1. FLUXO

N/A

2. HISTÓRICO DE REVISÕES

Versão	Data	Alteração
00	12/05/2022	Emissão Inicial do Documento.
01	30/04/2025	Ajuste regra para acesso remoto, alteração de elaborador e aprovador.
02	13/07/2026	Reestruturação do documento; inclusão de compromisso de melhoria contínua, estrutura para objetivos de SI, lista de políticas específicas correlatas e inclusão da classificação do documento.

3. OBJETIVO

Estabelecer diretrizes institucionais para a utilização dos recursos de tecnologia e ativos de informação no âmbito das atividades da organização, assegurando conformidade com a legislação aplicável e alinhamento aos princípios de segurança da informação.

4. CAMPO DE APLICAÇÃO

Esta política aplica-se a todos os colaboradores, prestadores de serviço, parceiros e terceiros que utilizem recursos de tecnologia ou ativos de informação da organização.

5. RESPONSABILIDADES E EXECUÇÃO

Departamento ou Função	Responsabilidades
Diretoria/Alta Gestão	Avaliar e aprovar a política corporativa.
Gestão da Qualidade	Controlar o fluxo documental corporativo, incluindo versionamento, codificação, homologação formal, arquivamento, obsolescência e aderência ao processo documental do SGQ.
Gestão de Segurança da Informação	Elaborar, revisar, manter, divulgar, treinar e monitorar o cumprimento das políticas e controles de segurança da informação aplicáveis.
Gestão de Infraestrutura de TI	Implementar e administrar os controles técnicos necessários ao cumprimento da política, incluindo gerenciamento dos dispositivos de segurança, perfis de acesso e manutenção da infraestrutura tecnológica.

Colaboradores	Cumprir as diretrizes estabelecidas nos documentos corporativos e comunicar desvios, inconsistências ou necessidade de revisão ao responsável da área.

6. TERMOS E DEFINIÇÕES

- **Ativo de Informação -** Qualquer informação ou recurso que tenha sido gerado e/ou tenha valor para a organização.
- **Segurança da Informação -** Conjunto de medidas destinadas a proteger a confidencialidade, integridade e disponibilidade das informações.
- **SGSI (Sistema de Gestão de Segurança da Informação) -** Sistema de gestão que estabelece, implementa, mantém e melhora continuamente a segurança da informação na organização.

7. DESCRIÇÃO

7.1. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação na organização é fundamentada nos seguintes princípios:

7.1.1. Confidencialidade

As informações devem ser acessadas exclusivamente por pessoas autorizadas, de acordo com suas responsabilidades e necessidades de negócio.

7.1.2. Integridade

As informações devem ser protegidas contra alterações não autorizadas, indevidas ou acidentais, garantindo sua exatidão e completude.

7.1.3. Disponibilidade

As informações e os recursos associados devem estar disponíveis sempre que necessários para a execução das atividades da organização.

7.1.4. Responsabilidade

Todos os envolvidos no uso, tratamento ou acesso às informações são responsáveis por agir de acordo com esta política e com as normas internas aplicáveis.

7.2. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

A organização estabelece as seguintes diretrizes gerais:

- A segurança da informação é responsabilidade de todos os colaboradores e partes autorizadas.
- As informações são consideradas ativos essenciais para o funcionamento do negócio e devem ser protegidas ao longo de todo o seu ciclo de vida.
- A organização compromete-se a cumprir os requisitos legais, regulatórios e contratuais aplicáveis, incluindo aqueles relacionados à proteção de dados pessoais.

- Dados pessoais tratados pela organização são considerados ativos de informação e devem receber proteção adequada, conforme legislação aplicável (LGPD 13.709/2018).
- Medidas de segurança devem ser proporcionais aos riscos identificados, considerando o impacto potencial para o negócio, para os titulares de dados e para as partes interessadas.
- A organização compromete-se com a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI), avaliando periodicamente sua adequação, suficiência e eficácia por meio de auditorias internas, análises críticas pela Alta Direção e implementação de ações corretivas e preventivas.
- Esta Política estabelece a estrutura de referência para a definição dos objetivos de segurança da informação da organização, os quais devem ser mensuráveis (quando aplicável), compatíveis com os princípios de Confidencialidade, Integridade e Disponibilidade definidos no item 7.1, comunicados às partes interessadas pertinentes, monitorados periodicamente e revisados no mínimo anualmente, em conjunto com a revisão desta Política.
- A organização deve realizar controle de acesso das informações conforme o nível de classificação do documento.
- A organização compromete-se a fazer o monitoramento e registro dos incidentes de segurança, assim como o monitoramento do desempenho e eficácia do SGSI, através de indicadores de performance.
- O descumprimento desta política poderá resultar na aplicação de medidas administrativas, disciplinares ou legais, conforme aplicável.

