SUMÁRIO

1. Quadro de Revisões 2
2. Objetivo 4
3. Abrangência 4
4. Definições e Siglas 4
5. Documentos e Registros de Referência 5
6. Responsabilidades 6
6.1 Alta Direção 6
6.2 Comitê de Segurança da Informação e Proteção de Dados Pessoais (CSIPD) 6
6.3 Segurança da Informação 6
6.4 Gente e Gestão 7
6.5 Marketing 7
6.6 Jurídico 7
6.7 Tecnologia da Informação 8
6.8 Gestores 8
6.9 Equipes de Desenvolvimento 8
6.10 Colaboradores 8
7. Disposições Gerais 9
7.1 Documentos Adjacentes e Complementares 9
7.2 Plano de Comunicação 9
7.3 Adoção de Comportamento Seguro 9
7.4 Relação com Terceiros 11
7.5 Segurança da Informação no Gerenciamento de Projetos 11
7.6 Propriedade Intelectual 11
8. Sanções 11
9. Vigência 12

1. Quadro de Revisões

Versão	Data	Resumo da alteração	Motivo	Autor	Aprovador
1.0	29/06/2012	Elaboração do documento		Segurança da Informação	
2.0	28/06/2013	Revisão		Segurança da Informação	
3.0	09/05/2014	Revisão		Segurança da Informação	
4.0	20/01/2015	Revisão		Segurança da Informação	
4.1	16/06/2015	Revisão		Segurança da Informação	
4.2	27/07/2016	Revisão		CORPSEC/INFOSEC	
5.0	27/02/2017	Revisão		CORPSEC/INFOSEC	
6.0	15/03/2018	Atualização do padrão do documento para políticas; alteração de itens de procedimentos de acordo com as alterações no ambiente.	Novo padrão de documento de políticas e alterações nos procedimentos de gestão internos	Bruno F. Cardoso	
7.0	21/03/2018	Correção da versão do rodapé	Ajustes	Roberto Malicscki	
8.0	07/03/2019	Revalidação sem alteração	Revalidação do documento	Julio Amaral	
9.0	06/08/2020	Atualização do documento; adequações a LGPD e uso dos recursos tecnologia.		PG Advogados	
10.0	22/10/2020	Revisão	Tornar PSI mais diretiva	Patrícia Leonardelli	
11.0	24/11/2020	Revisão	Melhoria	Patricia Leonardelli; aprovado pelo Comitê de Segurança da Informação e Proteção de Dados Pessoais – Emerson Tobar	
12.0	17/08/2021	Atualização do sumário	Correção	Patrícia Leonardelli	
13.0	05/05/2022	Adicionados itens sugeridos pela auditoria de clientes	Melhoria	Bruno F. Cardoso	
14.0	18/11/2022	Ajustes para conformidade com PRD-GPR-001 e PRD-TEC-011; Inserção das Políticas que constam do item 8 ao item 23; inserção de referência do código de ética da Neogrid no item sanções; Inserção dos itens 7.1, 7.4; 7.5; 7.7 e ajustes no item 7.2 e 7.3	Melhoria	Patricia Leonardelli;Pablo Cardoso	Carlos Alberto Soares Pereira CTO
15.0	31/01/2023	Ajuste no item 4 adicionando a definição de dispositivo móvel; Ajuste no item 17 "Política para uso dos ativos".	Melhoria	Patricia Leonardelli	Jean Carlo Klaumann - CEO
16.0	12/04/2024	Revisão periódica.	Melhorias	Diogo Ribeiro de Souza	Nicolas Simone CPTO
17.0	06/03/2025	Análise jurídica no documento Atualização da Declaração do Apoio da Alta Direção	Revisão Anual	Bruno Lechinski	Diogo Ribeiro de Souza CTO

DECLARAÇÃO DE APOIO ALTA DIREÇÃO

Prezados stakeholders, colaboradores, parceiros de negócio e clientes,

A Neogrid reafirma seu compromisso inabalável com a segurança da informação e proteção de dados. Em um cenário digital dinâmico, reconhecemos a informação como nosso patrimônio mais valioso, exigindo gestão de riscos eficaz para assegurar nosso crescimento e a confiança em nós depositada.

Nosso Sistema de Gestão de Segurança da Informação (SGSI) é uma decisão estratégica, continuamente aprimorado para garantir confidencialidade, integridade e disponibilidade. A Alta Direção está plenamente comprometida, provendo recursos adequados. Monitorado mensalmente, nosso SGSI alinha-se aos rigorosos padrões ISO 27001:2022, SOC 1 e SOC 2, CIS Control v8 e NIST Cybersecurity Framework.

Reiteramos nosso compromisso com a melhoria contínua do SGSI, otimizando gestão de incidentes e riscos. Fortaleceremos programas de conscientização e privacidade de dados, aderiremos a padrões e classificações da informação, e priorizaremos fornecedores seguros. Contamos com a postura proativa de todos para proteger nossos ativos e manter a máxima satisfação de nossos clientes.

Diogo Ribeiro de Souza

CHIEF TECHNOLOGY OFFICER – CTO

2. Objetivo

Esta política tem por proposito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores da Neogrid adotar padrões de comportamento seguro, adequados às metas e necessidades da Neogrid;

Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

Resguardar as informações da Neogrid, orientando os requisitos básicos de confidencialidade, integridade e disponibilidade;

Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros;

Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da Neogrid como resultado de falhas de segurança.

3. Abrangência

Esta política se aplica a todos os colaboradores da Neogrid, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a Neogrid. Tais como, empregados, prestadores de serviço, colaboradores, que possuíram, possuem ou virão a possuir acesso às informações da Neogrid e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura Neogrid.

4. Definições e Siglas

- **Classificação:** Garantir que todas as informações tenham classificação de segurança, empregadas de maneira clara, conforme - PRD–TEC–011 Procedimento de Classificação, Tratamento e Transferência de Informações, permitindo que sejam adequadamente protegidas quanto ao seu acesso e uso, sendo que aquelas já consideradas sem utilidade ou com prazo de retenção atingido sejam descartadas de forma segura, conforme descrito no documento PRD-GPR-001-Procedimento Controle de Documentos e Registros e PRD-TEC-047-Processo IMACD – Instalação, Movimentação, Adição, Mudança e Descartes de Ativos de TI.

  As informações de propriedade da Neogrid, sob sua guarda ou do público em geral devem ser tratadas de forma ética e sigilosa em acordo com as leis vigentes, sendo o acesso a estas informações, realizado quando devidamente autorizado e protegido.

- **Responsabilidade na Criação, Seleção e Aquisição:** Garantir que a criação de novos produtos e serviços, a seleção de mecanismos de segurança e a aquisição de bens e serviços levem em consideração o balanceamento dos seguintes aspectos: risco, tecnologia, austeridade no gasto, qualidade, velocidade e impacto no negócio.

  O contrato com os colaboradores e prestadores de serviços deve prever sua adesão aos termos e condições desta Política de Segurança da Informação, precedido por Termos de Responsabilidade e Sigilo que tratem da Segurança da Informação, relacionado com o escopo de sua contratação e sanções administrativas ou pecuniárias em caso de sua violação.

- **Conscientização de todos:** Assegurar a conscientização em todos os níveis da empresa

quanto a adoção de comportamento seguro, em face de suas atribuições e responsabilidades.

- **Continuidade dos Negócios:** Garantir a continuidade dos negócios, de forma a reduzir a um período aceitável a interrupção causada por desastres ou falhas de segurança, através da combinação de ações de prevenção e recuperação, conforme descrito no Plano de Continuidade de Negócios.

- **Conformidade:** Cumprir o atendimento das leis que regulamentam as atividades da Neogrid de forma a adequar-se à legislação e regulamentações aplicáveis.

- **Prevenção:** Assegurar que providências sejam tomadas de forma a prevenir quaisquer ações ou situações que possam expor a **Neogrid** à perda financeira, material ou humana, direta ou indiretamente, potenciais ou reais, comprometendo seu negócio.

- **Detecção:** Garantir que meios tecnológicos e processuais sejam empregados de maneira efetiva a fim de que eventos e incidentes de segurança sejam detectados no menor tempo possível possibilitando que as respostas a estes sejam realizadas adequadamente visando o menor impacto possível aos negócios.

- **Utilização dos recursos:** Garantir que os recursos colocados à disposição sejam utilizados apenas para as finalidades aprovadas pela Neogrid e com obtenção de aprovação da gestão direta.

- **Autenticação:** Garantir que toda utilização de recursos de tecnologia seja autenticada com ID único de usuário e senha e/ou outro item de autenticação (por exemplo, certificado digital), conforme descrito na POL-TEC-008 – Política de Senhas.

- **Análise de Risco:** Estabelecer ou fazer uso de uma metodologia ou processo de avaliação de risco continuada que identifica ameaças, vulnerabilidades e resulta em uma avaliação de risco formal.

- **Inventário:** Garantir a existência de um inventário contendo a lista de todos os dispositivos e equipes autorizadas a usar os mesmos.

- **Comunicação de Descumprimento:** Comunicar à equipe de Segurança da Informação sobre qualquer descumprimento da Política e documentos complementares de Segurança da Informação.

- **Dispositivo Móvel:** São tecnologias digitais que permitem a mobilidade e o acesso à Internet, podemos citar como exemplo Notebooks, Smartphones e Tablets.

- **Notebook**: Computador Portátil, leve, projetado para ser transportado e utilizado em diferentes lugares com facilidade.

- **Smartphone:** Telefone móvel ou celular que utiliza de um sistema operacional (SO) e funciona como um pequeno computador.

5. Documentos e Registros de Referência

NBR ISO IEC 27001:2022
PRD-GPR-001 Procedimento Controle de Documentos e Registros

6. Responsabilidades

7. Alta Direção

- Aprovar, apoiar e suportar a Política de Segurança da Informação perante todas as áreas da organização como processo mandatório;
- Decidir sobre as penalidades cabíveis ao descumprimento desta Política e demais documentos complementares que a suportam.

8. Comitê de Segurança da Informação e Proteção de Dados Pessoais (CSIPD)

- Avaliar e sugerir alterações na Política de Segurança e documentos relacionados.
- Monitorar alterações que possam afetar a segurança da informação e, caso necessário, propor as iniciativas de melhoria do nível de segurança.
- Apoiar na identificação de possíveis casos de violação da Política Segurança da Informação e seus documentos e encaminhar para avaliação da área envolvida.
- Demais deveres e responsabilidades bem como o seu funcionamento estão descritos no documento de Diretrizes do Comitê de Segurança da Informação e Proteção de Dados Pessoais da Neogrid.

9. Segurança da Informação

- Apurar e tratar incidentes relativos aos aspectos físicos e lógicos da Segurança da Informação;
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras e incidentes de segurança;
- Avaliar e propor ajustes, aprimoramentos e modificações desta Política e documentos que a suportam;
- Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
- Determinar a elaboração de indicadores, relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;
- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da Neogrid, mantendo-se atualizado em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;
- Estabelecer procedimentos para os sistemas de controle de acesso da Neogrid, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários.
- Analisar os riscos relacionados à segurança da informação da Neogrid e apresentar relatórios periódicos sobre tais riscos, acompanhados de proposta de aperfeiçoamento do ambiente de controle da Neogrid, quando for o caso;

- Realizar trabalhos de análise de vulnerabilidade de visão contínua, com o intuito de aferir o nível de segurança dos sistemas e dos demais ambientes em que circulam as informações da Neogrid;

- Apoiar os gestores na identificação de áreas sensíveis que necessitam de controles específicos de segurança física ou lógica;

- Analisar os casos de violação desta Política e dos documentos complementares que a suportam, encaminhando-os à Diretoria, quando for o caso;

- Zelar pela disseminação, educação e repasse de conhecimento quanto a cultura de Segurança da Informação dentro da organização, bem como pelo cumprimento desta Política e documentos que a suportam, além de estabelecer, implementar, manter e melhorar continuamente o SGSI e todos os seus requisitos para atender normas e conformidades de clientes internos e externos;

- Avaliar os requisitos de segurança da informação e sugerir controles de segurança no gerenciamento de projetos estratégicos da Neogrid.

10. Gente e Gestão

- Apoiar a aplicação de treinamentos sobre esta Política para os colaboradores e terceiros;

- Atuar no suporte e apoio na manutenção de processos e procedimentos relativos à área, como cadastro e inventário de crachás de acesso físico entre outros.

- Manter os documentos dos processos dentro do prazo de validade, conforme PRD

11. Marketing

- Disponibilizar aos gestores informações que podem ser divulgadas externamente (informações públicas) e ajudar na identificação e classificação delas.

12. Jurídico

- Analisar, apoiar e orientar, em todos os temas relacionados com segurança da informação, de acordo com os aspectos legais e jurídicos, nas contratações de terceiros e no cumprimento de exigências legislativas relacionadas à segurança da informação.

- Apoiar na apuração de responsabilidade de acordo com o processo disciplinar praticado na empresa ou com o contrato estabelecido.

- Orientar e apoiar no tratamento disciplinar em caso de violação desta Política;

13. Tecnologia da Informação

- Reportar incidentes de segurança da informação e dar apoio tecnológico e suporte a equipe de Segurança da Informação na apuração e tratamento de incidentes relativos aos aspectos lógicos da Segurança de Informações nos sistemas e aplicações.
- Implementar controles e melhorias de TI que melhorem os níveis adequados de Segurança da Informação nos ambientes, propor soluções e tecnologias que melhorem os níveis de controle e segurança das informações utilizadas nos ambientes da organização.
- Realizar o acompanhamento e resultado de uma mudança de sistema, principalmente nos sistemas e na infraestrutura tecnológica da Neogrid, preservando os controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações.
- Manter processo de salvaguarda das informações e dos dados necessários para completa recuperação dos seus sistemas (backup), a fim de atender os requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes ou sua recuperação dentro do prazo acordado. A POL-TEC-004-Política de Backup e a POL-TEC-020 Política de Backup e Restore – Produtos da Neogrid apresentam os processos que viabilizam este item este item.

14. Gestores

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- Assegurar a aplicabilidade desta Política **(POL- TEC- 001 Política de Segurança da Informação)** junto aos seus colaboradores, nos processos sob sua responsabilidade.
- Autorizar ou não, a revelação de qualquer informação de propriedade ou sob a responsabilidade da Neogrid.
- Identificar e notificar violações ou qualquer ação duvidosa praticada pelos colaboradores no uso das informações de propriedade da Neogrid.
- Manter a informação documentada dos seus processos de forma atualizada e dentro da validade conforme PRD-GPR-001 Procedimento Controle de Documentos e Registros.

15. Equipes de Desenvolvimento

- Ter compromisso com o desenvolvimento seguro de código, seguindo as melhores práticas de segurança da informação, como OWASP. Orientando-se na POL-TEC-023 Desenvolvimento de Software, PRD-TEC- 053 Procedimento de Desenvolvimento Seguro Engenharia de Produto e PRD-TEC- 057 Procedimento Desenvolvimento Administração Sistemas Corporativos

16. Colaboradores

- Estar cientes das políticas, procedimentos e instruções de segurança da informação da organização, bem como das penalidades administrativas e/ou legais quando do descumprimento destas.

