GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

ARTEFATO GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

SECRETARIA DE COORDENAÇÃO E GOVERNANÇA DAS EMPRESAS ESTATAIS

DIRETORIA DE ORÇAMENTO DE ESTATAIS

COORDENAÇÃO-GERAL DE GESTÃO DA INFORMAÇÃO DE ESTATAIS

BRASÍLIA - 2018

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO
SECRETARIA DE COORDENAÇÃO E GOVERNANÇA DAS EMPRESAS ESTATAIS

Fernando Antonio Ribeiro Soares
Secretário

André Nunes
Diretor do Departamento de Orçamento de Estatais

Gerson Batista Pereira
Coordenador-Geral de Gestão da Informação de Estatais

EQUIPE TÉCNICA
Natal Henrique Troz Guglilhermi – SEST
Otávio Porto Barbosa – SEST

UNIVERSIDADE DE BRASÍLIA

Márcia Abrahão Moura
Reitora

Sanderson Cesar Macedo Barbalho
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Georges Daniel Amvame Nze (Pesquisador Sênior)
Claudia Jacy Barrenco Abbas (Pesquisador Sênior)
Edna Dias Canedo (Pesquisador Sênior)
Rodrigo de Souza Goncalves (Pesquisador Sênior)
Adyr Andrade de Menezes
Amanda Aline Figueiredo Carvalho
Bruno Justino Garcia Praciano
Demétrio Antônio da Silva Filho
Fabricio de Oliveira Taguatinga
Glauber Luiz Lopes da Silva
Jean Victor Ribeiro Vieira
João Batista Alves Diniz
Jorge Guilherme Silva dos Santos
José Maria dos Reis Lisboa
Leomar Camargo de Souza
Marcus Vinicius Bomfim Guimaraes Barbalho
Moramay Coutinho Guimarães Coelho
Pedro Thiago Rocha de Alcântara
Priscilla Gonçalves da Silva e Souza
Rafaella Aparecida Rosa Lima
Rosa Cristina Portela Dias Jácome
Ruyther Parente da Costa
Victor Matheus da Silva

B823g

Brasil. Ministério do Planejamento, Desenvolvimento e Gestão.

Governança de tecnologia da informação : artefato gestão de riscos de segurança da informação / Ministério do Planejamento, Desenvolvimento e Gestão, Secretaria de Coordenação e Governança das Empresas Estatais, Coordenação-Geral de Gestão da Informação de Estatais; Universidade de Brasília. -- Brasília : MP, 2018.
16 p.

1. Governança Digital 2. Tecnologia da Informação 3. Empresa Estatal 4. Administração Pública I. Título II. Universidade de Brasília.

CDU 658.115:004

HISTÓRICO DE VERSÕES

14/03/2018 | Versão 1.0

Descrição: Inclusão dos artefatos, definição do processo, adequação do passo-a-passo, objetivos e capa ao processo.

Autor: Edna Dias Canedo e Priscilla Gonçalves da Silva e Souza.

Revisor: Natal Henrique Troz Guglilhermi e Otávio Porto Barbosa.

SUMÁRIO

INTRODUÇÃO

Em observância às normas e diretrizes de Tecnologia da Informação (TIC) do Poder Executivo Federal, disseminadas pela Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão (SETIC/MP), na condição de Órgão Central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e, conforme preconiza o Decreto Presidencial nº 7.579, de 11 de outubro de 2011, o Ministério do Planejamento, Desenvolvimento e Gestão (MP), como Órgão Setorial integrante do SISP, vincula-se aos preceitos definidos pelo Sistema relativamente à governança e gestão de tecnologia da informação.

Diante do tema e também em decorrência de orientação do TCU, conforme Acórdão 3051/2014 a SEST deve atuar no desenvolvimento de ações que promovam a disseminação da cultura de Governança de TIC nas Empresas Estatais, para facilitar o cumprimento dos objetivos definidos e exigidos no planejamento estratégico, como também na racionalização de recursos e retorno financeiro/operacional.

VISÃO GERAL

2.1. Objetivo

Identificar e apontar os passos necessários, de acordo com práticas listadas em literatura e conhecimento prático, para a Gestão de Riscos de Segurança da Informação nas diferentes Empresas Estatais.

