|  |  |
| --- | --- |
| Nome da organização: | |
| Data do Mapeamento | DD/MM/AAAA |
| Responsáveis pelo mapeamento de dados | |
| [Nome(s) completo(s) do(s) aluno(s)] do grupo | |
| Aluno 1 | |
| … | |
| Aluno n | |

# CONTEXTO ORGANIZACIONAL

[Forneça um resumo com no mínimo dois parágrafos do contexto organizacional].

# Papéis de USUÁRIOS DA INFORMAÇÃO

|  |  |
| --- | --- |
| Nome do Papel | Descrição do Papel do Usuário |
| [Nome do papel do usuário] | [Descrição do papel do usuário na organização, bem como as necessidades de utilização dos dados] |

# Categorias de Dados MESTRES

[O mapeamento deverá englobar cinco categorias de dados mestres]

### NOME DA CATEGORIA

[Descrição das categorias dados mestres]

#### Descrição dos atributos da categoria

[Descrição dos atributos que cada categoria deverá conter]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nome | Descrição | Domínio | Tamanho | Obrigatório  (S/N) | Nível de Privacidade (Público[[1]](#footnote-1), Interno[[2]](#footnote-2), Confidencial[[3]](#footnote-3) e Secreta[[4]](#footnote-4)) |
|  |  |  |  |  |  |

# Política de gerenciamento de acesso

[Esta seção descreverá quatro itens de uma política de acesso para os dados mestres identificados.]

## Autorização de acesso

[Esta seção deve definir quem pode acessar os dados e sob quais condições. Isso pode incluir a necessidade de aprovação do gerente, a conclusão de treinamento de segurança de dados e a assinatura de acordos de confidencialidade.]

## Restrições de acesso

[Esta seção deve estabelecer limitações sobre como os dados podem ser acessados, como horários permitidos, locais de acesso e restrições geográficas.]

## Proteção de dados

[Esta seção deve descrever as medidas de segurança que serão implementadas para proteger os dados, como criptografia, backups regulares, autenticação de usuários e restrições de acesso baseadas em funções.]

## Monitoramento de dados

[Esta seção deve descrever como o acesso aos dados será monitorado para garantir que as políticas sejam seguidas. Isso pode incluir a revisão regular de logs de acesso e auditorias internas e externas.]

1. **Público**: Informação que pode ser divulgada para qualquer pessoa sem que haja implicações para a instituição. [↑](#footnote-ref-1)
2. **Interno**: Informação que não devem sair dom âmbito da organização. Entretanto, caso isso venha a ocorrer, as consequências não serão críticas. [↑](#footnote-ref-2)
3. **Confidencial**: O acesso a esse tipo de informação é realizado de acordo com estrita necessidade, isto é, os usuários só podem acessá-las se forem fundamentais para a execução de suas funções na organização. O funcionamento da organização pode ficar seriamente comprometido se essas informações forem acessadas de forma não autorizada. [↑](#footnote-ref-3)
4. **Secreta**: O acesso interno ou externo de pessoas não autorizadas a esse tipo de informação é extremamente crítico para a organização. É importantíssimo que a quantidade de pessoas autorizadas seja extremamente restrito. [↑](#footnote-ref-4)