SEFAZ-RJ

Subsecretaria de Tecnologia da Informação e Comunicação

Processo de Gestão de Riscos de Segurança da Informação

Agosto de 2022

Secretaria de Fazenda

GOVERNO DO ESTADO RIO DE JANEIRO

SUBTIC SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Sumário

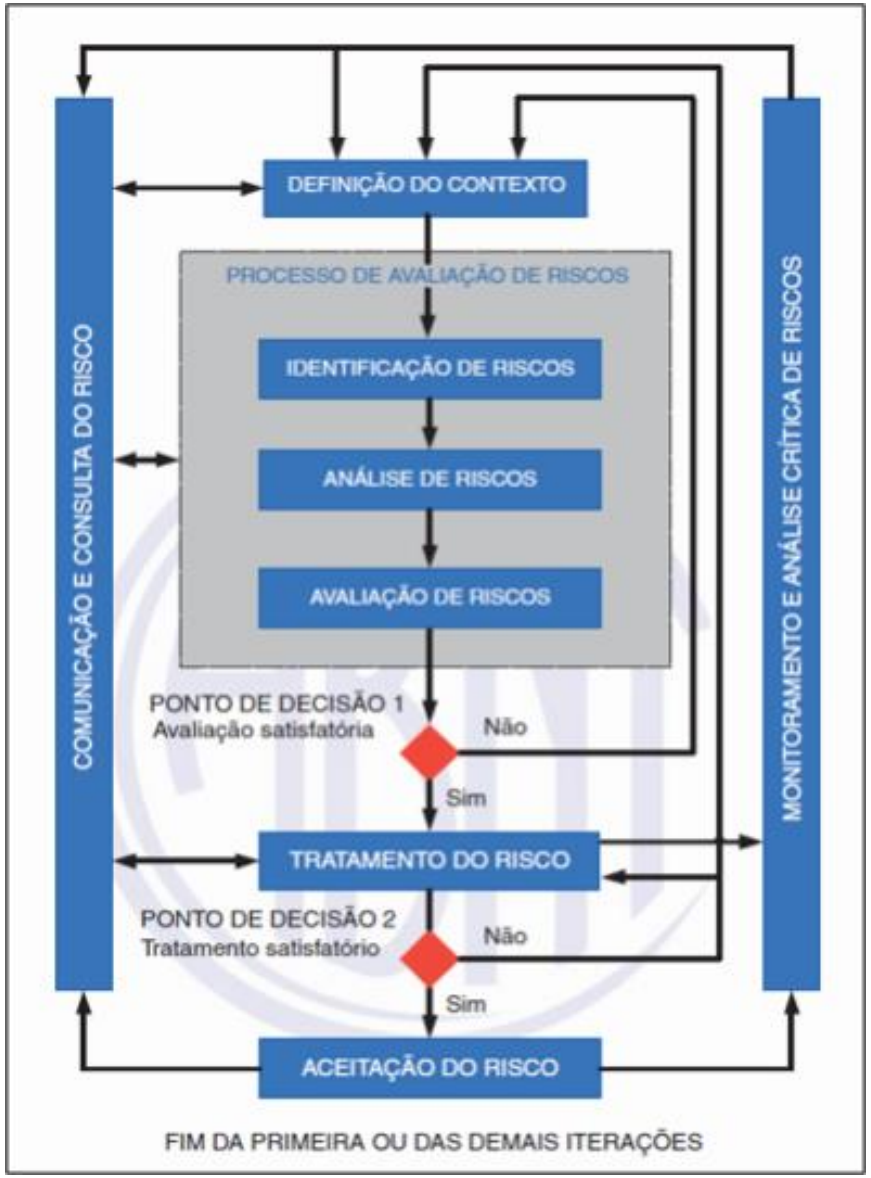
- Visão geral (fluxograma)
  - Contexto, análise e avaliação de riscos
  - Tratamento dos riscos e melhoria contínua
- Papéis e responsabilidades
- Documentos gerados
- Ferramentas
- Indicador de Processo
- Descrição das Atividades

Visão geral (fluxograma)

Gestão de Risco na ABNT NBR ISO/IEC 27005:2019

Um fluxograma geral de gestão de riscos de segurança da informação é previsto na ABNT NBR ISO/IEC 27005:2019, conforme ilustração ao lado.

