PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO GP/TRT19 N.º 22, DE 22 DE MARÇO DE 2022

Revisa o Processo de Gestão de Riscos de TIC, no âmbito do Tribunal Regional do Trabalho da 19ª Região.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA NONA REGIÃO, no uso de suas atribuições legais e regimentais estabelecidas no inciso VII do artigo 24 do Regimento Interno e tendo em vista o contido no PROAD n.º 313, de 20/1/2022,

CONSIDERANDO a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), instituída pela Resolução CNJ n.º 370, de 28 de janeiro de 2021;

CONSIDERANDO a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída pela Resolução CNJ n.º 396, de 7 de junho de 2021;

CONSIDERANDO a Resolução n.º 104, de 5 de outubro de 2016, que institui a Política de Gestão de Riscos e de Controles Internos do Tribunal Regional do Trabalho da 19ª Região;

CONSIDERANDO a necessidade de orientar a condução da Política de Segurança da Informação (PSI) em vigor no TRT da 19ª Região, visando garantir e incrementar a segurança da informação e das comunicações;

CONSIDERANDO a Resolução n.º 166, de 8 de maio de 2019, que dispõe sobre a Política de Governança de Tecnologia da Informação e Comunicação do TRT da 19ª Região; e

CONSIDERANDO as boas práticas de Governança de TIC que visam garantir a disponibilidade e integridade dos sistemas, aplicativos, dados e de documentos digitais do TRT da 19ª Região,

RESOLVE:

Art. 1º **Revisar** o Processo de Gestão de Riscos de Tecnologia da Informação e Comunicação (PGR-TIC) do Tribunal Regional do Trabalho da 19ª Região, instituído pelo Ato n.º 83/GP/TRT 19ª, de 08 de agosto de 2019.

Art. 2º O processo de gestão de riscos de TIC deverá observar como metodologia o Plano de Gerenciamento de Riscos do TRT19 (PGR-TRT), instituído pelo Ato TRT 19ª GP n.º 86, de 5 de outubro de 2017, e as disposições da Resolução Administrativa n.º 104, de 5de outubro de 2016, que institui a Política de Gestão de Riscos e de Controles Internos do TRT19.

Art. 3º Para os fins deste Ato, entende-se como:

ATO GP/TRT19 N.º 22, DE 22 DE MARÇO DE 2022

I - Tecnologia da Informação e Comunicação (TIC): ativo estratégico que suporta processos institucionais por meio da conjugação de recursos, processos de trabalho e técnicas que são utilizadas para obter, processar, armazenar, fazer uso e disseminar informações.

II - Gestão de riscos: conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos, contribuindo para a redução da materialização de eventos que impactem negativamente seus objetivos;

III - Gestão de riscos de Tecnologia da Informação e Comunicações (TIC): gestão de riscos aplicada ao escopo de TIC.

Art. 4º O processo definido visa a atingir os seguintes objetivos:

I – Definir um processo sistemático para gerenciar riscos referentes à Segurança da Informação e Comunicações (SIC), projetos e processos de TIC, provendo insumos para aumentar a proteção contra eventos indesejados;

II – Direcionar os esforços e investimentos financeiros, tecnológicos e humanos para sustentar a adequada gestão de riscos de TIC;

III – Estar em conformidade com normatizações e regulamentações relacionadas ao assunto.

Art. 5º O Processo de Gestão de Riscos de TIC observará o disposto no Manual do Processo de Gestão de Riscos de TIC, anexo a este Ato e dele parte integrante.

Art. 6º O Manual do Processo de Gestão de Riscos de TIC, com o fluxograma e a descrição do processo estará disponível no Portal da Governança de TIC, no sítio eletrônico do Tribunal Regional do Trabalho da 19ª Região.

Art. 7º O Processo estabelecido neste Ato será revisto sempre que alterados os procedimentos de Gestão de Riscos de TIC.

Art. 8º Este Ato entra em vigor na data de sua publicação.

