**Plano de Gestão de Riscos de Segurança da Informação da <Sigla da estatal>**

**Controle de Versões**

*<Inserir os dados das versões.>*

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

**1.**                  **Introdução**

*<A introdução do* ***Plano de Gerenciamento de Riscos*** *de SI deve fornecer uma visão geral de todo o documento. Ela deve incluir a finalidade, o escopo, as definições, os acrônimos, as abreviações, as referências e a visão geral deste* ***Plano de Gerenciamento de Riscos*** *de SI>*

**1.1**               **Finalidade**

*<Especifique a finalidade deste* ***Plano de Gerenciamento de Riscos*** *de SI>*

**1.2**               **Escopo**

*<Uma breve descrição do escopo deste* ***Plano de Gerenciamento de Riscos*** *de SI>*

**1.3**               **Definições, Acrônimos e Abreviações**

*<Esta subseção deve fornecer as definições de todos os termos, acrônimos e abreviações necessárias à adequada interpretação do* ***Plano de Gerenciamento de Riscos*** *de SI da estatal>*

**1.4**               **Referências**

*<Esta subseção deve fornecer uma lista completa de todos os documentos mencionados em qualquer outra parte do* ***Plano de Gerenciamento de Riscos*** *de SI. Cada documento deverá ser identificado por título, número do relatório (se aplicável), data e organização de publicação. Especifique as fontes a partir das quais as referências podem ser obtidas. Essas informações poderão ser fornecidas fazendo-se referência a um apêndice ou a outro documento>]*

**1.5**               **Visão Geral**

*<Esta subseção descreve o que o restante do* ***Plano de Gerenciamento de Riscos*** *de SI contém e explica como o documento está organizado>*

**2.**                  **Resumo dos Riscos**

*<uma breve descrição dos riscos gerais que podem ocorrer na estatal, relacionados a SI>*

**3.**                  **Tarefas de Gerenciamento de Riscos**

*<uma breve descrição das tarefas de gerenciamento de riscos de SI a serem executadas pela estatal. Nesta seção, você deve descrever o método a ser usado para identificar riscos e como a lista de riscos de SI será analisada e priorizada.*  *As estratégias de gerenciamento de riscos de SI que serão usadas, incluindo estratégias de diminuição, impedimento e/ou prevenção para os riscos mais significativos ("dez principais riscos").*  *Como o status de cada risco significativo e suas atividades de diminuição serão monitoradas. Revisão dos riscos e programações de relatórios.  Uma revisão dos riscos deverá fazer parte da revisão de aceitação de cada iteração/fase >*

**4.**                  **Organização e Responsabilidades***Uma lista dos grupos e pessoas específicos que estarão envolvidos nas atividades de gerenciamento de riscos de SI e uma descrição das tarefas e responsabilidades de cada um.]*

**5.**                  **Orçamento**

*<O orçamento disponível para o gerenciamento dos riscos de SI (quando essas informações ainda não estiverem incluídas no orçamento geral da estatal>*

**6.**                  **Ferramentas e Técnicas**

*<uma lista das ferramentas e/ou técnicas que serão usadas para armazenar informações sobre riscos, avaliar riscos e rastrear os status dos riscos ou gerar relatórios de gerenciamento de riscos>*

**7.**                  **Itens de Risco a Serem Gerenciados**

*<uma lista dos itens de risco que foram identificados>*

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

­<nome completo da autoridade máxima da Estatal >

<cargo da autoridade máxima da Estatal >

**Observações:**

**Finalidade**

A finalidade do Plano de Gerenciamento de Riscos de SI é garantir que os riscos sejam corretamente identificados, analisados, documentados, diminuídos, monitorados e controlados. Ele descreve a abordagem que será usada para identificar, analisar, priorizar, monitorar e diminuir os riscos. O Plano de Gerenciamento de Riscos de SI deve ser atualizado quando houver alguma mudança nos riscos ou nas estratégias de diminuição de riscos.

Um evento de segurança da informação, segundo a ABNT (2005), é uma ocorrência identi­ficada de um sistema, serviço ou rede que indica uma possível violação da política de seguran­ça da informação ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança da informação.

Um risco de segurança é um evento possível e potencialmente danoso a uma organiza­ção, isto é, um evento hipotético, que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significante. Sem chance de ocorrência futura, um evento hipotético não se configura como risco. Sem impacto negativo significante, um evento hipotético não se configura como risco. É também importante destacar que, mesmo que um evento futuro negativo tenha 50% de chance de ocorrer e impacto negativo valorado, haverá sempre uma incerteza associada a tal estimativa. Isto é, podemos ter baixa, média ou alta confiança de que o evento tem 50% de chance de ocorrer, bem como podemos ter baixa, média ou alta confiança de que o impacto negativo real será do valor que estimamos. Dessa forma, um risco poderia, de modo abstrato, ser obtido pela fórmula abaixo:

Risco de Segurança = Chance de ocorrência \* Impacto negativo estimado \* Incerteza re­lacionada com as medidas.

São exemplos de eventos de segurança da informação:

1. O funcionário X não está usando crachá;
2. O firewall X não está bloqueando a porta 1521 na máquina Y;
3. A senha do usuário X é fraca;
4. Um curto-circuito ocorreu no estabilizador na tarde de hoje;
5. Faz 2 meses que o backup do banco de dados Z não é realizado;
6. A chave da sala de servidores sumiu;
7. Faltou energia no bloco C hoje à tarde;
8. A cerca foi rompida na noite de ontem;
9. O alarme de detecção de intrusos disparou três vezes seguidas;
10. O alarme de detecção de intrusos está quebrado.

A compreensão dos eventos que ocorrem no ambiente de uma organização é essencial para que os riscos sejam avaliados com maior precisão. No caso específico da GRSI, os eventos estão relacionados aos ativos. Dessa forma, após o levantamento de ativos, é possível uma melhor estimativa dos eventos possíveis que poderão estar associados a cada ativo crítico.

Exemplo de um Processo de Gerenciamento de Riscos de SI:

