GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

ARTEFATO GESTÃO DE RISCOS DE TIC

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 TIC / 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.
21 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

13/03/2018 | 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 Pedro Thiago Rocha de Alcântara.

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 TIC 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 TIC

3.1. Definição

A Gestão de Riscos visa identificar, avaliar e reduzir continuamente os riscos relacionados a TIC dentro dos níveis de tolerância definidos pela gestão executiva da organização.

Nesse sentido, faz-se necessária a definição de políticas e diretrizes para o tratamento de riscos e gerenciamento da segurança da informação.

3.2. Passo a passo

Para implantação da Gestão de Riscos de TIC é preciso executar as seguintes atividades:

1 - O Comitê de TIC deve elaborar a Política de Gestão de Riscos de TIC da Estatal e aprova-la de acordo com as normas do Comitê de TIC.

2 - O Comitê de TIC deve elaborar a Política de Segurança da Informação da Estatal, tendo em vista a conformidade legal e regulatória, e aprova-la de acordo com as normas do Comitê.

3 - O Comitê de TIC deve definir formalmente os papeis e responsabilidades dos envolvidos na Gestão de Riscos de TIC.

4 - O Plano de Gestão de Riscos de TIC deve ser definido pelos responsáveis pela área de Gestão de Riscos de TIC.

5 - O Comitê de TIC deve assegurar que o Plano de Gestão de Riscos esteja em conformidade legal e regulatória.

6 - O Comitê de TIC deve definir os indicadores para avaliação de desempenho para a Gestão de Riscos.

7 - A análise de riscos deve ser realizada pelos responsáveis pela área de Gestão de Riscos de TIC da Estatal.

8 - A identificação e a gestão dos riscos diretos devem ser realizadas pelos responsáveis pela Gestão de Riscos de TIC da Estatal.

9 - A identificação e a gestão dos riscos dos requisitos devem ser realizadas pelos responsáveis pela Gestão de Riscos de TIC da Estatal.

10 - Os benefícios da Gestão de Riscos devem ser comunicados e documentados a todas as partes interessadas da Estatal.

ARTEFATOS

4.1. Documentos

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

Estabelecer Políticas de Gestão de Riscos	
 Política de Gestão de riscos de TIC	Nome: Política de Gestão de Riscos de TIC
	Objetivo: Documentar a política de Gestão de Riscos estabelecida para a Estatal.
 Política de Segurança da Informação	Nome: Política de Segurança da Informação
	Objetivo: Documentar a política de Segurança da Informação estabelecida para a Estatal.
Definir Práticas da Gestão de Riscos	
 Plano de Gestão de Riscos	Nome: Plano de Gestão de Riscos
	Objetivo: Definir os processos, artefatos, papeis e ferramentas da Gestão de Riscos.

4.1.1 Política de Gestão de Riscos de TIC

Política de Gestão de Riscos da <Sigla da estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Introdução

<Introduzir a politica de gestão de riscos, ressaltando seu papel na organização.>

2. Governança

<Descrever a estrutura de governança referente a gestão de riscos.>

2.1. Estrutura
2.2. Comitê de Riscos
2.3. Diretoria de Riscos
2.4. Comitê de Investimentos

3. Processo de Investimento e Papel do Controle de Risco

<Descrever a estrutura de governança referente a gestão de riscos.>

4. Política de Gerenciamento de Riscos

<Descrever política de gerenciamento de riscos definindo os riscos importantes para organização, mapeando a gestão desses riscos.>

Observações:

A Política de Gestão de Risco tem como objetivo descrever os princípios, conceitos e valores que norteiam o grupo GPS na gestão dos riscos de liquidez, riscos de mercado, risco de crédito, concentração, riscos operacionais e contraparte.

A Política também descreve o controle, gerenciamento, monitoramento, mensuração e o ajuste permanente dos riscos inerentes a cada um dos riscos, inclusive em situações de estresse. É concebida de modo a conferir transparência com relação às rotinas e o processo formal praticado pelos Gestores no gerenciamento dos riscos.

