renova PARTNERS	**Política de Segurança da Informação - PSI**		Código: **PO-SI-001**
Data Criação: **06/03/2024**	Tipo: **POLÍTICA**	Vigência: **Indeterminado**	Versão: 08

Sumário

1. TERMOS E DEFINIÇÕES

Aceitação do Risco: Consiste na decisão de aceitar um risco;

Acionista: Trata-se de qualquer pessoa física e/ou jurídica incorporada ao quadro societário do **Grupo Renova;**

Análise de Riscos: Consiste no processo de compreender a natureza do risco e determinar o nível de risco;

Ativo: São todos os bens do **Grupo Renova** que têm valor econômico, incluindo a informação e todos os recursos utilizados para o seu tratamento, tráfego e armazenamento;

Avaliação de Riscos: Consiste no processo de comparar o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;

CGSI: Consiste no Comitê de Gestão de Segurança da Informação;

Cliente: Trata-se de qualquer pessoa física e/ou jurídica que contrata serviços do **Grupo Renova;**

Colaborador: Trata-se de qualquer pessoa física contratada pelo **Grupo Renova;**

CID: Trata-se da Confiabilidade da Informação e serve para especificar as propriedades de confidencialidade, integridade e disponibilidade reunidas;

Confidencialidade: Trata-se da garantia de que a informação não seja revelada ou esteja disponível para terceiros não autorizados;

Disponibilidade: Trata-se da garantia de que a informação esteja sempre acessível e disponível quando necessário, considerando: a prontidão: ser acessível sempre que necessário; a continuidade da operação: manter-se disponível mesmo quando houver falhas nos sistemas; e a robustez: atender a todos os usuários do sistema sem que haja uma degradação que comprometa o resultado;

Fornecedor: Trata-se de qualquer pessoa jurídica contratada pelo **Grupo Renova;**

Gestão de Riscos: Trata-se de atividades coordenadas para dirigir e controlar uma empresa em relação ao risco;

Grupo Renova: São todas as empresas pertencentes ao Grupo, quais sejam: Renova Invest Assessoria de Investimentos Ltda., RNV Corretora de Seguros Ltda. e Altera Capital Consultoria e Gestora de Investimentos Ltda., além de outras que porventura venham a ser constituídas futuramente;

Incidente de Segurança da Informação: Consiste no evento de segurança da informação indesejado ou inesperado, que tem uma significativa probabilidade de comprometer as operações de negócios, ameaçando a segurança da informação;

Informação: Todo e qualquer conteúdo ou dado que tenha valor para alguma empresa ou pessoa, podendo estar guardado para uso restrito ou exposto ao público para consulta ou aquisição;

Integridade: Consiste na garantia da salvaguarda e completeza da informação e dos métodos de processamento;

ISO 27001: Consiste nas diretrizes para implementação de um Sistema de Gestão de Segurança da Informação;

ISO 31000: Consiste nas diretrizes para implementação de um processo de gestão de riscos;

Parceiro: Trata-se de qualquer terceiro que tenha ligação com o **Grupo Renova** e suas informações, e que não tenha nenhum vínculo societário, contrato de trabalho ou contrato de prestação de serviços direto com qualquer uma das empresas do **Grupo Renova** (Ex. gerenciadoras, colaborador de consórcio);

Prestador de Serviços: Trata-se de qualquer pessoa jurídica contratada pelo **Grupo Renova;**

PSI: Consiste na Política de Segurança da Informação;

Risco Residual: Trata-se do risco remanescente após o tratamento de risco;

Segurança da Informação: Consiste na preservação do sigilo, da integridade e disponibilidade de informações;

SGSI: Trata-se do Sistema de Gestão de Segurança da Informação;

Sócio: Trata-se de qualquer pessoa física e/ou jurídica pertencente ao quadro societário de qualquer empresa do **Grupo Renova**;

Tratamento do risco: Consiste no processo de seleção e implementação de medidas para modificar um risco;

Usuário: Trata-se de todo Acionista, Sócio, Colaborador ou Prestador de Serviços que contribui para a execução de atividades e que tenha acesso aos recursos tecnológicos disponibilizados pelo **Grupo Renova;**

