Resumo Público Política de Segurança Cibernética do Sistema Ailos

Público-Alvo: Dirigentes, colaboradores e prestadores de serviço das Cooperativas Central e Filiadas e Sociedade em geral		Versão Nro: **03**
Aprovado por: Conselho de Administração	**Data aprovação reunião:** 30/01/2023	
Área Responsável pelo documento: Estratégias de Segurança da Informação		

A Política de Segurança Cibernética do Sistema Ailos estabelece os princípios e diretrizes para a adequada proteção dos ambientes de tecnologia da informação, próprios e de terceiros, que participam, direta ou indiretamente, dos processos de negócios das Cooperativas do Sistema Ailos, procurando estar em conformidade com normas internas e externas, leis e regulamentações vigentes.

Além desses aspectos, esta Política reflete o comprometimento com os padrões de segurança dos serviços financeiros disponibilizados a sociedade em geral, assegurando o cumprimento da missão e visão do Sistema Ailos, objetivando mitigar o risco cibernético.

Nota: Fique atento! Esta Política está sujeita a revisão, com periodicidade mínima anual.

Princípios

Ética – Adota-se a ética como princípio nos negócios e nos relacionamentos com todas as partes interessadas, conforme previsto no Código de Conduta Ética do Sistema Ailos.

Equidade – Considera-se que todos são iguais e devem ser tratados com dignidade e respeito. Desse modo, temos compromisso com a proteção da informação em todos os níveis e de todas as pessoas e instituições, sem qualquer tipo de discriminação ou segregação.

Transparência - Considera-se que a responsabilidade para com a segurança da informação deve ser fundamentada na transparência e na publicidade adequada das informações pertinentes, a fim de assegurar a participação do público interessado, especialmente dos cooperados, dirigentes e colaboradores.

Conformidade – Busca-se continuamente a aderência às leis do nosso país, as definidas pelo Banco Central do Brasil e as demais regulamentações internas aplicáveis ao modelo de negócio do Sistema Ailos.

Este documento é de propriedade intelectual do Sistema Ailos. É proibida a publicação ou reprodução deste documento sem a sua autorização prévia.

Resumo Público Política de Segurança Cibernética do Sistema Ailos

Público-Alvo: Dirigentes, colaboradores e prestadores de serviço das Cooperativas Central e Filiadas e Sociedade em geral		Versão Nro: **03**
Aprovado por: Conselho de Administração	**Data aprovação reunião:** 30/01/2023	
Área Responsável pelo documento: Estratégias de Segurança da Informação		

Diretrizes

a) Implementar e manter os controles de proteção aos dados, sistemas e infraestruturas de TI contra ameaças internas e externas;

b) Estabelecer e praticar controles efetivos para identificação e tratamento de incidentes de Segurança Cibernética;

c) Disseminar continuamente a cultura de Segurança Cibernética adequada para proteção do Sistema Ailos, por meio de programa de conscientização.

d) Garantir que toda informação, sob sua custódia ou responsabilidade seja protegida e gerenciada adequadamente assegurando a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

e) Realizar avaliação dos riscos de segurança da informação e segurança cibernética em níveis aceitáveis, buscando melhorar os controles de segurança da informação de forma contínua.

Segurança Cibernética

O Sistema Ailos considera a segurança um fator determinante para o desenvolvimento sustentável do cooperativismo e para uma comunidade mais próspera e desenvolvida, assim como para se tornar padrão de excelência em serviços financeiros nas regiões de sua atuação. Desta forma nossos processos de controle utilizam padrões sólidos e testados de mercado, abrangendo mas não limitando-se a:

Controles Tecnológicos de Segurança Cibernética

1. Gestão de Vulnerabilidades Cibernéticas:

Mantemos processos de gestão contínua das vulnerabilidades com o objetivo de prevenir, detectar e reduzir os riscos de incidentes no Sistema Ailos.

Este documento é de propriedade intelectual do Sistema Ailos. É proibida a publicação ou reprodução deste documento sem a sua autorização prévia.

2. Gestão de Incidentes:

Registros padronizados de todos os softwares, sistemas e infraestrutura de TI nos auxiliam a monitorar e a responder incidentes de Segurança Cibernética, assim como, testar periodicamente nossos procedimentos para situações de crise.

3. Continuidade de Negócios:

Mantemos e testamos planos de continuidade de negócios para os cenários de indisponibilidades ocasionadas por incidentes de Segurança Cibernética.

4. Classificação de Dados e Informações:

Mantemos processos de classificação de ativos de informação considerando a criação/compra, o uso/processamento, o armazenamento/transmissão e o descarte/destruição.

5. Treinamento e Conscientização:

Incorporamos Segurança da Informação nos programas de conscientização e treinamento obrigatórios de nossos colaboradores e prestadores de serviço e/ou fornecedores.

6. Proteção na Cadeia de Fornecimento:

Condicionamos que todos os softwares, sistemas e infraestrutura de TI contratados no Sistema Ailos, que tratem informações, contenham cláusulas de confidencialidade e exigências de controles de Segurança Cibernética.

Deixamos clara a necessidade de comunicar ao time de Segurança da Informação da Central Ailos incidentes de Segurança Cibernética ocorridos nos ambientes de prestadores de serviços e/ou fornecedores contratados.

Além disso, periodicamente solicitamos comprovação da existência de controles de Segurança Cibernética para a nossa cadeia de fornecimento.

7. Desenvolvimento Seguro de Software:

Este documento é de propriedade intelectual do Sistema Ailos. É proibida a publicação ou reprodução deste documento sem a sua autorização prévia.

Público-Alvo: Dirigentes, colaboradores e prestadores de serviço das Cooperativas Central e Filiadas e Sociedade em geral		Versão Nro: **03**
Aprovado por: Conselho de Administração	**Data aprovação reunião:** 30/01/2023	
Área Responsável pelo documento: Estratégias de Segurança da Informação		

Os sistemas de informação desenvolvidos internamente passam por uma análise de segurança cibernética a qual evidencia os controles necessários, abrangendo mas não se limitando ao que diz respeito sobre:

a) Identificação, autenticação, autorização e não repúdio;

b) Comunicação segura de dados e informações;

c) Armazenamento seguro de dados e informações;

d) Rastreabilidade de operações executadas.

8. Contratação de Serviços em Nuvem:

Seguimos um processo formal para homologação, contratação, medição, revisão e desligamento de softwares, sistemas e infraestrutura de TI hospedados em estruturas de nuvem pública, privada ou similar.

9. Gestão de Riscos de TI

Fazemos gerenciamento e controle da organização em relação a potenciais ameaças, realizando um conjunto de atividades coordenadas que objetiva minimizar e tratar os riscos.

Histórico de Revisões

Versões	Data	Alterações
01	21/02/2019	Elaboração do documento.
02	12/03/2021	Revisão do documento, alterando as descrições das atividades cibernéticas exercidas pela Central Ailos.
03	26/12/2022	Alteração diretrizes. Inclusão Seção 9. Gestão de Riscos de TI

Este documento é de propriedade intelectual do Sistema Ailos. É proibida a publicação ou reprodução deste documento sem a sua autorização prévia.