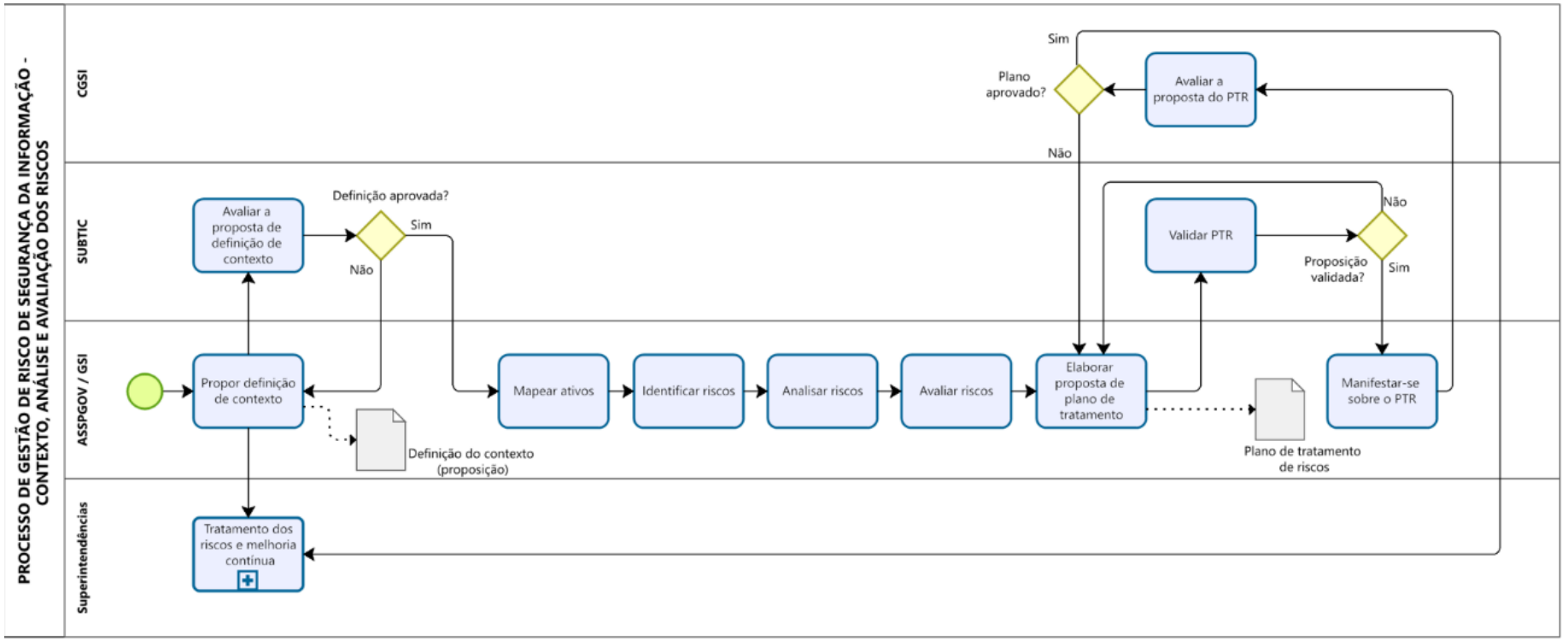
Este foi utilizado como base para elaboração do Processo de Gestão de Risco de Segurança da Informação (PGRSI) no âmbito da SEFAZ-RJ (contexto, análise, avaliação de riscos, tratamento dos riscos e melhoria contínua).



Visão geral (fluxograma)

Processo de Gestão de Risco de Segurança da Informação (PGRSI) no âmbito da SEFAZ-RJ

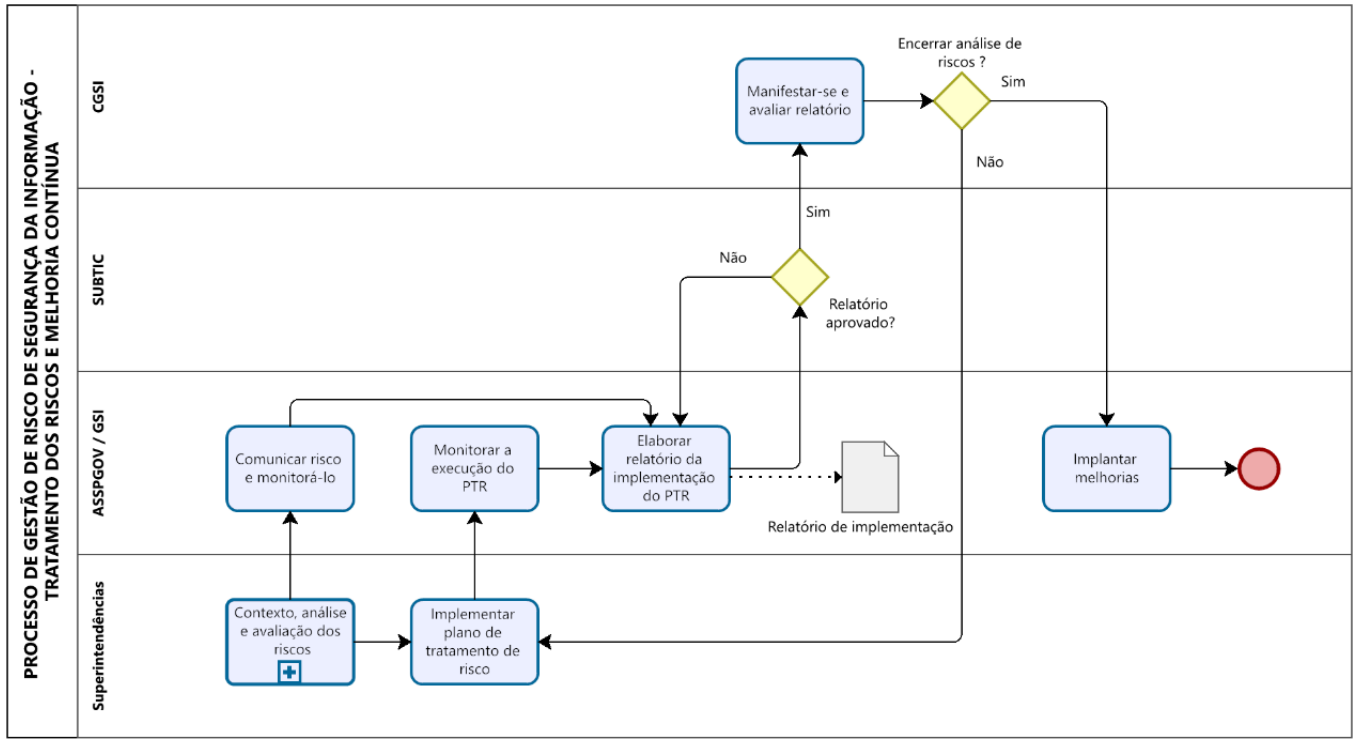
CONTEXTO, ANÁLISE E AVALIAÇÃO DE RISCOS



Visão geral (fluxograma)

Processo de Gestão de Risco de Segurança da Informação (PGRSI) no âmbito da SEFAZ-RJ

TRATAMENTO DOS RISCOS E MELHORIA CONTÍNUA



Papéis e responsabilidades

Papéis SEFAZ-RJ	Responsabilidades
Assessoria de Planejamento e Governança (ASSPGOV) / GSI (Gestor de Segurança da Informação)	Responsáveis pela gestão do processo e acompanhamento da execução das atividades relacionadas à gestão dos riscos de segurança da informação.
Subsecretaria de Tecnologia da Informação e Comunicação (SUBTIC)	Instância executiva máxima de Tecnologia da Informação e Comunicação (TIC) no âmbito da SEFAZ-RJ.
Superintendências de TIC	Áreas que gerenciam os sistemas, dados, serviços e infraestrutura de TIC, responsáveis pela implementação dos controles definidos no tratamento dos riscos.
Comitê de Governança de segurança da Informação (CGSI)	Responsável pela avaliação das proposições e documentos produzidos no processo de gestão de risco de segurança da informação, subsidiando a tomada de decisão pela Administração, bem como pela aprovação ou rejeição final de documentos e proposições referentes ao mapeamento, análise, avaliação e tratamento de riscos e às propostas de melhoria do processo.

Documentos gerados

Documentos	Responsável	Descrição do documento
Definição do escopo (contexto)	ASSPGOV / GSI	Definição da abrangência da análise a ser realizada (quais ativos, serviços e processos serão analisados).
Relatório de Análise e Plano de Tratamento de Riscos	ASSPGOV / GSI	Documento que detalha os riscos encontrados na análise. Elenca qual o tratamento a ser dado aos riscos identificados, com base em critérios previamente definidos (quais riscos deverão ser mitigados e quais deverão ser aceitos, com a respectiva justificativa).
Relatório de Melhorias (implementação)	ASSPGOV / GSI	Documento onde são descritas as melhorias para o processo, com vistas a aumentar a eficácia da Gestão de Riscos de Segurança da Informação.

Ferramentas

Sistemas na SEFAZ-RJ	Descrição
Excel / BIZAGI	Utilizados para gerenciar e executar a gestão de riscos.
SEI-RJ	Sistema de processo administrativo eletrônico.
SEI-RJ	Utilizado em deliberações do CGSI.

Indicador de processo

Descrição	Método de apuração / fórmula de cálculo	Frequência
Quantidade de análises em que o risco residual proposto foi alcançado (sucesso do plano de tratamento).	Quantidade de análises em que o risco residual proposto foi alcançado dividido pela quantidade de análises realizadas.	Anual

Descrição das Atividades

1	Propor definição de contexto	
Descrição	Compreende a proposição dos objetivos, escopo e limites da avaliação de riscos a ser realizada, com a identificação das partes interessadas e observada a Política de Segurança da Informação. As exclusões do escopo devem também ser definidas e justificadas.	
Considerações importantes	A proposta de definição de contexto é elaborada pela Assessoria de Planejamento e Governança em conjunto com o Gestor de Segurança da Informação. O documento é encaminhado para avaliação do Subsecretário de Tecnologia da informação e Comunicação (autoridade máxima de TIC).	
Papéis	Assessoria de Planejamento e Governança / GSI.	
Entradas	Plano Estratégico e Diretor de Tecnologia da Informação e Comunicação (PEDTIC), PGRSI anterior, dentre outros.	
Saídas	Definição do contexto da Gestão de Riscos (GR) (proposição).	
Atividades	Definir Contexto	Identificar o propósito da avaliação de riscos a ser realizada. Esta definição guiará a definição do escopo (p. ex. suportar o PGRSI, conformidade legal, requisitos de segurança para uma solução de TIC). Descrever o escopo (que pode abranger a SEFAZ-RJ como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação) e limites da avaliação de risco a ser realizada, bem como listar as partes interessadas na análise de riscos.
	Formalizar a proposta (criação do SEI-RJ)	No caso do escopo da GR estar vinculado ao PGRSI, ele constará no SEI do respectivo PGRSI. No entanto, se for uma análise de risco pontual, poderá ser criado um expediente específico para formalizá-lo.
	Encaminhar à autoridade máxima de TIC	ASSPGOV/GSI remete o documento para avaliação da SUBTIC, que poderá solicitar ajustes ou validá-lo para posterior submissão à consideração superior.

Descrição das Atividades

2	Avaliar a proposta de definição de contexto	
Descrição	A autoridade máxima de TIC avalia o contexto proposto para a análise de riscos a ser executada, podendo aprová-lo ou não. Em caso de não-aprovação, encaminha para as correções necessárias.	
Considerações importantes	A manifestação da autoridade máxima de TIC deve ser formalizada dentro do SEI respectivo.	
Papéis	Subsecretário de Tecnologia da informação e Comunicação	
Entradas	Proposta de definição de contexto.	
Saídas	Decisão aprovando a definição de contexto ou propondo correções/ajustes.	
Atividades	Avaliar a proposta	Análise do contexto proposto, com base nas informações contidas no documento proposto por ASSPGOV/GSI.
	Aprovar proposta	Aprovar o documento.
	Solicitar ajustes	Não aprova o documento e informa o ASSPGOV/GSI para realização dos ajustes indicados.

