Sumário

1. *Quadro de revisões*

Versão	Data	Resumo da alteração	Motivo	Autor
1.0	29/05/2026	Criação do documento	Implantação ISO 27017	Matheus Borges (Clavis) Marcus Vinicius Cabrera de Oliveira Aramis Tobler Bonfanti Evellyn Grein

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.

A informação constitui o ativo mais estratégico da Neogrid. A preservação de sua Confidencialidade, Integridade e Disponibilidade (CID) é imperativa para a continuidade operacional e a confiança de nossos clientes. Este Guia tem como objetivo estabelecer as diretrizes técnicas e operacionais para a gestão segura de ativos em nuvem, garantindo que a utilização de infraestruturas (IaaS, PaaS) e a oferta de serviços (SaaS) estejam em total conformidade com os controles da ISO/IEC 27017. Este documento atua como um aditamento técnico à Política de Segurança da Informação da Neogrid, detalhando a aplicação prática dos controles de segurança no ecossistema de computação em nuvem.

3. Abrangência

Este Guia aplica-se a todos os ativos de informação processados ou armazenados em ambientes de nuvem sob responsabilidade da Neogrid. Sua observância é mandatória para:

- **Times Internos:** Administradores de nuvem, desenvolvedores e arquitetos de soluções.
- **Parceiros e Terceiros:** Provedores de serviços (CSPs), fornecedores de tecnologia e parceiros de integração que possuam acesso lógico ou operacional aos ambientes de nuvem da Neogrid ou que forneçam componentes para a cadeia de suprimentos de software.

4. Documentos e Registros de Referência

ABNT NBR ISO/IEC 27001:2022: Sistemas de Gestão da Segurança da Informação – Requisitos.

ABNT NBR ISO/IEC 27002:2022: Controles de Segurança da Informação.

ABNT NBR ISO/IEC 27017:2015: Código de prática para controles de segurança da informação com base na ISO/IEC 27002 para serviços em nuvem.

Diretrizes de Cloud, FinOps e Infosec (Neogrid Way).

POL-TEC-012: Política de Segurança da Informação para Parceiros e Terceiros.

POL-TEC-023 Desenvolvimento de Software

Matriz de Responsabilidade Compartilhada Cloud.

PRD-GPR-020 Procedimento de Gestão de Mudança Neogrid

PRD-GPR-032- Procedimento Auditoria Interna do Sistema de Gestão de Segurança da Informação

PRD-TEC-046 Procedimento Administração de Rede

PRD-TEC- 048 Procedimento Gerenciamento de Acesso Lógico

PRD-TEC-051 Gestão de chaves criptograficas - Cliente e a Neogrid

PRD-TEC-052: Procedimento de Avaliação de Segurança de Fornecedores.

PRD-TEC-054-Procedimento de Registro e Monitoramento de Eventos de Segurança da Informação

PRD-TEC-055: Procedimento de Gestão de Incidentes de Segurança da Informação.

PRD-TEC-059: Procedimento de Gestão de Vulnerabilidades.PLA-TEC-001: Plano de Disponibilidade e Capacidade de Serviços de TI.

PLA-GRP-004: PCN - Plano de Continuidade de Negócio.

5. Responsabilidades

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas definições e fronteiras descritas na Matriz de Responsabilidade Compartilhada Cloud.

5.1 Fronteiras de Atuação Híbrida (ISO 27017: 6.1.1)

A Neogrid documenta e estabelece formalmente a divisão de papéis de segurança em nuvem em três esferas: a responsabilidade herdada do Provedor de Infraestrutura (CSP), as obrigações operacionais da Neogrid como Provedora do Serviço (SaaS) e as configurações sob gestão exclusiva do Cliente (Usuário do Serviço). Os acordos comerciais e técnicos devem refletir explicitamente este alinhamento mútuo.

6. Diretrizes

6.1 Gerais

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes do Programa Geral de Conscientização da ISO 27001 e pelas regras globais de Governança corporativa.

6.1.1 Política de Segurança e Alinhamento de Risco (ISO 27017: 5.1.1)

As diretrizes de segurança em nuvem integram a postura de governança da Neogrid, mitigando os riscos associados a ambientes virtuais, multilocatários e acessos administrativos de terceiros. A segurança é nativa (Security by Design) desde a concepção de novas arquiteturas e produtos.

