Poder Judiciário

TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO

PROCESSO DE GESTÃO DE RISCO DE TIC

HISTÓRICO DE VERSÕES

Data	Descrição
junho/2017	Instituição do processo por meio da Portaria GP Nº 677/2017
abril/2019	Atualização do processo por meio da Portaria GP Nº 319/2019
abril/2024	Readequação do processo às recomendações do CSJT e alinhamento às novas metodologias
abril/2026	Revisão do processo com: - Correções de erros materiais. - Melhoria na descrição da Abrangência. - Melhoria na descrição dos Critérios de Risco e Nível de Risco

1. INTRODUÇÃO

Este documento tem por objetivo estabelecer o Processo de Gestão de Riscos de TIC no âmbito do Tribunal Regional do Trabalho da 16ª Região - TRT16.

A gestão de risco é o processo de planejar, organizar, dirigir e controlar os recursos humanos e materiais de uma organização, no sentido de minimizar ou aproveitar os riscos e incertezas sobre essa organização.

Espera-se, com esse processo, tornar a gestão de riscos de Tecnologia da Informação do TRT16 eficaz, buscando aumentar a probabilidade de cumprimento da missão institucional, melhorar a governança, estabelecer uma base confiável para a tomada de decisão e o planejamento e melhorar a eficácia e eficiência operacional.

2. OBJETIVO

Atender às demandas de avaliação de riscos de ativos, contratações, programas, projetos, serviços, processos, operações de TIC, baseando-se na Norma ABNT NBR ISO 31000:2018 e na Norma ABNT NBR ISO/IEC 27005:2019 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação.

3. ABRANGÊNCIA

O Processo de Gestão de Riscos de TIC aplica-se aos ativos críticos de TIC definidos no âmbito do Plano de Continuidade de Negócio e do Plano de Continuidade de Serviços de TIC do Tribunal Regional do Trabalho da 16ª Região.

O processo também poderá ser aplicado a contratações, programas, projetos, serviços, processos, operações e demais ativos de TIC, conforme deliberação da governança de TIC ou necessidade identificada pela SETIC.

4. TERMOS E DEFINIÇÕES

- **Ameaça**: ação de origem humana (intencional ou acidental) ou ambiental, que explora uma vulnerabilidade presente num ativo e provoca impactos na organização;
- **Ativo**: qualquer recurso que possui valor para a organização e cujo risco precisa ser controlado e gerenciado. Pode ser uma operação, uma atividade, um projeto, um programa, um serviço, um processo, um objetivo estratégico;
- **Apetite para o risco**: nível de risco que o Tribunal está disposto a assumir;
- **BPMN** (acrônimo de *Business Process Modeling Notation*): Notação gráfica que descreve a lógica dos passos de um processo de negócio. É um padrão internacional de modelagem que permite modelar o processo de uma maneira unificada e padronizada;
- **Controle**: políticas, práticas, procedimentos, estruturas organizacionais, dispositivos de hardware e funções de software, que visam eliminar vulnerabilidades ou minimizar os impactos causados por incidentes;
- **Controles propostos**: controles adicionais a serem realizadas com vistas a mitigar os riscos;
- **Contexto Externo**: é o ambiente externo no qual a unidade de TIC se situa e busca atingir seus objetivos (ambiente cultural, financeiro, regulatório, econômico, entre outros);
- **Contexto Interno**: é o ambiente interno no qual a unidade de TIC busca atingir seus objetivos (governança, estrutura organizacional, políticas, normas, objetivos, diretrizes, cultura organizacional, entre outros);
- **Evento de Segurança da Informação:** ocorrência identificada de um estado de sistema, serviço ou rede, indicando 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;
- **Eficácia do controle:** é o fator que aplicado ao nível de risco demonstra o potencial do controle de fazer com que o nível do risco caia;
- **Impacto**: consequência sobre os ativos e negócios de uma organização, caso uma ameaça venha a se efetivar. Pode ser tangível (exemplo: perdas financeiras) ou intangíveis (exemplo: perda de credibilidade). Pode corresponder ao produto “S” (severidade) por “R” (relevância) ou somente a severidade a depender do modelo de cálculo de risco adotado;
- **Incidente de segurança**: materialização de uma ameaça. Um incidente de segurança provoca danos a um ou mais ativos, além de impactos ao negócio;
- **Perfil de risco**: uma descrição geral dos riscos de TI (identificados) a que uma organização está exposta;
- **Probabilidade**: possibilidade de concretização de uma ameaça. Pode variar de 1 - Muito Baixa a 5 - Muito Alta;
- **PSR:** é o resultado da multiplicação de três grandezas ou dimensões: Probabilidade, Severidade e Relevância;
- **Nível de risco**: é uma indicação numérica da magnitude de um risco expressa em termos da combinação da sua probabilidade multiplicada pelo seu impacto;
- **Relevância**: grau de importância do ativo para o negócio da organização. Pode variar de 1-Muito baixa a 5-Muito alta;

- **Resposta ao risco**: 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: evitar, aceitar, mitigar, compartilhar;
- **Risco**: é a combinação da probabilidade de que algum incidente ocorra e sua consequência;
- **Risco inerente**: é o nível de risco, sem levar em conta os controles aplicados ou poderiam ter sido aplicados pela organização;
- **Risco residual**: é o nível de risco remanescente após a organização ter aplicado ações de controle do risco;
- **Severidade**: medida do grau em que um ativo será afetado, caso uma ameaça venha a se efetivar. Pode variar de 1-Muito baixa a 5-Muito alta;
- **TIC**: Tecnologia da Informação e Comunicação;
- **Vulnerabilidade**: fragilidade de um ativo que pode ser explorada por uma ameaça.

5. PAPÉIS E RESPONSABILIDADES

Na Tabela abaixo estão descritos os papéis, responsabilidades e responsáveis relacionados ao Processo de Gestão de Riscos de TIC.

Papel	Responsabilidade	Responsável
Dono Processo	- Assegurar que todos os envolvidos na execução do processo sejam informados das mudanças e suporte efetuados; - Aprovar as atualizações do processo; - Buscar a qualidade e eficiência do processo.	Secretário de Tecnologia da Informação e Comunicação
Gerente do Processo	- Buscar a eficiência e a efetividade do processo; - Manter o desenho do processo atualizados, garantindo que estejam adequados aos propósitos da organização; - Produzir informações gerenciais (indicadores); - Promover a execução das atividades do processo;	Chefe da Divisão de Infraestrutura e Segurança da Informação
Proprietário do ativo	- Tratar os riscos dos ativos sob sua responsabilidade; - Documentar o tratamento dos riscos; - Justificar os riscos não tratados.	Chefe da unidade

As revisões deste processo deverão ser submetidas à aprovação do Subcomitê de Tecnologia da Informação e Comunicação (STIC), conforme previsto na Política de Gestão de Riscos de TIC.

6. CRITÉRIOS DE RISCOS

Os critérios de riscos correspondem aos parâmetros utilizados para avaliar a magnitude dos riscos identificados, permitindo sua classificação e priorização.

No âmbito do TRT16, os riscos serão avaliados com base em critérios qualitativos de probabilidade, severidade e relevância, os quais servirão de base para a determinação do nível de risco.

6.1. Critérios de Probabilidade

A probabilidade representa a possibilidade de concretização de uma ameaça ou incidente no contexto analisado.

A avaliação da probabilidade deverá considerar fatores como histórico de ocorrências, existência de vulnerabilidades, exposição do ativo, dependência de terceiros, frequência de utilização e efetividade dos controles existentes.

Peso	Probabilidade	Descrição
5	Muito Alta	Praticamente Certo. Ocorrência quase garantida no prazo associado ao objetivo (≥ 95%)
4	Alta	Muito Provável. Repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerá nesse horizonte (65% ≤ P < 95%)
3	Média	Provável. Repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte (35% ≤ P < 65%)
2	Baixa	Pouco provável. O histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo (5% ≤ P < 35%)
1	Muito Baixa	Improvável. Acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência (P < 5%)

6.2. Critérios de Severidade

A severidade representa o grau de comprometimento do ativo, processo, serviço ou objetivo institucional caso o risco venha a se concretizar.

A avaliação da severidade deverá considerar fatores como indisponibilidade de serviços, perdas financeiras, prejuízos operacionais, impactos legais, danos à imagem institucional, descumprimento normativo e comprometimento da continuidade dos serviços.

