

Política de Gestão de Riscos

Versão 1.0

CÓDIGO	VERSÃO	APROVAÇÃO	REVISÃO
3K-POL-004	1.0	Diretoria	Anual

1. Objetivo

Esta Política estabelece os princípios, a estrutura e o processo de gestão de riscos da **3K BUSINESS LTDA** ("**3K Business**"), com o objetivo de identificar, avaliar, tratar e monitorar os eventos que possam afetar seus objetivos, seus clientes, a continuidade de suas operações e sua reputação.

2. Abrangência

Aplica-se a todas as atividades, projetos, produtos, sistemas e processos da 3K Business, bem como a sócios, administradores, colaboradores e prestadores de serviços.

3. Referências

- ABNT NBR ISO 31000:2018 — Gestão de riscos: diretrizes;
- ABNT NBR ISO/IEC 27001 e 27005 — segurança da informação e gestão de riscos de segurança da informação;
- Lei nº 13.709/2018 (LGPD) e Lei nº 12.846/2013 (Lei Anticorrupção).

4. Princípios

- A gestão de riscos é integrada às decisões de negócio, ao planejamento e à execução dos projetos;
- As decisões consideram as melhores informações disponíveis e são documentadas;
- Todo risco relevante tem um responsável (dono do risco) designado;
- O processo é contínuo, proporcional ao porte da empresa e melhorado a partir das lições aprendidas.

5. Categorias de risco

Categoria	Exemplos
Estratégico	Concentração de receita em poucos clientes; mudanças de mercado ou de tecnologia.

Categoria	Exemplos
Operacional	Falhas de processo, atrasos de entrega, dependência de pessoas-chave.
Tecnológico e cibernético	Indisponibilidade de sistemas, vulnerabilidades, ataques, perda de dados.
Proteção de dados	Tratamento inadequado ou vazamento de dados pessoais de clientes e usuários finais.
Legal e regulatório	Descumprimento contratual, legal ou regulatório; mudanças na legislação.
Integridade	Lavagem de dinheiro, financiamento do terrorismo, corrupção e fraude.
Financeiro	Inadimplência de clientes, falta de liquidez, fraude em pagamentos.
Terceiros	Falhas ou descontinuidade de provedores de nuvem, hospedagem, APIs e demais fornecedores.
Reputacional	Associação da marca a clientes, incidentes ou práticas inadequadas.

6. Processo de gestão de riscos

6.1. Identificação

Os riscos são identificados na análise de novos clientes e projetos, na contratação de fornecedores, em mudanças relevantes de sistemas e processos, na análise de incidentes e na revisão periódica do Registro de Riscos.

6.2. Análise

Cada risco é analisado segundo a **probabilidade** de ocorrência e o **impacto** caso ocorra, ambos em escala de 1 a 5. O nível de risco é o produto dos dois fatores (de 1 a 25).

Nota	Probabilidade	Impacto
1	Rara — improvável nos próximos anos	Insignificante — sem efeito perceptível para clientes
2	Improvável — pode ocorrer em alguns anos	Menor — efeito pontual, resolvido internamente
3	Possível — pode ocorrer no ano	Moderado — afeta clientes ou prazos de forma limitada
4	Provável — deve ocorrer no ano	Maior — perda financeira relevante, dados expostos ou indisponibilidade prolongada
5	Quase certa — ocorre com frequência	Severo — compromete a continuidade, gera sanção legal ou dano reputacional grave

6.3. Avaliação

Nível	Pontuação	Resposta exigida
Baixo	1 a 4	Aceitar e monitorar na revisão periódica.

Nível	Pontuação	Resposta exigida
Moderado	5 a 9	Plano de tratamento definido em até 90 dias.
Alto	10 a 16	Plano de tratamento em até 30 dias e reporte à Diretoria.
Crítico	20 a 25	Ação imediata, decisão da Diretoria e acompanhamento até a redução do nível.

6.4. Tratamento

Para cada risco acima do nível baixo, o dono do risco define uma ou mais respostas:

- **Evitar:** não realizar a atividade que gera o risco (por exemplo, recusar um cliente);
- **Mitigar:** implementar controles que reduzam a probabilidade ou o impacto;
- **Transferir:** compartilhar o risco por meio de contratos, seguros ou fornecedores especializados;
- **Aceitar:** manter o risco de forma consciente, com aprovação registrada da Diretoria quando o nível for alto ou crítico.

6.5. Monitoramento e análise crítica

O Registro de Riscos é revisado ao menos **semestralmente** e sempre que ocorrer incidente, mudança relevante no negócio ou novo requisito legal. A eficácia dos controles é verificada e os níveis são reavaliados.

6.6. Registro e comunicação

Os riscos são mantidos em um Registro de Riscos que contém, no mínimo: identificação, descrição, categoria, causas, consequências, probabilidade, impacto, nível, dono do risco, controles existentes, plano de tratamento, prazo e situação. Os riscos altos e críticos são reportados à Diretoria.

7. Principais riscos e controles

Risco	Principais controles
Indisponibilidade de sistemas mantidos para clientes	Monitoramento e observabilidade das aplicações, alertas, backups e procedimentos de restauração.
Vazamento ou acesso indevido a dados	Controles da <u>Política de Segurança da Informação</u> : acesso mínimo, autenticação multifator, criptografia e gestão de segredos.
Relação com cliente envolvido em ilícitos	<u>KYC</u> , autodeclaração de PEP, consulta da instituição parceira a listas restritivas e PEP, <u>monitoramento de PLD/FT</u> .
Fraude em pagamentos ou troca de dados bancários	Confirmação de alterações por canal independente e conferência de titularidade das contas.
Dependência de pessoas-chave	Documentação técnica, repositórios centralizados e compartilhamento de conhecimento entre a equipe.
Falha de fornecedor de nuvem ou infraestrutura	Avaliação prévia de fornecedores, backups em local distinto e plano de recuperação.

Risco	Principais controles
Inadimplência	Análise do cliente no onboarding, marcos de pagamento contratuais e acompanhamento financeiro.

8. Gestão de riscos de terceiros

Fornecedores que tratem dados de clientes ou que sejam críticos para a operação são avaliados antes da contratação quanto a integridade, segurança da informação e continuidade, e os contratos contêm cláusulas de confidencialidade, proteção de dados e responsabilidades. A avaliação é revista periodicamente.

9. Continuidade de negócios

A 3K Business mantém procedimentos para responder a incidentes e recuperar os serviços críticos, incluindo backups periódicos com testes de restauração, documentação dos ambientes e definição de responsáveis e canais de comunicação com clientes.

10. Governança e responsabilidades

- **Diretoria:** aprova esta Política, define o apetite a risco, decide sobre riscos altos e críticos e provê recursos para o tratamento;
- **Responsável por Riscos e Compliance:** coordena o processo, mantém o Registro de Riscos, acompanha os planos de tratamento e reporta à Diretoria;
- **Donos de risco (líderes técnicos e gestores de projeto):** identificam, avaliam e tratam os riscos de suas áreas e implementam os controles;
- **Colaboradores:** cumprem os controles e comunicam imediatamente riscos, falhas e incidentes.

As funções de Responsável por Compliance e PLD/FT, por Riscos e por Segurança da Informação podem ser exercidas pela mesma pessoa, conforme designação formal da Diretoria, de modo compatível com o porte da empresa.

11. Vigência e revisão

Esta Política entra em vigor na data de sua aprovação pela Diretoria e é revisada ao menos anualmente, ou antes, sempre que houver mudança relevante no negócio ou na legislação.