Publique-se no D.E.J.T e no B.I.

Original assinado
JOSÉ MARCELO VIEIRA DE ARAÚJO
Desembargador-Presidente

Publicado no B.I. n.º 3 e no D.E.J., de 23/3/2022.

MANOEL MESSIAS FEITOZA

Tribunal Regional do Trabalho
19ª Região | Alagoas

Manual de Processo

Processo de Gestão de Riscos de TIC

Versão do documento: 1.0
Dezembro de 2021

Sumário

Objetivo 3
Propósito do processo 3
Escopo 3
Definições e abreviações 3
Benefícios esperados 4
Regras Gerais 4
Papéis e Responsabilidades 4
Indicadores de Desempenho 5
Controles de execução do processo 5
Fluxograma 5
Descrição das Tarefas 6

Objetivo

Estabelecer as diretrizes da gestão de riscos relacionada à segurança da informação, ao ambiente tecnológico, aos projetos e aos processos de Tecnologia da Informação e Comunicações (TIC), e definir o processo de Gerenciamento de Riscos de TIC do TRT da 19ª Região.

Propósito

Este processo tem como propósito definir a gestão de riscos de TIC no âmbito do TRT da 19ª Região, garantindo que os riscos sejam conhecidos, monitorados e tratados, promovendo a manutenção de um nível de risco aceitável.

Escopo

Este processo é aplicável a todas as unidades pertencentes à Secretaria de Tecnologia da Informação e Comunicações, responsáveis por gerenciar, manipular e operar informações, projetos, processos, produtos e serviços relacionados à área de TIC no âmbito do TRT 19ª Região.

Definições e abreviações

Para efeitos deste manual, aplicam-se as definições da Política de Segurança da Informação e Comunicações, além das seguintes:

- Risco: fator ou evento incerto que pode causar impactos negativos, dificultando ou impossibilitando o cumprimento dos objetivos; ou positivos, com potencial de agregar valores;
- Risco de Segurança da Informação: probabilidade de impacto negativo nos objetivos da organização caso as suas informações não estejam protegidas adequadamente;
- Controle: qualquer medida que visa minimizar um risco ou grupo de riscos;
- Nível ou índice de risco: magnitude de um risco ou combinação de riscos;
- Identificação de riscos: etapa da gestão de riscos que visa localizar, listar e caracterizar os riscos;
- Análise de riscos: etapa da gestão de riscos que visa compreender a natureza dos riscos e determinar o nível de risco. A análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos. A análise de riscos inclui a estimativa de riscos;
- Avaliação de riscos: etapa da gestão de riscos onde são definidos quais os riscos identificados na análise serão aceitos ou tratados, bem como priorizar o

tratamento dos mesmos;

- Tratamento de riscos: etapa da gestão de riscos onde são implementadas ações e controles visando reduzir o nível de risco para um patamar aceitável;

- Plano de Tratamento de Riscos (PTR): descreve as ações de tratamento de riscos, identificando os responsáveis, com o objetivo de reduzir os riscos a níveis aceitáveis.

Benefícios esperados

A implementação do Processo de Gestão de Riscos de TIC no TRT da 19ª Região promoverá os seguintes benefícios:

- Manutenção de níveis aceitáveis de riscos de TIC;

- Aderência à Política de Segurança da Informação e Comunicações (PSI) da instituição, promovendo a confidencialidade, disponibilidade e integridade das informações.

Papéis e Responsabilidades

Papel	Descrição	Responsabilidades
Comitê de Governança de Tecnologia da Informação e Comunicação	Comitê multidisciplinar , formado por representantes de todas as áreas estratégicas do órgão e pelo titular da área de Tecnologia da Informação e Comunicação	• Responsável pela avaliação das proposições e documentos produzidos no processo de gestão de risco, subsidiando a tomada de decisão pela Administração.
Comitê Gestor de Segurança da Informação	Comitê multidisciplinar formado por magistrados e servidores, de assessoramento da Administração na área de Segurança da Informação.	• Responsável pela avaliação das proposições e documentos produzidos no processo de gestão de risco, referente à segurança da informação.

