**1. Objetivo**

Esta política estabelece diretrizes, controles e responsabilidades para garantir a confidencialidade, integridade e disponibilidade das informações, reduzindo riscos de incidentes e garantindo a conformidade com a LGPD, as Normas Regulamentadoras e as normas internacionais de segurança da informação.

Os objetivos principais são:

a) Prevenir acessos, alterações, destruições ou divulgações não autorizadas;
b) Proteger dados em todos os formatos (digital e físico);
c) Garantir a rastreabilidade e a governança de segurança em todos os setores e sistemas utilizados pelo Grupo NST.

**2. Base Legal**

- **LGPD**:
  - Art. 46 – Dever de adoção de medidas de segurança;
  - Art. 47 – Sigilo e confidencialidade;
  - Art. 50 – Boas práticas e governança.
- **Normas Regulamentadoras do MTE**:
  - NR-7 – Retenção de ASO e prontuários médicos por 20 anos;
  - NR-9 – Registros de riscos ambientais e medidas de controle;
  - NR-1 – Disposições gerais de SST.
- **Normas ISO**:
  - ISO 27001 – Segurança da informação;
  - ISO 27701 – Gestão da privacidade da informação.
  - ISO 27035 – Gestão de Incidentes de Segurança.

**3. Definições Específicas**

- **Segurança da Informação**: medidas para preservar a confidencialidade, integridade e disponibilidade de dados.
- **Controle de Acesso**: restrição e gerenciamento do acesso a dados e sistemas.
- **Criptografia**: técnica para proteger dados em repouso e em trânsito.
- **Backup Seguro**: cópia de dados armazenada com criptografia e proteção contra acessos indevidos.
- **Incidente de Segurança**: evento que compromete ou ameaça a segurança da informação.

**4. Escopo de Aplicação**

Aplica-se a todos os setores do Grupo NST, abrangendo:

- Área médica e de exames;
- Setor técnico de SST e engenharia de segurança do trabalho;
- Administrativo e financeiro;
- Comercial e atendimento ao cliente;
- TI e suporte;
- Terceiros com acesso a dados ou sistemas.

**5. Diretrizes e Procedimentos**

**5.1 Proteção Lógica (Digital)**

- Uso obrigatório de credenciais individuais e intransferíveis para acesso aos sistemas (SOC, TALLOS, LAUDAR, LARP, MD NET e UNISIST).
- Implementação de autenticação multifator (MFA) para usuários com acesso a dados sensíveis.
- Bloqueio automático de sessão após 15 minutos de inatividade.
- Monitoramento contínuo de logs de acesso e alterações.
- Atualizações de software e sistemas aplicadas imediatamente após disponibilização pelo fabricante.

**5.2 Proteção Física**
- Controle de acesso físico a áreas onde dados sensíveis são armazenados, por meio de chave ou biometria.
- Proibição de retirada não autorizada de documentos físicos ou mídias externas.
- Instalação de câmeras de segurança em áreas críticas, com gravações retidas por no mínimo 90 dias.

**5.3 Backup e Continuidade de Negócio**
- Backup diário criptografado, armazenado localmente e em nuvem segura com redundância geográfica.
- Testes trimestrais de restauração de backup para garantir integridade.
- Plano de Continuidade de Negócio (PCN) e Plano de Recuperação de Desastres (DRP) atualizados anualmente.

**5.4 Monitoramento e Prevenção**
- Verificação periódica de vulnerabilidades nos sistemas realizada pelos próprios fabricantes.
- Implementação de firewall e antivírus corporativo com atualização automática.
- Bloqueio de dispositivos USB não autorizados.

**5.5 Resposta a Incidentes**
- Seguir a **Política 6 – Gestão de Incidentes de Segurança** para investigação, comunicação e mitigação.
- Registro das não conformidades e seus tratamentos no Registro de Ação Corretiva - NST.

**6. Responsabilidades**
- **Encarregado/DPO**: supervisionar conformidade e gestão de riscos; coordenar resposta a incidentes.
- **Consultor de TI**: implementar e monitorar controles técnicos; gerenciar backups; realizar testes de segurança.
- **Gestores de Área**: zelar pelo cumprimento desta política nas equipes.
- **Colaboradores**: proteger suas credenciais, não compartilhar senhas e reportar incidentes.
- **Fornecedores de Tecnologia**: cumprir cláusulas contratuais de segurança e apoiar investigações.

**7. Gestão de Riscos**
- Avaliação de riscos realizada semestralmente para identificar e tratar ameaças à segurança da informação.
- Priorização de riscos com base no impacto e na probabilidade de ocorrência.
- Implementação de planos de ação corretivos e preventivos.

**8. Auditoria e Revisão**
- Revisão desta política a cada 12 meses ou quando houver alteração legislativa, mudança significativa nos processos ou incidentes de segurança relevantes.
- Auditorias internas são realizadas semestralmente.

**9. Disposições Finais**
- O descumprimento desta política pode resultar em medidas disciplinares, civis e penais.
- A adesão às diretrizes aqui descritas é obrigatória para todos os colaboradores, prestadores e fornecedores com acesso a dados ou sistemas do Grupo NST.

**10. Controle de Registros**

| Identificação | Armazenamento | Proteção | Recuperação | Retenção | Disposição |
|---|---|---|---|---|---|
| Registro de Ação Corretiva – NST | Arquivo Eletrônico no servidor | *Backup* | Por numeração | Indeterminado | Não aplicável |

**11. Histórico de Revisões**

| Revisão | Data | Alteração |
|---|---|---|
| 00 | 11/08/2025 | Texto original. |