# Sumário

1. Quadro de revisões ..... 1
2. Objetivo ..... 2
3. Abrangência ..... 3
4. Definições e Siglas ..... 3
5. Documentos e Registros de Referência ..... 3
6. Responsabilidades ..... 3
   6.1. Gestores de Contratos (Gestor da área) ..... 4
   6.2. Parceiro ou Terceiro Contratado ..... 4
7. Diretrizes ..... 4
   7.1. Gerais ..... 4
   7.2. Acesso lógico e uso aceitável ..... 5
   7.3. Requisitos Específicos para Provedores de Nuvem (ISO 27017) ..... 6
8. Segurança no uso dos ativos ..... 7
9. Segurança da Informação e Privacidade ..... 8
10. Término de Contrato de Serviço/Produto ..... 8
11. Violação de Conduta ..... 8
12. Avaliações Periódicas ..... 9
13. Sanções ..... 9
14. Vigência ..... 9

## 1. *Quadro de revisões*

| Versão | Data | Resumo da alteração | Motivo | Autor | Aprovador |
|---|---|---|---|---|---|
| 1.0 | 01/10/2020 | Criação da Política. | Necessidade de documentação e formalização do processo. | Patrícia Magrin Leonardelli Aprovada pelo Diretor Emerson Tobar | |
| 2.0 | 28/05/2021 | Alterado os documentos relacionados. | Referências atualizadas. | Leandro Dix | |
| 3.0 | 30/05/2022 | Atualização e revisão do documento. | Revisão periódica. | Bruno F. Cardoso | |
| 4.0 | 22/11/2022 | Ajustes para conformidade com PRD-GPR-001 e PRD-TEC-011; Ajustes nas Diretrizes; Melhoria nas responsabilidades dos gestores; inserção dos itens 8, 9, 10 e 11. | Melhorias | Pablo Cardoso; Patricia Leonardelli | Carlos Alberto Pereira - CTO |
| 5.0 | 06/01/2023 | Ajuste no item 'responsabilidade'; Melhoria nos itens 6.2, 6.3, 6.6 e 7 Retiradas as referências a documentos classificados como internos. Alterada a classificação do documento para "Pública" | Melhorias | Patricia Leonardelli | Carlos Alberto Pereira - CTO |
| 6.0 | 28/03/2024 | Atualização e revisão do documento. | Ajustes nos itens 6.2 e 6.4. | Lucas Corrêa | Nicolas Simone - CPTO |
| 7.0 | 13/03/2025 | Atualização e revisão do documento. | | Bruno Lechinski dos Santos | Diogo Ribeiro de Souza - CTO |
| 8.0 | 23/04/2026 | Revisão anual | Revisão Anual | Evellyn Grein | Helder Mendes |
| 9.0 | 28/05/2026 | Inserção de items ISO 27017 | Revisão Anual | Aramis Tobler Bonfanti Evellyn Grein Marcus Vinicius Cabrera de Oliveira | Helder Mendes |

## 2. *Objetivo*

A informação é o principal elemento de negócio da Neogrid e, dessa forma, deixar de manter a sua confidencialidade, integridade e disponibilidade são fatores críticos para o negócio.

Esta política determina as diretrizes para parceiros e terceiros na aderência às políticas corporativas da Neogrid, incluindo requisitos específicos para o fornecimento e uso de serviços em nuvem (SaaS, PaaS, IaaS), visando mitigar riscos e garantir a proteção dos ativos de informação.

Esta política não sobrepõe as diretrizes estabelecidas na Política de Segurança da Neogrid, que tem aplicabilidade interna.

## 3. *Abrangência*

Esta diretriz aplica-se a todos os parceiros e terceiros que possuam qualquer modalidade de contratação ou relacionamento com a Neogrid, independentemente da natureza do vínculo. O escopo abrange, de forma não exaustiva, prestadores de serviços, fornecedores, distribuidores de software e parceiros de tecnologia, dedicando atenção especial aos Provedores de Serviços em Nuvem (CSPs) que processam dados ou hospedam serviços fundamentais para a companhia.

## 4. *Definições e Siglas*

**NDA (Non-Disclosure Agreement)**: Acordo legal que impede a divulgação de informações confidenciais entre as partes.

**DPO (Data Protection Officer)**: Profissional responsável por garantir o cumprimento das leis de proteção de dados.

**Zero Trust**: Modelo de segurança que não confia em nenhum acesso por padrão, exigindo verificação contínua.

## 5. Documentos e Registros de Referência

ISO/IEC 27001:2022 Sistema de gestão da segurança da informação

ISO/IEC 27017:2015 Segurança da Informação em Nuvem

POL-TEC-001 Política de Segurança da Informação

PRD-GPR-001 Procedimento Controle de Documentos e Registros

## 6. Responsabilidades

### *6.1. Gestores de Contratos (Gestor da área)*

- Quando da contratação de fornecedores, parceiros ou terceiros que venham a acessar a rede interna e os dados da Neogrid, o Gestor do contrato deverá garantir, de preferência contratualmente, que todos estejam cientes das políticas corporativas da Neogrid, incluído esta Política e a POL-TEC-001 Política de Segurança da Informação.
- Solicitar requisição de acesso de terceiro para: concessão/remoção de direito de acesso, alteração de nível de acesso, desativação/ativação de login.

