MANUAL DE PROCEDIMENTO

MPR/STI-034-R00

GESTÃO DE RISCOS DE TI

12/2018

REVISÕES

Revisão	Aprovação	Aprovado Por	Modificações da Última Versão
R00	12/12/2018	STI	Versão Original

ÍNDICE

PARTICIPAÇÃO NA EXECUÇÃO DOS PROCESSOS

ÁREAS ORGANIZACIONAIS

1) Gerência Técnica de Planejamento e Projetos

a) Monitorar Riscos de Tecnologia da Informação

GRUPOS ORGANIZACIONAIS

a) Gerentes da STI

1) Monitorar Riscos de Tecnologia da Informação

b) GTPP/STI - Servidores

1) Mapear Riscos Relativos à STI

2) Monitorar Riscos de Tecnologia da Informação

c) STI - Empresa de Apoio

1) Monitorar Riscos de Tecnologia da Informação

1. DISPOSIÇÕES PRELIMINARES

1.1 INTRODUÇÃO

Este manual contém processos que cobram as atividade de identificação, análise e tratamento de riscos de TI.

O MPR estabelece, no âmbito da Superintendência de Tecnologia da Informação - STI, os seguintes processos de trabalho:

a) Mapear Riscos Relativos à STI.

b) Monitorar Riscos de Tecnologia da Informação.

1.2 REVOGAÇÃO

Item não aplicável.

1.3 FUNDAMENTAÇÃO

Resolução nº 381, de 14 de junho de 2016, art. 31 e alterações posteriores

1.4 EXECUTORES DOS PROCESSOS

Os procedimentos contidos neste documento aplicam-se aos servidores integrantes das seguintes áreas organizacionais:

Área Organizacional	Descrição
Gerência Técnica de Planejamento e Projetos - GTPP	A Gerência Técnica de Planejamento e Projetos é responsável por formular estratégias e padrões relacionados com a governança de tecnologia da informação para a sistematização e disponibilização de informações gerenciais, visando dar suporte ao processo decisório da Agência, e coordenar, supervisionar, acompanhar, controlar e avaliar a execução das atividades relacionadas com a governança de tecnologia da informação no âmbito da Superintendência de Tecnologia da Informação, além de manter o Plano Diretor de Tecnologia da Informação.

Grupo Organizacional	Descrição
Gerentes da STI	Os gerentes da STI são os responsáveis pelas gerências GTPP, GTAS, GESI e GEIT
GTPP/STI - Servidores	Servidores lotados na GTPP/STI
STI - Empresa de Apoio	Empresa contratada pela Anac para trabalhar em loco apoiando a GESI.

1.5 ELABORAÇÃO E REVISÃO

O processo que resulta na aprovação ou alteração deste MPR é de responsabilidade da Superintendência de Tecnologia da Informação - STI. Em caso de sugestões de revisão, deve-se procurá-la para que sejam iniciadas as providências cabíveis.

Compete ao Superintendente de Tecnologia da Informação aprovar todas as revisões deste MPR.

1.6 ORGANIZAÇÃO DO DOCUMENTO

O capítulo 2 apresenta as principais definições utilizadas no âmbito deste MPR, e deve ser visto integralmente antes da leitura de capítulos posteriores.

O capítulo 3 apresenta as competências, os artefatos e os sistemas envolvidos na execução dos processos deste manual, em ordem relativamente cronológica.

O capítulo 4 apresenta os processos de trabalho referenciados neste MPR. Estes processos são publicados em outros manuais que não este, mas cuja leitura é essencial para o entendimento dos processos publicados neste manual. O capítulo 4 expõe em quais manuais são localizados cada um dos processos de trabalho referenciados.

O capítulo 5 apresenta os processos de trabalho. Para encontrar um processo específico, deve-se procurar sua respectiva página no índice contido no início do documento. Os processos estão ordenados em etapas. Cada etapa é contida em uma tabela, que possui em si todas as informações necessárias para sua realização. São elas, respectivamente:

a) o título da etapa;

b) a descrição da forma de execução da etapa;

c) as competências necessárias para a execução da etapa;

d) os artefatos necessários para a execução da etapa;

e) os sistemas necessários para a execução da etapa (incluindo, bases de dados em forma de arquivo, se existente);

f) os documentos e processos administrativos que precisam ser elaborados durante a execução da etapa;

g) instruções para as próximas etapas; e

h) as áreas ou grupos organizacionais responsáveis por executar a etapa.

