2025.2
V. 2

# Política
## Segurança Anti-Fraude

VRDEBANK

# 01. Objetivo

A Política de Segurança Anti-Fraude do VrdeBank estabelece diretrizes e procedimentos para prevenir, detectar e responder a atividades fraudulentas que possam afetar nossos clientes, colaboradores e operações. A segurança anti-fraude é uma prioridade absoluta para garantir a confiança, integridade e proteção dos dados e recursos do banco.

# 02. Escopo

Esta Política se aplica a toda organização, aos seus colaboradores, parceiros, sejam eles pessoas físicas ou jurídicas que atuam para ou em nome do VRDEBANK em quaisquer operações, a terceiros que de qualquer forma se relacionem com o banco, bem como aos clientes, cujos dados são tratados pelo Vrde.

VRDEBANK

# 03. Definições

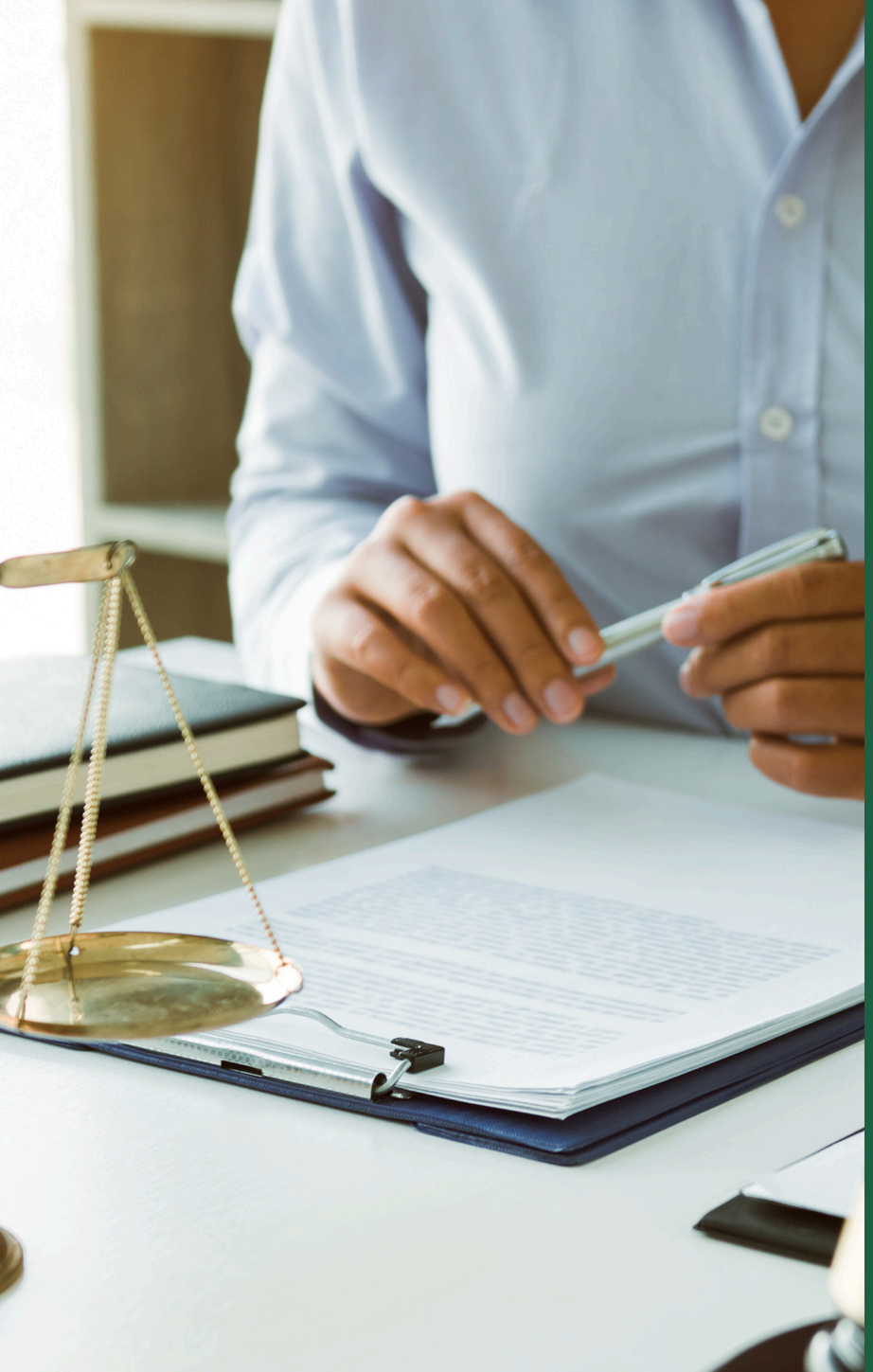
1. Fraude: Qualquer atividade intencional ou enganosa destinada a obter ganho financeiro ou causar dano ao banco ou aos clientes;
2. Colaboradores: Todos os funcionários, terceirizados e consultores que têm acesso aos sistemas e informações do banco;
3. Phishing: Método utilizado por fraudadores para obter informações confidenciais, como senhas e números de cartão de crédito, disfarçando-se de entidades confiáveis;
4. Vishing: Método parecido ao phishing, porém utiliza ligações telefônicas para enganar as vítimas e obter informações confidenciais;
5. Malware: Software malicioso projetado para danificar computadores ou sistemas, roubar informações ou ganhar acesso não autorizado;
6. Insider Threat: Risco de fraude ou comprometimento de segurança causado por colaboradores internos com acesso privilegiado a informações sensíveis.

