POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

BROKERS CORPORATE OFFICE

Versão: 1.0
Data de Vigência: 30 de outubro de 2025
Responsável: Wilson Fernando Maciel - CEO
Última Revisão: 30 de outubro de 2025

---

1. OBJETIVO E ABRANGÊNCIA

Esta Política de Segurança da Informação estabelece diretrizes, princípios e responsabilidades para proteção dos ativos de informação da Brokers Corporate Office, suas subsidiárias (incluindo Vault By Brokers) e parceiros comerciais.

Aplicabilidade: Esta política aplica-se a todos os colaboradores, prestadores de serviços, parceiros, clientes e terceiros que tenham acesso aos sistemas, dados e informações da organização.

---

2. PRINCÍPIOS FUNDAMENTAIS

2.1 Confidencialidade

- Garantir que as informações sejam acessadas apenas por pessoas autorizadas
- Proteger dados sensíveis de clientes, parceiros e da organização

2.2 Integridade

- Assegurar a exatidão e completude das informações
- Prevenir modificações não autorizadas ou acidentais

2.3 Disponibilidade

- Manter sistemas e informações acessíveis quando necessário
- Garantir continuidade dos serviços críticos

2.4 Autenticidade

- Verificar a identidade de usuários e sistemas
- Garantir a origem legítima das informações

---

3. CLASSIFICAÇÃO DA INFORMAÇÃO

3.1 Informações Públicas

- Materiais institucionais e de marketing
- Informações disponíveis no site corporativo
- Sem restrições de divulgação

3.2 Informações Internas

- Documentos operacionais e administrativos
- Acesso restrito a colaboradores
- Não destinadas ao público externo

3.3 Informações Confidenciais

- Dados de clientes e parceiros
- Contratos e acordos comerciais
- Informações financeiras e estratégicas
- Acesso mediante autorização específica

3.4 Informações Críticas

- Dados bancários e transacionais
- Credenciais de acesso a sistemas
- Informações regulatórias e de compliance
- Máximo nível de proteção

---

4. CONTROLES DE ACESSO

4.1 Autenticação

- Credenciais únicas e intransferíveis para cada usuário
- Senhas fortes com no mínimo 12 caracteres
- Autenticação multifator (MFA) para sistemas críticos
- Renovação periódica de senhas (máximo 90 dias)

4.2 Autorização

- Acesso baseado no princípio do menor privilégio
- Revisão trimestral de permissões

- Segregação de funções em operações críticas
- Aprovação formal para concessão de acessos

4.3 Monitoramento

- Registro de logs de acesso e operações
- Retenção de logs por no mínimo 5 anos
- Análise periódica de acessos suspeitos
- Alertas automáticos para atividades anômalas

---

5. PROTEÇÃO DE DADOS

5.1 Dados em Trânsito

- Criptografia TLS 1.3 ou superior para transmissões
- VPN para acesso remoto a sistemas corporativos
- Proibição de envio de dados sensíveis por e-mail não criptografado

5.2 Dados em Repouso

- Criptografia AES-256 para dados armazenados
- Backups criptografados e testados mensalmente
- Armazenamento seguro com controle de acesso físico

5.3 Descarte de Informações

- Destruição segura de documentos físicos (trituração)
- Sanitização completa de dispositivos antes do descarte
- Certificação de destruição quando aplicável

---

6. SEGURANÇA EM DESENVOLVIMENTO

6.1 Desenvolvimento Seguro

- Revisão de código e testes de segurança
- Análise de vulnerabilidades antes da implantação
- Gestão de vulnerabilidades com correções em até 30 dias (críticas: 7 dias)

6.2 Ambientes

- Segregação entre desenvolvimento, homologação e produção
- Dados anonimizados em ambientes não produtivos
- Controles de mudança formais

---

7. GESTÃO DE INCIDENTES

7.1 Detecção e Resposta

- Canal 24/7 para reporte de incidentes: security@brokersco.com.br
- Equipe de resposta a incidentes (IRT) designada
- Classificação e priorização de incidentes

7.2 Procedimentos de Resposta

1. **Contenção:** Isolar sistemas afetados
2. **Erradicação:** Remover a causa do incidente
3. **Recuperação:** Restaurar operações normais
4. **Lições Aprendidas:** Documentar e implementar melhorias

