POLÍTICA DE SEGURANÇA CIBERNÉTICA

Sumário

1 OBJETIVO

Esta Política de Segurança Cibernética – PSI ("Política") tem como objetivo estabelecer os princípios e diretrizes de cibersegurança para proteger, de forma eficiente, eficaz, segura e transparente, os ativos de informação. Busca-se garantir a proteção, disponibilidade, integridade, confidencialidade e autenticidade dos dados e das informações essenciais para a condução das atividades do Conglomerado QI Tech ("QI Tech").

A implementação desta Política está em conformidade com a legislação e regulamentações aplicáveis, originadas pelos órgãos reguladores, e os padrões internacionais de segurança, como a ISO 27001 e o NIST de modo a assegurar a continuidade das operações e mitigar riscos cibernéticos no ambiente corporativo.

2 ABRANGÊNCIA

Esta Política aplica-se a todos os colaboradores, prestadores de serviços e parceiros estratégicos, no âmbito do Conglomerado Qi Tech ("Qi Tech"). É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Planejamento e Sistemas de Informações sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

3 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Consideramos os ativos de informação como os bens mais valiosos no mercado financeiro, e, por isso, nosso compromisso é tratá-los com a máxima responsabilidade. Estamos alinhados aos princípios fundamentais de segurança da informação, que visam preservar a propriedade da informação, com ênfase em sua confidencialidade, integridade e disponibilidade. Isso permite o uso e o compartilhamento controlado da informação, além do monitoramento contínuo e tratamento de incidentes relacionados a ataques cibernéticos. Os princípios são:

- **Confidencialidade**: Assegurar que as informações sejam acessadas exclusivamente por pessoas autorizadas, de forma controlada e restrita.
- **Integridade**: Garantir que as informações permaneçam íntegras, sem alterações indevidas, sejam acidentais ou intencionais.

- **Disponibilidade**: Garantir que as informações estejam sempre acessíveis às pessoas autorizadas a utilizá-las, quando necessário.

4 PAPÉIS E RESPONSABILIDADES

4.1 Alta Diretoria

- Aprovar a PSI, prover recursos e patrocínio.

4.2 Comitê de Segurança da Informação (CSI)

- Deliberar sobre riscos, incidentes e exceções; e
- Revisar a PSI anualmente.

4.3 Segurança da Informação (SI)

- Definir controles;
- Monitorar ameaças; e
- Conduzir resposta a incidentes.

4.4 DevOps

- Implementar e operar controles técnicos; e
- Gerenciar vulnerabilidades.

4.5 Gestores de Áreas

- Garantir cumprimento pelos membros da equipe; e
- Classificar informações.

4.6 Colaboradores e Terceiros

- Cumprir a PSI; e
- Reportar incidentes imediatamente.

5 ESTRUTURA DE CONTROLES

Para assegurar transparência, rastreabilidade e aderência à regulamentação, os controles de segurança da informação deste documento são estruturados de acordo com o NIST.

Os controles seguem o ciclo **Planejar → Implementar → Monitorar → Melhorar (PDCA).**

5.1 Gestão de exceções e risco residual

Exceções devem ser formalizadas, incluindo a justificativa, avaliação de risco residual, data limite e aprovação do Comitê de Segurança da Informação.

5.2 Integração com o NIST e CSF

Cada controle também é etiquetado às funções **IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER** e **RECUPERAR,** permitindo avaliação de maturidade e priorização de investimentos.

6 CONTROLES DA SEGURANÇA DA INFORMAÇÃO

Nesta seção, os controles estão organizados segundo as 6 (seis) Funções do NIST Cybersecurity Framework (CSF) 2.0: Govern (GV), Identify (ID), Protect (PR), Detect (DE), Respond (RS) e Recover (RC). Para cada Função, apresentamos (1) uma explicação objetiva em linguagem acessível e (2) os requisitos essenciais que materializam o controle no Conglomerado QI Tech.

6.1 GV – Govern | Governar

Define a estratégia, papéis, políticas e métricas que direcionam a segurança cibernética de toda a organização.

6.2 ID – Identify | Identificar

Estabelece compreensão clara de ativos, operações, pessoas e riscos para orientar controles adequados.

6.3 PR – Protect | Proteger

Implementa salvaguardas para garantir a entrega de serviços críticos e limitar ou conter o impacto de ameaças.

6.4 DE – Detect | Detectar

Permite a identificação tempestiva de eventos de segurança cibernética.

6.5 RS – Respond | Responder

Define ações e procedimentos para conter o impacto de eventos detectados.

6.6 RC – Recover | Recuperar

Estabelece planos para restaurar serviços afetados e melhorar a resiliência pós incidente.

7 SANÇÕES DISCIPLINARES

O descumprimento desta política pode acarretar sanções disciplinares, conforme as normas internas da Instituição e legislação aplicável.

8 BASE NORMATIVA

8.1 Normas Internas

	Função. Categoria (CSF 2.0)	Seção PSI	Norma/Procedimento (Exemplo)
GV – Govern Governar	GV.OV – Contexto Organizacional	8.1	
	GV.RM – Gestão de Riscos	8.1	
	GV.PO – Políticas & Procedimentos	8.1	
	GV.SY – Funções & Responsabilidades	8.1	
	GV.RR – Revisão & Melhoria	8.1	
ID – Identify Identificar	ID.AM – Gestão de Ativos	8.2	
	ID.BE – Ambiente de Negócio	8.2	
	ID.DC – Governança de Dados	8.2	
	ID.RA – Avaliação de Riscos	8.2	
PR – Protect Proteger	PR.AC – Controle de Acesso	8.3	DTI-20 - Política de Gestão de Acesso; DTI-20.A - Manual de Gestão de Acessos aos Ativos de Informação - Interno e Externo; DTI-20.B - Manual Para Solicitação de Acesso aos Bancos de Dados; DTI-20.C - Relatório de Revisão de Acesso; DTI-13.C - Norma para Acesso Remoto
	PR.AW – Conscientização	8.3	DTI-10.B Programa de Conscientização SI
	PR.DS – Proteção de Dados	8.3	DTI-02 - Norma de Uso de RETICs; DTI-16 - Procedimento para descarte seguro de mídias; DTI-21 - Política Interna de Privacidade e Tratamento de Dados
	PR.IP – Proteção de Identidade	8.3	DTI-20 - Política de Gestão de Acesso
	PR.MA – Manutenção Segura	8.3	
	PR.PT – Proteção Tecnológica	8.3	DCA-63 Controle de Acesso Físico; DTI-19 Manual Uso Internet & Comunicação
DE – Detect Detectar	DE.AE – Anomalia & Evento	8.4	
	DE.CM – Monitoramento Contínuo	8.4	DTI-13 Gestão de Vulnerabilidades
	DE.DP – Detecção de Ameaça	8.4	
RS – Respond Responder	RS.MI – Mitigação	8.5	DTI-11 Política Gestão Incidentes; DTI-04 Normativo Violação Dados Pessoais
	RS.CO – Coordenação	8.5	DTI-11 Política Gestão Incidentes; DTI-04 Normativo Violação Dados Pessoais

	RS.AN – Análise	8.5	DTI-11 Política Gestão Incidentes; DTI-04 Normativo Violação Dados Pessoais
	RS.IM – Melhoria	8.5	DTI-11 Política Gestão Incidentes; DTI-04 Normativo Violação Dados Pessoais
RC – Recover Recuperar	RC.RP – Planejamento de Recuperação	8.6	DCA-21 PCN/DRP
	RC.IM – Melhoria Pós-Recuperação	8.6	
	RC.CO – Coordenação de Recuperação	8.6	

8.2 Normas Externas

Resolução BACEN 4.893/2021	Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Ela também especifica a necessidade de monitoramento contínuo de riscos operacionais, cibernéticos, e outros riscos que possam impactar a solidez das instituições financeiras
Resolução BACEN 85/2021	Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.
Regras e Procedimentos de Deveres Básicos, do Código AGRT, ANBIMA	Estabelece as regras e os procedimentos para o uso dos Selos ANBIMA e para atendimento aos deveres básicos e à manutenção das estruturas internas mínimas que devem ser observadas por todas as instituições participantes que desempenham as atividades previstas nos Códigos ANBIMA
Lei Geral de Proteção de Dados (LGPD) – 13.709/2018	Regula o **tratamento de dados pessoais** no Brasil, buscando **garantir a privacidade e a proteção dos dados** dos cidadãos. A LGPD estabelece normas sobre como dados pessoais devem ser coletados, armazenados, processados e compartilhados, além de garantir direitos aos titulares dos dados, como o direito de acesso, correção e exclusão de suas informações pessoais.

9 CONTROLE DE VERSIONAMENTO

Esta política entra em vigor na data de sua aprovação e deve ser amplamente divulgada a todos os colaboradores e parceiros. Esta política será revisada anualmente ou sempre que houver mudanças relevantes no ambiente tecnológico, regulatório ou organizacional.

v.	data	descrição da alteração	elaborado	aprovado

5	04/2022	Revisão da Política.	Riscos e Controles Internos	Segurança da Informação
6	08/2023	Revisão da Política.	Segurança da Informação	Segurança da Informação
7	04/2024	Adequação Regulatória	Compliance	Segurança da Informação
8	05/2025	Criação de Política por Conglomerado e Segregação da Política de Segurança da Informação.	Segurança da Informação	Comitê de Segurança da Informação