POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA PREFEITURA MUNICIPAL DE PEDRANÓPOLIS/SP

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA PREFEITURA MUNICIPAL DE PEDRANÓPOLIS/SP

Município	Pedranópolis/SP
Entidade	Prefeitura Municipal de Pedranópolis/SP
Período	Ano de 2024
Responsável	Adalberto Junior dos Santos
Cargo	Encarregado do Setor de Computação
Período de Vigência	01/01/2024 a 31/12/2024

1. Objetivo

A política de segurança da informação da Prefeitura Municipal de Pedranópolis/SP, tem como objetivo proteger os ativos de informação contra ameaças internas e externas, garantindo a confidencialidade, integridade e disponibilidade dos dados.

2. Escopo

Esta política se aplica a todos os funcionários, contratados, fornecedores e parceiros desta Prefeitura de Pedranópolis/SP que tenham acesso a informações confidenciais ou sistemas de informação.

3. Responsabilidades

- A secretaria municipal de ciência, inovação e tecnologia da informação (setor do T.I.) é responsável por aprovar e revisar regularmente a política de segurança da informação, além de garantir recursos adequados para sua implementação.
- Os gerentes de departamento são responsáveis por garantir a aplicação e conformidade com esta política em suas respectivas áreas.

- Todos os funcionários são responsáveis por seguir as diretrizes estabelecidas nesta política e relatar quaisquer violações ou incidentes de segurança da informação.

4. Classificação da Informação

- As informações devem ser classificadas de acordo com seu nível de sensibilidade, utilizando categorias como "Público", "Interno" e "Confidencial".
- Os funcionários devem ser treinados para reconhecer e tratar adequadamente as informações de acordo com sua classificação.

5. Controles de Acesso

- O acesso às informações deve ser restrito apenas aos funcionários autorizados, com base no princípio do menor privilégio.
- Os funcionários devem ter credenciais únicas e seguras para acessar os sistemas de informação.
- O acesso físico a áreas restritas deve ser controlado e monitorado.

6. Segurança da Rede e dos Sistemas

- Todos os dispositivos e sistemas devem ser protegidos por firewalls, antivírus e outras medidas de segurança adequadas.
- As atualizações de segurança devem ser aplicadas regularmente em todos os sistemas e softwares.
- Os backups dos dados críticos devem ser realizados regularmente e armazenados de forma segura.

7. Segurança Física

- As instalações da organização devem ser protegidas por medidas de segurança física, como câmeras de vigilância, controles de acesso e alarmes.
- Os dispositivos de armazenamento de dados, como discos rígidos e dispositivos USB, devem ser mantidos em locais seguros quando não estiverem em uso.

8. Conscientização e Treinamento

- Todos os funcionários devem receber treinamento regular sobre segurança da informação, incluindo políticas e procedimentos relevantes.
- Campanhas de conscientização sobre segurança da informação devem ser realizadas regularmente para manter os funcionários atualizados sobre as ameaças em evolução.

9. Monitoramento e Relatórios

- Os incidentes de segurança da informação devem ser monitorados e registrados regularmente.
- Os funcionários devem relatar imediatamente quaisquer incidentes de segurança da informação à equipe de TI ou ao responsável pela segurança da informação.

10. Conformidade e Revisão

- Esta política de segurança da informação será revisada anualmente para garantir sua eficácia e conformidade com as leis e regulamentos aplicáveis.
- A conformidade com esta política será monitorada regularmente e quaisquer violações serão tratadas de acordo com os procedimentos estabelecidos.

Pedranópolis,10 de janeiro de 2024.