O escopo de uma política de risco é triplamente limitado:

(1) O monitoramento de risco aplica-se às carteiras agregadas dos clientes, englobando ativos adquiridos diretamente, via carteiras administradas, ou indiretamente, via Fundos Exclusivos, Restritos, Abertos ou Fechados. Nesses casos, no entanto, as políticas específicas aplicadas, como por exemplo a composição da carteira, os parâmetros e limites de alocação, e as regras gerais de monitoramento são definidos diretamente com cada cliente;

(2) Em relação aos Fundos Abertos que não sejam Fundos Exclusivos e Fundos Restritos, a política de risco aplica-se no nível dos próprios fundos, inobstante as políticas individuais dos clientes. Nesses casos, principalmente em relação à política de risco de liquidez e à política de risco de crédito, os presentes processos podem sobrepor-se, sem se substituir, às políticas individuais de cada cliente; e
(3) Em relação às políticas institucionais de risco, estas aplicam-se sobre todas as empresas do grupo e Colaboradores, sem exceção. Os processos de gerenciamento de risco operacional e o plano de contingência são, destarte, desenvolvidos tendo em vista o funcionamento das empresas integrantes do grupo GPS.

Governança:

Estrutura

A área de risco da Gestão da Política de Riscos (GPS) é integrada e tem jurisdição sobre a GPS Planejamento e sobre a CFO. É formada pelo Comitê de Risco e pela Diretoria de Risco.

Comitê de Risco

Responsabilidades: O Comitê de Risco (“CR”) é o órgão da Gestora incumbido de:
(i) dar orientações gerais e aprovar a política de risco;
(ii) estabelecer objetivos e metas de risco para as diversas áreas da gestora e para a própria área de risco;
(iii) estabelecer parâmetros e métricas para cada uma das políticas de risco, controlando-as, solicitando relatórios e o desenvolvimento de sistemas;
(iv) avaliar resultados e performance da Diretoria de risco, solicitar modificações e correções;
(v) orientar as diversas áreas da GPS, indicando riscos, solicitando revisões de processo, metas e indicadores; e
(vi) evitar desenquadramentos, erros ou falhas, gerir riscos operacionais, crédito, mercado, contraparte, concentração e contraparte.
(vii) prestar reporte ao Comitê Executivo sobre decisões que gerem impacto no negócio.
(viii) as decisões são formalizadas em ATAS e circuladas a todos os membros do comitê. GPS – Política de Gestão de Riscos.

Diretoria de Risco

Responsabilidades: A Diretoria de Risco (“DdR’’) é responsável pela definição e execução das práticas de gestão de riscos de performance, de liquidez, de crédito, e operacionais descritas neste documento, assim como pela qualidade do processo e metodologia, bem como a guarda dos documentos que contenham as justificativas das decisões tomadas.
Funções: A Diretoria de Risco estará incumbida de:
(i) implementar a Política, planejando a execução e executando os procedimentos definidos pelo Comitê de Risco;
(ii) redigir os manuais, procedimentos e regras de risco;

(iii) acompanhar desenquadramentos apontados e aplicar os procedimentos definidos na Política aos casos fáticos;
(iv) produzir relatórios de risco e levá-los ao comitê de risco e para a área causadora e/ou solucionadora do incidente de risco;

Garantia de Independência

O Comitê de Risco é subordinado ao Comitê Executivo (Coex), sendo que suas decisões se submetem ao Coex, portanto o único colegiado que pode retificar as decisões do Comitê de Risco é o Coex, desta forma a independência do Comitê de Risco é garantida no âmbito tático e limitada no campo estratégico.

Comitê de Investimentos

Responsabilidades: O comitê de investimentos é órgão colegiado que determina que tipo de veículo de investimento que poderá ser recomendado pela GPS. O patrocinador submete ao comitê o veículo em questão e após sabatina o comitê delibera no tocante a aprovação ou não. Todos os veículos recomendados pela GPS devem possuir aprovação neste comitê.

Processo de Investimento e Papel do Controle de Risco

O processo de investimento da GPS busca formular uma política de investimento eficaz e individualizada para cada cliente de forma a identificar o perfil de risco do cliente que se enquadrará em um portfólio que atenda o apetite de risco de cada cliente conforme identificado através da aplicação do questionário de perfil de risco. Desta forma há um direcionamento congruente à disciplina de investimentos ao longo do tempo. Para isso, observam-se algumas variáveis, escolhidas e trabalhadas diretamente com o cliente:

- Retorno desejado;
- Horizonte de investimento;
- Tolerância ao risco de cada investidor.

4.1.2 Política de Segurança da Informação

Política de Segurança da Informação e Comunicação da <Sigla da estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Introdução

<Introduzir a politica de segurança, ressaltando seu papel na organização.>

2. Autenticação

<Apresentar política de autenticação.>

2.1. Política de Senha

<Detalhar política de senha.>

2.2. Política de E-mail

<Detalhar política de uso de e-mail.>

2.3. Política de Acesso a Internet

<Descrever a política de acesso a internet.>

3. Política de uso de Estação de Trabalho

<Descrever a política de segurança em relação a uso de estações de trabalho.>

4. Política Social

<Descrever fatores sociais da política de segurança.>

5. Vírus e Códigos Maliciosos

<Descrever a política de segurança em relação a vírus e códigos maliciosos>

6. Equipe de Segurança

<Descrever a equipe de segurança>

6.1. Membros da Equipe Técnica

<Listar Membros da Equipe Técnica.>

Nome	E-mail	Ramal	Celular

6.2. Membros da Equipe de Segurança

<Listar Membros da Equipe de Segurança.>

Versão	E-mail	Ramal	Celular

Observações:

Política de Segurança da Informação e Comunicações (PoSIC) tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso da Estatal contra ameaças e vulnerabilidades. Desse modo, a Política busca preservar os seus ativos de informação, assim como a sua imagem institucional.

A PoSIC estabelece o comprometimento da alta direção organizacional da estatal, com vistas a prover apoio para a implantação da Gestão dos Riscos de Segurança da Informação e Comunicações (GRSIC).

As diretrizes da segurança da informação estabelecidas na PoSIC aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pela estatal, e que devem ser seguidas pelos usuários, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação. Independentemente da forma ou do meio pelo qual a informação seja apresentada ou compartilhada, deverá ser sempre protegida adequadamente, de acordo com a Política.

Os requisitos de segurança da informação e comunicações da estatal devem ser explicitamente citados em todos os termos de compromisso celebrados entre a instituição e terceiros, por meio de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política, devendo também ser exigido termo de confidencialidade.

A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços da Estatal. Essa proteção deve ser de acordo com o valor, sensibilidade e criticidade da informação, devendo ser desenvolvido, para este fim, sistema de classificação da informação. Os dados, as informações e os sistemas de informação da Estatal devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

O monitoramento, auditoria e conformidade de ativos de informações observarão o seguinte:

a) O uso dos recursos de tecnologia da informação e comunicações disponibilizados pela Estatal é passível de monitoramento e auditoria, devendo ser implementados e mantidos, à medida do possível, mecanismos que permitam a sua rastreabilidade;

b) A entrada e saída de ativos de informação da Estatal deverá ser registrada e autorizada por autoridade competente mediante procedimento formal;

c) A TIC manterá registros e procedimentos específicos, tais como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas institucionais, à rede interna e à internet.

Controle de Acesso e Uso de Senhas

As regras de controle de acesso a todos os sistemas institucionais, intranet, internet, informações, dados e às instalações físicas da Estatal deverão ser definidas e regulamentadas, por meio de normas internas, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da instituição.

Uso de E-Mail

O correio eletrônico é um recurso de comunicação institucional da Estatal e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta PoSIC e das normas específicas, além das demais diretrizes do Governo Federal.

Acesso à Internet

O acesso à rede mundial de computadores (internet), no ambiente de trabalho, deve ser regido por normas e procedimentos específicos, atendendo às determinações desta PoSIC, e demais orientações governamentais e legislação em vigor.

