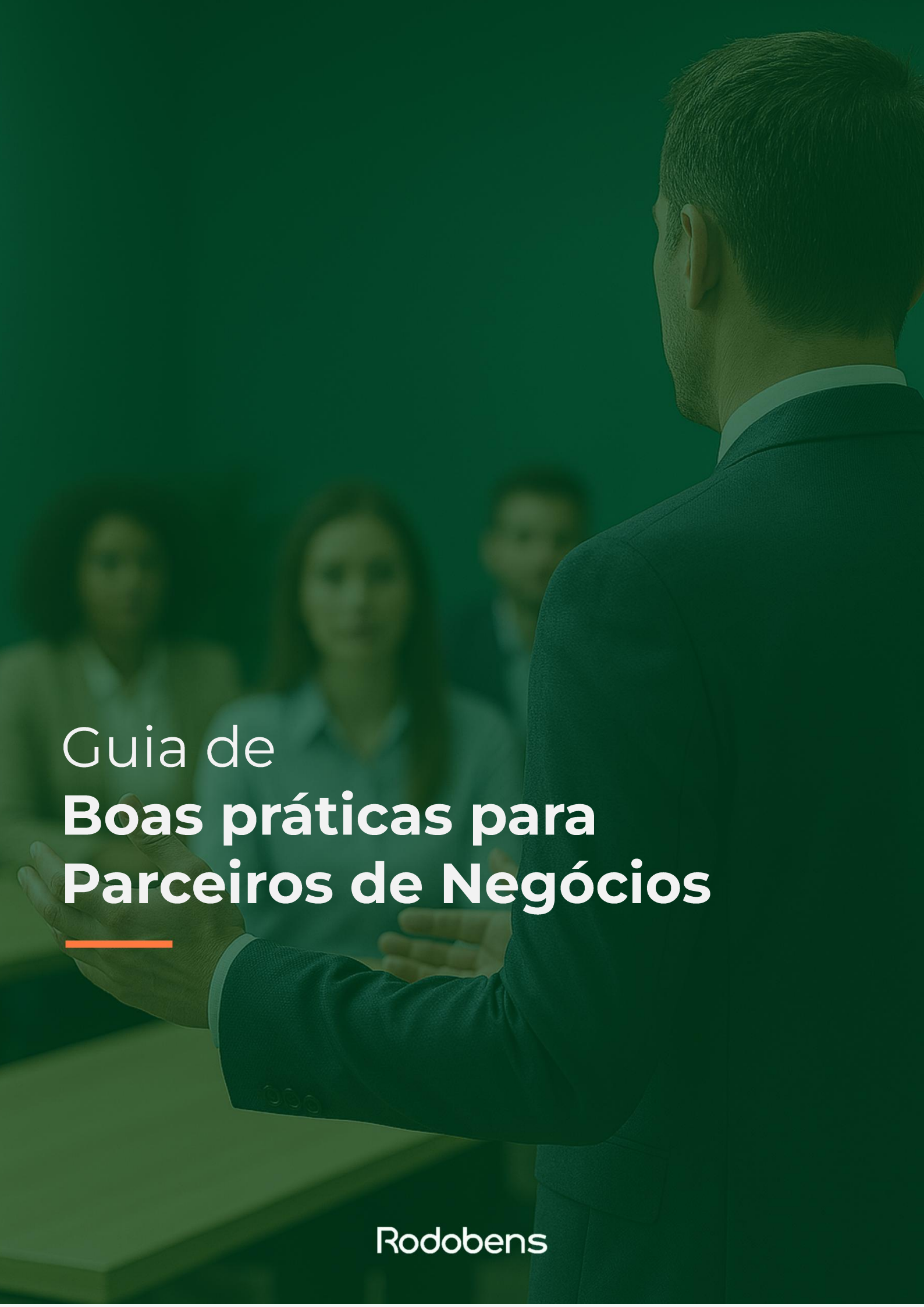


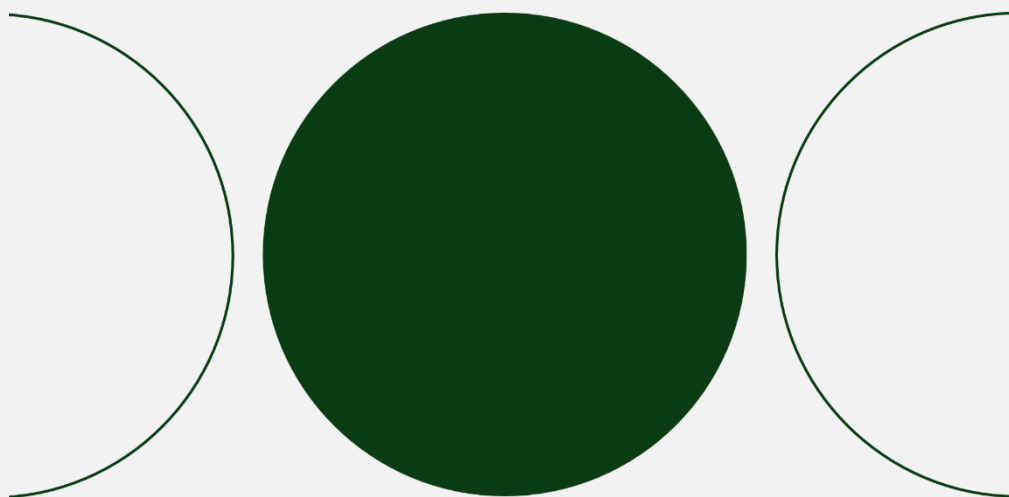
A man in a dark suit is seen from the back, gesturing with his hands as he presents to a group of people seated in the background. The scene is overlaid with a dark green semi-transparent filter.

Guia de **Boas práticas para Parceiros de Negócios**

Rodobens

Sumário

1. Apresentação.....	3
2. Objetivos.....	3
3. Público-alvo.....	3
4. Boas práticas de Ética.....	4
5. Boas práticas de segurança da informação e cibersegurança	5
6. Boas práticas de proteção de dados	9
7. Boas práticas sobre PLD/FT.....	11
8. Boas práticas para gestão de riscos operacionais.....	15
9. Capacitação e cultura.....	18
10. Conformidade e supervisão	18
11. Apoio e reporte	18
12. Canais de comunicação	19



1. Apresentação

Rodobens S/A, inscrita no CNPJ sob o nº 59.981.829/0001-65, estabelecida na Avenida Murchid Homsí, nº 1404, Bairro Vila Diniz, CEP: 15.013-000 e suas empresas controladas, disponibilizam este **Guia de Boas Práticas** para os seus parceiros de negócios sobre ética, segurança da informação e cibernética, proteção de dados pessoais, prevenção à lavagem de dinheiro e ao financiamento do terrorismo e gestão de riscos operacionais.

A Rodobens é um grupo econômico, composto por empresas atuantes nos ramos de consórcio, serviços financeiros, seguros, venda de automóveis novos, seminovos e veículos comerciais e locação de veículos, propiciando para seus clientes experiência diferenciada, com a oferta de múltiplas soluções de qualidade, segurança e tradição da marca.

Para conhecer mais sobre a Rodobens, consulte o site institucional www.rodobens.com.br.

2. Objetivos

O presente Guia tem como objetivos: **orientar** os parceiros de negócios acerca de temas relevantes ao relacionamento comercial estabelecido entre as partes e **proteger** informações, ativos, processos e a reputação da companhia.

Este documento apresenta informações de natureza contributiva e não exaustiva. Recomenda-se a consulta a especialistas para aprofundamento nos temas tratados e adequação ao segmento de atuação do parceiro de negócios.

3. Público-alvo

Este Guia de Boas Práticas é direcionado aos **Parceiros de Negócios da Rodobens**, assim considerados os **terceiros, pessoas físicas ou jurídicas**, com os quais a Rodobens mantém vínculo comercial, abrangendo **fornecedores, intermediários, distribuidores ou quaisquer outros que atuem, direta ou indiretamente, na cadeia de valor**, na promoção, comercialização, operacionalização ou viabilização de seus produtos e serviços.





