

# REINO CAPITAL

REINO GESTÃO DE PATRIMÔNIO E CONSULTORIA LTDA

## POLÍTICA DE RISCO OPERACIONAL

<b>Empresa:</b>	Reino Gestão de Patrimônio e Consultoria Ltda
<b>Nome Fantasia:</b>	Reino Capital
<b>CNPJ:</b>	55.911.132/0001-67
<b>Sede:</b>	Av. República do Líbano, 251, Salas 1420/1422, Torre D, Pina, Recife/PE
<b>Aprovação:</b>	Diretoria da Sociedade
<b>Responsável:</b>	Wagner Oliveira de Albuquerque Maranhão – Diretor Jurídico, Compliance e PLDFT



## 1. INTRODUÇÃO E OBJETIVO

---

O risco operacional é definido como a possibilidade de ocorrência de perdas resultantes de falhas, deficiências ou inadequações de processos internos, pessoas, sistemas ou decorrentes de eventos externos. A presente Política estabelece as diretrizes para a identificação, avaliação, monitoramento, mitigação e reporte dos riscos operacionais da REINO CAPITAL.

Esta Política está alinhada com as melhores práticas internacionais de gestão de riscos (COSO ERM, ISO 31000) e com as exigências regulatórias aplicáveis ao mercado de valores mobiliários.

## 2. ABRANGÊNCIA

---

Esta Política aplica-se a todos os processos, sistemas, Colaboradores e atividades da REINO CAPITAL, incluindo as atividades de consultoria de valores mobiliários, gestão operacional e relacionamento com clientes.

## 3. CATEGORIAS DE RISCO OPERACIONAL

---

Os riscos operacionais da REINO CAPITAL são classificados nas seguintes categorias:

### 3.1 Risco de Processos

Riscos decorrentes de falhas ou inadequações nos processos internos da Sociedade, incluindo processos de suitability, gestão de carteiras, relacionamento com clientes e cumprimento de obrigações regulatórias.

### 3.2 Risco de Pessoas

Riscos associados a erros humanos, fraudes internas, falta de qualificação, rotatividade excessiva de Colaboradores ou comportamentos inadequados.

### 3.3 Risco de Sistemas

Riscos relacionados a falhas nos sistemas de tecnologia da informação, incluindo indisponibilidade de sistemas, erros de processamento, falhas de segurança cibernética e perda de dados.

### 3.4 Risco de Eventos Externos

Riscos decorrentes de eventos externos à Sociedade, como desastres naturais, mudanças regulatórias, ações de terceiros, pandemias ou outros eventos imprevisíveis.

### 3.5 Risco Legal e Regulatório

Riscos decorrentes de exposição a penalidades, multas, sanções ou prejuízos financeiros e reputacionais resultantes do descumprimento de leis, regulamentos ou contratos.

### 3.6 Risco de Reputação

Riscos associados à percepção negativa da imagem da REINO CAPITAL por parte de clientes, parceiros, reguladores ou do público em geral, que possam impactar negativamente os negócios da Sociedade.

## 4. PROCESSO DE GESTÃO DE RISCOS

### 4.1 Identificação

A identificação de riscos operacionais é realizada de forma contínua, por meio de:

- Avaliações periódicas de risco realizadas pelo Compliance em conjunto com os responsáveis por cada área.
- Análise de incidentes e quase-acidentes ocorridos na Sociedade.
- Monitoramento de alterações regulatórias e do ambiente de negócios.
- Benchmarking com as melhores práticas do setor.

### 4.2 Avaliação

Os riscos identificados são avaliados considerando dois fatores:

- Probabilidade de ocorrência: alta, média ou baixa.
- Impacto potencial: alto, médio ou baixo.

A combinação desses fatores determina o nível de risco (crítico, alto, médio ou baixo), que orientará a priorização das ações de mitigação.

### 4.3 Mitigação

Para cada risco identificado, o Compliance, em conjunto com a Diretoria, define as medidas de mitigação adequadas, que podem incluir:

- Aprimoramento de processos e controles internos.
- Treinamento e capacitação de Colaboradores.
- Implementação de novos sistemas ou ferramentas tecnológicas.
- Contratação de seguros, quando aplicável.

- Transferência do risco a terceiros especializados.

#### 4.4 Monitoramento

Os riscos e as medidas de mitigação adotadas são monitorados continuamente pelo Compliance, que avalia a eficácia dos controles e propõe ajustes quando necessário. Os resultados do monitoramento são reportados à Diretoria em base trimestral.

### 5. PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

A REINO CAPITAL mantém um Plano de Continuidade de Negócios para assegurar a continuidade das operações críticas em caso de eventos disruptivos. O PCN abrange:

- Identificação dos processos e sistemas críticos para a continuidade das operações.
- Definição de procedimentos alternativos para situações de indisponibilidade.
- Estabelecimento de responsabilidades e fluxos de comunicação em situações de crise.
- Procedimentos para recuperação de sistemas e dados.

O PCN deve ser testado anualmente e atualizado sempre que houver mudanças relevantes na estrutura operacional da Sociedade.

### 6. GESTÃO DE INCIDENTES

Todos os incidentes operacionais — incluindo erros de processamento, falhas de sistemas, comportamentos inadequados e eventos externos que afetem as operações — devem ser reportados imediatamente ao Compliance.

O Compliance é responsável por: (i) registrar e investigar os incidentes; (ii) identificar as causas raiz; (iii) propor e acompanhar a implementação de medidas corretivas; e (iv) manter base de dados histórica de incidentes para análise de tendências.