O capítulo 6 apresenta as disposições finais do documento, que trata das ações a serem realizadas em casos não previstos.

Por último, é importante comunicar que este documento foi gerado automaticamente. São recuperados dados sobre as etapas e sua sequência, as definições, os grupos, as áreas organizacionais, os artefatos, as competências, os sistemas, entre outros, para os processos de trabalho aqui apresentados, de forma que alguma mecanicidade na apresentação das informações pode ser percebida. O documento sempre apresenta as informações mais atualizadas de nomes e siglas de grupos, áreas, artefatos, termos, sistemas e suas definições, conforme informação disponível na base de dados, independente da data de assinatura do documento. Informações sobre etapas, seu detalhamento, a sequência entre etapas, responsáveis pelas etapas, artefatos, competências e sistemas associados a etapas, assim como seus nomes e os nomes de seus processos têm suas definições idênticas à da data de assinatura do documento.

2. DEFINIÇÕES

A tabela abaixo apresenta as definições necessárias para o entendimento deste Manual de Procedimento.

2.1 Sigla

Definição	Significado
GTPP	Gerência Técnica de Planejamento e Projetos
STI	Superintendência de Tecnologia da Informação

3. ARTEFATOS, COMPETÊNCIAS, SISTEMAS E DOCUMENTOS ADMINISTRATIVOS

Abaixo se encontram as listas dos artefatos, competências, sistemas e documentos administrativos que o executor necessita consultar, preencher, analisar ou elaborar para executar os processos deste MPR. As etapas descritas no capítulo seguinte indicam onde usar cada um deles.

As competências devem ser adquiridas por meio de capacitação ou outros instrumentos e os artefatos se encontram no módulo "Artefatos" do sistema GFT - Gerenciador de Fluxos de Trabalho.

3.1 ARTEFATOS

Não há artefatos descritos para a realização deste MPR.

3.2 COMPETÊNCIAS

Para que os processos de trabalho contidos neste MPR possam ser realizados com qualidade e efetividade, é importante que as pessoas que venham a executá-los possuam um determinado conjunto de competências. No capítulo 5, as competências específicas que o executor de cada etapa de cada processo de trabalho deve possuir são apresentadas. A seguir, encontra-se uma lista geral das competências contidas em todos os processos de trabalho deste MPR e a indicação de qual área ou grupo organizacional as necessitam:

Competência	Áreas e Grupos
Analisa documentos e artefatos da STI, levando em consideração a aprovação ou reprovação dos mesmos, seguindo as diretrizes da ANAC.	GTPP/STI - Servidores
Avalia documento de serviço com base em ferramentas de análise de risco.	GTPP/STI - Servidores
Demonstra, com antecedência, o risco do não cumprimento das metas intermediárias da Superintendência.	GTPP/STI - Servidores
Gerencia riscos de acordo com as melhores práticas.	GTPP/STI - Servidores
Implementa processos internos de gerenciamento de risco.	GTPP/STI - Servidores

3.3 SISTEMAS

Nome	Descrição	Acesso
GFT - Processos de Trabalho	Módulo de Processos de Trabalho do GFT	\\sperj1208\gft\aplicacao\files\6.exe

3.4 DOCUMENTOS E PROCESSOS ADMINISTRATIVOS ELABORADOS NESTE MANUAL

Não há documentos ou processos administrativos a serem elaborados neste MPR.

4. PROCEDIMENTOS REFERENCIADOS

Procedimentos referenciados são processos de trabalho publicados em outro MPR que têm relação com os processos de trabalho publicados por este manual. Este MPR não possui nenhum processo de trabalho referenciado.

5. PROCEDIMENTOS

Este capítulo apresenta todos os processos de trabalho deste MPR. Para encontrar um processo específico, utilize o índice nas páginas iniciais deste documento. Ao final de cada etapa encontram-se descritas as orientações necessárias à continuidade da execução do processo. O presente MPR também está disponível de forma mais conveniente em versão eletrônica, onde pode(m) ser obtido(s) o(s) artefato(s) e outras informações sobre o processo.

5.1 Mapear Riscos Relativos à STI

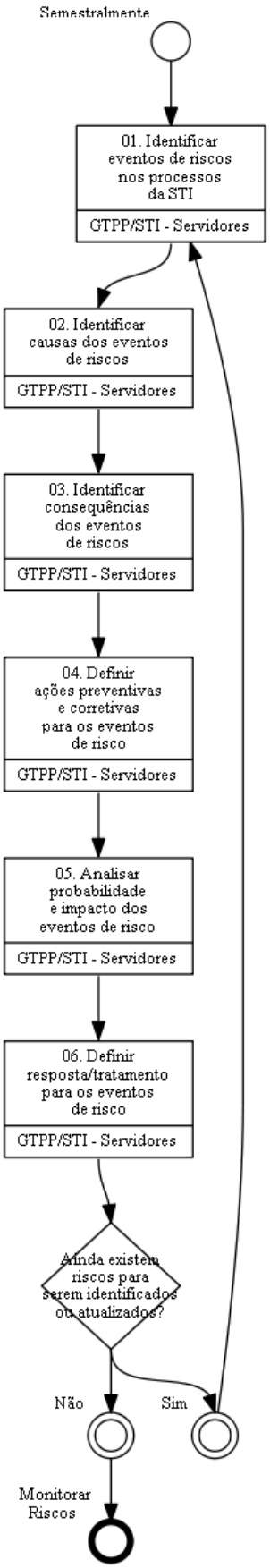
Mapeamento dos riscos inerentes às atividades da STI

O processo contém, ao todo, 6 etapas. A situação que inicia o processo, chamada de evento de início, foi descrita como: "Semestralmente", portanto, este processo deve ser executado sempre que este evento acontecer. Da mesma forma, o processo é considerado concluído quando alcança seu evento de fim. O evento de fim descrito para esse processo é: "Monitorar Riscos.

O grupo envolvido na execução deste processo é: GTPP/STI - Servidores.

Para que este processo seja executado de forma apropriada, é necessário que o(s) executor(es) possua(m) as seguintes competências: (1) Gerencia riscos de acordo com as melhores práticas; (2) Analisa documentos e artefatos da STI, levando em consideração a aprovação ou reprovação dos mesmos, seguindo as diretrizes da ANAC; (3) Avalia documento de serviço com base em ferramentas de análise de risco; (4) Implementa processos internos de gerenciamento de risco; (5) Demonstra, com antecedência, o risco do não cumprimento das metas intermediárias da Superintendência.

Abaixo se encontra(m) a(s) etapa(s) a ser(em) realizada(s) na execução deste processo e o diagrama do fluxo.


Semestralmente
01. Identificar eventos de riscos nos processos da STI
GTPP/STI - Servidores
02. Identificar causas dos eventos de riscos
GTPP/STI - Servidores
03. Identificar consequências dos eventos de riscos
GTPP/STI - Servidores
04. Definir ações preventivas e corretivas para os eventos de risco
GTPP/STI - Servidores
05. Analisar probabilidade e impacto dos eventos de risco
GTPP/STI - Servidores
06. Definir resposta/tratamento para os eventos de risco
GTPP/STI - Servidores
Ainda existem riscos para serem identificados ou atualizados?
Não
Sim
Monitorar Riscos

01. Identificar eventos de riscos nos processos da STI
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: Nesta etapa, utilizando a planilha fornecida pela SPI e os relatórios disponibilizados pela Auditoria, são identificados os eventos de riscos inerentes às atividades dos processos de trabalho da STI
COMPETÊNCIAS: - Analisa documentos e artefatos da STI, levando em consideração a aprovação ou reprovação dos mesmos, seguindo as diretrizes da ANAC.
SISTEMAS USADOS NESTA ATIVIDADE: GFT - Processos de Trabalho.
CONTINUIDADE: deve-se seguir para a etapa "02. Identificar causas dos eventos de riscos".

02. Identificar causas dos eventos de riscos
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: Identificados os riscos, a equipe que faz o acompanhamento dos riscos deve levantar as possíveis causa dos eventos de risco da forma mais completa e analítica possível.
COMPETÊNCIAS: - Avalia documento de serviço com base em ferramentas de análise de risco.
CONTINUIDADE: deve-se seguir para a etapa "03. Identificar consequências dos eventos de riscos".

03. Identificar consequências dos eventos de riscos
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: Uma vez identificados os riscos e seus eventos de causa, é necessários que sejam identificadas as consequências da materialização do risco. São analisados ativos, sistemas e grupos de usuários que podem ser afetados bem como o custo que isso pode trazer à Agência.
COMPETÊNCIAS: - Gerencia riscos de acordo com as melhores práticas.
CONTINUIDADE: deve-se seguir para a etapa "04. Definir ações preventivas e corretivas para os eventos de risco".

04. Definir ações preventivas e corretivas para os eventos de risco
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: esta etapa não possui detalhamento.
COMPETÊNCIAS: - Implementa processos internos de gerenciamento de risco.

CONTINUIDADE: deve-se seguir para a etapa "05. Analisar probabilidade e impacto dos eventos de risco".

05. Analisar probabilidade e impacto dos eventos de risco
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: esta etapa não possui detalhamento.
CONTINUIDADE: deve-se seguir para a etapa "06. Definir resposta/tratamento para os eventos de risco".

06. Definir resposta/tratamento para os eventos de risco
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: esta etapa não possui detalhamento.
COMPETÊNCIAS: - Demonstra, com antecedência, o risco do não cumprimento das metas intermediárias da Superintendência.
CONTINUIDADE: caso a resposta para a pergunta "Ainda existem riscos para serem identificados ou atualizados?" seja "sim", deve-se seguir para a etapa "01. Identificar eventos de riscos nos processos da STI". Caso a resposta seja "não", esta etapa finaliza o procedimento.

5.2 Monitorar Riscos de Tecnologia da Informação

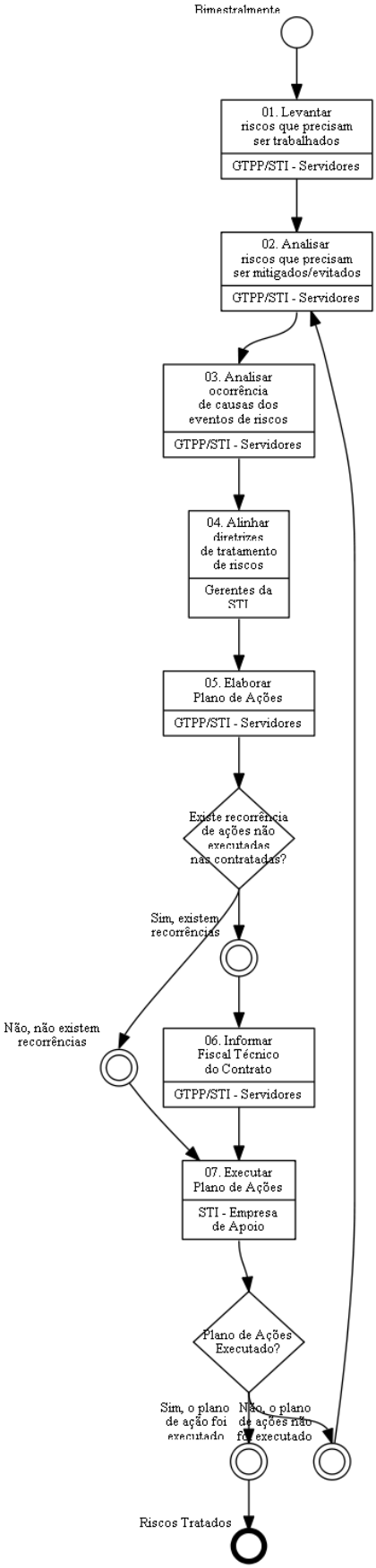
Monitoramento dos riscos relativos à tecnologia da informação

O processo contém, ao todo, 7 etapas. A situação que inicia o processo, chamada de evento de início, foi descrita como: "Bimestralmente", portanto, este processo deve ser executado sempre que este evento acontecer. Da mesma forma, o processo é considerado concluído quando alcança seu evento de fim. O evento de fim descrito para esse processo é: "Riscos Tratados.

A área envolvida na execução deste processo é a GTPP. Já os grupos envolvidos na execução deste processo são: Gerentes da STI, GTPP/STI - Servidores, STI - Empresa de Apoio.

Para que este processo seja executado de forma apropriada, é necessário que o(s) executor(es) possua(m) as seguintes competências: (1) Gerencia riscos de acordo com as melhores práticas; (2) Implementa processos internos de gerenciamento de risco.

Abaixo se encontra(m) a(s) etapa(s) a ser(em) realizada(s) na execução deste processo e o diagrama do fluxo.