- Respeitar as limitações de autorização e direitos de acesso a locais, informação e sistemas de informação concedidos.
- Utilizar somente os direitos de acesso a si concedidos com respeito à privacidade de outros colaboradores.
- Zelar pela segurança das informações da Neogrid e sob sua guarda.
- Cumprir com diretrizes estabelecidas nesta Política e documentos que a suportam.
- Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive na Internet.
- Zelar pela segurança da sua identidade digital, não compartilhando, divulgando ou transferindo a terceiros.
- Responder por toda e qualquer atividade realizada nos equipamentos da Neogrid realizada mediante o uso de sua identidade digital.
- Reportar quaisquer vulnerabilidades encontradas e/ou possíveis Incidentes de Segurança de Informação através do **Formulário de Demandas INFOSEC**.

17. Disposições Gerais

18. Documentos Adjacentes e Complementares

O sistema de gestão de segurança da Informação, prevê que sejam criados documentos adicionais que forneçam informações adicionais e complementares. Estes documentos estão disponíveis para consulta no SharePoint Corporativo e devem ser seguidos por todo os abrangidos por esta política.

19. Plano de Comunicação

A Neogrid apresenta em seu PLAN-GPR-002 Plano de Comunicação do SGSI as diretrizes que devem ser adotadas por todos os colaboradores, parceiros e terceiros para comunicações internas e externas relevantes para o Sistema de Gestão de Segurança da Informação (SGSI).

20. Adoção de Comportamento Seguro

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações da Neogrid, com destaque para os seguintes itens:

- Diretores, gerentes, coordenadores, funcionários e prestadores de serviços devem assumir atitude proativa e engajada no que diz respeito à proteção das informações da Neogrid.
- Os colaboradores da Neogrid devem compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação

de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.

- Todo tipo de acesso e/ou uso de informação da Neogrid, quando não for explicitamente autorizado, é proibido.

- Informações classificadas como confidenciais não podem ser transportadas em meios como pen-drive, hd externo, CD; DVD, papel etc.).

- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.).

- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não-protegido. A POL-TEC-008 – Política de Senhas apresenta o processo que viabiliza este item.

- Sempre que possível, os sistemas de informação da Neogrid deverão possuir um único conjunto de credenciais (ex. nome de usuário e senha) para cada usuário, de modo que se possa garantir a rastreabilidade de cada acesso a estes sistemas. Exceções a esta política deverão ser tratadas com a equipe de Segurança da Informação.

- As recomendações para uso de internet e de correio eletrônico devem ser rigorosamente seguidas. Arquivos e links de origem desconhecida e/ou não solicitados nunca devem ser abertos e/ou executados.

- Quando a informação não for mais necessária e conforme o DCO-TEC-042 Tabela de Temporalidade, deverão ser descartados conforme descrito no PRD-TEC-047-Processo IMACD – Instalação, Movimentação, Adição, Mudança e Descartes de Ativos de TI.

- O acesso à informação através de equipamentos pessoais deve vir precedido de aprovação prévia e estar em conformidade com as diretrizes descritas nesta política. A POL-TEC-019 Política para uso de Dispositivos Móveis e BYOD apresenta o processo que viabiliza este item. apresenta o processo que viabiliza este item.

- Qualquer tipo de dúvida sobre a Política de Segurança da Informação e documentos que a suportam, deve ser imediatamente esclarecido com a equipe de Segurança da Informação através do Formulário Demandas INFOSEC.

- Respeitar a obrigatoriedade do uso das ferramentas de segurança e proteção implementadas no ambiente, tais como: antivírus, MFA para as credenciais corporativas, criptografia dos discos dos equipamentos, GPOs etc.;

- É expressamente proibido intervir no bom funcionamento, adulterar, alterar ou desativar toda e qualquer ferramenta de segurança e proteção dos equipamentos ou do ambiente computacional da Neogrid sem autorização prévia e acompanhamento da área responsável pelo recurso de proteção;

- É proibido utilizar os recursos da Neogrid para atividade pessoal;

- É proibido realizar cópias de qualquer nível de classificação de documentos para nuvem em repositórios pessoais como: dropbox, google drive, evernote, entre outros;

- A realização de apresentações, documentos e outras informações com conteúdo técnicos e de gestão, desenvolvidos pelos colaboradores da Neogrid ao público externo por meio de seminários, congressos, visitas, workshops, jornais, revistas, redes sociais, trabalhos de

conclusão de cursos de especialização e MBA, teses de mestrado e doutorado, etc. devem ter prévia autorização da Neogrid e, visando a proteção do patrimônio intelectual e conhecimentos desenvolvidos pela Neogrid, tais materiais devem seguir as orientações da equipe de Marketing.