VRDEBANK

# 04. Princípios da Segurança Anti-Fraude

1. Prevenção Proativa: Implementar controles e procedimentos robustos para mitigar o risco de fraude desde o ponto de entrada e realizar avaliações regulares de vulnerabilidades e implementar correções de segurança;
2. Monitoramento Contínuo: Utilizar ferramentas de monitoramento para detectar padrões de comportamento suspeitos e atividades anômalas e monitorar transações financeiras e de dados em tempo real para identificar atividades fraudulentas rapidamente;
3. Autenticação Forte: Implementar autenticação multifatorial para acesso a contas e sistemas sensíveis, bem como exigir verificações adicionais para transações financeiras de alto valor ou sensíveis;
4. Educação e Conscientização: Realizar treinamentos regulares sobre reconhecimento e prevenção de fraudes e educar os clientes sobre práticas seguras e sinais de atividades fraudulentas;
5. Resposta Rápida e Eficiente: Manter um plano de resposta a incidentes de fraude que inclua procedimentos claros para mitigação imediata através de uma equipe dedicada a responder prontamente aos incidentes;
6. Cooperação e Colaboração interinstitucional: Colaborar com autoridades competentes, instituições financeiras e parceiros para investigar e resolver casos de fraude, bem como compartilhar informações relevantes e melhores práticas com a comunidade financeira para fortalecer as defesas contra fraudes;
7. Avaliação Contínua: Realizar auditorias periódicas para avaliar a eficácia das políticas e procedimentos anti-fraude e Incorporar feedback dos clientes e colaboradores para melhorar continuamente as práticas de segurança;
8. Conformidade e Legislação: Cumprir integralmente com as regulamentações relacionadas à segurança de dados e prevenção de fraudes, adaptando as práticas de segurança anti-fraude às mudanças regulatórias e tecnológicas relevantes.

VRDE BANK



# 05. Responsabilidades

1. Diretoria Executiva: Responsável por definir a estratégia anti-fraude, alocar recursos adequados e garantir conformidade com regulamentos;
2. Encarregado de Dados - DPO: Encarregado de liderar as iniciativas de segurança anti-fraude, coordenando com os times de TI e Compliance;
3. Comitê de Fraude: Equipe dedicada à análise de fraudes, investigação de incidentes e implementação de medidas preventivas;
4. Compliance: Certificar e garantir a execução das melhores práticas de segurança anti-fraude com base nas normas internas, bem como receber e dar encaminhamento nos relatos recebidos no canal de denúncias sobre o tema;
5. Colaboradores, Parceiros e Clientes: Buscar praticar as melhores práticas de segurança anti-fraude através das normas internas, legislação vigente e demais orientações publicadas nos veículos oficiais do VRDE.

VRDEBANK

# 06. Medidas de Prevenção

1. Autenticação Forte: Implementar autenticação multifatorial para acesso a contas e sistemas sensíveis;
2. Monitoramento Contínuo de Movimentações: Utilizar ferramentas de monitoramento para detectar comportamentos anômalos e transações suspeitas;
3. Monitoramento Interno: As redes e sistemas corporativos devem ser administrados, monitorados e protegidos de acordo com as exigências e requisitos de Segurança da Informação do VRDE, considerando sempre as melhores práticas do mercado e acompanhando o desenvolvimento da tecnologia. Além disso, devem ser protegidos contra acessos não autorizados por meio de tecnologias de rede regularmente atualizadas;
4. Educação e Conscientização: Promover treinamentos regulares para colaboradores e clientes sobre reconhecimento e prevenção de fraudes;
5. Política de Senhas: Estabelecer políticas claras para o uso seguro de senhas e exigir sua alteração regularmente;
6. Controle dos dispositivos: Todos os dispositivos tecnológicos disponibilizados pelo VRDE para colaboradores, prestadores de serviço e parceiros são modernos e protegidos por controles contra ataques cibernéticos, infecções e prevenção ao vazamento de dados;
7. Desenvolvimento de sistemas: A segurança deve ser incorporada desde o desenvolvimento inicial dos sistemas. Controles de segurança devem ser implementados ao longo de toda a vida útil desses sistemas para garantir a proteção das informações processadas, levando em consideração sua classificação e o nível de exposição ao risco.