Descrição das Atividades

3	Mapear ativos	
Descrição	Atividade que consiste em elencar os ativos que compõem o escopo, suas características, relacionamentos com sistemas, processos de negócio, responsáveis, tecnologias envolvidas, questionários de riscos a serem distribuídos, etc.	
Considerações importantes	O correto mapeamento dos ativos resulta em uma análise de riscos mais acurada.	
Papéis	Assessoria de Planejamento e Governança / GSI	
Entradas	Tabela/lista de ativos, serviços, sistemas das Superintendências de TIC, escopo da análise de riscos.	
Saídas	Atividade que consiste em elencar os ativos que compõem o escopo, suas características, relacionamentos com sistemas, processos de negócio, responsáveis, tecnologias envolvidas, questionários de riscos a serem distribuídos, etc.	
Atividades	Levantamento dos ativos	Verificar quais ativos que suportam o escopo e quem é o responsável.
	Relacionar ativos com sistemas e serviços	Relacionar os ativos com os sistemas e serviços tecnológicos.
	Vincular questionários tecnológicos	Para cada ativo, vincular questionário de riscos para cada tecnologia suportada pelo ativo.

Descrição das Atividades

4	Identificar riscos	
Descrição	Atividade que consiste na identificação de ameaças, vulnerabilidades e dos controles de Segurança da Informação e Comunicação (SIC) já implementados, relacionados aos ativos mapeados. Na ferramenta de análise de risco, os questionários utilizados identificam os controles, ameaças e vulnerabilidades envolvidos na análise, a partir da base de conhecimento.	
Considerações importantes	Poderão ser utilizados outros meios para identificar os riscos, tais como resultados análises de vulnerabilidades, entrevistas com gestores de ativos, processos, etc.	
Papéis	Assessoria de Planejamento e Governança / GSI	
Entradas	Mapeamento dos ativos	
Saídas	Encerramento da coleta de informações	
Atividades	Coleta das informações	Os questionários são distribuídos às áreas responsáveis pelos ativos, com prazo determinado para resposta. O Assessoria de Planejamento e Governança e o Gestor de Segurança da Informação monitoram e acompanham o preenchimento.
	Identificação dos riscos	Os questionários devem ser encerrados na ferramenta de análise de riscos para que os resultados sejam compilados.

Descrição das Atividades

5	Analisar riscos	
Descrição	Nessa atividade, são informados os valores para probabilidade, impacto e nível de risco de cada risco para o escopo analisado.	
Considerações importantes	Não Aplicável	
Papéis	Assessoria de Planejamento e Governança / GSI	
Entradas	Identificação dos riscos	
Saídas	Relatório de análise de riscos	
Atividades	Valores do probabilidade, impacto e nível de risco	Verificar necessidade de alteração dos valores na ferramenta de análise de riscos.
	Analisar resultados	Gerar relatório na ferramenta e analisar os resultados da análise de riscos realizada.

Descrição das Atividades

6	Avaliar riscos	
Descrição	Atividade que consiste na avaliação e proposição de tratamento para os riscos identificados, observando-se as diretrizes definidas pelo CGSI. Ao final, é elaborado o relatório de análise de riscos.	
Considerações importantes	Não Aplicável	
Papéis	Assessoria de Planejamento e Governança / GSI	
Entradas	Análise dos riscos	
Saídas	Relatório de avaliação de riscos	
Atividades	Avaliar riscos	Avaliar os riscos a partir da classificação resultante da análise de riscos e das características dos processos de negócio e ativos envolvidos, bem como escopo definido.
	Definição dos critérios para a proposição de tratamento dos riscos	Definir os critérios que irão nortear a proposta de Plano de Tratamento dos Riscos (PTR). Devem ser consideradas as restrições organizacionais, estruturais e tecnológicas, os requisitos normativos e/ou legais, os controles de segurança existentes e a análise custo/benefício.
	Elaborar relatório	Redigir um relatório de Análise e Avaliação de Riscos.

Descrição das Atividades

7	Elaborar proposta de Plano de Tratamento de Riscos	
Descrição	Atividade que compreende a elaboração de plano visando o tratamento dos riscos e a implantação de controles, dos responsáveis por sua implementação e prazos estabelecidos.	
Considerações importantes	O PTR deve ser validado e pelo Comitê de Governança de Segurança da Informação.	
Papéis	Assessoria de Planejamento e Governança / GSI	
Entradas	Relatórios de Análise e de Avaliação de Riscos	
Saídas	Proposta de Plano de Tratamento de Riscos	
Atividades	Elaborar PTR	Na ferramenta de análise de riscos devem ser identificados, para cada risco levantado, a estratégia de tratamento (aceitar, evitar, mitigar ou transferir) e ser informada a forma de implementação, o responsável e o prazo de execução. No caso de aceitação, deve ser indicada a justificativa. O documento, a ser submetido à consideração superior, é resultado da exportação dos dados da ferramenta utilizada para formato que permita sua inclusão no expediente respectivo.