2.2. Justificativa

A SEST, institucionalmente, como órgão de Coordenação e Governança das Empresas Estatais, deve promover e orientar a Governança de TIC dessas entidades. As iniciativas nesse sentido devem ser planejadas e priorizadas a partir do alinhamento dos investimentos de TIC aos objetivos estratégicos das organizações.

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

3.1. Definição

A Gestão de Riscos de Segurança da Informação visa identificar e tratar os riscos relativos à Segurança da Informação (SI) e às ameaças de vulnerabilidades dos ativos, os quais podem comprometer a confidencialidade, a integridade e a disponibilidade das informações da Estatal.

Nesse sentido, este processo define práticas para o tratamento e a gestão dos riscos de Segurança da Informação.

3.2. Passo a passo

Para implantação do processo de Gestão de Riscos de Segurança da Informação, é preciso executar as seguintes atividades:

1 - Determinar as fontes e categorias dos riscos de Segurança da Informação (SI) na Estatal.

2 - Definir parâmetros para realizar a análise e categorização dos riscos de SI e controlar o esforço da Gestão de Riscos de SI na Estatal.

3 - Estabelecer e manter a estratégia da Estatal a ser utilizada para a Gestão de Riscos de SI.

4 - Identificar e documentar os riscos de SI na Estatal em um formulário adequado.

5 - Avaliar e categorizar cada risco de SI identificado utilizando as categorias e os parâmetros de riscos definidos pela Estatal e determinar sua prioridade.

6 - Desenvolver um plano de mitigação de riscos de SI de acordo com a estratégia de Gestão de Riscos de SI da Estatal.

7 - Monitorar o status de cada risco de SI periodicamente e implementar o plano de mitigação de riscos de SI da Estatal.

8 - Definir um plano de tratamento de riscos de SI para a Estatal.

9 - Classificar e monitorar o clico de vida dos riscos de SI.

ARTEFATOS

4.1. Documentos

Os modelos dos documentos para a Gestão de Riscos de Segurança da Informação estão disponíveis para download no endereço eletrônico http://www.planejamento.gov.br/acesso-a-informacao/institucional/unidades/sest, conforme lista a seguir:

Definir Categorias e Parâmetros para os Riscos de SI	
 Formulário de Categorias e Parâmetros de Riscos de SI	Nome: Formulário de Categorias e Parâmetros de Riscos de SI
	Objetivo: Definir categorias e parametrizar critérios para a categorização dos riscos de SI.
Estabelecer o Plano de Gestão de Riscos de SI	
 Plano de Gestão de Riscos de Segurança da Informação	Nome: Plano de Gestão de Riscos de Segurança da Informação
	Objetivo: Definir uma abordagem para identificar, analisar, priorizar documentar e monitorar os riscos de SI.
Definir Ações para Tratamento dos Riscos de SI	
 Plano de Tratamento de Riscos de SI	Nome: Plano de Tratamento de Riscos de SI
	Objetivo: Determinar ações para mitigar os riscos de SI, definindo responsáveis, prazos, orçamento, entre outros aspectos.

4.1.1 Formulário de Categorias e Parâmetros de Riscos de SI

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:			

4.1.2 Plano de Gestão de Riscos de Segurança da Informação

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 >

A especificação das responsabilidades pela execução das atividades de gerenciamento de riscos de SI em uma

4. Organização e Responsabilidades

<uma lista dos grupos de pessoa

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:

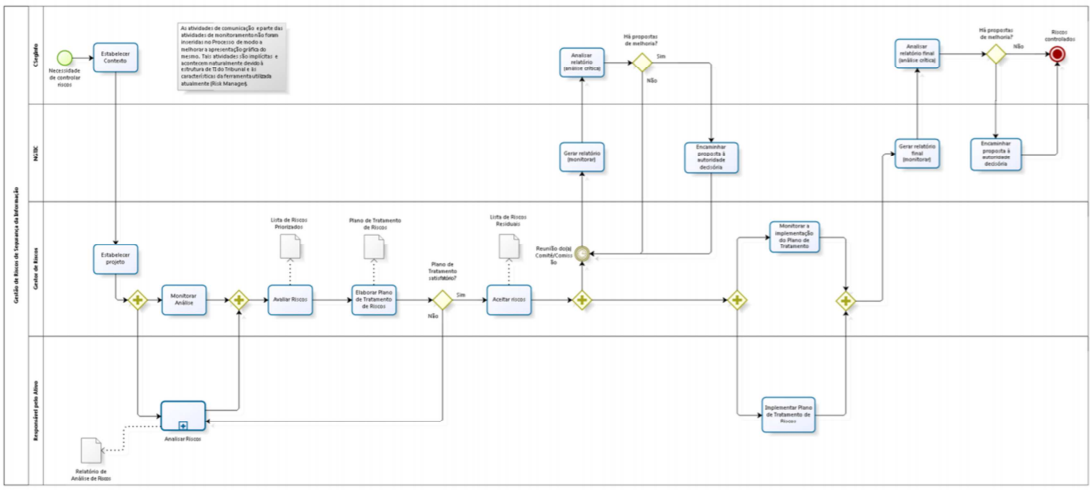
Risco de Segurança = Chance de ocorrência * Impacto negativo estimado * Incerteza relacionada com as medidas.

