Política

Segurança cibernética

Versão	Teor da revisão	Data
1.1	Emissão	10/11/2023
1.2	Transformação SCD	28/06/2024

SUMÁRIO

1. OBJETIVO

Em atenção à Resolução nº 4.893, de 26 de fevereiro 2021, do Conselho Monetário Nacional e à Lei n. 13.709/2018, essa política estabelece os princípios, conceitos, valores e práticas a serem adotados visando assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2. PÚBLICO-ALVO

Clientes e usuários da nossa instituição financeira, incluindo titulares de contas bancárias, investidores, parceiros comerciais e funcionários. Todos os indivíduos que interagem com nossos serviços online, plataformas digitais e sistemas de informação estão abrangidos por esta política de segurança cibernética.

3. PRINCÍPIOS

I. **Confidencialidade:** princípio de segurança da informação que garante que a informação seja acessada somente por pessoas ou processos que tenham autorização para acessá-las. Pressupõe a limitação do acesso à informação, sendo permitido o acesso somente às pessoas autorizadas e em circunstâncias que se apresentem efetivamente

necessário o acesso, protegendo informações que devem ser acessíveis apenas por um determinado grupo de usuários contra acessos não autorizados.

II. **Disponibilidade:** princípio de segurança da informação que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido. Pressupõe a garantia de acesso das pessoas devidamente autorizadas à informação sempre que o acesso for necessário, prevenindo interrupções das operações da Instituição por meio de um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.

III. **Integridade:** princípio de segurança da informação que garante a não-violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital. Pressupõe a garantia da veracidade, fidelidade e integridade da informação e dos métodos de seu processamento e eventual tratamento da informação, pois esta não deve ser alterada enquanto está sendo transferida ou armazenada, impedindo que a informação fique exposta ao manuseio por uma pessoa não autorizada e impedindo, também, alterações não aprovadas e sem o controle do controlador (corporativo ou privado) da informação.

4. PROCEDIMENTOS E OS CONTROLES

Para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética, a instituição, inclusive, no desenvolvimento de sistemas de informação seguros e na

adoção de novas tecnologias, adotará os seguintes procedimentos e os controles: autenticação, Criptografia, Prevenção e detecção de intrusão, Controles de acesso, Segmentação de rede de computadores, Manutenção de cópias de segurança dos dados e das informações, Registro, análise da causa e do impacto e controle dos efeitos de incidentes relevantes, Gestão de Prestadores de Serviço, Abrangência.

5. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A instituição comunicará à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidente de segurança, seja ele relativo ao ambiente cibernético ou não, que possa acarretar risco ou dano relevante aos titulares. A referida comunicação deverá ser feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I. a descrição da natureza dos dados pessoais afetados;

II. as informações sobre os titulares envolvidos;

III. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV. os riscos relacionados ao incidente;

V. a causa do incidente;

VI. o impacto do incidente;

VII. os motivos da demora, no caso de a comunicação não ter sido imediata; e

VIII. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente.

6. MANUTENÇÃO DE DOCUMENTAÇÃO

Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

I. o documento relativo à política de segurança cibernética;

II. o documento relativo ao plano de ação;

III. o documento relativo ao plano de resposta a incidentes;

IV. os relatórios anuais de que trata esta política;

V. a documentação referente às práticas de governança corporativa e de gestão e a verificação da capacidade do potencial prestador de serviço;

VI. os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, contado o prazo a partir da extinção do contrato.

VII. os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle da implementação e da efetividade:

a. da política de segurança cibernética, contado o prazo a partir da implementação;

b. do plano de ação, contado o prazo a partir da implementação;

c. do plano de resposta a incidentes, contado o prazo a partir da implementação;

d. dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, contado o prazo a partir da implementação.

7. DÚVIDAS

Em caso de dúvidas sobre o tema relacionado nessa política, contactar a área de Compliance e Controles Internos, através do e-mail: compliance@somoshbi.com.br.

8. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A Diretoria da instituição, ao aprovar esta Política de Segurança Cibernética e da Informação, institui um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética e da informação, buscando sempre manter a instituição em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui adotados, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

9. APROVAÇÃO DA POLÍTICA

Esta política foi aprovada pela Diretoria da Instituição em 28/06/2024, conforme ata de diretoria.