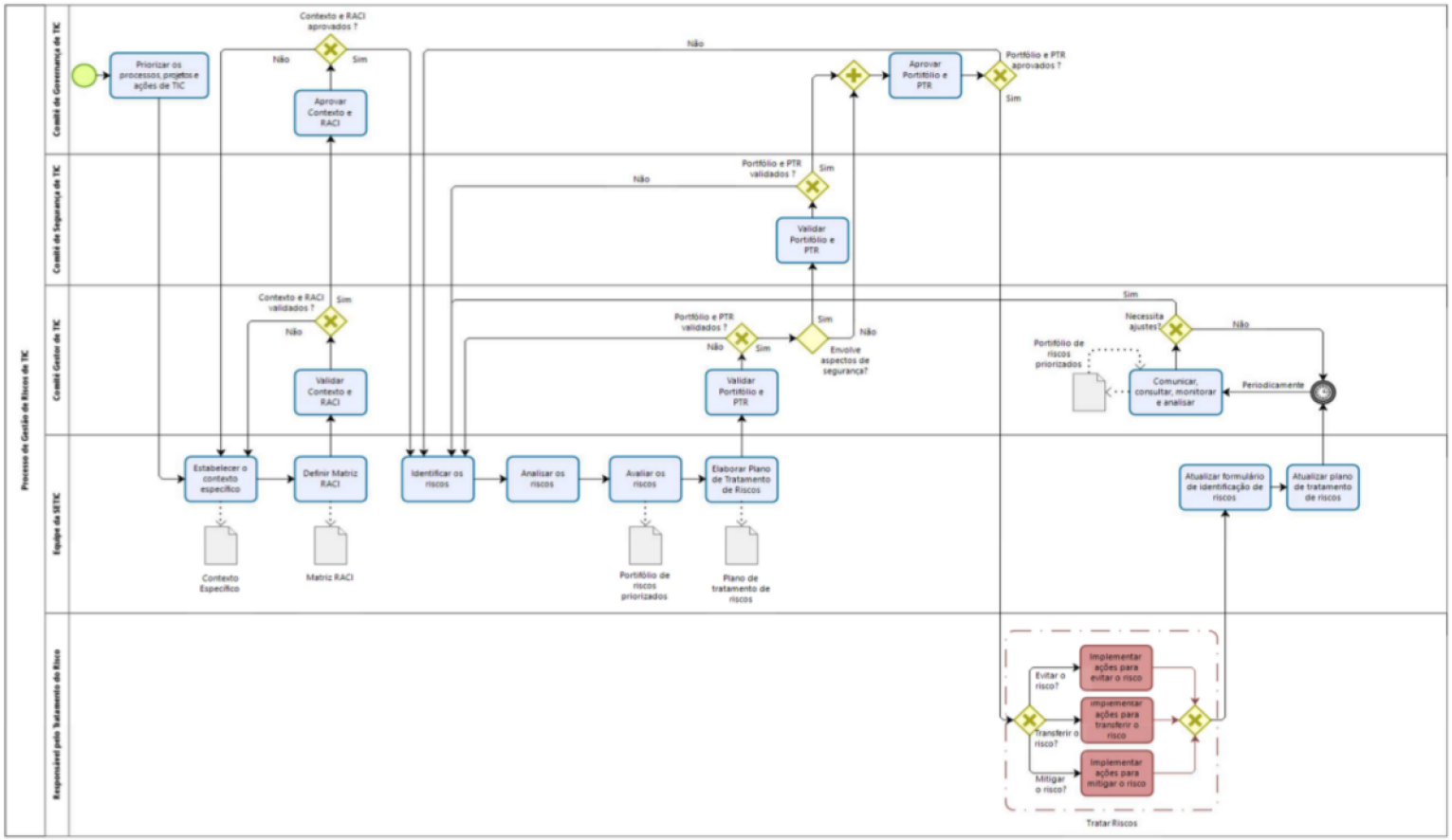
Comitê Gestor de TIC	Comitê formado por todos os gestores da SETIC	• Comitê interno da SETIC, responsável pela aprovação em primeiro nível de documentos gerados no processo e acompanhamento da execução das atividades relacionadas à gestão dos riscos de TIC.
Equipe da SETIC	Envolve os setores aos quais os riscos estão associados	• Responsável pela implementação do processo.
Responsável pelo Tratamento do Risco	Representante das áreas que gerenciam os sistemas, serviços e infraestrutura de TIC	• Responsável pela implementação dos controles definidos no tratamento dos riscos.