### *6.2. Parceiro ou Terceiro Contratado*

É de responsabilidade dos parceiros e terceiros, observar e seguir as diretrizes estabelecidas nas políticas e procedimentos corporativos da Neogrid que sejam pertinentes para o desenvolvimento do trabalho, destacando esta política;

Todas as atividades executadas devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras com relação à Segurança da Informação e Proteção de Dados.

Adicionalmente, os parceiros e terceiros devem obrigatoriamente realizar o assessment de Segurança da Informação da Neogrid, disponível em: https://neogrid.com/assessment.

## *7. Diretrizes*

### *7.1. Gerais*

Os parceiros ou terceiros devem cumprir com todos os requisitos das legislações aplicáveis e devem comprometer-se a seguir, integralmente, os seguintes itens:

- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade;
- Preencher e atender os requisitos de segurança da informação e privacidade acordados em contrato firmado entre as partes a fim de mitigar os riscos associados;
- Respeitar a confidencialidade conforme NDA (*Non Disclosure Agreement*) assinado.

- Assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades acordadas e aprovadas pela Neogrid;
- É de responsabilidade da Neogrid, os terceiros que tenham acesso aos sistemas e informação da empresa.
- Assegurar que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Assegurar a continuidade do processamento das informações críticas de negócios;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Responder, sempre que solicitado, os formulários de segurança disponibilizado pela Neogrid com questões relacionadas à Segurança da Informação, Governança de TI e Privacidade de dados;
- Cumprir as Políticas e Procedimentos da Neogrid, e esta Política;
- Comunicar imediatamente a área de Segurança da Informação da Neogrid através do e-mail infosec@neogrid.com, na identificação de qualquer incidente ou não conformidade de segurança da informação e, na identificação de qualquer incidente relacionado a privacidade de dados, comunicar também o DPO da Neogrid através do e-mail dpo@neogrid.com.

### *7.2. Acesso lógico e uso aceitável*

- Um NDA (*Non Disclosure Agreement*) com a empresa parceira deve ser providenciado, antes do início do processo de gestão de acessos a fim de mitigar os riscos associados com o acesso de terceiro aos ativos da Neogrid. O gestor do contrato tem a responsabilidade de buscar a assinatura deste termo, caso ele ainda não exista;
- A requisição de acesso lógico de terceiros aos ativos da Neogrid para: concessão ou remoção de direto de acesso, alteração no nível de acesso, desativação/ativação de login de terceiro, é feita pelo 'Gestor da área', que também é o gestor do contrato, por meio da ferramenta de Gestão de Identidade da Neogrid, conforme procedimento vigente. A solicitação será avaliada e aprovada de acordo com a necessidade, seguindo as diretrizes corporativas de Segurança da Informação e as políticas internas;

- É dever do gestor do contrato informar a validade da contratação no momento da solicitação do acesso.
- Os computadores de parceiros e terceiros não podem ser conectados na rede interna da Neogrid, deverão utilizar apenas da rede convidados (*guests).*
- Em caso de detecção de comportamento suspeito, possuindo origem a estação de trabalho do colaborador terceiro, o time de Infraestrutura, poderá bloquear o acesso dele ao ambiente da Neogrid, solicitando uma justificativa para o gestor do contrato para tal ação.
- O acesso a infraestrutura e sistemas internos da Neogrid devem ser acessados de maneira segura, partindo do conceito de Zero Trust, conforme procedimentos de segurança estabelecidos pela Neogrid.
- É proibido o acesso, download ou distribuição de qualquer conteúdo que viole direitos autorais e de propriedade da Neogrid. Da mesma forma, não é permitido acesso ou distribuição de conteúdo pornográfico de qualquer natureza ou conteúdo que viole o Estatuto da Criança e Adolescente;
- As credenciais de acesso disponibilizadas, quando aplicáveis, são de uso pessoal e intransferível, não podem ser divulgadas ou compartilhadas. O colaborador terceiro deve manter suas credenciais de acesso seguras, sendo de sua responsabilidade qualquer utilização indevida;
- É responsabilidade da empresa terceira comunicar ao gestor do contrato da Neogrid qualquer desligamento de seus colaboradores para que as devidas revogações de acesso sejam executadas.