Vírus: Trata-se de programa malicioso que se propaga infectando um equipamento, podendo causar danos como indisponibilidade de serviços ou comprometimento na integridade e confidencialidade de informações; e

Visitante: Trata-se de qualquer pessoa física que adentrar nas dependências do **Grupo Renova.**

2. OBJETIVO

A Política de Segurança da Informação (PSI) do **Grupo Renova** tem como objetivo:

a) Estabelecer diretrizes e orientações que permitam aos acionistas, sócios, colaboradores e prestadores de serviços das empresas que compõem o **Grupo Renova**, a seguir padrões de comportamento desejáveis e aceitáveis de acordo com a legislação e as boas práticas mundiais de segurança da informação;

b) Nortear a definição de procedimentos específicos de Segurança da Informação;

c) Definir mecanismos para preservar as informações do **Grupo Renova** quanto à confidencialidade, integridade e disponibilidade;

d) Orientar a implementação de controles e processos para atendimento dos requisitos para Segurança da Informação; e

e) Minimizar os riscos de perdas financeiras, de participação no mercado, de confiança dos clientes e parceiros, ou de qualquer outro impacto negativo no negócio do **Grupo Renova**, resultante de uma falha de segurança.

3. ABRANGÊNCIA

Esta Política de Segurança da Informação tem abrangência sobre todas as áreas e empresas que compõem o **Grupo Renova**.

4. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

O Sistema de Gestão de Segurança da Informação consiste no conjunto de políticas, procedimentos, diretrizes, recursos e atividades que buscam proteger os ativos de informação.

O SGSI é uma abordagem sistemática para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação do **Grupo Renova.**

São princípios que contribuem para o sucesso da implementação de um SGSI:

a) A consciência da necessidade de manter a segurança da informação;

b) Atribuição de responsabilidades para segurança da informação;

c) Incorporação de compromisso de gestão e os interesses dos *stakeholders*;

d) Reforçar os valores do **Grupo Renova;**

e) As avaliações de risco que determinam os controles apropriados para alcançar níveis aceitáveis de risco;

f) Segurança incorporada como um elemento essencial das redes e sistemas de informação;

g) A prevenção e detecção de incidentes de segurança da informação;

h) Assegurar uma abordagem global da gestão de segurança da informação; e

i) Contínua reavaliação da segurança da informação.

5. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O **Grupo Renova** adota o seguinte compromisso para a PSI:

"Gerir de forma eficiente e eficaz os dados e informações de clientes, acionistas, sócios, colaboradores e prestadores de serviços, de modo a mitigar os riscos relacionados à vulnerabilidade, vazamento ou perda de informações, em conformidade com os requisitos legais e regulamentares aplicáveis, assegurando, assim, a proteção e a integridade das informações."

6. DIVULGAÇÃO E DECLARAÇÃO DE RESPONSABILIDADE

A PSI deve ser de conhecimento de todos os Acionistas, Sócios, Colaboradores, Prestadores de Serviços do **Grupo Renova**, bem como de Clientes, Parceiros, Fornecedores e demais partes interessadas. Para tanto, deve ser divulgada da seguinte forma:

a) Impressa;

b) Nas campanhas de Segurança da Informação; e

c) Digital, através da rede corporativa e no Site do **Grupo Renova.**

A PSI deve estar disponível em local de acesso a todos e protegida contra alterações.

Todos os Acionistas, Sócios, Colaboradores e Prestadores de Serviços do **Grupo Renova** devem assinar o **"TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO"** comprometendo-se a agir de acordo com os seus requisitos.

7. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A informação do **Grupo Renova**, produzida ou recebida, deve ser utilizada com responsabilidade e de modo ético e seguro, em benefício exclusivo dos negócios corporativos, baseado nos seguintes princípios:

a) **Confidencialidade**: Garantir que o acesso à informação seja obtido somente por pessoas autorizadas e quando for de fato necessário;

b) **Integridade:** Garantir a exatidão e completude da informação e dos métodos de seu processamento, bem como da transparência no tratamento com os públicos envolvidos; e

c) **Disponibilidade**: Garantir que somente pessoas autorizadas tenham acesso à informação, sempre que necessário.

