1. OBJETIVO

A Política de Segurança da Informação do ICDS tem por finalidade a proteção dos dados de propriedade da organização e de seus usuários, estabelecendo diretrizes para garantir a privacidade, orientar o uso de recursos tecnológicos e possibilitar o controle e gerenciamento dos riscos decorrentes.

2. DESCRIÇÃO:

2.1 Princípios:

(i) Confidencialidade: garantir que as informações, fontes e sistemas sejam acessados apenas por pessoas autorizadas.

(ii) Integridade: garantir que as informações sejam corretas, confiáveis e sem alterações não autorizadas, preservando, assim, sua confiabilidade e originalidade;

(iii) Disponibilidade: garantir que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

(iv) Autenticidade: Garantia de que a informação é proveniente de uma fonte confiável e que não foi alterada por terceiros não autorizados, de forma a preservar a identidade e a credibilidade dos emissores e receptores da informação, bem como a validade dos dados transmitidos.

(v) Conformidade: assegurar a estrita observância de disposições legais aplicáveis, notadamente às relativas à LGPD (Lei Geral de Proteção de Dados Pessoais) e outras aplicáveis.

2.2 Diretrizes:

- Promover o tratamento e armazenamento de dados e informações estritamente necessários ao exercício das atividades da organização;

- Criar mecanismos de proteção contínua para todos os ativos de informação da organização, garantindo o acesso de informações de forma segura;

- Estabelecer critérios de segurança lógica de redes, computadores, sistemas e aplicativos;

- Estabelecer critérios de segurança física de computadores e servidores de rede, bem como padrões de instalação;

- Implementar sistemas de backup, recuperação de dados e armazenamento em nuvem;

- Realizar testes regulares de armazenamento e recuperação de dados;

- Realizar o mapeamento de riscos e implementar auditorias periódicas para avaliação dos controles;

- Adotar práticas de combate à pirataria e uso de softwares não autorizados;

- Implementar regramentos tendentes a garantir a utilização segura de hardware e software;

- Adotar regras de uso e de acesso à internet e e-mail;

- Estabelecer plano de continuidade do negócio, para possibilitar nível de funcionamento operacional suficiente em caso de interrupções ou incidentes;

- Implementar treinamentos, capacitações e conteúdos educativos para conscientização sobre a segurança da informação;

- Implementar canais de relacionamento e comunicação com os públicos interno e externo;

- Estabelecer plano de resposta à incidentes em caso de suspeita ou efetiva violação de segurança.

- Estabelecer controles de acesso e permissões de acordo com as responsabilidades e necessidades dos funcionários;

- Realizar a gestão adequada de senhas, incluindo a definição de políticas de senha fortes e a atualização periódica;

- Garantir a segurança física dos equipamentos e dispositivos utilizados pela organização, como laptops e smartphones;

- Garantir a segurança física das instalações da organização, incluindo o controle de acesso e a vigilância adequada.

3. Documentos Relacionados

Código de Princípios e Melhores Práticas Corporativas

4. Indicador

5. Histórico de Revisões

04.01.2024 – Elaboração do documento