### 7. TERCEIRIZAÇÃO E PRESTADORES DE SERVIÇO

A contratação de prestadores de serviço que participem de processos críticos da REINO CAPITAL deve considerar os riscos operacionais associados, incluindo:

- Avaliação da capacidade técnica e financeira do prestador.
- Verificação da existência de controles internos adequados.

- Definição contratual de SLAs (acordos de nível de serviço) e penalidades.
- Monitoramento periódico do desempenho e da conformidade do prestador.

## 8. CAPACITAÇÃO E CULTURA DE RISCO

---

A REINO CAPITAL promove uma cultura de consciência e gestão proativa de riscos. Todos os Colaboradores são responsáveis por identificar e reportar riscos operacionais em suas áreas de atuação. O Compliance promove treinamentos periódicos sobre gestão de riscos operacionais.

## 9. VIGÊNCIA E REVISÃO

---

Esta Política entra em vigor na data de sua aprovação pela Diretoria e deverá ser revisada anualmente ou sempre que houver alterações relevantes na estrutura operacional, no perfil de risco ou na legislação aplicável à Sociedade.



## APROVACAO E ASSINATURAS

O presente documento foi devidamente revisado, aprovado e adotado pela Diretoria da REINO GESTAO DE PATRIMONIO E CONSULTORIA LTDA (Reino Capital), CNPJ nº 55.911.132/0001-67, em conformidade com a Resolução CVM nº 19/2021 e demais normas regulatórias aplicáveis.

Recife/PE, 26 de março de 2026.


 Assinado digitalmente na ZapSign por  
JOAO GABRIEL TINTORI  
Data: 26/03/2026 16:48:15.672 (UTC-0300)

---

**Joao Gabriel Tintori**

Diretor Presidente | Diretor de Consultoria e Suitability

CPF nº 999.012.933-91

 Assinado digitalmente na ZapSign por  
Carlus Eduardo Tintori  
Data: 31/03/2026 17:26:25.705 (UTC-0300)

---

**Carlus Eduardo Tintori**

Diretor de Risco

CPF nº 052.708.783-13

 Assinado digitalmente na ZapSign por  
Wagner Maranhão  
Data: 26/03/2026 15:34:02.156 (UTC-0300)

---

**Wagner Oliveira de Albuquerque Maranhão**

Diretor Jurídico, Compliance e PLDFT

OAB/PE nº 32.182

# Relatório de Assinaturas

Datas e horários em UTC-0300 ( America/Sao\_Paulo)

Última atualização em 31 Março 2026, 17:26:26

Status: Assinado

Documento: 07 Politica De Risco Operacional.Pdf

Número: 7337127d-d853-4add-bbd0-7c0844fcdde4







Data da criação: 26 Março 2026, 15:20:28

Hash do documento original (SHA256): 8b360b0a0c724ed47c8f6c02005bdcf39a73c151cad51706405e9662a0fc7959



## Assinaturas

3 de 3 Assinaturas

<p>Assinado  via ZapSign by Truora</p> <p><b>JOAO GABRIEL TINTORI</b> Data e hora da assinatura: 26/03/2026 16:48:15 Token: 86c6c753-339d-4114-832f-557ca3c38e80</p>	<p>Assinatura</p>  <p>JOAO GABRIEL TINTORI</p>
<p><b>Pontos de autenticação:</b> Telefone: 5581999215083 E-mail: gabrieltintori@reinocapital.com.br</p>	<p>Localização aproximada: -8.114199, -34.900561 IP: 179.248.213.236 Dispositivo: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36</p>
<p>Assinado  via ZapSign by Truora</p> <p><b>CARLUS EDUARDO TINTORI</b> Data e hora da assinatura: 31/03/2026 17:26:25 Token: 36e9fa1d-bea2-4918-a1e6-2b3d83081eea</p>	<p>Assinatura</p>  <p>Carlus Eduardo Tintori</p>
<p><b>Pontos de autenticação:</b> Telefone: 5511917867788 E-mail: carlustintori@reinocapital.com.br Nível de segurança: Validado por código único enviado por e-mail</p>	<p>IP: 104.28.63.114 Dispositivo: Mozilla/5.0 (iPhone; CPU iPhone OS 18_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/26.3 Mobile/15E148 Safari/604.1</p>
<p>Assinado  via ZapSign by Truora</p> <p><b>WAGNER MARANHÃO</b> Data e hora da assinatura: 26/03/2026 15:34:02 Token: 1e40eca2-5bae-4dc6-9bcf-ef82e69c8e6c</p>	<p>Assinatura</p>  <p>Wagner Maranhão</p>
<p><b>Pontos de autenticação:</b> Telefone: 5581991323661 E-mail: wagnermaranhao@reinocapital.com.br Nível de segurança: Validado por código único enviado por e-mail</p>	<p>Localização aproximada: -8.084484, -34.895628 IP: 177.12.136.181 Dispositivo: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36</p>

## INTEGRIDADE CERTIFICADA - ICP-BRASIL

Assinaturas eletrônicas e físicas têm igual validade legal, conforme MP 2.200-2/2001 e Lei 14.063/2020.

[Confirme a integridade do documento aqui.](#)



Este Log é exclusivo e parte integrante do documento número 7337127d-d853-4add-bbd0-7c0844fcdde4, segundo os [Termos de Uso da ZapSign](#), disponíveis em [zapsign.com.br](https://zapsign.com.br)