6.1.2 Localização Geográfica e Restrições de Soberania (ISO 27017: 6.1.3)

A Neogrid monitora, mapeia e informa de maneira transparente aos seus clientes a localização geográfica dos ambientes de nuvem onde os dados do serviço são processados, armazenados ou replicados (Santiago Chile, US East, Us-East-1, US East 2, BR South ou data centers homologados dos provedores de infraestrutura contratados). Os dados sob custódia não serão transferidos para jurisdições internacionais sem prévia análise de conformidade legal e contratual.

Em paralelo, a organização mantém um canal estruturado de comunicação com entidades reguladoras e órgãos de proteção civil, segurança pública e privacidade.

Esta diretriz é operacionalizada e evidenciada por meio da manutenção e revisão periódica do documento **CAT-ADM-002 – Lista Contatos Autoridades Relevantes**, que cataloga os pontos de contato oficiais com órgãos competentes, incluindo a ANPD e autoridades policiais, para atuação em cenários de contingência ou incidentes cibernéticos em ambiente de computação em nuvem.

6.1.3 Conscientização e Treinamento em Nuvem (ISO 27017: 7.2.2)

Todos os colaboradores, gestores e terceiros relevantes com acesso ao ambiente de nuvem devem passar por programas periódicos de conscientização focados em riscos de segurança em nuvem, tratamento confidencial de informações lógicas e legislações aplicáveis.

6.1.4 Comunicação de Mudanças na Infraestrutura (ISO 27017: 12.1.2)

O PRD-GPR-020 Procedimento de Gestão de Mudança Neogrid prever a avaliação prévia de impactos de segurança gerados por atualizações do provedor de nuvem (CSP) e estabelecer mecanismos ágeis para notificar os clientes sobre alterações na aplicação (SaaS) que possam impactar seu nível de risco.

6.1.5 Gestão da Cadeia de Suprimentos Tecnológica (ISO 27017: 15.1.1, 15.1.2, 15.1.3)

Os provedores de nuvem e parceiros adjacentes de tecnologia são classificados como fornecedores críticos. Os acordos e contratos firmados devem prever obrigações de proteção contra malwares, criptografia, logs e backups, exigindo que sub-provedores conjugados mantenham ou excedam o nível de segurança da Neogrid.

7. Segurança no Uso dos Ativos

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes de infraestrutura do Neogrid Way (Seções 3 e 4).

7.1 Inventário, Classificação e Separação de Dados (ISO 27017: 8.1.1)

Todos os ativos lógicos e recursos instanciados em nuvem devem ser catalogados. O inventário operacional mantido pela Neogrid deve diferenciar e isolar logicamente:

- *Dados do Cliente:* Informações custodiadas e processadas pela aplicação a pedido do usuário.
- *Dados Originados do Serviço:* Logs, metadados de performance, telemetria e registros transacionais internos da plataforma.
- *Viabilização:* Este controle é garantido pela aplicação obrigatória do Padrão de Nomenclatura e Modelo de TAGs do Neogrid Way (Itens 3.3 e 3.4).

7.2 Gestão de Vulnerabilidades Técnicas e Atualizações (ISO 27017: 12.6.1)

A identificação, escaneamento, análise e remediação de vulnerabilidades ou desvios de configuração (drift) na infraestrutura e nos serviços em nuvem são regidos estritamente pelo PRD-TEC-059 – Procedimento de Gestão de Vulnerabilidades, que dita os critérios de severidade e prazos operacionais para aplicação de correções.

7.3 Padrões Criptográficos e Ciclo de Vida de Chaves (ISO 27017: 10.1.1, 10.1.2, 18.1.5)

É mandatória a aplicação de criptografia forte utilizando o algoritmo AES-256 para dados em repouso (at rest) e protocolos TLS 1.2 ou superior para dados em trânsito (in transit). O gerenciamento, a rotação automatizada e a guarda de chaves mestras de criptografia devem utilizar os serviços de KMS nativos e homologados do provedor.

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes do PRD-TEC- 051 Gestão de chaves criptograficas - Cliente e a Neogrid.

7.4 Segregação e Proteção de Redes Lógicas (ISO 27017: 13.1.3)

Ambientes de desenvolvimento, homologação e produção devem ser estritamente segregados em redes lógicas isoladas (VPCs/VNETs), aplicando firewalls virtuais e controles de WAF na borda da aplicação, conforme estabelecido no Neogrid Way (Item 3.5 e 4.1).

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes da POL-TEC-023 Desenvolvimento de Software.

7.5 Sincronização de Relógios e Tempo Lógico (ISO 27017: 12.4.4)

Todas as instâncias, microsserviços e ativos de rede em nuvem devem ter seus relógios locais sincronizados via protocolo NTP utilizando como referência o servidor de tempo padrão fornecido nativamente pelo CSP, assegurando a integridade cronológica de logs de auditoria.

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes do PRD-TEC- 046 Procedimento Administração de Rede.

7.6 Gestão de Capacidade e Continuidade de Negócio (ISO 27017: 12.1.3, 12.3.1)

A capacidade computacional do ambiente de nuvem é monitorada continuamente através de ferramentas de telemetria e FinOps para mitigar o risco de indisponibilidade por escassez de recursos. Devem ser estruturadas políticas automatizadas de snapshots georreplicados, com testes semestrais obrigatórios de restauração de dados corporativos.

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes da PLA-TEC-001 Plano de Disponibilidade e Capacidade de Serviços de TI e o PLA-GRP-004 PCN - Plano de Continuidade de Negócio.

7.7 Licenciamento Comercial em Ambientes Elásticos (ISO 27017: 18.1.1)

A instalação de qualquer software comercial em ambiente de nuvem que possua elasticidade e escalabilidade automática (auto-scaling) deve passar por validação prévia de conformidade de licenciamento para impedir o uso excessivo ou violação de direitos autorais de processamento de terceiros.

8. Acesso Lógico e Uso Aceitável

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelo PRD-TEC- 048 Procedimento Gerenciamento de Acesso Lógico e pelas configurações lógicas do Identity Provider (IdP) corporativo.

8.1 Governança de Acessos dos Usuários do Cliente (ISO 27017: 9.1.2, 9.2.1, 9.2.2, 9.4.1)

A Neogrid fornece ao cliente mecanismos para a gestão autónoma de utilizadores dentro da aplicação. O cancelamento de acesso deve ser refletido de imediato no ambiente de produção.

Caso a interface de autoatendimento não esteja disponível para determinada funcionalidade, o cliente deve solicitar a exclusão via Portal de Chamados, com SLA de atendimento prioritário para garantir a revogação célere.

8.2 Autenticação Forte e Acesso Administrativo Privilegiado (ISO 27017: 9.2.3)

É obrigatória a aplicação de técnicas de Autenticação de Múltiplos Fatores (MFA) para o acesso lógico de todos os administradores da Neogrid ao plano de controle e consoles de gerenciamento da nuvem. O mesmo mecanismo de segurança deve ser disponibilizado para a camada administrativa dos clientes.

8.3 Proteção de Credenciais e Informações Secretas (ISO 27017: 9.2.4)

Os procedimentos de armazenamento de credenciais de autenticação de usuários devem utilizar técnicas seguras de criptografia unidirecional (*hashing* com *salt*). O método de custódia e proteção dessas credenciais deve ser transparente e disponibilizado para análise crítica dos clientes.

8.4 Monitoramento de Programas Utilitários e Automações (ISO 27017: 9.4.4)

O uso de utilitários de linha de comando (CLI), scripts de infraestrutura como código (IaC) ou ferramentas de automação com capacidade de contornar regras normais de segurança deve ser estritamente restrito a pessoal autorizado, sendo suas execuções registradas e auditadas regularmente.

9. Segurança da Informação e Privacidade

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelo Padrão de Logging e Observabilidade (Neogrid Way - Item 8) e pelo Plano Corporativo de Resposta a Incidentes.

9.1 Geração, Proteção e Imutabilidade de Logs de Eventos (ISO 27017: 12.4.1, 12.4.3, 18.1.3)

A Neogrid coleta e centraliza logs de auditoria e segurança em repositórios isolados e protegidos por regras de imutabilidade. As trilhas devem registrar ações do console, comandos de operadores privilegiados e eventos críticos da aplicação, conforme o padrão estabelecido no Item 8 do Neogrid Way, sendo estritamente vedada a alteração de logs salvos.

