Política

Segurança cibernética

Versão	Teor da revisão	Data
1.1	Emissão	10/11/2023
1.2	Transformação SCD	28/06/2024
1.3	Revisão Anual	28/07/2025

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. DIRETRIZES DE SEGURANÇA CIBERNÉTICA

A segurança cibernética na nossa instituição é guiada por práticas que visam garantir a proteção das informações de clientes, usuários e da própria organização. As diretrizes principais incluem:

- Uso Ético e Transparente das Informações: Os dados são tratados com sigilo e utilizados apenas para as finalidades autorizadas, conforme previsto em lei.
- Controle de Acesso: Apenas pessoas autorizadas têm acesso às informações, sempre de forma individualizada, rastreável e compatível com suas funções.
- Proteção Técnica e Organizacional: Utilizamos medidas como autenticação, criptografia, segmentação de rede, cópias de segurança e sistemas de prevenção e detecção de intrusões.
- Responsabilidade Compartilhada: Todos os colaboradores e parceiros são responsáveis por garantir a segurança da informação e devem relatar riscos ou incidentes à área responsável.
- Prevenção e Resposta a Incidentes: Adotamos processos de monitoramento contínuo, testes de vulnerabilidades e ações preventivas e corretivas em caso de falhas.

5. PROCEDIMENTOS E CONTROLES

Adotamos um conjunto de procedimentos e controles técnicos e organizacionais com o objetivo de proteger os dados e os sistemas utilizados pela instituição. Entre eles, destacam-se:

- Autenticação Segura: Acesso aos sistemas e arquivos exige login e senha, com políticas de atualização periódica e armazenamento seguro das credenciais.
- Criptografia: Utilizada para proteger informações classificadas como sigilosas, tanto em trânsito quanto em repouso.

- Prevenção e Detecção de Intrusões: Utilizamos sistemas que monitoram o ambiente digital e identificam acessos indevidos ou comportamentos suspeitos.
- Controles de Acesso: Os acessos são concedidos com base no perfil de cada usuário, respeitando o princípio do menor privilégio.
- Backup de Dados: Realizamos cópias de segurança periódicas para garantir a recuperação das informações em caso de falhas.
- Segmentação de Rede: As redes são separadas por tipo de serviço e nível de sensibilidade das informações, reduzindo riscos de propagação de ameaças.

6. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA À ANPD

A instituição está comprometida com a transparência e a proteção dos dados pessoais. Em caso de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados, comunicamos prontamente:

- À Autoridade Nacional de Proteção de Dados (ANPD), conforme determina a Lei Geral de Proteção de Dados (LGPD).
- Aos titulares afetados, quando necessário, de forma clara e objetiva.

A comunicação inclui informações sobre a natureza do incidente, os dados afetados, as medidas adotadas para conter os impactos e as ações corretivas implementadas.

7. MANUTENÇÃO DE DOCUMENTAÇÃO

A instituição mantém a documentação relacionada à segurança cibernética disponível para fins de auditoria e fiscalização, conforme exigido pelos órgãos reguladores. Entre os principais registros estão:

- A Política de Segurança Cibernética vigente;
- O plano de ação e o plano de resposta a incidentes;
- Relatórios anuais sobre a implementação das medidas de

segurança;

- Contratos com prestadores de serviços relevantes, especialmente os que envolvem armazenamento e processamento de dados;
- Evidências de controles e práticas de governança adotadas.

Esses documentos são arquivados e preservados pelo prazo legal, assegurando transparência, rastreabilidade e conformidade regulatória.

8. DIVULGAÇÃO

A Política de Segurança Cibernética é divulgada de forma clara e acessível a todos os públicos relevantes, incluindo colaboradores, prestadores de serviço e usuários. Essa divulgação ocorre por meio:

- Da disponibilização em canais internos da empresa;
- De treinamentos e ações de conscientização;
- E da publicação de um resumo público desta política na página oficial da instituição, permitindo que clientes e usuários conheçam os principais compromissos e práticas adotadas em segurança da informação.

A comunicação é feita de forma transparente, com linguagem adequada e compatível com as funções e responsabilidades dos envolvidos.

9. DÚVIDAS

Caso tenha dúvidas sobre esta política ou precise de esclarecimentos relacionados à segurança da informação, você pode entrar em contato com a área responsável por meio do e-mail: compliance@somoshbi.com.br

Nosso time está disponível para orientar sobre boas práticas, esclarecer responsabilidades e responder a eventuais questionamentos sobre o tratamento de dados e a segurança cibernética.

10. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A alta administração da HBI reitera seu compromisso com a segurança da informação e do ambiente cibernético, promovendo a melhoria contínua das práticas, controles e políticas adotadas.

Esse comprometimento garante que a instituição:

- Esteja em conformidade com as normas legais e regulatórias;
- Atue de forma preventiva frente a riscos cibernéticos;
- Proteja os dados e a privacidade de seus clientes, parceiros e colaboradores;
- Mantenha a confiança e a integridade em seus processos digitais.

11. APROVAÇÃO DA POLÍTICA

Esta Política de Segurança Cibernética foi aprovada pela Diretoria da HBI em 30 de junho de 2025, conforme previsto no processo de revisão anual.

A versão atual (1.3) reflete as atualizações regulatórias, operacionais e tecnológicas avaliadas no período, mantendo o compromisso da instituição com a proteção de dados e a segurança das informações.