**Plano de Tratamento de Riscos da <Sigla da estatal>**

**Controle de Versões**

*<Inserir os dados das versões.>*

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

1. **Introdução**

*<Descrever o documento e sua importância para a estatal].*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Riscos Identificados e Tratados | | | | | | | | | |
| Ativo | Ameaça | Descrição do tratamento a ser realizado | Estimativas/Restrições | | | | | | |
| Custo | | Esforço | Prazo | | Restrições | Responsável |
|  |  |  |  | |  |  | |  |  |
| **Datas** | | | | | | | | |  |
| Data de Início: | | | | Data prevista para a Finalização: | | | Data de Finalização: | |  |

1. **Riscos de Segurança da Informação Identificados e Tratados**

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

­<nome completo da autoridade máxima da Estatal >

<cargo da autoridade máxima da Estatal >

**Observações:**

A finalidade deste documento é determinar com precisão quem é responsável pela implementação de controles, em que espaço de tempo, com qual orçamento, entre outras características no tratamento dos riscos de SI da estatal. É preciso definir a metodologia de avaliação e tratamento de riscos à informação e definir o nível aceitável de riscos de acordo com a norma ISO/IEC 27001.

O tratamento de risco é uma etapa do processo de gestão de risco posterior a etapa de avaliação de risco – na avaliação de risco todos riscos precisam ser identificados, e o riscos que não são aceitáveis devem ser selecionados. A principal tarefa na etapa de tratamento de risco é selecionar uma ou mais opções para tratar cada risco inaceitável, isto é, decidir como mitigar todos estes riscos.

Tratamento dos riscos é o processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco.

O Tratamento do Risco de SI é a fase da gestão de riscos que envolve a decisão entre reter, evi­tar, transferir (compartilhar) ou reduzir os riscos. A entrada para o Tratamento dos Riscos de SI é uma lista de riscos priorizados conforme critérios de avaliação em relação aos cenários de incidente que levaram a tais riscos. Os objetivos a serem alcançados com o tratamento dos riscos são:

a. a definição de quais controles serão empregados para reduzir alguns destes ris­cos;

b. a retenção ou aceitação de outros riscos;

c. a ação de evitar outros riscos;

d. a transferência de alguns desses riscos a outros agentes; e

e. a definição de um *plano de tratamento do risco*.

As saídas da fase de tratamento são (i) o plano de tratamento do risco e (ii) a lista de riscos residuais, ambos sujeitos à decisão de aceitação pelos altos gestores da organização.

A Figura abaixo apresenta um fluxograma básico da atividade de tratamento do risco.



São aspectos gerais que devem ser considerados no tratamento do risco, conforme a ISO/IEC (2007):

a. as opções devem ser selecionadas baseadas em três aspectos: (i) nos resultados da apreciação do risco; (ii) no custo esperado para implementar as opções; e (iii) nos benefícios esperados com as opções;

b. quando largas reduções de risco podem ser obtidas com poucas despesas, essas opções devem ser implementadas. Outras opções de tratamento dependem de julgamento melhor exercitado;

c. as consequências adversas de riscos devem ser reduzidas a níveis mínimos, até quando isso for prático;

d. os riscos raros e severos devem ser cuidadosamente considerados pelos gesto­res. Nesses casos, podem ser necessários controles custosos, que não são econo­micamente justificados (exemplo: relativos à continuidade de negócios);

e. as opções para tratamento não são mutuamente exclusivas. Uma combinação de opções pode ser praticável;

f. alguns tratamentos reduzem mais de um risco (exemplo: treinamentos).

Exemplo de Tratamento de Riscos:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Riscos Identificados e Tratados | | | | | | | | | |
| Ativo | Ameaça | Descrição do tratamento a ser realizado | Estimativas/Restrições | | | | | | |
| Custo | | Esforço | Prazo | | Restrições | Responsável |
| Arquivos de backup | Dano ou destruição de arquivos de backup | Manter as cópias de backup das informações críticas | 400,00 | | 2 horas | 01 dia | | Não há | Analista de Infraestrutura |
| Senhas | Muito tempo sem trocar a senha de acesso | Implementar troca automática de senha a cada 30 dias | 1000,00 | | 5 horas | 03 dias | | Número mínimo de caracteres | Desenvolvedor |
| **Datas** | | | | | | | | |  |
| Data de Início:  31/07/2017 | | | | Data prevista para a Finalização:  31/07/2017 | | | Data de Finalização:  31/07/2017 | |  |