Descrição das Atividades

8	Validar o Plano de Tratamento de Riscos	
Descrição	A autoridade máxima de TIC valida, ou não, o Plano de Tratamento de Riscos.	
Considerações importantes	Não Aplicável	
Papéis	Subsecretário de Tecnologia da informação e Comunicação	
Entradas	Plano de Tratamento de Riscos	
Saídas	Decisão aprovando o PTR ou propondo correções/ajustes.	
Atividades	Avaliar PTR	Análise do PTR, com base nas informações contidas no documento proposto por ASSPGOV/GSI.
	Aprovar proposta	Aprovar o documento.
	Solicitar ajustes	Não aprova o documento e informa o ASSPGOV/GSI para realização dos ajustes indicados.

Descrição das Atividades

9	Manifestar-se sobre a proposta de Plano de Tratamento de Riscos	
Descrição	Tecer comentários acerca do PTR.	
Considerações importantes	O GSI assessora a CGSI nas questões relacionadas à Segurança da Informação. Portanto, as observações que julgar necessárias servirão para subsidiar a CGSI na tomada de decisão em relação ao PTR.	
Papéis	ASSPGOV/GSI	
Entradas	Proposta de Plano de Tratamento de Riscos	
Saídas	Considerações acerca do PTR	
Atividades	Opinar sobre a proposição	Manifestação sobre a proposta de PTR, sugerindo à CGSI sua aprovação ou alterações que entender necessárias.

Descrição das Atividades

10	Avaliar proposta de Plano de Tratamento de Riscos	
Descrição	Atividade que compreende a ciência sobre os resultados da análise e avaliação de riscos e a apreciação da proposta do Plano de Tratamento de Riscos.	
Considerações importantes	A proposta de PTR encaminhada por ASSPGOV/GSI deve ser aprovada pelo CGSI pois a implementação de controles pode representar a utilização de recursos financeiros, humanos e tecnológicos, influenciando na execução de outros projetos estratégicos já planejados para o período.	
Papéis	Comitê de Governança de Segurança da Informação	
Entradas	Proposta de PTR (feitas por ASSPGOV/GSI)	
Saídas	Decisão aprovando a proposta de PTR ou determinando correções/ajustes.	
Atividades	Avaliar a proposição encaminhada	Considerando as manifestações de ASSPGOV/GSI, analisar os resultados da análise e avaliação de riscos realizada e o Plano de Tratamento de Riscos proposto, em especial no que diz respeito aos critérios de aceitação de riscos.
	Aprovar a proposta	Aprovado o PTR, inicia-se a implementação dos controles.
	Solicitar ajustes	Não aprovar o documento, mediante despacho, e devolver o expediente para ajustes.

Descrição das Atividades

11	Implementar Plano de Tratamento de Riscos	
Descrição	Nessa atividade, as Superintendências de TIC implementam os controles para mitigar os riscos elencados, dentro de um prazo definido no PTR.	
Considerações importantes	É importante que a implementação dos controles seja realizada de acordo com o PTR, dentro dos prazos e utilizando os recursos previstos.	
Papéis	Superintendências de TIC	
Entradas	Plano de Tratamento de Riscos	
Saídas	Controles implementados	
Atividades	Delegar as atividades de implementação dos controles	A implementação dos controles deverá ser delegada de acordo com as responsabilidades estabelecidas no PTR.
	Gerenciar implementação	Cada área deverá planejar e promover a execução das ações, conforme prazo e forma ajustados.
	Registrar a execução das ações	Na ferramenta de análise de riscos deve ser registrada a execução das atividades, o que permitirá o acompanhamento da implementação do PTR.

Descrição das Atividades

12	Monitorar a execução do Plano de Tratamento de Riscos	
Descrição	Esta fase tem por objetivo monitorar a execução do PTR, com a finalidade de assegurar sua implementação dentro dos prazos definidos.	
Considerações importantes	Não aplicável	
Papéis	Assessoria de Planejamento e Governança / GSI	
Entradas	Plano de Tratamento de Riscos	
Saídas	Implementação do Plano	
Atividades	Monitorar PTR	ASSPGOV/GSI são responsáveis por acompanhar o andamento das ações delegadas às equipes técnicas, a fim de aferir sua correspondência com a atividade definida no PTR, bem como o cumprimento dos prazos ali estabelecidos.
	Sugerir ações de correção	Caso detectado que os prazos não estão sendo cumpridos ou que ações não estão sendo executadas conforme planejado, cabe a ASSPGOV/GSI sugerir ações de correção.

Descrição das Atividades

13	Comunicar risco e monitorá-lo	
Descrição	Nesta atividade, ASSPGOV/GSI comunicam o risco às partes interessadas e efetuam o monitoramento dos riscos já avaliados, a fim de evitar que eles se concretizem.	
Considerações importantes	O monitoramento dos riscos é importante pois eles podem ser alterados em função de mudanças no ambiente externo e interno, podendo ser necessária a implementação de medidas para tratá-los.	
Papéis	Assessoria de Planejamento e Governança / GSI	
Entradas	Relatório de análise de riscos, monitoramento do ambiente	
Saídas	Comunicação do risco e suas alterações	
Atividades	Comunicação dos riscos	Informar às partes interessadas o nível de risco analisado e avaliado e possíveis alterações.
	Monitoramento de riscos	Analisar e monitorar os riscos já avaliados para verificar se alguma ocorrência pode ter modificado os níveis de risco, ensejando alguma ação para controlá-los.

Descrição das Atividades

14	Elaborar relatório de implementação do PTR	
Descrição	Atividade que compreende a elaboração de relatório com as informações e resultados da execução do Plano de Tratamento de Riscos, bem como propostas de melhorias para o próximo ciclo. O relatório é apresentado à autoridade máxima de TIC. Se aprovado, é então encaminhado ao Comitê de Governança de Segurança da Informação para manifestação. Caso contrário, é encaminhado para readequação.	
Considerações importantes	A área técnica elabora proposição de documento de análise crítica, abordando aspectos técnicos, que deve ser validado pela alta administração, agregando os aspectos organizacionais e estratégicos.	
Papéis	Assessoria de Planejamento e Governança / GSI	
Entradas	Monitoramento do PTR	
Saídas	Relatório de implementação do PTR e sugestões de melhoria	
Atividades	Elaborar relatório	Redigir o documento com as informações e resultados da execução do PTR, bem como propostas de melhorias.
	Encaminhar para avaliação	Encaminhar relatório para avaliação do SUBTIC e, após, à consideração superior. O CGSI poderá devolver o relatório para ajustes.

Descrição das Atividades

15	Manifestar-se sobre o relatório	
Descrição	ASSPGOV/GSI se manifestam sobre o relatório apresentado, já validado pelo SUBTIC.	
Considerações importantes	ASSPGOV/GSI tecem observações sobre o documento.	
Papéis	ASSPGOV/GSI	
Entradas	Relatório de implementação do PTR e manifestações da ASSPGOV/GSI	
Saídas	Manifestações acerca do documento	
Atividades	Manifestar-se sobre o relatório	Manifestação sobre os resultados apresentados e a proposta de melhorias, a fim de auxiliar a CGSI na tomada de decisão.

Descrição das Atividades

16	Avaliar relatório	
Descrição	Atividade que compreende a ciência e avaliação dos resultados do PTR e das propostas apresentadas para melhoria da Gestão de Riscos, bem como a realização da Análise Crítica sobre a análise de riscos como um todo.	
Considerações importantes	Não aplicável	
Papéis	Comitê de Governança de Segurança da Informação	
Entradas	Relatório de proposta de melhoria, manifestações do Comitê de Governança de Segurança da Informação	
Saídas	Aprovação do relatório de implementação do PTR	
Atividades	Avaliação dos relatórios	Avaliação dos resultados do PTR e das propostas apresentadas para melhoria da Gestão de Riscos.

Descrição das Atividades

17	Implantar melhorias	
Descrição	Nesta atividade, as melhorias propostas e aprovadas são implementadas ou planejadas para o próximo ciclo, com vistas a aumentar a eficácia do PGRSI.	
Considerações importantes	Não aplicável	
Papéis	Assessoria de Planejamento e Governança / GSI	
Entradas	Relatório de melhorias aprovado	
Saídas	Implementação das melhorias	
Atividades	Implementar melhorias	Realizar ou planejar as ações aprovadas para o próximo ciclo.