8. DIRETRIZES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A PSI do **Grupo Renova** estabelece os principais controles de proteção, organizados em diretrizes específicas:

a) As informações do **Grupo Renova**, sejam de Clientes, Acionistas, Sócios, Colaboradores, Prestadores de Serviços e/ou Parceiros, devem ser tratadas de forma ética, sigilosa e em conformidade com esta Política e demais Normas de Segurança da Informação, evitando-se o uso indevido ou a exposição inadequada dessas informações.

b) A informação deverá ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;

c) A identificação de cada acionista, sócio, colaborador e prestador de serviços, deve ser única, pessoal e intransferível, responsabilizando-o integralmente pelas ações realizadas;

d) A senha de acesso deve ser mantida em sigilo, sendo proibido seu compartilhamento; e

e) Todos os riscos quanto às informações do **Grupo Renova** devem ser reportados para a área de Tecnologia da Informação (TI), para que sejam devidamente analisados, avaliados e tratados.

9. COMITÊ DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

O Comitê de Gestão de Segurança da Informação é formado por representantes das principais áreas do **Grupo Renova,** e consiste no órgão responsável por revisar e atualizar esta PSI periodicamente, garantindo sua conformidade com as exigências legais e regulamentares.

Para manter um nível satisfatório de segurança das informações, cabe ao CGSI adotar as seguintes cautelas:

a) O controle de acesso dos Acionistas, Sócios, Colaboradores e Prestadores de Serviços aos ativos de informação deve ser devidamente aprovado pelo responsável pela informação, a qual o acesso permitirá a manipulação, quer seja para simples consulta ou para alteração, conforme Norma de Controle de Acesso;

b) O uso dos e-mails sob domínio@renovainvest.com.br, domínio@rnvcorretora.com.br, e/ou domínio@alteracapital.com.br, serão permitidos para Acionistas, Sócios, Colaboradores e Prestadores de Serviços. Quanto à transmissão de dados, este recurso deve ser utilizado para garantir a privacidade na comunicação dos dados, conforme Norma de Correio Eletrônico e Transmissão de Dados (NOR 013);

c) As cópias de segurança (*backups*), de informações devem ser consideradas vitais para o sistema e para a retomada das atividades da área em caso de contingência, conforme Norma de Cópias de Segurança Backup (NOR 010);

d) As regras para o desenvolvimento seguro de sistemas e *softwares* devem ser estabelecidas e aplicadas aos desenvolvimentos realizados, conforme Norma de Desenvolvimento Seguro (NOR 015);

e) A concessão de acesso remoto para os Acionistas, Sócios, Colaboradores e Prestadores de Serviços deve ser autorizada formalmente e solicitada ao responsável pela área de TI, ocasião em que deverá ser indicado o tipo de acesso, permissão e as informações a serem acessadas, conforme Norma de Acesso Remoto (NOR 002);

f) Por dispositivo móvel, entende-se qualquer equipamento eletrônico com atribuições de mobilidade no manuseio da informação e destina-se ao uso em serviço para realização das atividades e para comunicação com qualquer empresa pertencente ao **Grupo Renova**, Fornecedores ou Clientes, devendo ser utilizado somente para esta finalidade, conforme Norma de Dispositivos Móveis;

g) As informações devem ser classificadas e manuseadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: **Pública, Interno Confidencial Leitura, Confidencial Edição e Confidencial BTG.** Além disso, devem ser tratadas, armazenadas e descartadas de maneira correta para garantir os aspectos de segurança da informação no negócio, conforme Norma de Classificação e Manuseio da Informação;

h) Os ativos tangíveis e intangíveis de informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, conforme Norma de Gestão de Ativos (NOR 005);

i) As mídias devem ser gerenciadas de forma adequada, conforme os requisitos de segurança da informação informados na Norma de Gerenciamento de Mídias (NOR 026);

j) Estão estabelecidas na Norma de Gerenciamento de Chaves Criptográficas (NOR 006), um conjunto de regras para garantir a padronização das técnicas criptográficas, a aplicação adequada das mesmas e as responsabilidades para manter a segurança no transporte ou armazenamento das informações independente do meio utilizado;

k) Um processo de gestão de mudanças deve estar em vigor, para assegurar que os controles e modificações em sistemas ou recursos de processamento de informações sejam realizados de forma planejada, evitando falhas operacionais ou de segurança no ambiente produtivo do **Grupo Renova**, em conformidade com a Norma de Gerenciamento de Mudanças de TI (NOR 007).