Uso das Redes Sociais

A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações da Estatal, deve ser regida por normas internas especificas e deve estar em consonância tanto com a PoSIC quanto com os objetivos estratégicos da instituição.

Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação devem observar critérios e controles de segurança, com vistas a garantir o respeito aos atributos básicos de segurança da informação.

Membros da Equipe Técnica

Competências e Responsabilidades

- Dar suporte à promoção da cultura de segurança da informação e comunicações;
- Aprovar a Política de Segurança da Informação e Comunicações (PoSIC);
- Aprovar programa orçamentário específico para as ações de SIC, conforme proposto pelo Comitê de Segurança da Informação e Comunicação.
- Promover e disseminar a cultura de segurança da informação e comunicações;

Coordenar a elaboração da Política de Segurança da Informação e Comunicações

4.1.3 Plano de Gestão de Riscos

Plano de Gestão de Riscos de TI para a <Sigla da estatal>

Controle de Versões
<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Objetivo do Plano de Gestão de Riscos

<Descrever o objetivo do Plano de Gestão de Riscos da estatal>

2. Gestão de Riscos

<Usar as seções seguintes para identificar os componentes do Plano de Gestão de Riscos>

2.1. Processos de Riscos

<Descrever os Processos de Gestão dos Riscos a serem adotados.

2.2. Documentos Padronizados de Risco

<Descrever os documentos padronizados a serem usadas nos processos dos riscos. Indique onde estão armazenados, como serão usados, e os responsáveis envolvidos>

2.3. Responsabilidades dos Riscos da Equipe do Projeto
<Descrever as responsabilidades referentes aos processos dos riscos de cada membro do projeto, mesmo que já citados em outros tópicos do documento. Ressaltar as divisões de responsabilidade entre compras, projetos e jurídico.>

Membro da Equipe	Responsabilidades

2.4. Ferramentas Usadas
<Listar as ferramentas que o projeto empregará. Descreve como serão usadas e o responsável por isso.>

Ferramenta	Descrição	Quando aplicar	Responsavel

3. Identificar os Riscos
< Descrever como os riscos serão determinados e documentados. >

3.1. Estrutura Analítica dos Riscos

<Determinar as categorias e subcategorias de riscos e melhor forma de agrupá-las de modo a facilitar seu gerenciamento.>

3.2. Riscos

<Descrever riscos identificados e como serão tratados (Tipos de Contrato, Cláusulas, Requisitos de bônus de desempenho, seguros, ...)>

4. Análise Qualitativa dos Riscos

<Descrever como será feita a análise qualitativa dos riscos.>

4.1. Definições de Probabilidade e Impacto dos Riscos

<Definir como será feio a Avaliação de probabilidade e impacto dos riscos.>

5. Análise Quantitativa dos Riscos

<Descrever como será feita a análise quantitativa dos riscos.>

6. Planejar as respostas aos Riscos

<Descrever como os riscos serão tratados e como serão determinadas as respostas aos riscos.>

6.1. Reservar Contingências

<Identificar as Estratégias de respostas de contingência quantificando as reservas de contingência e determinando como serão usadas.>

6.2. Estratégias para Riscos Negativos ou Ameaças

<Identificar as Estratégias para riscos negativos ou ameaças.>

6.3. Estratégias para Riscos Positivos ou Oportunidades

<Identificar as Estratégias para riscos positivos ou oportunidades>

7. Controlar os Riscos

<Descrever como os riscos serão monitorados e controlados >

Observações:

Gerenciar os riscos do projeto requer um Plano de gerenciamento dos riscos descrevendo como os processos de riscos serão estruturados e executados iniciando pela identificação dos riscos, suas análises qualitativa e quantitativa, seu plano de respostas e concluindo com a forma que os riscos serão controlados e monitorados.
O Plano de gerenciamento dos riscos é desenvolvido e aprovado durante a fase de planejamento do projeto e é um plano auxiliar do Plano de gerenciamento do projeto.