Indicadores de Desempenho

Os indicadores descritos a seguir irão avaliar o desempenho da central de serviços.

Descrição do Indicador	Método de apuração / fórmula de cálculo	Frequência
Percentual de Risco de TIC após o tratamento dos risos	(quantidade de riscos residuais/ quantidate total de riscos identificados) x 100	anual

Fluxograma


Processo de Gestão de Riscos de TIC
Comitê de Governança de TIC
Comitê de Segurança de TIC
Comitê Gestor de TIC
Equipe da SETIC
Responsável pelo Tratamento do Risco
Priorizar os processos, projetos e ações de TIC
Contexto e RACI aprovados ?
Não
Sim
Aprovar Contexto e RACI
Não
Aprovar Portifólio e PTR
Portfólio e PTR aprovados ?
Sim
Portfólio e PTR validados ?
Sim
Não
Validar Portifólio e PTR
Contexto e RACI validados ?
Sim
Não
Validar Contexto e RACI
Portfólio e PTR validados ?
Não
Sim
Sim
Não
Envolve aspectos de segurança?
Validar Portifólio e PTR
Sim
Necessita ajustes?
Não
Portifólio de riscos priorizados
Comunicar, consultar, monitorar e analisar
Periodicamente
Estabelecer o contexto específico
Definir Matriz RACI
Identificar os riscos
Analisar os riscos
Avaliar os riscos
Elaborar Plano de Tratamento de Riscos
Atualizar formulário de identificação de riscos
Atualizar plano de tratamento de riscos
Contexto Específico
Matriz RACI
Portifólio de riscos priorizados
Plano de tratamento de riscos
Evitar o risco?
Implementar ações para evitar o risco
Transferir o risco?
Implementar ações para transferir o risco
Mitigar o risco?
Implementar ações para mitigar o risco
Tratar Riscos

Descrição das Tarefas

Priorizar os processos, projetos e ações de TIC		
Descrição	Priorizar os processos de trabalho, projetos e ações de TIC que devem ter os riscos gerenciados e tratados com prioridade, em face da dimensão dos prejuízos que possam causar	
Papéis	Comitê de Governança de TIC	
Considerações importantes	Pode-se levar em consideração os seguintes critérios de escolha: I – alinhamento com a ENTIC-JUD ou ENSEC; II – impacto em caso de incidentes; III – complexidade do processo de trabalho alvo.	
Entradas	Rol de processos, projetos de ações que precisam ter os riscos gerenciados	
Saídas	Processos, projetos e ações priorizados	
Atividades	Priorizar	Priorizar os processos, projetos e ações de TIC
Ferramentas		

Estabelecer o contexto específico	
Descrição	Observar o contexto geral definido na Política de Gestão de Riscos do TRT 19ª Região (PGR-TRT) e ajustar, quando necessário: I – os fatores internos e externos, adicionando ou excluindo as categorias de eventos que não se aplicam ao processo de trabalho; II – os critérios de riscos, avaliando e redefinindo de acordo com as necessidades específicas, âmbito e escopo de atuação; III – a escala de probabilidade, redefinindo o número de ocorrências para cada descritor; IV – a escala de impacto, redefinindo o custo e o prazo e;