### *7.3. Requisitos Específicos para Provedores de Nuvem (ISO 27017)*

Para garantir a integridade, confidencialidade e disponibilidade dos ativos da Neogrid, todos os parceiros e provedores de serviços (especialmente CSPs) devem aderir aos seguintes controles:

- O Terceiro deve adotar a metodologias, garantindo que os requisitos de segurança e privacidade sejam integrados desde a fase de concepção até a implementação do serviço. Isso inclui a realização de análises de risco e testes de segurança regulares antes da disponibilização de novas funcionalidades ou infraestruturas.
- Em arquiteturas de multilocação, o provedor deve garantir o isolamento lógico e físico rigoroso dos dados da Neogrid. É mandatório que o acesso aos ativos da companhia seja segregado de

outros clientes por meio de controles de rede, criptografia e permissões de banco de dados, impedindo qualquer forma de acesso cruzado ou vazamento de informações.

- O acesso de colaboradores do parceiro aos ativos e dados da Neogrid deve ser restrito ao pessoal essencial para a operação. Deve-se aplicar rigorosamente o princípio do privilégio mínimo, assegurando que os acessos sejam concedidos apenas na medida do necessário, com justificativa documentada e por tempo limitado.
- É obrigatória a utilização de métodos de autenticação forte (MFA) para todo e qualquer acesso administrativo, técnico ou privilegiado aos serviços em nuvem, consoles de gerenciamento e interfaces de configuração que sustentem as operações da Neogrid.
- O parceiro deve manter um processo formal de gestão de mudanças e notificar a Neogrid, com antecedência prévia, sobre alterações significativas na infraestrutura, localização geográfica de data centers ou processos críticos que possam impactar o nível de segurança originalmente acordado.
- O provedor deve garantir o provisionamento e o desprovisionamento imediato de contas de acesso conforme o status contratual de seus colaboradores ou conforme a necessidade do serviço. Contas inativas ou de colaboradores desligados devem ser revogadas em tempo real para evitar acessos não autorizados.
- Qualquer incidente de segurança, real ou suspeito, que afete os serviços prestados à Neogrid deve ser comunicado imediatamente, sendo que o parceiro compromete-se a cooperar integralmente com investigações, fornecendo logs de auditoria, registros de eventos e evidências técnicas necessárias para análises forenses e remediação de danos; caso seja comprovada sua responsabilidade pelo incidente, o parceiro deverá adotar as medidas necessárias para mitigação dos impactos e responder pela reparação integral dos danos causados à Neogrid e/ou a terceiros.
-

## 8. *Segurança no uso dos ativos*

Terceiro é responsável:

- Pela proteção dos dispositivos físicos contendo informação da Neogrid que estão sob sua guarda;

- Garantir a segurança e a integridade do recurso de TI em uso, mantendo-o nas condições originais. É de responsabilidade do terceiro zelar pela conservação e boas condições da Infraestrutura e equipamentos;
- Comunicar imediatamente ao setor de TI da Neogrid e ao Gestor da área a ocorrência de qualquer anomalia no uso dos recursos de TI;
- Utilizar senhas que contenham, pelo menos, oito caracteres, compostos de letras números e símbolos, evitando o uso de nomes, sobrenomes, número de documentos, placas de carros, números de telefone, datas que possam ser relacionadas com o colaborador. As senhas temporárias devem ser alteradas imediatamente. As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese.

## *9. Segurança da Informação e Privacidade*

Os contratos com Parceiros e Terceiros deverão estar contemplados com cláusulas com referências aos requisitos de Segurança da Informação e Privacidade a ser seguido pelos contratados, bem como a obrigatoriedade do cumprimento das Políticas, Procedimentos e Normas da Neogrid que sejam pertinentes à Segurança da informação, Privacidade e para o desenvolvimento do trabalho.

## *10. Término de Contrato de Serviço/Produto*

O término do contrato de prestação de serviço por terceiros é acompanhado por Suprimentos.

## *11. Violação de Conduta*

São consideradas violações à Política as seguintes situações, não se limitando as:

- Quaisquer ações ou situações que possam expor a Neogrid à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
- Uso indevido ou acesso indevido a dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa da Neogrid;

- Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da Neogrid;
- A não-comunicação imediata de quaisquer descumprimentos desta Política ou qualquer outra determinada pela Neogrid.

## *12. Avaliações Periódicas*

A Neogrid poderá realizar, sempre que achar necessário, avaliações para atestar a efetividade da implementação de controles de segurança baseados nas boas práticas determinadas pela ISO/IEC 27001:2022 e ISO/IEC 27017:2015, devendo para isso, comunicar o parceiro com antecedência.

## *13. Sanções*

A violação a um controle ou a não-aderência a essa Política e a outras Políticas e Procedimentos da Neogrid e suas definições são consideradas violações graves, podendo ser aplicadas penalidades pecuniárias de acordo com os termos contratuais, sem prejuízo da apuração de todos os danos causados e eventual indenização.

## *14. 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 e das normas complementares devem ser devidamente comunicadas as partes interessadas.