REINO CAPITAL

REINO GESTÃO DE PATRIMÔNIO E CONSULTORIA LTDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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

1. INTRODUÇÃO E OBJETIVO

A informação é um ativo estratégico fundamental para a REINO CAPITAL. A presente Política de Segurança da Informação estabelece as diretrizes e controles necessários para assegurar a confidencialidade, integridade e disponibilidade das informações da Sociedade, de seus clientes e de seus parceiros de negócios.

Esta Política está alinhada com as melhores práticas internacionais (ISO/IEC 27001) e com as normas regulatórias aplicáveis ao mercado de valores mobiliários, em especial a Resolução CVM nº 35/2021 e as orientações do Banco Central do Brasil.

2. ABRANGÊNCIA

Esta Política aplica-se a todos os Colaboradores da REINO CAPITAL — sócios, diretores, funcionários, estagiários, prestadores de serviço e terceirizados — bem como a todos os sistemas, dispositivos, redes e informações utilizados no exercício das atividades da Sociedade.

3. PRINCÍPIOS FUNDAMENTAIS

A segurança da informação na REINO CAPITAL é regida pelos seguintes princípios:

- Confidencialidade: garantir que a informação seja acessível apenas a pessoas autorizadas.
- Integridade: assegurar que a informação seja precisa, completa e não seja alterada de forma não autorizada.
- Disponibilidade: garantir que a informação esteja acessível e utilizável quando necessária por pessoas autorizadas.
- Autenticidade: assegurar que a identidade dos usuários e a origem das informações sejam verificáveis.
- Responsabilidade: garantir que as ações dos usuários possam ser rastreadas.

4. CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações da REINO CAPITAL são classificadas nas seguintes categorias:

4.1 Informação Pública

Informações que podem ser divulgadas livremente ao público sem qualquer restrição. Ex.: materiais de marketing aprovados, informações institucionais disponíveis no site.

4.2 Informação Interna

Informações destinadas ao uso interno da Sociedade, que não devem ser divulgadas externamente sem autorização. Ex.: procedimentos operacionais, comunicações internas.

4.3 Informação Confidencial

Informações sensíveis cujo acesso é restrito a Colaboradores com necessidade específica. Ex.: dados de clientes, estratégias de investimento, informações financeiras, contratos.

4.4 Informação Estritamente Confidencial

Informações altamente sensíveis cujo acesso é restrito à Diretoria e ao Compliance. Ex.: informações privilegiadas de mercado, dados de due diligence, informações sobre investigações.

5. CONTROLES DE ACESSO

O acesso às informações e sistemas da REINO CAPITAL deve ser concedido com base no princípio do menor privilégio — cada Colaborador deve ter acesso apenas às informações necessárias para o exercício de suas funções.

5.1 Gerenciamento de Senhas

- Senhas devem ter no mínimo 8 caracteres, combinando letras maiúsculas e minúsculas, números e caracteres especiais.
- Senhas devem ser alteradas a cada 90 dias ou imediatamente em caso de suspeita de comprometimento.
- É vedado compartilhar senhas com outros Colaboradores.
- Senhas não devem ser armazenadas em locais de fácil acesso (post-its, planilhas não protegidas).

5.2 Bloqueio de Estações de Trabalho

- As estações de trabalho devem ser bloqueadas sempre que o Colaborador se afastar, mesmo que por breve período.
- O bloqueio automático deve ser configurado para ocorrer após no máximo 5 minutos de inatividade.

5.3 Controle de Acessos Remotos

O acesso remoto aos sistemas da REINO CAPITAL deve ser realizado exclusivamente por meio de conexões seguras (VPN ou equivalente), com autenticação de dois fatores quando disponível.

6. SEGURANÇA DE DISPOSITIVOS

6.1 Dispositivos Corporativos

- Todos os dispositivos corporativos devem possuir antivírus e softwares de segurança atualizados.
- Atualizações de sistema operacional e aplicativos devem ser aplicadas prontamente.
- A instalação de softwares não licenciados ou não autorizados é expressamente proibida.
- Dispositivos não devem ser emprestados a terceiros, incluindo familiares.

6.2 Dispositivos Pessoais (BYOD)

O uso de dispositivos pessoais para acesso a informações corporativas somente é permitido mediante autorização prévia do Compliance e adoção das medidas de segurança definidas pela Sociedade.

7. USO DA INTERNET E E-MAIL

Os recursos de internet e e-mail corporativos devem ser utilizados exclusivamente para fins profissionais. É vedado:

- Acessar sites com conteúdo impróprio, ilegal ou que possa comprometer a segurança dos sistemas.
- Transmitir informações confidenciais por e-mail pessoal ou aplicativos de mensagens não autorizados.
- Abrir anexos ou clicar em links de remetentes desconhecidos ou suspeitos.
- Realizar downloads de software ou arquivos de fontes não confiáveis.

O Compliance poderá monitorar, por amostragem e sem aviso prévio, as mensagens eletrônicas enviadas e recebidas pelos Colaboradores, para fins de controle e segurança.

8. ARMAZENAMENTO E BACKUP

As informações corporativas devem ser armazenadas exclusivamente nos sistemas e repositórios oficiais da REINO CAPITAL. As seguintes práticas são obrigatórias:

- Realização de backup periódico das informações críticas, com frequência mínima diária para dados sensíveis.
- Armazenamento dos backups em local seguro e segregado do local de origem.
- Teste periódico de restauração dos backups para verificar sua integridade e funcionalidade.
- Manutenção de registros pelo prazo mínimo exigido pela regulamentação aplicável (mínimo de 5 anos).

9. GESTÃO DE INCIDENTES DE SEGURANÇA

Qualquer incidente de segurança da informação — incluindo acessos não autorizados, perdas de dados, suspeita de vírus ou vazamento de informações — deve ser comunicado imediatamente ao Compliance.

O Compliance é responsável por coordenar a resposta ao incidente, que incluirá: (i) identificação e contenção do incidente; (ii) erradicação da causa raiz; (iii) recuperação dos sistemas afetados; (iv) análise pós-incidente; e (v) comunicação às autoridades reguladoras, quando legalmente exigido.

10. PLANO DE CONTINUIDADE DE NEGÓCIOS

A REINO CAPITAL mantém um Plano de Continuidade de Negócios (PCN) que define os procedimentos para manutenção das operações críticas em caso de interrupção significativa dos sistemas ou da infraestrutura.

O PCN deve ser testado anualmente e revisado sempre que houver alterações significativas nos sistemas ou processos da Sociedade.

11. DESCARTE SEGURO DE INFORMAÇÕES

O descarte de mídias, equipamentos e documentos físicos contendo informações deve ser realizado de forma segura:

- Documentos físicos confidenciais devem ser destruídos por fragmentadora antes do descarte.
- Mídias digitais (pen drives, HDs, notebooks) devem ter seus dados apagados de forma irreversível antes do descarte ou reutilização.
- O descarte de equipamentos de TI deve ser documentado e certificado.

12. TREINAMENTO E CONSCIENTIZAÇÃO

Todos os Colaboradores devem receber treinamento sobre segurança da informação no momento do ingresso na Sociedade e, posteriormente, com periodicidade anual. O Compliance é responsável por coordenar testes periódicos de segurança, incluindo simulações de phishing e outras ameaças.

13. SANÇÕES

A violação desta Política sujeita o Colaborador às sanções previstas no Código de Ética e Conduta da REINO CAPITAL, sem prejuízo das penalidades cíveis e criminais eventualmente cabíveis.

14. 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 legislação aplicável, nos sistemas da Sociedade ou no cenário de ameaças cibernéticas.

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

ZapSign By Truora

Status: Assinado
Documento: 03 Politica De Seguranca Da Informacao.Pdf
Número: 10ec548a-409e-4528-b196-8de8ab093f44
Data da criação: 26 Março 2026, 15:20:27
Hash do documento original (SHA256):
eeb3902d74ba029b668d276eda35e16133d6f9b5682a7202ab4c560182e73950

Assinaturas

3 de 3 Assinaturas

Assinado via ZapSign by Truora

JOAO GABRIEL TINTORI
Data e hora da assinatura: 26/03/2026 16:48:15
Token: 86c6c753-339d-4114-832f-557ca3c38e80

Assinatura
JOAO GABRIEL TINTORI

Pontos de autenticação:
Telefone: 5581999215083
E-mail: gabrieltintori@reinocapital.com.br

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

Assinado via ZapSign by Truora

CARLUS EDUARDO TINTORI
Data e hora da assinatura: 31/03/2026 17:26:25
Token: 36e9fa1d-bea2-4918-a1e6-2b3d83081eea

Assinatura
Carlus Eduardo Tintori
Carlus Eduardo Tintori

Pontos de autenticação:
Telefone: 5511917867788
E-mail: carlustintori@reinocapital.com.br
Nível de segurança: Validado por código único enviado por e-mail

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

Assinado via ZapSign by Truora

WAGNER MARANHÃO
Data e hora da assinatura: 26/03/2026 15:34:02
Token: 1e40eca2-5bae-4dc6-9bcf-ef82e69c8e6c

Assinatura
Wagner Maranhão
Wagner Maranhão

Pontos de autenticação:
Telefone: 5581991323661
E-mail: wagnermaranhao@reinocapital.com.br
Nível de segurança: Validado por código único enviado por e-mail

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

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.