7.3 Comunicação

- Notificação à ANPD em até 72 horas (quando aplicável)
- Comunicação a clientes afetados conforme LGPD
- Relatórios internos e externos quando necessário

---

8. SEGURANÇA FÍSICA E AMBIENTAL

8.1 Controles Físicos

- Controle de acesso físico às instalações
- Monitoramento por câmeras em áreas críticas
- Proteção contra incêndios e desastres naturais

8.2 Equipamentos

- Inventário atualizado de ativos
- Proteção contra roubo e uso não autorizado
- Descarte seguro de equipamentos

---

9. CONTINUIDADE DE NEGÓCIOS

9.1 Backup e Recuperação

- Backups diários automáticos
- Armazenamento em locais geograficamente distribuídos
- Testes de recuperação trimestrais
- RTO (Recovery Time Objective): 4 horas
- RPO (Recovery Point Objective): 1 hora

9.2 Plano de Continuidade

- Plano de Continuidade de Negócios (PCN) documentado
- Plano de Recuperação de Desastres (PRD) testado anualmente
- Equipe de crise designada

---

10. CONFORMIDADE E AUDITORIAS

10.1 Requisitos Legais

- Conformidade com LGPD (Lei 13.709/2018)
- Aderência a requisitos do Banco Central
- Atendimento a normas da CVM quando aplicável
- Compliance com requisitos de parceiros (Celcoin, exchanges)

10.2 Auditorias

- Auditorias internas semestrais
- Auditorias externas anuais
- Testes de penetração (pentest) anuais
- Relatórios de auditoria disponíveis para autoridades

---

11. TREINAMENTO E CONSCIENTIZAÇÃO

11.1 Programa de Capacitação

- Treinamento obrigatório anual em segurança da informação
- Campanhas de conscientização trimestais
- Simulações de phishing e engenharia social
- Material educativo disponível permanentemente

11.2 Responsabilidades

- Todo colaborador é responsável pela segurança
- Gerentes devem garantir compliance de suas equipes
- Área de TI/Segurança presta suporte técnico

---

12. GESTÃO DE TERCEIROS

12.1 Due Diligence

- Avaliação de segurança antes da contratação
- Cláusulas de segurança em contratos

- Acordo de Confidencialidade (NDA) obrigatório

12.2 Monitoramento

- Revisão anual de contratos e segurança
- Auditorias periódicas em fornecedores críticos
- Incidentes de terceiros tratados como internos

---

13. USO ACEITÁVEL

13.1 Recursos Corporativos

- Uso de recursos para fins profissionais
- Proibição de software não autorizado
- Navegação segura e responsável na internet

13.2 Dispositivos Móveis

- Política de BYOD (Bring Your Own Device) regulamentada
- MDM (Mobile Device Management) obrigatório para acesso corporativo
- Criptografia de dispositivos móveis

13.3 Trabalho Remoto

- Uso obrigatório de VPN
- Proteção de rede Wi-Fi doméstica
- Segregação de ambientes pessoal e profissional

---

14. PENALIDADES

O descumprimento desta política pode resultar em: - Advertências verbais e escritas - Suspensão de acessos - Rescisão contratual (colaboradores e prestadores) - Medidas legais cabíveis

---

15. REVISÃO E ATUALIZAÇÃO

15.1 Periodicidade

- Revisão anual obrigatória
- Revisão extraordinária após incidentes relevantes
- Atualização conforme mudanças regulatórias

15.2 Aprovação

Esta política foi aprovada pela alta administração e é de cumprimento obrigatório.

Aprovado por:
Wilson Fernando Maciel
CEO - Brokers Corporate Office
30 de outubro de 2025

---

16. CONTATOS

Responsável pela Política:
Wilson Fernando Maciel
CEO - Brokers Corporate Office
E-mail: wilson@brokersco.com.br

Equipe de Segurança da Informação:
E-mail: security@brokersco.com.br
Telefone: +55 (35) XXXX-XXXX

Canal de Denúncias:
E-mail: compliance@brokersco.com.br
Canal confidencial disponível 24/7