- É proibido compartilhar conteúdos sensíveis e sigilosos com assistentes de IA não homologada, como por exemplo: Código fonte das soluções da organização, dados financeiros e conteúdos classificados como confidenciais, conforme PRD–TEC–011 Procedimento de Classificação, Tratamento e Transferência de Informações.

21. Relação com Terceiros

Toda aquisição de serviços deve estar suportada por um contrato, de acordo com procedimentos estabelecidos pela área Jurídica, assegurando que a entrega cumpra os requerimentos de Segurança da Informação e Privacidade da Neogrid, bem como a POL-TEC-012 Política de Segurança da Informação de Terceiros. Adicionalmente, deverá cumprir quaisquer requisitos de segurança do negócio mediante uma análise de potenciais riscos.

22. Segurança da Informação no Gerenciamento de Projetos

Todos os projetos da Neogrid deverão ser avaliados os requisitos de Segurança da Informação onde seja possível identificar os riscos de Segurança que possa envolver o projeto bem como seus controles de mitigação. O documento PRD-TEC-058 Procedimento de Avaliação de Requisitos de Segurança em Projetos.

23. Propriedade Intelectual

As informações e os recursos tecnológicos utilizados pelos colaboradores são de exclusiva propriedade da Neogrid ou estão sob a sua responsabilidade, não podendo ser interpretados como de uso pessoal.

Todos os colaboradores, terceiros (fornecedores) ou prestadores de serviço devem ter ciência de que o uso das informações e dos sistemas de informação da Neogrid podem ser monitorados, e que os registros assim obtidos podem ser utilizados para detecção de violações da presente Política de Segurança da Informação e dos demais documentos complementares de Segurança da Informação da Neogrid, podendo estas, servir de evidência para a aplicação de sanções, medidas disciplinares, processos administrativos e/ou legais.

É proibido a utilização de dispositivos móveis removíveis para armazenar ou copiar informações de propriedade da Neogrid.

24. Sanções

O não cumprimento de qualquer um dos itens desta política ou de seus documentos associados implicará na aplicação de medidas disciplinares, sem prejuízo à Neogrid, pleitear ressarcimentos, quando da ocorrência de prejuízo direto ou indireto, tanto material quanto moral.

Os casos eventualmente não previstos neste documento, ou a adoção de soluções de exceção serão analisados pela Segurança da Informação e, se necessário, Comitê de Segurança da Informação e Proteção de Dados (CSIPD), e submetidos à decisão da Diretoria de Tecnologia e

Desenvolvimento, em conjunto com demais partes interessadas.

Em nenhum momento será admitido, a qualquer usuário, invocar o desconhecimento destas normas para justificar violações ou sua falta de cumprimento sem prejuízo a ressarcimentos financeiros e/ou materiais. A Neogrid se reserva o direito de tomar medidas e sanções administrativas, legais e penais aplicáveis.

A inobservância às normativas estabelecidas sujeitará a quem tenha infringido e aqueles que colaborarem com a infração às sanções previstas na Lei, ou nos contratos pelos quais se vinculam a Neogrid, sem prejuízo de outras sanções previstas na legislação pertinente ao país da infração e responderão pessoalmente pelos eventuais danos e prejuízos causados a Neogrid ou a terceiros, conforme POL-GEP-062 Política de Medidas Disciplinares.

O Código de Ética da Neogrid apresenta as diretrizes.

25. Vigência

Essa política entra em vigor a partir da data de sua publicação e sua revisão deve ocorrer no máximo a cada doze meses, ou sempre que se fizer necessária.

As alterações desta Política de Segurança da Informação e das normas complementares devem ser devidamente comunicadas aos colaboradores.