Bimestralmente
01. Levantar riscos que precisam ser trabalhados
GTPP/STI - Servidores
02. Analisar riscos que precisam ser mitigados/evitados
GTPP/STI - Servidores
03. Analisar ocorrência de causas dos eventos de riscos
GTPP/STI - Servidores
04. Alinhar diretrizes de tratamento de riscos
Gerentes da STI
05. Elaborar Plano de Ações
GTPP/STI - Servidores
Existe recorrência de ações não executadas nas contratadas?
Sim, existem recorrências
Não, não existem recorrências
06. Informar Fiscal Técnico do Contrato
GTPP/STI - Servidores
07. Executar Plano de Ações
STI - Empresa de Apoio
Plano de Ações Executado?
Sim, o plano de ação foi executado
Não, o plano de ações não foi executado
Riscos Tratados

01. Levantar riscos que precisam ser trabalhados
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: Bimestralmente, é verificado quais riscos encontram-se mais próximos a curva de apetite a risco estipulada pelos gestores. São analisados também eventos que podem ter contribuído para o aumento do impacto ou da probabilidade de ocorrência de algum risco.
COMPETÊNCIAS: - Gerencia riscos de acordo com as melhores práticas.
CONTINUIDADE: deve-se seguir para a etapa "02. Analisar riscos que precisam ser mitigados/evitados".

02. Analisar riscos que precisam ser mitigados/evitados
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: Os riscos são analisados de forma criteriosa avaliando-se o contexto no qual a organização está inserida bem como o alcance de seus objetivos institucionais.
COMPETÊNCIAS: - Implementa processos internos de gerenciamento de risco.
CONTINUIDADE: deve-se seguir para a etapa "03. Analisar ocorrência de causas dos eventos de riscos".

03. Analisar ocorrência de causas dos eventos de riscos
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: É verificado se as causas para os eventos de risco estão se materializando bem como da sua evolução. Nesto momento, os servidores que estão acompanhando os riscos devem elaborar um relatório de diagnóstico dos riscos que será entregue aos gestores das áreas assim como ao Superintendente.
CONTINUIDADE: deve-se seguir para a etapa "04. Alinhar diretrizes de tratamento de riscos".

04. Alinhar diretrizes de tratamento de riscos
RESPONSÁVEL PELA EXECUÇÃO: Gerentes da STI.
DETALHAMENTO: De posse do Relatório de Diagnóstico dos Riscos, os gerentes funcionais alinharão as diretrizes que deverão ser tomadas para o tratamento dos riscos identificados. Será elaborada também uma proposta de plano de ação para que deverá ser entregue aos servidores que executam o gerenciamento do risco.
CONTINUIDADE: deve-se seguir para a etapa "05. Elaborar Plano de Ações".

05. Elaborar Plano de Ações
RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.

DETALHAMENTO: Com base nos insumos fornecidos pelos Gerentes funcionais, a equipe de acompanhamento de riscos elaborará um plano de ações contemplando o que deve ser feito para tratar e mitigar os riscos em destaque. É avaliado com atenção especial se os riscos em questão estão ligados à atividades executadas por empresa contratada para prestação de serviços.
CONTINUIDADE: caso a resposta para a pergunta "Existe recorrência de ações não executadas nas contratadas?" seja "sim, existem recorrências", deve-se seguir para a etapa "06. Informar Fiscal Técnico do Contrato". Caso a resposta seja "não, não existem recorrências", deve-se seguir para a etapa "07. Executar Plano de Ações".

06. Informar Fiscal Técnico do Contrato

RESPONSÁVEL PELA EXECUÇÃO: GTPP/STI - Servidores.
DETALHAMENTO: Caso o risco analisado seja reccorente em ações executadas pela contratada, o fiscal técnico é comunicado para que ele então oriente a contrata sobre quais ações devem ser tomadas para o tratamento ou mitigação do risco.
CONTINUIDADE: deve-se seguir para a etapa "07. Executar Plano de Ações".

07. Executar Plano de Ações

RESPONSÁVEL PELA EXECUÇÃO: STI - Empresa de Apoio.
DETALHAMENTO: esta etapa não possui detalhamento.
CONTINUIDADE: caso a resposta para a pergunta "Plano de Ações Executado?" seja "sim, o plano de ação foi executado", esta etapa finaliza o procedimento. Caso a resposta seja "não, o plano de ações não foi executado", deve-se seguir para a etapa "02. Analisar riscos que precisam ser mitigados/evitados".

6. DISPOSIÇÕES FINAIS

Em caso de identificação de erros e omissões neste manual pelo executor do processo, a STI deve ser contatada. Cópias eletrônicas deste manual, do fluxo e dos artefatos usados podem ser encontradas em sistema.