RESUMO

Estabelecer as diretrizes e procedimentos para assegurar a conformidade das operações com as normas legais e regulamentares aplicável.

ÍNDICE

1. INTRODUÇÃO

1.1. Objetivo

Esta política tem como objetivo estabelecer princípios, diretrizes e procedimentos para assegurar a confidencialidade, integridade e disponibilidade das informações da Turcambio Corretora de Câmbio Ltda, garantindo a continuidade das operações e mitigando riscos de segurança da informação e cibernética.

Inclui também diretrizes específicas para resposta a incidentes e recuperação em caso de falhas técnicas, ataques cibernéticos ou desastres, conforme acordado com o prestador de serviço Online Data Cloud, provedor da infraestrutura tecnológica.

1.2. Escopo

Aplica-se a todos os colaboradores, prestadores de serviços, parceiros comerciais e clientes com acesso aos sistemas e dados sob responsabilidade da Turcambio, incluindo recursos hospedados na Online Data Cloud, conforme contrato TURCAMBIO-PROPOSTA-CLOUD-170818-V1 e seus aditivos.

2. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Confidencialidade: acesso restrito às informações apenas a pessoas autorizadas.

Integridade: proteção contra alterações indevidas ou não autorizadas nas informações.

Disponibilidade: garantia de acesso à informação por usuários autorizados sempre que necessário.

Esses princípios são a base da nossa atuação e norteiam as práticas adotadas na gestão de dados, sistemas e infraestrutura.

3. ANÁLISE DE RISCOS

3.1. Identificação de Riscos

Falhas de hardware em servidores;

Erros de software, inclusive falhas em sistemas de backup e replicação;

Ataques cibernéticos (ransomware, phishing, DDoS);

Ameaças físicas como incêndios, enchentes e quedas de energia;

Acesso indevido ou manipulação por erro humano;

Uso indevido de credenciais ou senhas fracas.

3.2. Avaliação de Impacto

Riscos que afetem sistemas críticos como os servidores TURCAMBIO-BD02 e TURCAMBIO-APP-WEB01_01 podem interromper serviços essenciais, impactando diretamente a operação de câmbio, atendimento ao cliente e processos financeiros.

4. ESTRATÉGIA DE RECUPERAÇÃO E CONTINUIDADE

4.1. Backup e Recuperação

Backups diários, semanais e mensais com retenção conforme contrato.

Armazenamento em nuvem privada e locais físicos seguros.

Testes periódicos de restauração com acompanhamento da equipe de TI.

4.2. Redundância de Sistemas

Infraestrutura com redundância física e lógica;

Failover automático e alta disponibilidade para serviços críticos.

4.3. Plano de continuidade de Negócios

Procedimentos claros de contingência;
Suporte 24x7 via Service Desk da Online Data Cloud;
Possibilidade de trabalho remoto para manter a operação

5. SEGURANÇA CIBERNÉTICA E BOAS PRÁTICAS

5.1. Acesso e autenticação

Credenciais intransferíveis;
Autenticação forte (senhas complexas);
Bloqueio automático de sessão por inatividade;
Acesso concedido apenas com base em necessidade e perfil de risco.

5.2. Prevenção a vazamento de dados

Classificação da informação (confidencial, interna, pública);
Antivírus, firewall, antispam e DLP (Data Loss Prevention);
Proibição de compartilhamento de informações sensíveis sem autorização.

5.3. Gestão de incidentes

Monitoramento 24x7 com sistemas de detecção de intrusão;
Rastreabilidade completa (logs de autenticação, ações de usuários);
Resposta a incidentes com comunicação imediata à equipe responsável.

5.4. Gestão de vulnerabilidades

Varreduras periódicas (interna e externa);
Correções de segurança priorizadas por criticidade;
Testes de intrusão regulares nos sistemas.

5.5. Conscientização de Segurança

Treinamento obrigatório sobre segurança digital e LGPD para novos colaboradores;
Campanhas periódicas de sensibilização sobre boas práticas e fraudes comuns.

6. BOAS PRÁTICAS RECOMENDADAS AO USUÁRIO

Não compartilhar senhas e manter sigilo sobre credenciais;

Atualizar regularmente dispositivos e softwares utilizados para acesso aos sistemas;

Instalar e manter ativo antivírus confiável;

Desconfiar de e-mails suspeitos ou solicitações não verificadas;

Em caso de dúvida ou comportamento suspeito, comunicar imediatamente a equipe de compliance.

7. COMUNICAÇÃO E ATENDIMENTO A INCIDENTES

Compliance e PLD: conformidade@turcambio.com.br

Financeiro: financeiro@turcambio.com.br

TI e infraestrutura: ti@turcambio.com.br

Canal confidencial: https://siscompliance.com.br/turcambio/#/home

Todos os eventos suspeitos ou violações devem ser reportados imediatamente.

8. TREINAMENTOS, AUDITORIAS E ATUALIZAÇÕES

Simulações e testes de continuidade de negócio realizados periodicamente;
Auditorias internas de controles e compliance;
Atualização anual obrigatória da política ou sempre que houver mudanças relevantes na infraestrutura, no negócio ou na legislação.

9. LEGISLAÇÃO E NORMAS APLICÁVEIS

Resolução BACEN nº 4.893/2021
Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)
ISO/IEC 27001 – Gestão da Segurança da Informação

10. DISPOSIÇÕES FINAIS

Esta política é um compromisso da Turcambio com a integridade dos dados, a privacidade dos clientes e a resiliência operacional, sendo de observância obrigatória por todos os envolvidos direta ou indiretamente com os sistemas e dados da empresa.
Sua revisão será feita a cada dois anos ou sempre que houver mudanças legais, tecnológicas ou operacionais relevantes.

11. INFORMAÇÕES DE CONTROLE

Vigência: 06.06.2025 a 06.06.2027.

Versão	Item alterado	Descrição resumida da alteração	Motivo	Data da Publicação
01	Não se aplica	Criação da política	1ª. Versão	06.06.2025

12. RESPONSÁVEIS PELO DOCUMENTO

Etapa	Responsável	Nome da Área
Elaboração	Marcio Ronei Varchaki	Compliance

Revisão	Roberta Ávila Ferreira	Diretoria de Riscos e Compliance
Aprovação	Leonardo Domingos Ribeiro	Diretoria Geral e Asministrativa

Diretoria de Riscos e Compliance