**Formulário de Categorias e Parâmetros de Riscos de Segurança da Informação (SI) da <Sigla da estatal>**

**Controle de Versões**

*<Inserir os dados das versões.>*

|  |  |  |  |
| --- | --- | --- | --- |
| Versão | Data | Autor | Notas da Revisão |
|  |  |  |  |

**1.Objetivos**

<*Inserir o objetivo do formulário de categoria e parâmetros de riscos >*

**2.** **Parametrização de critérios de tratamento e de aceitação de riscos**

*<inserir a parametrização e os critérios de tratamento e aceitação dos riscos>*

|  |  |  |  |
| --- | --- | --- | --- |
| Parametrização de critério de tratamento e de aceitação de riscos | | | |
| Classe de Riscos | Valores Limites de Risco  Limite Superior (S) | | Ações a serem tomadas no tratamento de riscos. |
| Limite Inferior (I) | Limite Superior (S) |
|  |  |  |  |

Aprovado em \_\_\_ de \_\_\_\_\_\_\_\_\_\_ de \_\_\_\_\_.

­<nome completo da autoridade máxima da Estatal >

<cargo da autoridade máxima da Estatal >

**Observações :**

*No processo de gestão de riscos são necessários critérios para avaliar o nível dos riscos e para decidir sobre qual tratamento deve ser realizado.Para tanto são utilizados critérios que sistematizam este processo: critérios para a avaliação de riscos e de impactos, e critérios para a aceitação de riscos*

As faixas (ou classes) definidas pelos critérios de avaliação de riscos e de aceitação de riscos neste caso estabelecem:

o Risco Muito Baixo (MB): nível de risco entre 1 e 2;

o Risco Baixo (B): nível de risco entre 3 e 4;

o Risco Moderado (M): nível de risco igual a 5;

o Risco Alto (A): nível de risco entre 6 e 7;

o Risco Muito Alto (MA): nível de risco entre 8 e 9.

Definição de ações a serem tomadas para o tratamento de riscos em cada faixa. Este aspecto estabelece a estratégia da organização para tratar os riscos, dependendo dos resultados obtidos na estimativa de riscos. Aspectos como custo-benefício de tratamentos também devem ser levados em conta. A seguir um exemplo de possível estratégia de tratamento de riscos (baseada em Canongia e outros, 2010), que pode ser modificada pelo Gestor de Riscos:

o Risco Muito Baixo (MB): risco tolerável, nenhuma ação é necessária;

o Risco Baixo (B): risco tolerável, nenhuma ação imediata é necessária, porém o risco deve ser monitorado; Recomenda-se tratar os riscos nesta classe apenas se restrições (como custo e esforço de tratamento) não forem significativas.

Risco Moderado (M): situação de atenção. Se possível o risco deve ser tratado em médio prazo. O risco deve monitorado frequentemente;

Restrições (como custo e esforço de tratamento) podem ser consideradas para priorizar o tratamento de riscos nessa classe.

o Risco Alto (A): risco intolerável, situação de grande preocupação. Ações devem ser tomadas rapidamente e os resultados precisam ser monitorados frequentemente para avaliar se a situação mudou com as ações. Recomenda-se o tratamento de riscos independentemente de restrições (como custo e esforço de tratamento).

o Risco Muito Alto (MA): risco intolerável. Requer ações de tratamento imediatas. As ações devem ser monitoradas continuamente para avaliar se os efeitos são os esperados. Os riscos devem ser tratados independentemente de restrições (como custo e esforço de tratamento).

A Tabela abaixo apresenta um formulário para a parametrização de critério de tratamento e de aceitação de riscos. Para cada classe de consequência devem ser definidos: os valores limites de risco (inferior e superior) para a classe, e as ações a serem tomadas para tratar os riscos da classe.

|  |  |  |  |
| --- | --- | --- | --- |
| Parametrização de critério de tratamento e de aceitação de riscos | | | |
| Classe de Riscos | Valores Limites de Risco | | Ações a serem tomadas no tratamento de riscos. |
| Limite Inferior (I) | Limite Superior (S) |
| Muito Baixo (MB | Risco (MB-I) | Risco (MB-S) | Ações para a classe de ricos MB |
| Baixo (B) | Risco (B-I) | Risco (B-S) | Ações para a classe de ricos B |
| Moderado (M) | Risco (M-I) | Risco (M-S) | Ações para a classe de ricos M |
| Alto (A) | Risco (A-I) | Risco (A-S) | Ações para a classe de ricos A |
| Muito Alto (MA) | Risco (MA-I) | Risco (MA-S) | Ações para a classe de ricos MA |
| Responsável pela informação:  Data: | | | |