

Política de Segurança Cibernética

Resumo para divulgação pública conforme Resolução BCB nº 85/2021

Documento P004 • 2ª Versão • 2026





Objetivo

Estabelecer princípios, diretrizes e controles para prevenir, detectar e responder a incidentes cibernéticos, protegendo as informações e sistemas da Turcambio e os dados de seus clientes.

Abrangência

Esta política se aplica a:



Todos os colaboradores e funcionários da Turcambio



Prestadores de serviços de TI e infraestrutura



Parceiros com acesso a redes, sistemas ou dados



Clientes que interagem com os canais digitais

Princípios de Segurança



Confidencialidade

Informações acessíveis apenas a pessoas e sistemas expressamente autorizados



Integridade

Informações protegidas contra modificações não autorizadas ou acidentais



Disponibilidade

Sistemas operacionais e acessíveis sempre que necessário



Rastreabilidade

Todas as ações sobre ativos de informação são registradas e auditáveis



Conformidade

Práticas em observância à legislação e normas regulatórias vigentes

Objetivos de Segurança Cibernética



IDENTIFICAR

Ativos e riscos cibernéticos



PROTEGER

Controles e medidas preventivas



DETECTAR

Eventos e incidentes em tempo real



RESPONDER

Contenção e comunicação de incidentes



RECUPERAR

Restauração e lições aprendidas

Principais Controles e Medidas Adotadas



Controle de Acesso

Credenciais individuais para todos os usuários
Senhas com complexidade mínima e bloqueio automático
Revisão periódica de acessos privilegiados



Proteção de Dados

Transmissão por protocolos criptográficos seguros
Bloqueio de dispositivos removíveis não autorizados
Proibição de canais não autorizados para dados confidenciais



Monitoramento 24x7

Acompanhamento contínuo dos ambientes tecnológicos
Registro seguro de logs de autenticação e operações
Alertas de disponibilidade e desempenho



Proteção contra Ameaças

Antivírus/antimalware em todos os dispositivos
Firewall dedicado e anti-DDoS
Restrição de softwares não homologados



Backups e Recuperação

Backups diários com criptografia em nuvem



Gestão de Vulnerabilidades

Avaliações periódicas dos ambientes
Pentest anual por empresa independente
Tratamento e acompanhamento das fragilidades

Gestão de Incidentes Cibernéticos

Plano de Ação e Resposta — PL001

1

Identificação

Deteção por sistemas ou colaboradores e abertura de chamado

2

Classificação

Avaliação de impacto e definição de prioridade e escalada

3

Contenção

Ações imediatas para limitar o espalhamento do incidente

4

Erradicação

Eliminação da causa raiz e restauração da segurança

5

Recuperação

Retorno dos serviços ao estado operacional seguro

6

Pós-Incidente

Documentação, lições aprendidas e melhoria dos controles

 Incidentes relevantes são comunicados tempestivamente ao Banco Central do Brasil

Regulação e Governança

Base Regulatória

Res. BCB nº 85/2021 Política de segurança cibernética

Res. CMN nº 4.893/2021 Contratação de serviços de dados

Res. BCB nº 538/2025 Atualização regulatória aplicável

Lei nº 13.709/2018 Lei Geral de Proteção de Dados (LGPD)

ISO/IEC 27001:2022 Referencial de gestão da informação

NIST CSF Framework internacional de boas práticas

Governança — 3 Linhas de Defesa

1^a

Linha • Operação

Todos os colaboradores e TI

2^a

Linha • Controle

Compliance e Riscos

3^a

Linha • Auditoria

Auditoria Interna Independente

Pessoas, Continuidade e Transparência

Conscientização e Treinamento

- Treinamento anual obrigatório em segurança cibernética, LGPD e prevenção a fraudes
- Integração de novos colaboradores com orientações de segurança
- Campanhas periódicas sobre phishing, engenharia social e uso seguro de credenciais
- Comunicados e alertas sobre ameaças e boas práticas digitais

Continuidade de Negócios

- Estratégias de contingência para serviços críticos
- Simulações e testes periódicos de continuidade
- RTO máximo de 4h e RPO máximo de 24h para ambientes críticos
- Múltiplos cenários contemplados

Política revisada anualmente • Relatório anual submetido à Diretoria e disponível ao Banco Central do Brasil



Segurança é compromisso de todos.

A Turcambio está comprometida com a proteção dos dados de seus clientes e a segurança de seus sistemas, em conformidade com as melhores práticas e a legislação vigente.