	V – a matriz de classificação de riscos.	
Papéis	Equipe da SETIC	
Considerações importantes	O contexto específico deve estabelecer os objetivos, escopo e limites da avaliação de riscos a ser realizada com a identificação das partes interessadas. As exclusões do escopo devem também ser definidas e justificadas.	
Entradas	Processos, pojetos e ações de TIC priorizados e PGR-TRT	
Saídas	Definição do contexto específico	
Atividades	Definir contexto específico	Identificar o propósito da avaliação de riscos a ser realizada.
Ferramentas		

Definir Matriz RACI		
Descrição	As responsabilidades específicas para cada atividade da gestão de riscos serão distribuídas em uma matriz RACI (Responsável, Responsabilizado,Consultado, Informado).	
Papéis	Equipe da SETIC	
Considerações importantes	A definição de contexto e a matriz RACI (Responsável, Aprovador, Consultado, Informado) são elaboradas pela equipe da SETIC, validadas pelo Comitê Gestor de TIC - CGESTIC e aprovadas pelo Comitê de Governança de TIC - CGTIC.	
Entradas	Contexto Específico	
Saídas	Matriz RACI	
Atividades	Definir matriz RACI	Incluir as responsabilidades específicas na matriz RACI
Ferramentas		

Validar Contexto e RACI

Descrição	Validar o Contexto e a Matriz RACI	
Papéis	Comitê Gestor de TIC	
Considerações importantes	O contexto e a matriz RACI são validados pelo Comitê Gestor de TIC - CGESTIC.	
Entradas	Contexto Específico e Matriz RACI	
Saídas	Contexto Específico e Matriz RACI validados e/ou aprovados	
Atividades	Validar matriz RACI	Validar a Matriz RACI elaborada pela Equipe de TIC
	Validar Contexto	Validar o Contexto elaborado pela Equipe de TIC
Ferramentas		

Aprovar Contexto e RACI		
Descrição	Aprovar o Contexto e a Matriz RACI	
Papéis	Comitê de Governança de TIC	
Considerações importantes	O contexto e a matriz RACI são aprovadas pelo Comitê de Governança de TIC - CGTIC.	
Entradas	Contexto Específico e Matriz RACI	
Saídas	Contexto Específico e Matriz RACI validados e/ou aprovados	
Atividades	Aprovar matriz RACI	Aprovar a Matriz RACI elaborada pela Equipe de TIC
	Aprovar Contexto	Aprovar o Contexto elaborado pela Equipe de TIC
Ferramentas		

Identificar os riscos

Descrição	A identificação dos riscos tem como propósito conhecer quais riscos podem influenciar o cumprimento dos objetivos da Instituição.	
Papéis	Equipe da SETIC	
Considerações importantes	Para auxiliar a identificação de riscos, podem ser utilizadas técnicas e ferramentas como brainstorming, questionários, entrevistas, checklist, análise SWOT (forças, fraquezas, oportunidades e ameaças), análise de dados históricos, análise de premissas, opiniões especializadas, necessidades das partes interessadas e diagramas de causa e efeito.	
Entradas	Modelo de Planilha de identificação de riscos	
Saídas	Encerramento da coleta de informações	
Atividades	Coleta das informações	As planilhas são distribuídos às áreas responsáveis, com prazo determinado para resposta.
	Identificação dos riscos	Compilar as planilhas
Ferramentas	Planilha de Identificação de Riscos	

Analisar os riscos		
Descrição	A análise dos riscos tem como propósito definir o nível de risco, a partir dos níveis de probabilidade e de impacto.	
Papéis	Equipe da SETIC	
Considerações importantes	Para definir o nível de impacto, deve-se avaliar quais dimensões (custo, prazo, escopo e qualidade) do objetivo do processo de trabalho serão influenciadas direta ou indiretamente. Para que o nível do risco seja definido, os níveis de probabilidade e de impacto são relacionados.	
Entradas	Identificação dos Riscos	
Saídas	Relatório de Análise de Riscos	
Atividades	Analisar resultados	Analisar resultados da análise de riscos realizada
Ferramentas	Planilha de Análise de Riscos	

