1. OBJETIVO

Garantir a integridade, confidencialidade, autenticidade e disponibilidade contra ameaças, internas ou externas, garantindo a continuidade do negócio e o cumprimento de requisitos legais quanto as informações processadas pela organização junto a terceiros.

2. APLICAÇÃO

Sistema: ☒ SGI – NBR ISO 9001: 2015 / NBR ISO 14001:2015 / NBR ISO 27001:2022 / NBR ISO 45001:2024 LQN - NBR ISO/IEC 17025

Site: Betim/ MG ☒ Manaus / AM Outros / BR

Esta política se aplica a todos os funcionários, partes interessadas e qualquer pessoa que tenha acesso a informações tratadas pelo SGI.

3. HISTÓRICO DAS REVISÕES

Rev.	Data de Emissão	Válido a partir	Descrição	Revisado por
01.000	22/01/2026	26/01/2026	Publicação inicial	Saulo Lima / 11618

Nota: Revisões anteriores estão disponíveis no backup do sistema Fluig.

3. DEFINIÇÕES / REFERÊNCIAS

3.1 Siglas:

- **TI**: Tecnologia da Informação;
- **SGI:** Sistema de Gestão Integrado;
- **VPN**: *Virtual Private Network* (Rede Privada Virtual);
- **DLP:** Prevenção de Vazamento de Dados
- **SO**: Sistema Operacional;
- **IDS**: *Intrusion Detection System* (Sistema de Detecção de Intrusões);
- **CSRF:** *Cross-Site Request Forgery*;
- **XSS:** Cross-Site Scripting;
- **IM:** Instant Messengers) Mensagens Instantâneas;
- **IPS**: *Intrusion Prevention System* (Sistema de Prevenção de Intrusões).

3.2 Termos:

- **Uso Legítimo**: Refere-se à utilização dos recursos de TI para atividades profissionais que estão alinhadas com os objetivos da organização, respeitando as diretrizes de segurança e privacidade.
- **Confidencialidade e Privacidade**: Proteção de informações sensíveis, tanto da organização quanto dos clientes, garantindo que só pessoas autorizadas tenham acesso a essas informações.
- ***Malware***: *Software* malicioso projetado para causar danos a sistemas, como vírus, *worms*, *trojans*, etc.
- **Acesso Remoto**: Acesso aos sistemas da organização por usuários externos ou distantes da rede interna, realizado com a devida segurança, como o uso de VPN's.

- **Fortgate:** É um equipamento de segurança que protege redes contra ataques, vírus, acessos não autorizados e outros riscos.
- **AD:** Active Directory é um serviço da Microsoft usado para organizar e controlar computadores, usuários e recursos dentro de uma organização.

3.3 Referências:

- **ISO/IEC 27001** - Sistema de Gestão de Segurança da Informação: Norma internacional que define os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão de segurança da informação, garantindo proteção contínua dos ativos de TI.
- **Lei Geral de Proteção de Dados (LGPD)** - Lei nº 13.709/2018: Regula o tratamento de dados pessoais no Brasil, impondo responsabilidades sobre a proteção da privacidade e a segurança da informação, aplicáveis também aos recursos de TI utilizados para esse fim.

4. RESPONSABILIDADES

Gestor do Contrato (dono do processo):

- Identificar a criticidade do fornecedor antes da contratação.
- Garantir que o fornecedor receba e aceite as políticas de segurança da organização.
- Monitorar a entrega do serviço e reportar desvios de segurança.

Departamento de TI e Segurança da Informação:

- Realizar a avaliação técnica de segurança (Questionário de Risco).
- Configurar acessos remotos via VPN com MFA e monitorar logs de atividade de terceiros.
- Apoiar na definição dos requisitos técnicos que devem constar nos contratos.

Departamento Jurídico (DPO) / Compras:

- Assegurar que o Termo de Confidencialidade (NDA) e as cláusulas de proteção de dados (LGPD) estejam presentes em todos os instrumentos contratuais.
- Validar as garantias legais em caso de incidentes de segurança causados pelo fornecedor.

Fornecedor (Terceiro):

- Cumprir integralmente as normas de segurança estabelecidas no contrato.
- Notificar a organização sobre qualquer incidente de segurança em até 24 horas através dos canais de comunicação divulgados.

Denúncias/Incidentes:

- Permitir auditorias e vistorias quando solicitado pela organização.

5. METODOLOGIA

5.1 Introdução

A política de segurança da informação para fornecedores da NANSEN estabelece diretrizes e requisitos para garantir a proteção dos dados e informações confidenciais compartilhados com terceiros. Esta política se aplica a todos os fornecedores que têm acesso ou lidam com informações sensíveis da organização.

Todos as interações com terceiros devem incluir obrigações de segurança, tais como:

- **Acordo de Confidencialidade (NDA):** Proibição de compartilhamento de dados com terceiros.
- **Direito de Auditoria:** A organização reserva-se o direito de auditar os controles do fornecedor anualmente.
- **Notificação de Incidentes:** O fornecedor deve notificar qualquer violação de dados em no máximo 24 horas após a descoberta.

5.2 Compromisso com a segurança da informação

- Todos os fornecedores devem demonstrar compromisso com a segurança da informação e concordar em cumprir as políticas e procedimentos estabelecidos pela NANSEN Instrumentos de Precisão Ltda.
- A segurança da informação deve ser considerada uma prioridade em todas as interações e atividades realizadas em nome da organização.

5.3 Requisitos de segurança da informação

- Os fornecedores devem implementar medidas de segurança adequadas para proteger os dados da organização contra acesso não autorizado, divulgação, alteração ou destruição.
- Os dados compartilhados com os fornecedores devem ser protegidos por criptografia ou outros métodos de segurança apropriados durante a transmissão e armazenamento.
- Os fornecedores devem ter políticas e procedimentos claros para lidar com incidentes de segurança da informação e notificar imediatamente a NANSEN Instrumentos de Precisão Ltda, em caso de violação de dados.

5.4 Controle de acesso

- Os fornecedores devem implementar controles de acesso adequados para garantir que apenas pessoal autorizado tenha acesso às credenciais e aos dados da empresa.

5.5 Confidencialidade e privacidade

- Os fornecedores devem concordar em manter a confidencialidade de todas as informações confidenciais da organização e não divulgar ou compartilhar essas informações com terceiros sem autorização prévia.
- Os dados compartilhados com os fornecedores só podem ser usados para os fins especificados no contrato ou acordo entre as partes e não devem ser utilizados para qualquer outra finalidade sem consentimento prévio.

5.6 Auditoria e conformidade

- Os fornecedores podem ser submetidos a auditorias para garantir a conformidade com esta política e outros requisitos de segurança da informação.

- Os fornecedores devem cooperar totalmente com qualquer auditoria ou revisão conduzida pela NANSEN e fornecer acesso às informações e recursos necessários para verificar a conformidade com as políticas de segurança aqui estabelecidas.

5.7 Responsabilidades e sanções

- Os fornecedores são responsáveis por garantir que seus colaboradores e subcontratados cumpram os requisitos desta política.
- Violações desta política por parte dos fornecedores podem resultar em medidas corretivas, rescisão do contrato ou outras sanções, conforme apropriado.

6 INFORMAÇÃO DOCUMENTADA RETIDA

Formulário	Identificação	Processo / Área	Armazenamento	Recuperação	Proteção	Retenção Tempo	Disposição
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

7 ANEXOS

Não aplicável.