**Plano de Segurança da Dev Solutions 1. Introdução**

A Dev Solutions é uma empresa especializada em desenvolvimento de software, focada  em oferecer soluções inovadoras e serviços de alta qualidade para seus clientes. Devido à  importância dos dados manipulados, é essencial garantir a segurança das informações,  prevenindo acessos não autorizados, vazamentos e ataques cibernéticos.

**2. Objetivo**

Este documento tem como objetivo estabelecer boas práticas de segurança para todos os  funcionários da Dev Solutions, garantindo a proteção das informações da empresa e de  seus clientes.

**3. Princípios Gerais**

**Principio C.I.D.A.l**

* **Confidencialidade**: Proteger informações sensíveis contra acessos não  autorizados.
* **Integridade**: Garantir que os dados não sejam alterados ou corrompidos  indevidamente.
* **Disponibilidade**: Assegurar que as informações e sistemas estejam acessíveis  quando necessários.
* **Autenticidade**: Confirma que os dados e os usuários são genuínos.
* **Legalidade**: Garante que os procedimentos relacionados a informação e dados  sejam feitos de acordo com a lei

**4. Boas Práticas de Segurança**

**4.1. Acesso a Sistemas e Dados**

• Utilizar senhas fortes e alterá-las periodicamente.

• Não compartilhar credenciais de acesso com terceiros.

• Utilizar autenticação multifator sempre que possível.

• Bloquear a tela do computador ao se ausentar.

**4.2. Proteção de Informações Sensíveis**

• Não armazenar informações sensíveis em dispositivos pessoais ou em locais não  seguros.

• Evitar enviar dados sigilosos por e-mail sem criptografia.

• Armazenar documentos importantes apenas em repositórios autorizados e  seguros.

**4.3. Uso de Dispositivos e Redes**

• Utilizar apenas redes Wi-Fi seguras e evitar conexões públicas sem VPN. • Manter softwares e sistemas operacionais sempre atualizados.

• Utilizar apenas dispositivos autorizados para acessar sistemas da empresa.   
**4.4. Proteção contra Ameaças Cibernéticas**

• Estar atento a e-mails suspeitos e evitar clicar em links desconhecidos. • Não baixar ou instalar softwares não autorizados pela empresa. • Reportar imediatamente qualquer atividade suspeita ao setor de TI.

**5. Responsabilidades dos Funcionários**

• Cumprir todas as diretrizes de segurança estabelecidas pela empresa. • Participar de treinamentos e conscientização sobre segurança da informação. • Reportar incidentes de segurança imediatamente.

**6. Consequências do Descumprimento**

O descumprimento das diretrizes estabelecidas neste documento pode resultar em  sanções disciplinares, incluindo advertências, suspensão ou demissão, conforme a  gravidade da infração.