Tem como objetivo aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos no projeto e orientar a equipe do projeto sobre como os processos de riscos serão executados.

Processos de Riscos:

- Identificar os riscos

- Determinar quais riscos podem afetar o projeto e documentar suas características.

- Realizar a análise qualitativa dos riscos
- Avaliar a exposição ao risco para priorizar os riscos que serão objetos de análise ou ação adicional.

- Realizar a análise quantitativa dos riscos
- Efetuar a análise numérica do efeito dos riscos identificados nos objetivos gerais do projeto.

- Planejar as respostas aos riscos
- Desenvolver opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos do projeto.

- Controlar os riscos
- Monitorar e controlar os riscos durante o ciclo de vida do projeto.

Documentos padronizados de risco

Documento	Descrição
Plano de gerenciamento dos riscos	O Plano de Gerenciamento dos riscos tem como objetivo aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos no projeto e orientar a equipe do projeto sobre como os processos de riscos serão executados.
Registro dos riscos	O registro dos riscos é iniciado no processo de Identificar os riscos e é atualizado conforme os outros processos de gerenciamento dos riscos (análise qualitativa, quantitativa, planejar as respostas aos riscos e monitorar e controlar os riscos) são conduzidos, resultando em um aumento no nível e no tipo de informações contidas no registro dos riscos ao longo do tempo.

Responsabilidades dos Riscos da Equipe do Projeto

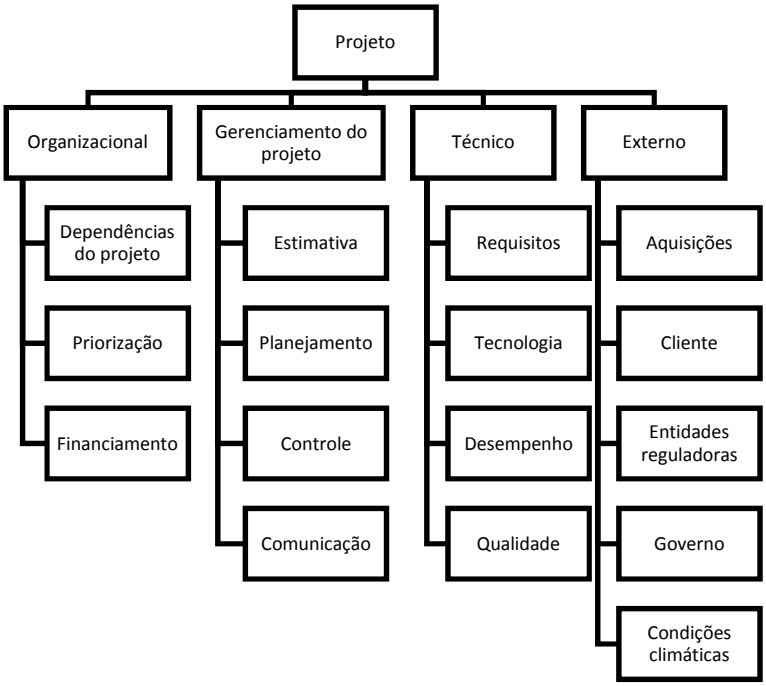
Membro da Equipe	Responsabilidades
GP	Certificar que os riscos foram identificados e tratados de modo a aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos no projeto. Monitorar os riscos conforme descrito neste plano. Divulgar informações pertinentes aos riscos do projeto
Advogado	Assessorar juridicamente o GP em relação às decisões contratuais relacionadas aos riscos
Patrocinador/Comitê do Projeto	Aprovar o plano de gerenciamento de riscos e suas reservas de contingências. Aprovar o uso das reservas de contingência.

Ferramentas Usadas

Ferramenta	Descrição da aplicação	Quando aplicar	Responsável
Brainstorming	Será usado para identificar riscos	No início do projeto e sempre que for necessário revisar os riscos identificados	Gerente do Projeto

Normalmente é usado o Brainstorming para identificar os riscos do projeto. O Gerente de projetos deverá compor uma equipe multidisciplinar para participar do brainstorming de modo que todas as áreas estejam bem representadas e que os riscos principais do projeto sejam identificados.