4. Boas práticas de Ética

A Rodobens S/A estabelece padrões elevados de ética, integridade, transparência e conformidade em todos os seus relacionamentos comerciais. Nesse contexto, **espera-se que todos os Parceiros de Negócios cumpram integralmente os princípios, diretrizes e regras previstos no Código de Conduta Ética para Parceiros de Negócios**, documento normativo de observância obrigatória.

O Código de Conduta Ética para Parceiros de Negócios disciplina, de forma completa, os temas relacionados à ética e integridade, incluindo prevenção à corrupção e fraudes, conflito de interesses, assédio, relacionamento com o poder público, direitos humanos, meio ambiente, canais de denúncia e demais condutas esperadas. Esse Código é **formalmente disponibilizado aos Parceiros de Negócios no ato da contratação**, como condição para o estabelecimento e manutenção do relacionamento comercial, e permanece disponível para consulta no site institucional da Rodobens.

O presente Guia de Boas Práticas possui caráter **orientativo e complementar**, com foco no apoio aos Parceiros de Negócios quanto a boas práticas de segurança da informação, proteção de dados pessoais, prevenção à lavagem de dinheiro e ao financiamento do terrorismo, gestão de riscos operacionais, capacitação e reporte, **não substituindo nem se sobrepondo ao Código de Conduta Ética**.

O descumprimento das diretrizes éticas previstas no Código poderá ensejar a adoção das medidas contratuais, administrativas e legais cabíveis, conforme a gravidade do caso.



5. Boas práticas de segurança da informação e cibersegurança

Em conformidade com a ISO 27001, BACEN – Resolução CMN nº 4893/2021 e Lei 13.709/2018 (LGPD), que disciplinam segurança da informação e cibersegurança, espera-se que o parceiro de negócios tenha implementado ou implemente as medidas abaixo.

5.1. Governança e política de segurança

- a) Manter Política de Segurança da Informação e Cibernética formal, aprovada pela direção, compatível com o porte e riscos do parceiro, com foco em confidencialidade, integridade e disponibilidade.
- b) Definir objetivos, diretrizes e controles de segurança, incluindo prevenção e tratamento de incidentes e proteção de informações sensíveis.
- c) Designar um responsável por segurança/cibersegurança, com autoridade para implementar controles e responder a incidentes.
- d) Revisar e atualizar política e procedimentos periodicamente, documentando versões e mudanças.
- e) Disponibilizar a política para os seus colaboradores e terceirizados relevantes.

5.2. Gestão de riscos e inventário

- a) Inventariar ativos relevantes, como: sistemas, endpoints, servidores, redes, aplicações, dados, provedores e integrações.
- b) Classificar a informação por relevância/sensibilidade, por exemplo: pública, interna, restrita e confidencial e definir regras de proteção por classe.

- c) Avaliar riscos periodicamente, como ameaças, vulnerabilidades e impactos, priorizando o que pode afetar negativamente a Rodobens.

5.3. Controles técnicos essenciais

- a) Controle de acesso por necessidade, com revisão periódica de perfis e remoção imediata em desligamentos.
- b) Autenticação forte (como Múltiplo Fator de Autenticação) para acesso remoto, e-mails corporativos, painéis administrativos e sistemas críticos.
- c) Criptografia para dados sensíveis em trânsito (ex.: TLS) e, quando aplicável, em repouso (discos, bancos, backups).
- d) Proteção contra malware (antivírus).
- e) Segmentação de rede (separar ambientes críticos/servidores de usuários e convidados; limitar movimento lateral).
- f) Prevenção e detecção de intrusão (firewall bem configurado, IDS/IPS quando aplicável, bloqueios de brute force).
- g) Prevenção de vazamento de informação (controles de compartilhamento, restrições de mídia removível quando necessário, DLP conforme risco).
- h) Vulnerabilidade e patches: varreduras periódicas, correções em prazo definido (ex.: críticas com prioridade) e evidências de tratamento.
- i) Backups regulares, com testes de restauração e proteção contra Ransomware (backup imutável/offline quando possível).

5.4. Logs, rastreamento e monitoramento

- a) Habilitar logs e rastreabilidade para eventos relevantes (acessos, alterações, falhas de autenticação, operações administrativas e integrações).
- b) Reter logs por período definido (conforme criticidade e requisitos legais/contratuais) e proteger logs contra alteração.
- c) Monitorar alertas de segurança (contas privilegiadas, acessos fora do padrão, anomalias) e ter rotina de análise.

5.5. Gestão de incidentes

- a) Estabelecer Plano de Ação e Resposta a Incidentes, com papéis, contatos, fluxos e medidas de contenção/erradicação/recuperação.
- b) Manter registro e análise de causa/impacto de incidentes relevantes e controlar seus efeitos (inclusive incidentes em terceiros/subcontratados).
- c) Executar simulações/testes para validar a resposta a incidentes e melhorias contínuas.
- d) Notificar a Rodobens imediatamente quando houver incidente que possa afetar dados, sistemas ou serviços relacionados ao contrato.

5.6. Continuidade de negócios e recuperação

- a) Ter procedimentos documentados para interrupção de serviços relevantes (incluindo troca de fornecedor e restabelecimento).
- b) Definir RTO/RPO (tempo máximo de recuperação e perda aceitável de dados) para serviços que suportam o contrato.

5.7. Segurança em terceiros e subcontratações

- a) Avaliar previamente fornecedores críticos (principalmente TI/nuvem/processamento/armazenamento), verificando capacidade de garantir confidencialidade, integridade, disponibilidade e recuperação.
- b) Exigir controles equivalentes dos subcontratados que manuseiem informações ou serviços relevantes.
- c) Formalizar em contrato requisitos de segurança, confidencialidade, segregação de dados, notificação de incidentes e direito de auditoria/ evidências.
- d) Controlar subcontratação: exigir que o parceiro seja notificado e consiga controlar/avaliar subcontratações relevantes.

5.8. Serviço em nuvem

- a) Antes de contratar serviço em nuvem, o parceiro deve documentar a avaliação de riscos e a capacidade do provedor.
- b) Garantir segregação lógica/física de dados de clientes/contratantes e controles de acesso adequados.
- c) Garantir backup, recuperação e continuidade mesmo em caso de troca/encerramento do contrato, com cláusulas claras de portabilidade e eliminação segura.

5.9. Segurança no ciclo de desenvolvimento de sistemas

- a) Quando o parceiro de negócios desenvolver, customizar ou manter sistemas, aplicações ou integrações relacionadas aos serviços prestados à Rodobens, espera-se que adote práticas de desenvolvimento seguro, compatíveis com o porte, criticidade e risco da solução, incluindo, quando aplicável:
- b) Adoção de boas práticas de codificação segura durante o desenvolvimento e manutenção de sistemas;
- c) Avaliação de riscos de segurança em alterações relevantes de aplicações, integrações ou componentes tecnológicos;
- d) Controles para gestão de vulnerabilidades em aplicações, incluindo dependências, bibliotecas e componentes de terceiros;
- e) Correção tempestiva de falhas de segurança identificadas, conforme criticidade e impacto potencial;
- f) Segregação adequada entre ambientes (desenvolvimento, homologação e produção), quando aplicável.

- g)** Essas práticas visam reduzir riscos associados a falhas de aplicação, vulnerabilidades exploráveis e ataques à cadeia de suprimentos de software.

5.10. Testes periódicos de segurança

- a)** De forma proporcional à criticidade dos serviços, sistemas ou dados envolvidos, o parceiro de negócios deve realizar testes periódicos de segurança, com o objetivo de identificar vulnerabilidades técnicas e falhas de configuração, incluindo, quando aplicável:
- b)** Testes de intrusão (pentest) ou avaliações técnicas de segurança em sistemas críticos;
- c)** Realização de testes após mudanças relevantes de arquitetura, tecnologia ou exposição externa;
- d)** Registro dos achados identificados e definição de plano de ação para tratamento e mitigação das vulnerabilidades;
- e)** Manutenção de evidências ou relatórios executivos dos testes realizados, para apresentação quando solicitado pela Rodobens.
- f)** Os testes de segurança contribuem para a identificação proativa de fragilidades e para o fortalecimento contínuo da postura de segurança da informação.



6. Boas práticas de proteção de dados

Em conformidade com a Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), espera-se que o parceiro de negócios tenha implementado ou implemente as medidas abaixo:

6.1. Conformidade legal e transparência

- a) Tratar dados pessoais somente para finalidades legítimas, específicas e informadas, compatíveis com o contrato ou relação comercial.
- b) Garantir que todo tratamento esteja amparado por hipótese autorizadora prevista na LGPD.
- c) Não tratar os dados para finalidades diferentes daquelas previamente alinhadas com a Rodobens.
- d) Implementar procedimentos para informar o titular dos dados acerca das possíveis formas de tratamento dos seus dados pessoais, por meio de cláusulas contratuais ou políticas de privacidade disponibilizadas no website.

6.2. Governança e responsabilidades

- a) Designar um responsável interno pelo tema de proteção de dados.
- b) Manter políticas ou diretrizes internas sobre privacidade e proteção de dados.
- c) Garantir que colaboradores e terceiros conheçam e cumpram essas diretrizes.

6.3. Minimização e qualidade dos Dados

- a) Coletar e tratar apenas os dados estritamente necessários para a finalidade pretendida.
- b) Manter os dados atualizados, corretos e relevantes.

- c) Eliminar ou anonimizar dados pessoais quando deixarem de ser necessários.

6.4. Prevenção e segurança

- a) Adotar medidas técnicas e administrativas mínimas para proteger os dados pessoais contra acessos não autorizados, vazamentos, perdas ou alterações indevidas.
- b) Controlar o acesso aos dados, garantindo que apenas pessoas autorizadas possam utilizá-los.
- c) Proteger dados pessoais armazenados e transmitidos, especialmente quando sensíveis.

6.5. Compartilhamento e uso por terceiros

- a) Compartilhar dados pessoais somente quando necessário, de forma compatível com a finalidade original e desde que não viole o contrato estabelecido com a Rodobens.
- b) Realizar avaliações de maturidade em proteção de dados e segurança da informação dos terceiros antes do compartilhamento de informações, bem como em revisões periódicas.
- c) Exigir que subcontratados ou terceiros adotem padrões equivalentes de proteção de dados.
- d) Formalizar obrigações de confidencialidade e proteção de dados nos contratos com terceiros.

6.6. Direitos dos titulares

- a) Estar preparado para atender solicitações de titulares, como acesso, correção, exclusão ou informação sobre o uso de seus dados.
- b) Cooperar com a Rodobens sempre que houver demandas relacionadas a direitos de titulares envolvendo dados tratados na parceria.
- c) Responder às solicitações dentro de prazos razoáveis e legais.

6.7. Incidentes de segurança

- a) Manter procedimentos para identificar, tratar e registrar incidentes envolvendo dados pessoais.
- b) Comunicar imediatamente à Rodobens qualquer incidente de segurança que possa afetar dados pessoais relacionados à parceria.
- c) Adotar medidas para mitigar danos e evitar reincidências.

6.8. Retenção e descarte de dados

- a) Definir prazos de retenção compatíveis com a finalidade e obrigações legais.
- b) Garantir o descarte seguro dos dados pessoais ao final do prazo ou da relação contratual.
- c) Evitar a manutenção indefinida de dados sem justificativa legal ou operacional.



7. Boas práticas sobre PLD/FT

Em conformidade com a **Lei nº 9.613/1998** de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLDFT) , bem como as normas específicas do Banco Central do Brasil (BACEN) – **Resolução BCB nº 119 de 27/7/2021**, da Superintendência de Seguros Privados (SUSEP) – **Circular SUSEP nº 612/2020**, e do Conselho de Controle de Atividades Financeiras (COAF) – **Resolução COAF nº 25/2013** e **Resolução COAF nº 36/2021**, espera-se que o parceiro de negócios tenha implementado ou implemente as medidas abaixo:

7.1. Compromisso com PLD/FT

- a) Atuar de forma ética e diligente na prevenção à lavagem de dinheiro e ao financiamento do terrorismo.
- b) Cumprir as orientações e procedimentos definidos pela Rodobens para PLD/FT.
- c) Não facilitar, direta ou indiretamente, operações suspeitas ou irregulares.

7.2. Identificação e conhecimento do cliente

- a) Coletar **informações completas, corretas e atualizadas** dos clientes no momento da contratação.
- b) Confirmar a identidade do cliente por meio de **documentos válidos e legíveis**.
- c) Verificar a **coerência das informações fornecidas** (ex.: renda, atividade profissional, endereço).
- d) Identificar o **beneficiário final de pessoa jurídica**, quando aplicável.

7.3. Identificação e conhecimento do colaborador

- a) Implementar o processo conheça o seu colaborador, tendo em vista a possibilidade de seu envolvimento, intencionalmente ou não, como meio para prática de ilícitos, especialmente em áreas críticas ou de relacionamento com clientes.
- b) Identificar adequadamente o colaborador, no momento da admissão, com coleta de dados e documentos básicos e manter o seu cadastro atualizado.
- c) Analisar a integridade e risco, considerando histórico profissional, vínculos relevantes e eventual exposição a riscos (ex.: acesso a informações sensíveis ou recursos financeiros).
- d) Classificar as funções conforme o risco apresentado.
- e) Monitorar continuamente os colaboradores, com reavaliações periódicas ou quando houver mudança de função, área ou indícios de comportamento atípico.

7.4. Situações atípicas (suspeitas de lavagem de dinheiro)

Confira a seguir algumas situações que podem indicar algo suspeito na relação com o **cliente**:

- a) Dados cadastrais difíceis de checar ou que não batem com fontes públicas.
- b) Pagamentos em dinheiro vivo, pagamentos realizados por terceiros ou em valores fracionados.
- c) Renda ou patrimônio incompatível com os pagamentos.
- d) Procurador representa várias empresas, sem explicação clara.

Na sequência, exemplos práticos de situações atípicas, que acendem o alerta de suspeita de lavagem de dinheiro.

Na Consórcio:

- a) Aumento expressivo do número de cotas pertencentes a um mesmo consorciado.
- b) Oferecimento de lances muito próximos ao valor do bem.
- c) Pagamento antecipado de quantidade expressiva de prestações vincendas ou de lance, não condizentes com a capacidade financeira do consorciado.

No Banco:

- a) Financiamento quitado antecipadamente ou em prazo muito curto.
- b) Aquisição de diversos veículos sem vínculo com a atividade econômica explorada pela empresa.
- c) Inúmeras contratações de financiamentos semelhantes.

Na Seguros:

- a) Mudança do titular do negócio ou bem anterior ao sinistro.

- b) Avisos de sinistros aparentemente legítimos, mas com frequência anormal.
- c) Apólices em nome de terceiros sem vínculo familiar.

E no Varejo Automotivo:

- a) Pagamentos em espécie superior a R\$30.000,00, no período de seis meses.
- b) Compra de veículo por pessoas física ou jurídica que não possui capacidade financeira para tal.
- c) Veículo adquirido com dinheiro de terceiro.

Não é preciso ter certeza de que há crime. Basta que a operação seja fora do comum ou sem justificativa plausível.

7.5. Coleta e envio de informações

- a) Garantir que todas as informações e documentos coletados sejam **enviados integralmente e sem alterações** para a Rodobens.
- b) Não **omitir, ajustar ou “simplificar”** informações para viabilizar a contratação.
- c) Assegurar que os dados coletados reflitam a **real situação do cliente**.

7.6. Proibição de condutas irregulares

- a) Não orientar o cliente a **fragmentar valores**, utilizar terceiros ou adotar qualquer prática para evitar controles.
- b) Não aceitar **documentos falsos**, incompletos ou sabidamente irregulares.
- c) Não realizar **operações em nome de terceiros**, sem prévia e expressa autorização.
- d) Não inserir **informações próprias ou de terceiros** no cadastro do cliente.
- e) **Não assinar documentos**, se passando pelo cliente.

7.7. Comunicação de suspeitas

- a) Comunicar **imediatamente à Rodobens** qualquer indício ou suspeita de lavagem de dinheiro ou financiamento do terrorismo.
- b) Utilizar os **canais indicados pela Rodobens** para reporte de situações atípicas.
- c) Manter **sigilo** sobre comunicações realizadas, não alertando o cliente ou terceiros.

7.8. Nomenclatura e apresentação ao público

- a) Utilizar em sua nomenclatura apenas termos que remetam claramente às atividades que efetivamente exerce, evitando palavras que indiquem modalidade ou atividade para a qual não possui autorização.

- b)** Não empregar termos que possam sugerir atividade não autorizada, especialmente quando tal expressão seja típica de instituição regulada (ex. Administradora de Consórcio, Banco)
- c)** Caso altere sua nomenclatura no decorrer do contrato, o parceiro deve comunicar a Rodobens.
- d)** Em domínios de internet, canais e materiais digitais, manter coerência com o escopo real da atuação, evitando qualquer indicação que gere confusão com instituições autorizadas pelo Banco Central.
- e)** Evitar qualquer formulação que possa confundir o cliente, transmitindo a impressão de pertencer a estrutura da Rodobens, reportando-se como parceiro.



8. Boas práticas para gestão de riscos operacionais

Em conformidade com o BACEN – Resolução nº 4557/2017 e CNSP – Resolução nº 382/2020, que regulam gestão de riscos operacionais, espera-se que o parceiro de negócios tenha implementado ou implemente as medidas abaixo:

8.1. O que são riscos operacionais

Riscos operacionais são eventos ou falhas que podem ocorrer em razão de:

- a) **Pessoas:** erro humano, conduta inadequada, falta de capacitação, má-fé;
- b) **Processos:** falhas operacionais, ausência de controles, descumprimento de procedimentos;
- c) **Sistemas e tecnologia:** indisponibilidade, falhas de segurança, uso inadequado de sistemas;
- d) **Eventos externos:** fraudes, incidentes cibernéticos, mudanças regulatórias, terceiros subcontratados.
- e) **Eventos climáticos:** como enchentes e tempestades podem atrasar entregas, prejudicar visitas técnicas e causar danos a documentos ou mercadorias de fornecedores terceirizados.
- f) **Falhas em recursos essenciais:** ausência de gerador de energia, internet redundante ou infraestrutura adequada.

Esses riscos podem surgir tanto na **atividade comercial** quanto na **prestação de serviços em geral**.

8.2. Importância da gestão de riscos

A adequada gestão de riscos operacionais é essencial para:

- a) Proteger os clientes e a própria Rodobens;
- b) Evitar responsabilização legal, regulatória ou contratual;

- c) Prevenir perdas financeiras e operacionais;
- d) Reduzir riscos de incidentes de segurança da informação e dados pessoais;
- e) Preservar a imagem e a credibilidade da Rodobens e do próprio parceiro;
- f) Garantir a manutenção da relação comercial.

Falhas operacionais de terceiros podem gerar impactos relevantes à Rodobens, mesmo quando não intencionais.

8.3. Principais Riscos Operacionais na Atuação de Terceiros

Exemplos de riscos operacionais aplicáveis a parceiros comerciais:

Na venda e relacionamento com clientes

- a) Informações incorretas, incompletas ou enganosas sobre produtos.
- b) Promessas comerciais fora das regras contratuais.
- c) Formalização inadequada de propostas e contratos, inclusive quando baseada em informações cadastrais genéricas, incorretas ou sem vínculo com o cliente.
- d) Atendimento inadequado ou não documentado.

Na prestação de serviços e fornecimento de produtos

- a) Execução do serviço em desacordo com o contrato.
- b) Uso indevido da marca Rodobens.
- c) Subcontratação não autorizada.
- d) Atrasos ou falhas na entrega de serviços ou soluções.

Em tecnologia, dados e informação

- a) Falhas de segurança da informação.
- b) Vazamento ou uso indevido de dados pessoais ou sigilosos.
- c) Acesso indevido a sistemas da Rodobens.
- d) Ausência de controles de continuidade e contingência.

Em aspectos legais e éticos

- a) Descumprimento de leis e regulamentos.
- b) Conflitos de interesse não declarados.
- c) Condutas que possam caracterizar fraude, corrupção ou irregularidades.

8.4. Identificação dos riscos

É importante que o parceiro de negócio identifique os riscos presentes em sua operação e no relacionamento estabelecido com a Rodobens.

Qualquer situação que **possa causar impacto negativo à Rodobens, aos clientes ou ao próprio parceiro** deve ser considerada um risco operacional.