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes da PRD-TEC-054-Procedimento de Registro e Monitoramento de Eventos de Segurança da Informação.

9.2 Rotulagem de Informações na Aplicação (ISO 27017: 8.2.2, 14.1.1)

A Neogrid documenta e divulga de forma transparente em seus manuais as funcionalidades que permitem aos clientes classificar, segmentar e rotular as suas próprias informações dentro do ecossistema SaaS, apoiando o cumprimento das políticas de privacidade e LGPD de ponta a ponta.

9.3 Resposta a Incidentes e Notificação Bidirecional (ISO 27017: 16.1.1, 16.1.2, 16.1.7)

O processo de gestão de incidentes prevê canais formais e fluxo bidirecional de comunicação. A Neogrid notificará os clientes afetados sobre eventos de segurança confirmados na infraestrutura de nuvem em prazos ágeis acordados em SLA, mantendo procedimentos estruturados para isolamento de dados e preservação de evidências digitais para fins forenses.

Em caso de sinistros, qualquer incidente ou não conformidade de segurança da informação deve ser comunicado imediatamente à área de Segurança da Informação da Neogrid através do e-mail infosec@neogrid.com. Caso o evento envolva a privacidade de dados pessoais, o Encarregado pelo Tratamento de Dados (DPO) também deve ser acionado em paralelo pelo e-mail dpo@neogrid.com.

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes do PRD-TEC-055 – Procedimento de Gestão de Incidentes de Segurança da Informação.

9.4 Práticas de Desenvolvimento Seguro (ISO 27017: 14.2.1)

O ciclo de vida de desenvolvimento de sistemas (SDLC) das soluções SaaS da Neogrid incorpora metodologias de proteção de código, revisões de arquitetura e análises de segurança em sua esteira de CI/CD, alinhado com as boas práticas de engenharia de software do mercado.

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes da POL-TEC-023 Desenvolvimento de Software.

10. Término de Contrato de Serviço/Produto

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas cláusulas de encerramento contratual e homologação de descarte de fornecedores.

10.1. Descarte Seguro, Devolução de Ativos e Cripto-exclusão (ISO 27017: 11.2.7, CLD.8.1.5)

Ao encerramento de um contrato, a Neogrid assegura ao cliente a oportunidade de extração prévia de seus dados. Após o período de retenção legal, o dado do cliente e seus respectivos backups

lógicos devem ser destruídos permanentemente. Como salvaguarda técnica em nuvem, procede-se com o processo de "Cripto-exclusão" (revogação/destruição definitiva das chaves criptográficas atreladas àquele ambiente no KMS). Exige-se também do CSP relatórios e garantias de destruição física de mídias e discos desativados.

11.Avaliações Períodicas

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas rotinas de auditoria interna e compliance da Neogrid.

11.1 Análise Crítica de Conformidade Independente (ISO 27017: 18.1, 18.2.1)

A Neogrid avalia continuamente a aderência deste Baseline. Para comprovar a segurança de sua infraestrutura sem comprometer a confidencialidade do ambiente multilocatário, a organização coleta e analisa anualmente as certificações independentes (ISO 27001, ISO 27017) de seus provedores de nuvem (CSP) e disponibiliza resumos executivos ou autoavaliações de conformidade de sua plataforma SaaS para assegurar a transparência com clientes e auditorias.

Esta diretriz é operacionalizada e evidenciada por meio dos controles estabelecidos nesta seção, tendo sua viabilização prática regida pelas diretrizes do PRD-GPR-032- Procedimento Auditoria Interna do Sistema de Gestão de Segurança da Informação e PRD-TEC-052 Procedimento de Avaliação de Segurança de Fornecedores.

11.2 Onde eu posso ver as informações de conformidade da Neogrid com a ISO/IEC 27017:2015?

Em processo de certificação ISO/IEC 27017:2015.

12. 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.

13. 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, devendo para isso, comunicar o parceiro com **antecedência.**

14. 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.

15. 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.