1. OBJETIVO

A CARE estabelece sua Política de Segurança da Informação e Privacidade, como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas do mercado, à normas internacionalmente aceitas e a legislação brasileira pertinente, com o objetivo de **garantir níveis adequados de proteção as informações e dados pessoais** operados pela organização, de seus clientes e colaboradores sob sua responsabilidade.

2. PROPÓSITO

- Esta política tem por propósito:
- Estabelecer diretrizes e normas de Segurança da Informação e Privacidade que permitam aos colaboradores da CARE adotarem **padrões de comportamento seguro**;
- Orientar quanto à adoção de **controles e processos** para atendimento dos requisitos de Segurança da Informação e Privacidade dos Dados Pessoais;
- Resguardar as informações da CARE, garantindo os **requisitos básicos de confidencialidade, integridade e disponibilidade**;
- Prevenir possíveis incidentes e responsabilidade legal envolvendo a instituição, colaboradores, clientes, fornecedores e parceiros;
- Minimizar os riscos de **perdas financeiras, de mercado, de confiança de clientes ou outros impactos negativos** no negócio da CARE como resultado de falhas de segurança.

3. POLÍTICA

Esta política se aplica a todos os colaboradores, fornecedores e parceiros da **CARE**, que possuem acesso às informações e dados pessoais da CARE e/ou fazem uso de recursos computacionais compreendidos na infraestrutura interna.

3.1. É Política da CARE:

- Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de **confidencialidade**, **integridade** e **disponibilidade** das informações e dados pessoais operados na **CARE** sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;
- Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Colaboradores, terceiros contratados, fornecedores e, onde pertinente, clientes.
- Garantir a educação e a conscientização sobre as práticas de segurança da informação e privacidade de dados adotadas pela **CARE** para Colaboradores, terceiros contratados, fornecedores e, onde pertinente, clientes.
- Atender integralmente requisitos de segurança da informação e privacidade dos dados pessoais aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

- Tratar integralmente incidentes de segurança da informação e a privacidade de dados pessoais, garantindo que eles sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;
- Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
- Melhorar continuamente a Gestão de Segurança da Informação e Privacidade através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

4. PAPÉIS E RESPONSABILIDADES

4.1. Comitê Gestor de Segurança da Informação - CGSI

Fica constituído o Comitê Gestor de Segurança da Informação - CGSI, contando com a participação de, pelo menos, um Diretor de Tecnologia, um Gerente de Tecnologia da Informação e pelo menos dois membros com conhecimento em tecnologia da informação, tanto com suporte a infraestrutura quanto com sistemas.

4.2. É responsabilidade do CGSI:

- Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;
- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;
- Garantir que as atividades de segurança da informação e privacidade de dados sejam executadas em conformidade com a PSIP;
- Promover a divulgação da PSIP e tomar as ações necessárias para disseminar uma cultura de segurança da informação e privacidade de dados pessoais no ambiente da **CARE**

5. PRINCÍPIOS DE USO DE IA

Todas as soluções de IA devem ser projetadas e implementadas com mecanismos robustos de segurança para proteger os dados contra acessos não autorizados, vazamentos, modificações indevidas e outros tipos de ataques cibernéticos. Os modelos de IA devem ser treinados e validados de forma a minimizar riscos à integridade e confidencialidade das informações.

O uso de IA deve ser realizado em conformidade com a legislação vigente de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR), quando aplicável. O processamento de dados pessoais por IA deve ser feito de forma transparente, garantindo o consentimento adequado dos titulares dos dados, sempre que necessário.

6. CLASSIFICAÇÃO E TRATAMENTO DE INCIDENTES

Todo incidente de segurança da informação deve ser classificado conforme sua criticidade e impacto, e tratado em conformidade com os procedimentos estabelecidos. A comunicação de incidentes críticos deve ser imediata ao CGSI, e as ações de contenção e mitigação devem ser iniciadas imediatamente.

7. SANÇÕES E PUNIÇÕES

As violações desta política ou de outras normas de segurança, ainda que por omissão, serão passíveis de penalidades que variam de advertência verbal a demissão por justa causa para colaboradores CLT, e rescisão imediata de contratos para terceiros ou fornecedores. O CGSI é responsável por analisar cada infração e deliberar sobre as punições.

Em casos de violação que impliquem em atividades ilegais ou danos à organização, o infrator será responsabilizado e sujeito a medidas legais cabíveis. A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado e recorrência, podendo o CGSI, repassar a informação da infração ao Gestor imediato que, aplicará a pena quando identificada a falta grave.

No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a Organização, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

6. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da **CARE** adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações e dados pessoais.

7. HISTÓRICO DAS ALTERAÇÕES

Data	Revisão	Histórico
18/11/2022	01	Aprovação inicial
22/12/2023	02	Revisão e inclusão do item 5. (utilização de IA responsável)
30/09/2024	03	Revisão de item 5. e inclusão item 6.