8.5. Registro dos riscos

Os riscos identificados devem ser **registrados internamente pelo parceiro**, de forma clara e rastreável, contendo, sempre que possível:

- a) Descrição do risco.
- b) Atividade, processo ou serviço afetado.
- c) Causas identificadas.
- d) Impactos potenciais (operacional, financeiro, legal, reputacional).
- e) Medidas de controle existentes.
- f) Ações corretivas ou preventivas propostas.

O registro é uma evidência de diligência e compromisso com boas práticas de governança.

8.6. Tratamento e mitigação de riscos

Após o registro, o risco deve ser tratado de maneira proporcional à sua relevância, por meio de:

- a) Correção tempestiva de falhas identificadas.
- b) Revisão de processos, fluxos e controles.
- c) Reforço de controles tecnológicos e de segurança da informação.
- d) Revisão de contratos ou procedimentos internos.



9. Capacitação e cultura

- a) Capacitar seus colaboradores em ética, segurança da informação e cibersegurança, proteção de dados, PLD/FT e riscos operacionais.
- b) Garantir que todos conheçam suas responsabilidades.
- c) Promover cultura de prevenção, ética e reporte de irregularidades.
- d) Assegurar compromissos formais de confidencialidade e integridade.

10. Conformidade e supervisão

- a) Atender às políticas, normas e diretrizes da Rodobens aplicáveis.
- b) Disponibilizar informações e evidências quando solicitadas.
- c) Submeter-se a auditorias, avaliações ou verificações, conforme previsto contratualmente.
- d) Implementar planos de ação para correção de não conformidades.

11. Apoio e reporte

O parceiro comercial deve fornecer informações completas e rápidas para que a Rodobens possa se defender em processos judiciais ou administrativos.

Eventuais riscos operacionais, incidentes de segurança, infrações éticas ou questões relacionadas à PLD/FT que possam impactar o relacionamento com a Rodobens devem ser reportados de imediato, ainda que não tenham se concretizado. Essa colaboração reduz riscos, assegura conformidade e mantém a confiança entre as partes.



12. Canais de comunicação

Caso seja necessário abordar temas discutidos neste Guia, entre em contato com a Rodobens por meio dos canais indicados abaixo.

Canal de denúncias:

- **Site:** <https://canaldedenuncia.com.br/empresasrodobens>
- **Telefone:** 0800 591 2354
- **E-mail:** rodobens@canaldedenuncia.com.br

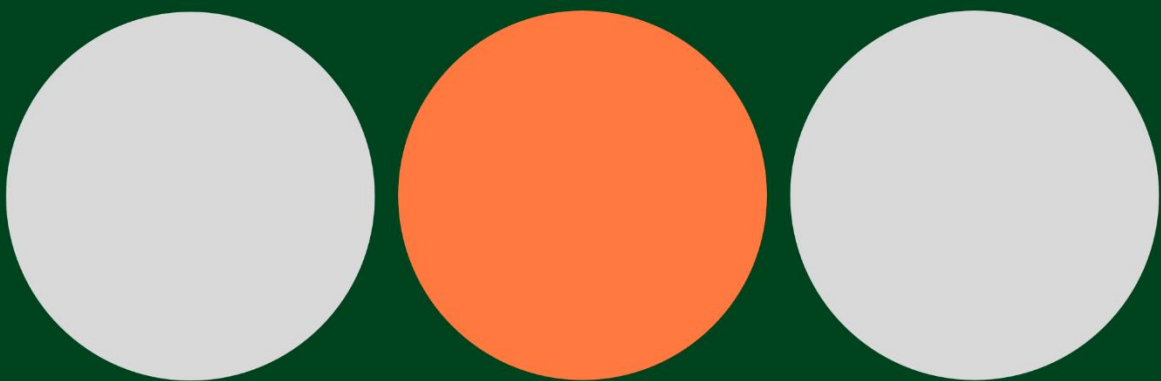
Segurança e proteção de dados

- **Email:** protecaodados.compliance@rodobens.com.br

Ética e PLDFT

- **E-mail:** compliance@rodobens.com.br

Rodobens



www.rodobens.com.br