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:



4.1.3 Plano de Tratamento de Riscos de SI

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:	

2. 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;

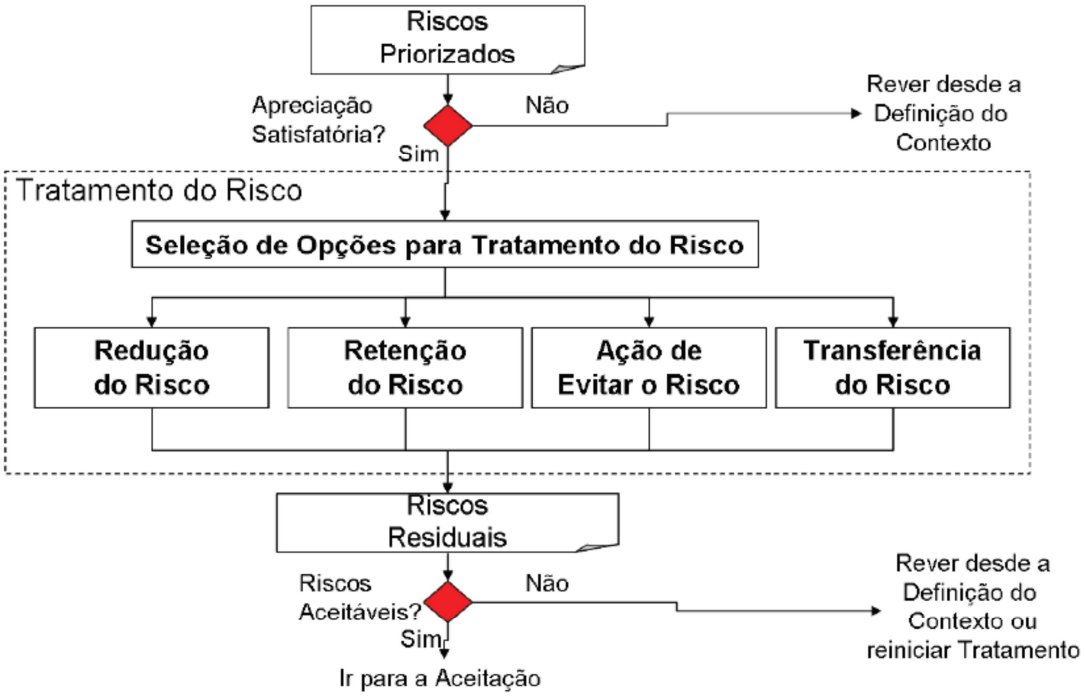
c. a ação de evitar outros riscos;

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	

REFERÊNCIAS BIBLIOGRÁFICAS

5.1. Documentos

- Planejamento Estratégico da Secretaria 2015-2018.
- Guia de Comitê de TIC do SISP (Versão 2.0 – 2016).
- Guia do PDTIC do SISP (Versão 2.0 Beta – 2015).
- Guia de Gerenciamento de Projetos do SISP (Versão 1.0 MGP-SISP – 2011).
- Guia de Metodologia de Gerenciamento de Portfólio de Projetos do SISP (Versão 1.0 MGPP-SISP – 2013).
- Guia de Processo de Software do SISP (Versão 1.0 PSW-SISP – 2012).
- Guia de Governança de Tecnologia da Informação e Comunicação (GovTIC) do SISP (Versão 2.0 – 2017).