l) Para garantia da proteção das informações de maneira eficaz e redução dos riscos de acesso não autorizado, perda ou dano à informação, durante e fora do expediente de trabalho, devem ser adotadas todas as medidas de segurança, conforme Norma de Mesa Limpa e Tela Protegida (NOR 008);

m) Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos de segurança da informação (Confidencialidade, Integridade e Disponibilidade), conforme Norma de Gestão de Riscos (NOR 009);

n) Todos os incidentes que afetem a segurança da informação devem ser reportados ao responsável pela área de TI, que analisará o incidente e reportará à Governança de TI Corporativa, e/ou ao Prestador de Serviços de suporte de TI, conforme Norma de Respostas à Incidentes de Segurança da Informação (NOR 011);

o) Os ambientes de produção e desenvolvimento devem ser segregados e rigidamente controlados;

p) Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação dos requisitos previstos nesta PSI, o responsável e/ou solicitante deverá documentá-las imediatamente ao CGSI, para que possibilite a adoção de medidas alternativas que minimizem os riscos, bem como um plano de ação para corrigi-los, monitorá-los ou eliminá-los;

q) Todos os Acionistas, Sócios, Colaboradores e Prestadores de Serviços do **Grupo Renova** devem passar por treinamento e conscientização sobre os procedimentos de segurança e uso correto dos ativos disponibilizados. Esses programas visam minimizar possíveis riscos de segurança, esclarecer suas responsabilidades e comunicar os procedimentos para notificação de incidentes; e

r) Todas as pessoas devem ser distintamente identificadas, sejam Acionistas, Sócios, Colaboradores, Prestadores de Serviços, Visitantes, Parceiros etc.

s) Para garantir a eficácia do SGSI e os principais controles de segurança é necessário o monitoramento e melhoria contínua. Para tanto, o **Grupo Renova** implementou a Norma de Indicadores e Métricas do SGSI (NOR 016).

Além disso, cabe ao CGSI cumprir as seguintes responsabilidades:

a) Garantir a disponibilidade de recursos financeiros para todas as ações de Segurança da Informação;

b) Manter o foco e promover a Segurança da Informação do Grupo Renova, aprovando políticas que reflitam o seu papel acima descrito;

c) Garantir que riscos à Segurança da Informação sejam identificados, avaliados e categorizados;

d) Sugerir ações para tratar os riscos e monitorar a sua implantação;

e) Dar direcionamento, revisar e atualizar a estratégia de Segurança da Informação, garantindo, assim, que a PSI, normas e procedimentos sejam adequadamente atualizados continuamente; e

f) Garantir treinamentos de conscientização sobre a Segurança da Informação, seja aos Acionistas, Sócios, Colaboradores e Prestadores de Serviços e, quando pertinente, a terceiros, Parceiros e Clientes.

10. MONITORAMENTO

O **Grupo Renova** deve monitorar e registrar o uso de todas as informações geradas, armazenadas ou transmitidas. Para isso, deve implementar controles adequados manter trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que considerar necessários, a fim de reduzir os riscos. O **Grupo Renova** reservar-se o direito de:

a) Implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônico, navegação, Internet, dispositivos móveis ou *wireless* e outros componentes da rede. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;

b) Inspecionar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente corporativo, incluído a ferramenta “whatsapp business”, visando assegurar o rígido cumprimento desta PSI;

c) Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso;

d) Bloquear os acessos a determinados sites nos equipamentos dos sócios, colaboradores e prestadores de serviço com o intuito de evitar vazamentos de dados (e-mail pessoal, whatsapp, etc), conteúdo impróprio (pornografia, violência, apostas, drogas e etc), e sites maliciosos (phishing, malware, ransomware); e

e) Instalar câmeras nas instalações físicas.

Para obter mais informações sobre as questões relativas ao monitoramento consultar a Norma de Monitoramento de Ativos (NOR 012).

11. RESPONSABILIDADES ESPECÍFICAS

11.1. Acionistas, Sócios, Colaboradores e Prestadores de Serviços

Os Acionistas, Sócios, Colaboradores e Prestadores de Serviços do **Grupo Renova**, independentemente de seu nível hierárquico, são responsáveis por cumprir, fazer cumprir e zelar pela efetivação das normas e princípios de segurança da informação, em conformidade com os critérios legais e éticos que regem todo o **Grupo Renova**.

Cada indivíduo é integralmente responsável por qualquer prejuízo ou dano que possa sofrer ou causar ao **Grupo Renova** e/ou a terceiros em decorrência do não cumprimento das diretrizes desta PSI e das normas nela referidas.

Adicionalmente, é responsabilidade de todos utilizar senhas seguras, devendo realizar a alteração de suas senhas conforme a periodicidade estabelecida pelo **Grupo Renova.**

Cabe a todos do **Grupo Renova**:

a) Cumprir fielmente as Políticas, Normas e Procedimentos de Segurança da Informação estabelecidas neste documento;

b) Buscar orientação com o responsável pela área de TI, quando houver dúvidas relacionadas à segurança da informação;

c) Assinar o **TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO**, formalizando a ciência da PSI, bem como assumindo a responsabilidade pelo seu cumprimento;

d) Proteger as informações contra o acesso, modificação, divulgação ou destruição não autorizada pelo **Grupo Renova**;

e) Assegurar que os recursos tecnológicos sejam utilizados somente para fins profissionais aprovados e de interesse do **Grupo Renova**; e

f) Comunicar imediatamente ao responsável pela área de TI, qualquer descumprimento ou violação desta Política e/ou de suas normas e procedimentos relacionadas.

11.2. Gestores

É responsabilidade de cada gestor inventariar, atribuir valor, analisar quanto aos riscos e classificar, conforme a Norma de Classificação e Manuseio da Informação, todos os ativos de informação necessários à sua área.

Garantir na sua área a implementação de mecanismos necessários para descarte seguro das informações.

Cabe a todo gestor:

a) Ter postura exemplar em relação à Segurança da Informação;

b) Cumprir e fazer cumprir esta PSI, as Normas e os Procedimentos de Segurança da Informação;

c) Especificar e solicitar previamente permissão de acesso, elencando os ativos de informação para serviços em geral que não sejam contratados;

d) Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI; e

e) Comunicar imediatamente o responsável pela área de TI em caso de eventuais violações da segurança da informação.

11.3. Proprietários de Ativos de Informação

O Proprietário da informação pode ser qualquer Acionista e/ou Sócio, o qual será responsável pela manutenção, revisão e cancelamento de autorização à determinada informação ou conjunto de informações pertencentes ao **Grupo Renova** ou sob sua guarda.

Cabe ao proprietário da informação:

a) Elaborar para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções das empresas pertencentes ao **Grupo Renova** às autorizações de acesso concedidas;

b) Manter registro e controle atualizado de todas as autorizações de acesso concedidas, determinando sempre que necessário a pronta suspensão do acesso ou alteração da autorização concedida;

c) Reavaliar as autorizações de acesso sempre que necessário ou solicitado, cancelando aquelas que não se fizerem mais necessárias; e

d) Participar, sempre que convocado, das reuniões do CGSI, prestando os esclarecimentos quando solicitado.

11.4. Área de Tecnologia da Informação

A área de TI será responsável por:

a) Fazer a gestão do uso de tecnologias necessárias ao bom andamento dos negócios do **Grupo Renova**, incluindo ações preventivas e tratamento de incidentes a fim de promover maior nível de segurança da Informação;

b) Ações direcionadas às questões técnicas que estão definidas;

c) Submeter ao CGSI as revisões da PSI e das Normas de Segurança da Informação, e após a aprovação, publicar e difundir as mesmas nas empresas pertencentes ao **Grupo Renova**;

d) Propor as metodologias e processos específicos para a Segurança da Informação, como por exemplo, Avaliação de Risco;

e) Propor e apoiar iniciativas que visem à segurança dos ativos de informação do **Grupo Renova**;

f) Promover junto ao responsável da área de TI, a conscientização dos Acionistas, Sócios, Colaboradores, Prestadores de Serviços e Parceiros, com relação a Segurança da Informação do **Grupo Renova**, por meio de campanhas, palestras, treinamentos e outros meios;

g) Apoiar a avaliação e a adequação de controles específicos de Segurança da Informação para novos sistemas ou serviços;

h) Analisar criticamente incidentes de Segurança da Informação em conjunto com o CGSI; e
i) Manter a comunicação efetiva com o CGSI, com o objetivo de mantê-lo adequadamente informado sobre assuntos relacionados ao tema, que afetem ou tenham potencial para afetar o **Grupo Renova**.