# 07. Detecção de Fraude

1. Análise de Padrões: Utilizar análise avançada de dados e padrões de comportamento para identificar atividades incomuns e fraudulentas;
2. Monitoramento de Transações: Implementar sistemas de monitoramento em tempo real para transações financeiras e atividades de login para detectar sinais de comprometimento de conta;
3. Ferramentas de IA e Machine Learning: Utilizar tecnologias emergentes para melhorar a detecção precoce de fraudes considerando sempre as novas formas de fraude.


# 07. Detecção de Fraude

1. Plano de Contingência: Manter um plano de resposta a incidentes que inclua procedimentos para mitigação rápida e comunicação interna e externa eficaz e acionamento imediato de equipe de resposta a incidentes para minimizar impactos e recuperar dados comprometidos;
2. Comunicação: Comunicação rápida e transparente com clientes afetados para mitigar danos à reputação e prejuizo aos correntistas;
3. Investigação Interna: Realizar investigações detalhadas para entender as causas e impactos de incidentes de fraude, bem como elaborar parecer com sugestões de melhorias para que o incidente não repita-se;
4. Cooperação Externa: Colaborar com autoridades competentes e parceiros para investigar e solucionar casos de fraude com transparência e eficiência.

VRDEBANK

# 09. Avaliação e Melhoria Contínua

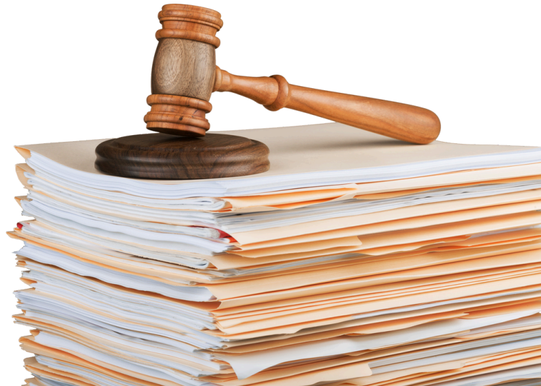
1. Avaliações Regulares: Realizar auditorias periódicas para avaliar a eficácia das políticas anti-fraude e identificar áreas de melhoria;
2. Feedback dos Clientes: Utilizar feedback dos clientes para melhorar os processos de segurança, prevenção de fraudes e linguagem utilizada para educar os mesmos quanto à prevenção contra fraudes.



# 10. Conformidade e Legislação

O VRDE está comprometido com o cumprimento dos requisitos da Lei Geral de Proteção de Dados em todas as atividades anti-fraude e setores da organização. Dessa forma, é imprescindível adotar práticas que estejam em conformidade com todas as leis e regulamentos relacionados à segurança de dados e prevenção de fraudes.

Todos os elencados no escopo dessa política também aderem a política de Privacidade e Proteção de dados, norma crucial para garantir a segurança dos nossos clientes, colaboradores e parceiros de negócios.



VRDEBANK

## 11. Comunicação e Divulgação

Tendo em vista a volatilidade das atividades fraudulentas, o Vrde compromete-se em manter clientes e colaboradores informados e atualizados sobre os riscos de fraude e as medidas de proteção adotadas pelo banco para mitigar tais riscos.

## 12. Disposições Finais

Para garantir a eficácia e a relevância contínua de nossas políticas, realizamos revisões regulares com base nas mudanças da legislação, nas tecnologias emergentes e nas práticas recomendadas. Nossos especialistas em segurança Anti-fraude e Compliance trabalham em conjunto para monitorar e adaptar nossas políticas de acordo com o arcabouço normativo atualizado.

Além disso, o programa de compliance do Vrde trabalha para assegurar que todas as diretrizes e normas estabelecidas sejam rigorosamente seguidas em todas as áreas da organização. Isso inclui a realização de auditorias internas, avaliações de risco, revisão constante dos processos internos e treinamentos periódicos.

VRDEBANK

# 13. Canal de Reporte

O meio oficial para reportar qualquer irregularidade quanto à Segurança Anti-Fraude, segurança cibernética, segurança da informação e qualquer desobediência a esta política é o canal de denúncias oficial do Vrde, que pode ser acessado clicando aqui.

As denúncias podem ser feitas de forma anônima e sem gerar qualquer tipo de represália ao denunciante.

VRDEBANK

VRDEBANK

# Política

## Segurança Anti-Fraude

2025.2