Avaliar os riscos		
Descrição	A avaliação de riscos utiliza os resultados da análise de riscos como subsídio para a tomada de decisões sobre quais riscos necessitam ser tratados e quais terão prioridade no tratamento.	
Papéis	Equipe da SETIC	
Considerações importantes	Deve-se confrontar os níveis de riscos com os controles existentes a fim de testar a eficácia e a eficiência destes. Existindo mais de um controle, deve-se calcular o risco residual de cada um e submetê-los à média aritmética simples.	
Entradas	Análise de riscos	
Saídas	Portifólio de riscos priorizados	
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.
Ferramentas	Planilha de Avaliação de Riscos	

Elaborar Plano de Tratamento de Riscos	
Descrição	O tratamento de riscos tem como propósito determinar a resposta mais adequada para modificar a probabilidade ou o impacto de um risco. Essa resposta conta com as seguintes opções: I – evitar: o objetivo dessa resposta é descontinuar as atividades que geram o risco; II – transferir: o objetivo dessa resposta é compartilhar ou transferir uma parte do risco a terceiros sendo que nem todos os riscos são totalmente transferíveis; III – mitigar: o objetivo dessa resposta é reduzir a probabilidade, o impacto, ou ambos; IV – aceitar: o objetivo dessa resposta é avaliar se os demais tipos de respostas ao risco são viáveis.

Papéis	Equipe da SETIC	
Considerações importantes	O tipo de resposta a ser utilizado deverá ser aplicado dentro do intervalo de tempo definido pelo Secretário da Unidade, ou cargo equivalente. O Comitê Gestor de TIC deverá avaliar o PTR confirmando o impacto dos riscos que serão aceitos e encaminhando para tratamentos os que devem ser evitados, transferidos ou mitigados. Caso envolva aspectos de segurança, o Comitê Gestor de Segurança da Informação deverá avaliar o PTR confirmando o impacto dos riscos que serão aceitos e encaminhando para tratamentos os que devem ser evitados, transferidos ou mitigados. O PTR deve ser aprovado pelo Comitê de Governança de TIC.	
Entradas	Portifólio de riscos priorizados	
Saídas	Plano de Tratamento de Riscos (PTR)	
Atividades	Elaborar PTR	Devem ser identificados, para cada risco levantado, a estratégia de tratamento (mitigar, evitar, transferir ou aceitar); para cada tratamento, deve ser informada a forma de implementação, o responsável e o prazo de execução. No caso de aceitação, deve ser indicada a justificativa.
Ferramentas	Planilha de Tratamento de Riscos	

Validar portifólio e PTR	
Descrição	Validar o portifólio de riscos identificados e o Plano de Tratamento de Riscos.
Papéis	Comitê Gestor de TIC e Comitê de Gestão de Segurança da Informação
Considerações importantes	O portifólio e o PTR são validados pelo Comitê Gestor de TIC – CGESTIC e, nos casos relacionados à Segurança da Informação, pelo Comitê de Gestão de Segurança da Informação - CGSI.
Entradas	Portifólio de Riscos Identificados e Plano de Tratamento de Riscos.

Saídas	Portifólio de Riscos Identificados e Plano de Tratamento de Riscos validados e/ou aprovados.	
Atividades	Validar Portifólio de Riscos Identificados	Validar o Portifólio de Riscos Identificados elaborado pela Equipe de TIC
	Validar Plano de Tratamento de Riscos	Validar o Plano de Tratamento de Riscos elaborado pela Equipe de TIC
Ferramentas		

Aprovar portifólio e PTR		
Descrição	Aprovar o portifólio de riscos identificados e o Plano de Tratamento de Riscos.	
Papéis	Comitê de Governança de TIC	
Considerações importantes	O Comitê de Governança de TIC – CGTIC fica responsável pela aprovação.	
Entradas	Portifólio de Riscos Identificados e Plano de Tratamento de Riscos.	
Saídas	Portifólio de Riscos Identificados e Plano de Tratamento de Riscos validados e/ou aprovados.	
Atividades	Aprovar Portifólio de Riscos Identificados	Aprovar o Portifólio de Riscos Identificados elaborado pela Equipe de TIC
	Aprovar Plano de Tratamento de Riscos	Aprovar o Plano de Tratamento de Riscos elaborado pela Equipe de TIC
Ferramentas		

Implementar ações para evitar o risco	
Descrição	Ação para evitar totalmente o risco.
Papéis	Responsável pelo tratamento de riscos

Considerações importantes	O objetivo dessa resposta é descontinuar as atividades que geram o risco.	
Entradas	Planilha de Tratamento de Riscos	
Saídas	Controles implementados	
Atividades	Implementar controles para evitar o risco	A implementação dos controles deverá ser delegada de acordo com as responsabilidades estabelecidas no PTR.
Ferramentas		

Implementar ações para transferir o risco		
Descrição	Compartilhar ou transferir uma parte do risco a terceiros. O objetivo dessa resposta é compartilhar ou transferir uma parte do risco a terceiros sendo que nem todos os riscos são totalmente transferíveis.	
Papéis	Responsável pelo tratamento de riscos	
Considerações importantes		
Entradas	Planilha de Tratamento de Riscos	
Saídas	Controles implementados	
Atividades	Implementar controles para transferir o risco	A implementação dos controles deverá ser delegada de acordo com as responsabilidades estabelecidas no PTR.
Ferramentas		

Implementar ações para mitigar o risco	
Descrição	Reduzir o impacto ou a probabilidade de ocorrência do risco. O objetivo dessa resposta é reduzir a probabilidade, o impacto, ou ambos.
Papéis	Responsável pelo tratamento de riscos
Considerações importantes	
Entradas	Planilha de Tratamento de Riscos

Saídas	Controles implementados	
Atividades	Implementar controles para mitigar o risco	A implementação dos controles deverá ser delegada de acordo com as responsabilidades estabelecidas no PTR.
Ferramentas		

Atualizar fomulário de identificação de riscos		
Descrição	Atualizar a planilha de identificação dos riscos após tratamento.	
Papéis	Equipe da SETIC	
Considerações importantes		
Entradas	Planilha de Tratamento de Riscos	
Saídas	Planilha de Identificação de Riscos atualizada	
Atividades	Atualizar planilha	Atualiza a planilha de identificação de riscos
Ferramentas		

Atualizar plano de tratamento de riscos		
Descrição	Atualizar Plano de Tratamento de Riscos	
Papéis	Equipe da SETIC	
Considerações importantes		
Entradas	Planilha de Tratamento de Riscos	
Saídas	Planilha de Tratamento de Riscos Atualizada	
Atividades	Atualizar planilha	Atualiza a planilha de tratamento de riscos com os controles utilizados
Ferramentas		

Comunicar, consultar, monitorar e analisar		
Descrição	O monitoramento e análise crítica tem como propósito monitorar regularmente e sugerir melhorias durante todas as atividades do Processo de Gestão de Riscos de TIC. A comunicação e consulta tem como propósito auxiliar todas as atividades do Processo de Gestão de Riscos, de forma a permitir a comunicação eficiente, bem como a consulta às informações pertinentes ao exercício de cada uma delas.	
Papéis	Comitê Gestor de TIC	
Considerações importantes		
Entradas	Portifólio de riscos priorizados	
Saídas	Portifólio de riscos priorizados atualizado	
Atividades	Monitorar e analisar	monitorar regularmente e sugerir melhorias durante todas as atividades do processo
	Comunicar e consultar	Promover comunicação eficiente e facilicar a consulta à informações
Ferramentas		