11.5. Área Jurídica

A área Jurídica será responsável por:

a) Colher a assinatura do **TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO** dos Acionistas, Sócios, Colaboradores e Prestadores de Serviços, bem como efetuar o seu arquivamento;

b) Atribuir na fase de ingresso de novos Acionistas e/ou Sócios, contratação de Colaboradores, Prestadores de Serviços e/ou Parceiros, quando aplicável, na medida em que houver acesso às informações confidenciais do **Grupo Renova**, a inserção de cláusulas que abordem o conhecimento da PSI e confidencialidade em contrato e, sobretudo, o reconhecimento de responsabilidade em caso de violação dessas disposições.

c) Acompanhar incidentes que violem significativamente a PSI e as Normas de Segurança da Informação;

d) Orientar a melhor forma de coleta e preservação de prova eletrônica, com o objetivo de manter sua eficácia para uso em juízo, quando necessário;

e) Elaborar e revisar documentos jurídicos relacionados à Segurança da Informação;

f) Acompanhar o processo disciplinar, validando as penalidades e exceções, quando houver;

g) Revisar periodicamente e sugerir adaptações desta PSI e Normas de Segurança da Informação de acordo com as necessidades e perfil de incidentes ao longo do tempo;

h) Receber as denúncias sobre violações da PSI e das Normas, devendo acionar o CGSI/Comitê de Compliance para estabelecimento da aplicação da sanção cabível (Penalidades); e

i) Analisar e adequar toda e qualquer regulamentação interna para que esteja em conformidade com a legislação vigente e pertinente à sua área de atuação.

11.6. Área de Pessoas & Cultura

A área de Pessoas & Cultura será responsável por

a) Atribuir e formalizar a responsabilidade quanto ao cumprimento da PSI na fase de ingresso de Acionistas e sócios, contratação de Colaboradores e/ou Prestadores de Serviços; e

b) Comunicar formal e prontamente à área de TI qualquer alteração no quadro funcional e societário do **Grupo Renova**, incluindo contratações, demissões, mudanças de cargo, funções ou outras modificações relevantes, com o objetivo de evitar acessos não autorizados ou desnecessário.

12. PENALIDADES

Toda e qualquer infração à PSI e às Normas de Segurança da Informação deverá ser informada ao CGSI e ao Comitê de Compliance e, por conseguinte, apurada por meio de procedimentos internos.

Se o CGSI ou Comitê de Compliance considerar apropriado, poderão ser adotadas medidas contra o Acionista, Sócio, Colaborador ou Prestador de Serviços envolvido, de acordo com a gravidade da irregularidade. As sanções podem variar desde uma carta de orientação, uma carta de repreensão, notificação, e, em casos mais graves, a retirada do quadro societário, rescisão do contrato de trabalho ou contrato de prestação de serviços, conforme previsto no Manual de Procedimentos e Supervisão de AI.

Ao Acionista, Sócio, Colaborador ou Prestador de Serviços suspeito de cometer violações à PSI e Normas de Segurança da Informação, será assegurado um tratamento justo e adequado, sendo que todas as medidas decorrentes da infração serão aplicadas de forma proporcional, com base nas Políticas e Procedimentos do **Grupo Renova**.

O **Grupo Renova** se exime de qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos a seus Acionistas, Sócios, Colaboradores e Prestadores de Serviços, reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas nos processos investigatórios, e adotar as medidas legais cabíveis.

13. PERIODICIDADE

Esta PSI será revisada e atualizada periodicamente, no mínimo 01 (uma) vez por ano, ou sempre que algum fato relevante ou evento justificar uma revisão antecipada, conforme análise e decisão do CGSI.

14. REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos.