PO.SEGINFO.0002

PÚBLICO

POLITICA DE SEGURANÇA CIBERNÉTICA

Publicado em: 02/2024 Versão: 01/2024 Revisão até: 02/2025

Este documento é aplicável às empresas do Grupo:

ACQIO

Elaboração	Aprovação
Cesar Searlini *Superintendente de Segurança da informação e Desenvolvimento.*	*Gustavo Danzi de Andrade* *CEO*

INDICE

1. OBJETIVO

A Política de Segurança da Informação e Cibernética ("Política") da Acqio Instituição de Pagamento SA ("ACQIO") estabelece de maneira formal as diretrizes adotadas pela empresa para disciplinar os procedimentos necessários à proteção de informações e dados, através de regras relacionadas à segurança, cujo principal objetivo é minimizar os riscos relativos a aos ativos da Acqio, garantindo assim, os princípios da confidencialidade, integridade e disponibilidade das Informações da Acqio, seus parceiros, clientes e todos os participantes de seu ecossistema.

2. ABRANGENCIA

O conteúdo desta Política se aplica e abrange todos os colaboradores e ambientes das empresas do Grupo Acqio denominado nesta Política como “Acqio”, incluindo Acqio Instituição de Pagamento SA, Esfera 5 ltda, Acqio Holding Participações, Acqio Franchising, Acqio Pagamentos, e Acqio Holding Financeira.

3. REFERÊNCIAS

Esta Política de Segurança da Informação e Cibernética foi construída com as referências normativas, legais e regulamentares abaixo:

- ISO/IEC 27001:2013 - Tecnologia da Informação - Técnicas de segurança - Sistemas de gestão da segurança da Informação - Requisitos.
- Resolução BCB 85/2020
- ISO 31000:2018 - Gestão de Riscos - Diretrizes.
- LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- OWASP - *Open Web Application Security Project* - Projeto Aberto de Segurança em Aplicações Web.
- PCI DSS - *Payment Card Industry – Data Security Standard* - Padrão de segurança de dados da indústria de cartões de pagamento.
- PCI PIN (*Payment Card Industry Personal Identification Number*)

4. SIGLAS E TERMOS

- **Grupo Acqio:** Todas as empresas da Acqio, incluindo Acqio Instituição de Pagamento SA, Esfera 5 ltda, Acqio Holding Participações, Acqio Franchising, Acqio Pagamentos, e Acqio Holding Financeira.

5. DIRETRIZES & PILARES

A presente Política é regida por sólidas diretrizes que norteiam todos os processos e procedimentos nos ambientes de tecnologia, segurança da informação e cibernética da Acqio. Os pilares da segurança cibernética adotados pela Acqio, seguem estruturados da seguinte maneira

5.1 Pilares

5.1.1 Classificação dos Ativos de Informação

A classificação da informação foi meticulosamente concebida, aderindo às melhores práticas de segurança e em conformidade com as regulamentações vigentes. O propósito fundamental é assegurar que todas as informações sejam devidamente classificadas e recebam o nível de proteção adequado. A classificação foi estruturada em quatro níveis distintos: **Pública, Privada, Restrita e Confidencial.**

- **Pública**: Informações que podem ser divulgadas dentro e fora da Acqio. A informação neste nível não necessita de mecanismos diferenciados de proteção.

- **Privada**: Informações que podem ser divulgadas a todos os colaboradores, mas não devem ser compartilhados externamente sem que exista autorização expressa.

- **Restrita**: Informação que pode ser compartilhada apenas internamente e com quem necessite da mesma para o desempenho de suas atividades profissionais envolvendo a ACQIO. Sua divulgação indevida para o público externo pode ocasionar em um risco médio ou um problema operacional à ACQIO.

- **Confidencial**: Informação cujo conteúdo só pode ser compartilhado com pessoas autorizadas, nos casos em que pela natureza da função que exercem, torna-se imprescindível conhecê-las. A exposição indevida desse tipo de informação implicaria em um dano considerado como grave podendo colocar a continuidade do negócio em risco.

5.2 Diretrizes

Políticas de Acesso e Controle: Estabelecer regras claras e robustas para o acesso a sistemas e dados, garantindo que apenas usuários autorizados tenham permissões específicas. Implementar autenticação de dois fatores (2FA) sempre que possível para reforçar a segurança das contas.

Atualizações de Sistemas e Aplicativos: Definir procedimentos para a aplicação regular de atualizações e patches de segurança em sistemas operacionais, softwares e aplicativos. Criar um cronograma de manutenção para garantir que as vulnerabilidades sejam corrigidas de maneira oportuna.

Conscientização e Treinamento: Realizar treinamentos regulares de conscientização em segurança cibernética para todos os colaboradores, abordando práticas seguras online e identificação de ameaças.

Monitoramento de Rede: Implementar ferramentas de monitoramento de rede para detectar atividades suspeitas, invasões ou comportamentos anômalos. Estabelecer alertas automáticos para notificar a equipe de segurança sobre possíveis incidentes.

Gestão de Incidentes: Desenvolver um plano abrangente de resposta a incidentes, delineando as etapas a serem seguidas em caso de violação de segurança. Designar uma equipe responsável pela investigação e resolução rápida de incidentes cibernéticos.

***Backup* e Recuperação de Dados:** Implementar políticas de backup regulares para garantir a disponibilidade e integridade dos dados. Testar periodicamente os procedimentos de recuperação de dados para assegurar eficácia em emergências.

Criptografia de Dados: Utilizar criptografia para proteger dados sensíveis durante a transmissão e armazenamento. Estabelecer políticas claras sobre o uso adequado de algoritmos criptográficos e chaves de criptografia.

Avaliação de Riscos: Realizar avaliações regulares de riscos para identificar novas ameaças e vulnerabilidades. Atualizar as estratégias de segurança com base nos resultados das avaliações de risco.

Segurança de Dispositivos Móveis: Implementar medidas de segurança para dispositivos móveis, como senhas, criptografia e controle remoto em caso de perda ou roubo. Estabelecer diretrizes claras para o uso seguro de dispositivos móveis no ambiente corporativo.

Conformidade com Regulamentações: Manter-se atualizado com as regulamentações de segurança cibernética pertinentes ao setor e garantir conformidade com as normas aplicáveis. Designar responsáveis pela gestão e documentação da conformidade com requisitos regulatórios.

6. PAPEIS E RESPONSABILIDADES

6.1 Lideranças & Gerências

A liderança desempenha um papel crítico no fortalecimento das práticas de Segurança da Informação na Acqio. Os gestores são chamados a cumprir as seguintes responsabilidades:

- Divulgação e Distribuição de Documentos
- Implementação e Monitoramento de Controles

6.2 Area de Segurança da Informação

A Área de Segurança da Informação desempenha um papel crucial na proteção dos ativos e na promoção de uma cultura de segurança robusta na ACQIO. Suas responsabilidades incluem:

- Elaboração e Atualização de Políticas
- Melhoria Contínua
- Programas Educacionais e de Conscientização
- Alinhamento Estratégico
- Integração de Requisitos
- Gestão de Resultados
- Manutenção de Certificações
- Orientação e Suporte
- Prevenção e Detecção de Incidentes.
- Controle de Vulnerabilidades Cibernéticas
- Gerenciamento de Acessos
- Monitoramento de Ativos Tecnológicos
- Sincronização Temporal
- Auditorias Periódicas
- Tratamento de Incidentes
- Segurança de Dados de Cartão

6.3 Diretoria de Tecnologia

A Diretoria de Tecnologia desempenha um papel fundamental na eficiência operacional e no planejamento estratégico, e no cascateamento das diretrizes de tecnologia da Acqio. Suas responsabilidades abrangem:

- Execução do Processo de Compras de Ativos
- Gerenciamento do Processo de Gestão de Mudanças
- Gestão da Capacidade
- Acompanhamento dos Planos de Continuidade do Negócio e Recuperação de Desastres
- Gestão de Ativos de Interatividade com Usuários Finais
- Elaboração e Manutenção do Inventário de Ativos
- Descarte Seguro de Informações
- Gestão de Ativos de Infraestrutura
- Implementação de Correções de Segurança

7. CONTATOS:

Colaboradores, fornecedores ou outras partes interessadas que observarem desvirtuamento de quaisquer diretrizes desta Política, poderão relatar o fato ao Canal indicado abaixo, de maneira identificada ou anônima: https://acqio.com.br/denuncia/

8. HISTÓRICO DE REVISÕES

Versão	Data de Revisão	Histórico da revisao	Responsavel
1.0	02/2024	Elaboração do documento	Cesar Searlini