Estrutura Analítica do Projeto



Probabilidade e Impacto dos Riscos

Probabilidade	% de certeza
1-Muito baixa	0 a 20%
2-Baixa	20 a 40%
3-Média	40 a 60%
4-Alta	60 a 80%
5-Muito Alta	> 80%

Impacto
1-Muito baixo
2-Baixo
3-Médio
4-Alto
5-Muito Alto

O impacto varia de acordo com a área impactada. Veja o quadro abaixo orientando como classificar o impacto.
Quando um risco impactar mais de uma área, deverá ser usada a área mais impactada.

	Muito baixo (Nota = 1)	Baixo (Nota = 2)	Médio (Nota = 3)	Alto (Nota = 4)	Muito alto (Nota = 5)
Custo	Até 2% no orçamento	De 2 a 5% no orçamento	De 5 a 8% no orçamento	De 8 a 10% no orçamento	Acima de 10% no orçamento
Tempo	Até 2% no	De 2 a 5% no	De 5 a 8% no	De 8 a 10% no	Acima de 10%

	prazo total	prazo	prazo	prazo	no prazo
Escopo		Mudança impactará no custo	Mudança impactará no custo e no tempo	Mudança impactará no custo, tempo e qualidade	

O grau do risco (G = I x P) está definido na matriz de probabilidade x impacto demonstrada abaixo.
Matriz de Probabilidade x Impacto

Probabilidade					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Impacto	1	2	3	4	5

Os graus de riscos serão priorizados da seguinte forma:
- Vermelho: risco elevado;
- Amarelo: risco médio;
- Verde: risco baixo.

Estratégias para Riscos Negativos ou Ameaças

Estratégia	Descrição	Exemplo
Eliminar	Remover em 100% a probabilidade que a ameaça ocorra.	Cancelar o projeto;
Transferir	Transferir total ou parcial o impacto em relação a uma ameaça para um terceiro.	Fazer um seguro;
Mitigar	Reduzir a probabilidade e/ou impacto de um risco.	Redundância de recursos;
Aceitar	De forma ativa, estabelecendo plano de contingência caso o evento ocorra; ou de forma passiva, o risco será tratado quando ocorrer.	

Estratégias para Riscos Positivos ou Oportunidades

Estratégia	Descrição

Explorar	Garantir que a oportunidade ocorra para explorar seus benefícios;
Compartilhar	Transferir total ou parcial a propriedade da oportunidade para um terceiro que tem maior capacidade de explorá-la;
Melhorar	Aumentar probabilidade e/ou impacto de uma oportunidade;
Aceitar	Tirar proveito caso a oportunidade ocorra.

O GP e os responsáveis definidos na matriz de responsabilidade devem acompanhar os riscos identificados, monitorar os riscos residuais, identificar novos riscos, executar os planos de respostas a riscos e avaliar sua eficácia durante todo o ciclo de vida do projeto.

O gerente de projeto executa o que foi planejado na análise de riscos e controla os riscos novos identificados durante a execução do projeto.
Este processo consiste de:

- Identificar, analisar, e planejar para riscos novos;
- Monitorar os riscos identificados;
- Analisar novamente os riscos existentes de acordo com as mudanças de contexto;
- Monitorar condições para ativar planos de contingência;
- Monitorar riscos residuais;
- Rever a execução do plano de respostas aos riscos para avaliar sua eficácia;
- Determina se as premissas do projeto ainda são válidas;
- Determinar se as políticas e os procedimentos de gestão de risco estão sendo seguidas;
- Determinar se as reservas de contingência de custo e prazo devem ser modificadas com os riscos do projeto.

Checklist

- Implementar a análise de risco aprovada.
- Identificar novos riscos e gerenciá-los adequadamente.
- Atualizar o plano de resposta de riscos com os riscos novos.
- Incluir um sumário dos riscos nas reuniões de status.
- Revisar todos os documentos impactados.
- Conduzir sessões para avaliar os riscos se necessário.

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).