7.3. PAPÉIS E RESPONSABILIDADES

7.3.1. Alta Direção

A Alta Direção é responsável por:

- aprovar esta Política de Segurança da Informação;
- assegurar que a segurança da informação esteja alinhada aos objetivos estratégicos da organização;
- prover os recursos necessários para a implementação e manutenção do SGSI.

7.3.2. Colaboradores e Terceiros

Todos os colaboradores, parceiros e terceiros autorizados são responsáveis por:

- conhecer e cumprir esta política;
- proteger as informações às quais tenham acesso;
- comunicar eventuais incidentes ou fragilidades relacionadas à segurança da informação.

7.3.3. Funções de Apoio à Segurança da Informação

As funções responsáveis pela segurança da informação devem:

- apoiar a implementação das diretrizes definidas nesta política;
- promover ações de conscientização e orientação;

- acompanhar o cumprimento das normas e políticas relacionadas à segurança da informação.

7.4. APROVAÇÃO E DIVULGAÇÃO

7.4.1. Aprovação e Compromisso

Esta Política deve ser formalmente aprovada pela Alta Direção.

A aprovação deve ser registrada por meio de assinatura eletrônica ou física.

7.4.2. Divulgação aos colaboradores, prestadores de serviço, parceiros e terceiros

Todos os colaboradores, prestadores de serviço, parceiros e terceiros, devem tomar conhecimento da política de segurança para desempenhar suas funções na organização através da política de segurança disponível no site da organização.

7.4.3. Controle de revisão

Esta política deve ser revisada, pela área de segurança da informação da organização, anualmente ou sempre que houver mudança significativa no negócio, legislação ou resultado de auditoria.

8. ANEXOS E DOCUMENTOS COMPLEMENTARES

Esta Política de Segurança da Informação é complementada pelas seguintes políticas específicas, que detalham as diretrizes aqui estabelecidas:

- POL-SI-HOS-001 – Política de Uso da Internet
- POL-SI-HOS-002 – Política de Uso do E-mail Corporativo
- POL-SI-HOS-003 – Política de Acesso aos Sistemas e Recursos de Rede
- POL-SI-HOS-004 – Política de Utilização dos Recursos de Informação
- POL-SI-HOS-006 – Política de Segurança Física e Lógica
- POL-SI-HOS-007 – Política de Descarte de Mídias
- POL-SI-HOS-008 – Política de Gestão de Incidentes
- POL-SI-HOS-009 – Política de Equipamentos Particulares ou Privados
- POL-SI-HOS-010 – Política de Acesso Remoto
- POL-SI-HOS-011 – Política de Backup
- POL-SI-HOS-012 – Política de Gestão de Ativos
- POL-SI-HOS-013 – Política de Utilização de Rede
- POL-SI-HOS-014 – Política de Classificação da Informação
- POL-SI-HOS-015 – Política de Gestão de Senha
- POL-SI-HOS-016 – Política de Continuidade de Negócio
- POL-SI-HOS-017 – Política de Gestão de Vulnerabilidade
- POL-SI-HOS-018 – Política de Privacidade de Dados
- POL-SI-HOS-019 – Política de Criptografia
- POL-SI-HOS-023 – Política de Ciclo de Vida de Software
- POL-SI-HOS-024 – Política de Fornecedores
- POL-SI-HOS-025 – Política de Gestão de Configuração

- POL-SI-HOS-026-Política de Proteção contra Código Malicioso
- POL-SI-HOS-027-Política de Transferência de Informações
- POL-SI-HOS-029-Política de Comunicação em Segurança da Informação
- POL-SI-HOS-030-Política de Monitoramento

Em caso de conflito entre esta Política e uma política específica, prevalece a diretriz de maior nível de proteção, devendo a divergência ser comunicada à Gestão de Segurança da Informação para ajuste do documento.

A política é complementada pelo organograma de SGSI:

- DOC-SI-HOS-001- Responsabilidades e Funções - Organograma SGSI

A política é complementada pelas Normas:

- NOR-SI-HOS-020-01-Norma de Papeis e Responsabilidades Segregadas 5-2
- NOR-SI-HOS-020-02-Norma de Revisão Independente da Segurança da Informação 5-35

9. REFERÊNCIAS NORMATIVAS

Referência documento ABNT NBR ISO/IEC27001.
Declaração de aplicabilidade: A.5.1, A.5.2, A.5.4, A.5.35, A.5.36, A.6.3

10. REGISTROS GERADOS

N/A

11. ASSINATURA E APROVAÇÃO

Assinatura elaborador:	Assinatura revisor:	Assinatura aprovador 1:	Assinatura aprovador 2:
Nome: [redacted] *Cargo:* [redacted]	Nome: [redacted] *Cargo:* [redacted]	Nome: [redacted] *Cargo:* [redacted]	Nome: [redacted] *Cargo:* [redacted]
Data:	Data:	Data:	Data:

12. HOMOLOGAÇÃO

Data:
Nome:
Cargo: