Política da Segurança da Informação Dados NetAdmin Software (Pública)

1. Nota sobre esta Versão Pública

Esta é uma versão pública e institucional da Política de Segurança da Informação da companhia. Existe uma versão de circulação interna, mais abrangente e com detalhamento técnico-operacional ampliado, que contempla objetivos, diretrizes e controles específicos de maior complexidade. Esta versão tem como propósito comunicar ao mercado, clientes, fornecedores, parceiros e partes interessadas o compromisso da companhia com a privacidade e a segurança da informação, em alinhamento com as melhores práticas e legislações vigentes.

2. Objetivo

Esta política tem o objetivo de estabelecer as diretrizes e normas de segurança da informação e proteção de dados pessoais da companhia, suportada por uma decisão estratégica da diretoria e desenvolvida no âmbito de um Sistema de Gestão da Segurança e Privacidade da Informação (SGSPI). Busca-se, em especial:

2.1. garantir a adoção de normas e procedimentos que permitam às partes interessadas seguir padrões de comportamento seguros, protetivos às informações sensíveis da companhia e adequados à legislação aplicável;

2.2. observar os pilares da segurança da informação (confidencialidade, integridade, disponibilidade);

2.3. prevenir incidentes de segurança como acessos indevidos, perda, destruição, divulgação ou modificação não autorizada de dados.

3. Termos e Definições

- **Dados Pessoais**: Informação relativa a pessoa natural identificada ou identificável.
- **Informações Sensíveis**: Dados com valor para a operação da companhia.
- **Informações**: Termo genérico que inclui os dois anteriores.
- **Legislação Aplicável**: Inclui LGPD, GDPR, CCPA e correlatas.

4. Aplicabilidade

4.1. Esta política se aplica a todos os colaboradores, parceiros, prestadores e terceiros com vínculo com a companhia.

4.2. A diretoria e os gestores da segurança estão comprometidos com a efetiva aplicação das diretrizes aqui estabelecidas, incluindo a melhoria contínua dos processos

5. Diretrizes

5.1. Ativos de informação:

- Os ativos estão inventariados e possuem proprietário definido.
- Somente softwares autorizados podem ser utilizados.
- Responsáveis pelos ativos devem ser profissionais capacitados.
- O compartilhamento de dados exige autorização formal do gestor.

5.2. Controle de Acesso:

- O acesso é restrito a pessoas autorizadas.
- Direitos de acesso são controlados desde a admissão até o desligamento.
- A liberação a sistemas requer autorização formal.

5.3. Controle de Acesso Físico:

- Entrada a ambientes seguros controlada por dispositivos de segurança.
- Visitantes e fornecedores devem ser acompanhados.
- Entregas devem ocorrer em locais designados, com acompanhamento.

5.4. Mesa Limpa:

- É proibido deixar documentos confidenciais à vista.
- Impressões devem ser recolhidas imediatamente.

5.5. Acesso Lógico

- Concedido conforme função e revisto periodicamente.
- Proibido o compartilhamento de credenciais.

5.6. Internet e Correio Eletrônico:

- Visitantes usam rede separada.
- E-mail é de uso exclusivo institucional.
- Padrão de e-mail anonimizado.

5.7. Código-Fonte:

- Acesso restrito e armazenado com controle de versão.
- Alterado somente por pessoal autorizado.

5.8. Revisão de Acessos

- Deve ocorrer sempre que houver mudança de função.
- Realizada anualmente ou sob demanda.

5.9. Acesso Privilegiado

- Concessão mediante autorização formal.
- Compartilhamento de senha somente em situações justificadas.

5.10. Utilitários Privilegiados

- Uso restrito à equipe de TI.
- Utilizados exclusivamente para administração de ambiente.

5.11. Acesso Remoto

- Realizado apenas via conexão segura e com ferramentas homologadas.

5.12. Senhas e Logon

- Senhas devem ser complexas, individuais e alteradas ao primeiro uso.

- Devem ser alteradas ao menor indício de comprometimento.

5.13. Dispositivos Móveis e Pessoais

- Acesso apenas por rede separada.
- Armazenamento de documentos somente em repositório seguro e autorizado.
- Exigência de proteção por senha.

5.14. Comunicação

- Proibido o uso de sistemas da companhia para atividades ilegais ou que prejudiquem a rede.

5.15. Fornecedores e Clientes

- Acordos documentados com terceiros.
- Em visitas a clientes, normas locais devem ser seguidas.

5.16. Conformidade Jurídica

- A companhia segue a legislação vigente e diretrizes da ANPD.
- Medidas técnicas e organizacionais são adotadas para proteção de dados.

5.17. Propriedade Intelectual

- Utilização somente de softwares licenciados.

5.18. Incidentes e Continuidade

- Diretrizes documentadas para gestão de incidentes.
- Plano de continuidade para garantir disponibilidade de serviços essenciais.

6. Responsabilidades

6.1. Colaboradores:

- Conhecer e cumprir a política.

- Relatar suspeitas de incidentes.
- Zelar pelas informações sob sua responsabilidade

6.2. Gestores

- Multiplicar a conscientização.
- Classificar e rotular informações.
- Garantir conhecimento da política no momento da contratação.

6.3. Equipe do SGSPI

- Atualizar e revisar a política.
- Promover a conscientização.
- Avaliar incidentes e recomendar medidas.

6.4. Recursos Humanos

- Garantir cumprimento dos processos de segurança na admissão.

7. Sanções.

7.1.1. As violações das normas que compõem esta Política, tanto por colaboradores quanto por terceiros, bem como as demais normas e procedimentos de segurança, devem ser comunicadas imediatamente ao gestor imediato, aos recursos humanos e ao SGSPI.

7.1.2. Violações são passíveis de penalidades administrativas, inclusive no que tange a comunicação às autoridades públicas competentes, se for o caso.

8. Casos Omissos

8.1.1. Os casos omissos deverão ser analisados pelo Comitê do SGSPI, que deliberará sobre cada caso específico e tomará as providências cabíveis.

8.1.2. As diretrizes estabelecidas nesta Política e nas demais normas de segurança da NETADMIN, não limitados a este conteúdo, espera que todos as partes envolvidas, sempre que possível, associem medidas que garantam a Segurança da Informação em todas as atividades da

companhia.

9. Referências

- Manual do SGSPI;
- NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação
- NBR ISO/IEC 27002 - Código de prática para a gestão da segurança da informação