POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. INTRODUÇÃO

Esta Política de Segurança Cibernética tem como objetivo estabelecer diretrizes, regras e responsabilidades voltadas à proteção das informações e dos sistemas tecnológicos da **DÉBITO DIRETO**, empresa atuante no setor de tecnologia. A segurança cibernética é essencial para garantir a confidencialidade, integridade e disponibilidade das informações, bem como para mitigar riscos e responder adequadamente a incidentes.

2. OBJETIVOS

- Proteger os ativos de informação da empresa contra ameaças internas e externas;
- Assegurar a conformidade com leis e regulamentos aplicáveis;
- Promover a cultura de segurança entre colaboradores, parceiros e fornecedores;
- Garantir a continuidade dos serviços em caso de incidentes cibernéticos.

3. ESCOPO

Esta política aplica-se a todos os colaboradores, estagiários, terceiros, prestadores de serviço e parceiros que tenham acesso a sistemas, redes e informações da empresa. Abrange também todos os dispositivos e plataformas utilizadas, sejam eles físicos ou virtuais, locais ou em nuvem.

4. DIRETRIZES GERAIS

4.1 **Controle de Acesso**

- O acesso a sistemas e informações deve ser concedido de acordo com o princípio do menor privilégio;
- Devem ser utilizados mecanismos de autenticação forte, como senhas complexas e autenticação multifator (MFA);
- Contas inativas ou desnecessárias devem ser desabilitadas imediatamente.

4.2 **Classificação da Informação**

- As informações devem ser classificadas em níveis de sensibilidade (pública, interna, confidencial e restrita);
- Medidas de proteção apropriadas devem ser aplicadas conforme a classificação.

4.3 **Segurança de Dispositivos**

- Todos os dispositivos devem possuir antivírus, firewall e software de monitoramento atualizados;
- É proibida a instalação de softwares não autorizados;

- A utilização de dispositivos móveis corporativos deve seguir políticas específicas de segurança.

4.4 **Uso Aceitável de Recursos**

- Os recursos de TI devem ser utilizados exclusivamente para fins profissionais;
- É vedado o acesso a sites, redes sociais e sistemas não relacionados às atividades da empresa, salvo autorização prévia.

5. GESTÃO DE RISCOS E INCIDENTES

5.1 **Avaliação de Riscos**

- A empresa realizará periodicamente avaliações de risco para identificar e tratar vulnerabilidades e ameaças;
- Devem ser utilizados frameworks de segurança reconhecidos (ex: NIST, ISO/IEC 27001).

5.2 **Tratamento de Incidentes**

- Todos os incidentes de segurança devem ser comunicados imediatamente ao time responsável;
- Deve existir um plano de resposta a incidentes com procedimentos claros de contenção, erradicação e recuperação;
- Incidentes devem ser registrados e analisados para evitar recorrências.

6. TREINAMENTO E CONSCIENTIZAÇÃO

- Todos os colaboradores devem participar de treinamentos regulares sobre segurança cibernética;
- Campanhas internas de conscientização devem ser realizadas periodicamente;
- Novos colaboradores devem passar por orientação sobre esta política durante o processo de integração.

7. AUDITORIA E CONFORMIDADE

- A conformidade com esta política será verificada por meio de auditorias internas e externas;
- Não conformidades devem ser corrigidas dentro dos prazos estabelecidos;
- A política será revisada anualmente ou sempre que houver mudanças relevantes no ambiente tecnológico ou regulatório.

8. RESPONSABILIDADES

- **Diretoria:** Aprovar a política e garantir os recursos necessários;

- **Área de Segurança da Informação:** Implementar, monitorar e revisar os controles de segurança;
- **Colaboradores:** Cumprir integralmente as diretrizes estabelecidas nesta política;
- **Fornecedores:** Atender aos requisitos de segurança previstos nos contratos e acordos de nível de serviço.

9. DISPOSIÇÕES FINAIS

- O descumprimento desta política poderá acarretar sanções administrativas e disciplinares, conforme regulamento interno;
- Esta política entra em vigor na data de sua publicação e deve ser amplamente divulgada a todos os envolvidos.

Débito Direto Serviços de Pagamentos Ltda
CNPJ 36936971000195
10/02/2025