Peso	Severidade	Descrição
5	Muito Alta	Compromete totalmente ou quase totalmente o atingimento do objetivo/resultado
4	Alta	Compromete a maior parte do atingimento do objetivo/resultado
3	Média	Compromete razoavelmente o alcance do objetivo/resultado
2	Baixa	Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado
1	Muito Baixa	Compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado

6.3. Critérios de Relevância

A relevância representa o grau de importância do ativo, processo, serviço, projeto ou informação para o TRT16.

A avaliação da relevância deverá considerar o quanto o ativo é essencial para a execução das atividades do Tribunal, para a continuidade dos serviços, para o cumprimento de obrigações legais e para o alcance dos objetivos estratégicos.

Peso	Relevância	Descrição
5	Muito Alta	Pode afetar todo o negócio e os prejuízos serão extremamente altos
4	Alta	Pode afetar um ou mais negócios e os prejuízos são muito altos
3	Média	Pode afetar uma parte do negócio e os prejuízos são razoáveis
2	Baixa	Pode afetar uma pequena parte do negócio e os prejuízos serão baixos
1	Muito Baixa	Compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado

7. NÍVEL DE RISCO

O nível de risco corresponde ao resultado da combinação entre a probabilidade de ocorrência de um evento e o impacto associado à sua concretização.

O objetivo da classificação do nível de risco é permitir a definição de prioridades de tratamento, direcionando os esforços e recursos para os riscos que representem maior ameaça ao alcance dos objetivos institucionais.

Os níveis de risco adotados no TRT16 são:

Muito Alto	riscos que comprometem diretamente a continuidade do negócio, exigindo tratamento imediato e prioritário
Alto	riscos que podem comprometer significativamente os objetivos do negócio e que devem ser tratados em cada ciclo de análise
Médio	riscos que devem ser monitorados continuamente e tratados conforme a disponibilidade de recursos e a existência de riscos mais críticos
Baixo	riscos que podem ser aceitos temporariamente, desde que monitorados
Muito baixo	riscos considerados aceitáveis, cujo tratamento é opcional

7.1. Modelo PSR

O modelo PSR é um modelo tridimensional de avaliação de riscos, calculado a partir da multiplicação da Probabilidade, da Severidade e da Relevância.

Fórmula: Nível de Risco = Probabilidade x Severidade x Relevância

Esse modelo é mais indicado para avaliações que demandam maior detalhamento e precisão, especialmente quando a importância do ativo ou processo influencia diretamente a criticidade do risco.

No modelo PSR, o impacto é representado pela multiplicação entre Severidade e Relevância.

Probabilidade														
	Muito Alta (5)	5	10	15	20	25	30	40	45	50	60	75	80	100	125
	Alta (4)	4	8	12	16	20	24	32	36	40	48	60	64	80	100
	Média (3)	3	6	9	12	15	18	24	27	30	36	45	48	60	75
	Baixa (2)	2	4	6	8	10	12	16	18	20	24	30	32	40	50
	Muito Baixa (1)	1	2	3	4	5	6	8	9	10	12	15	16	20	25
		1	**2**	**3**	**4**	**5**	**6**	**8**	**9**	**10**	**12**	**15**	**16**	**20**	**25**
		Impacto = Severidade X Relevância													

7.2. Modelo PI

O modelo PI é um modelo bidimensional de avaliação de riscos, calculado a partir da multiplicação da Probabilidade pelo Impacto.

Fórmula: Nível de Risco = Probabilidade x Impacto

Nesse modelo, o impacto é representado apenas pela Severidade, sem considerar a Relevância de forma separada.

O modelo PI é mais simples e pode ser utilizado em situações que demandem avaliações mais rápidas, com menor nível de detalhamento, especialmente quando a relevância do ativo já estiver implícita no contexto analisado.

Probabilidade						
	Muito Alta (5)	5	10	15	20	25
	Alta (4)	4	8	12	16	20
	Média (3)	3	6	9	12	15
	Baixa (2)	2	4	6	8	10
	Muito Baixa (1)	1	2	3	4	5
		Muito Baixo (1)	**Baixo (2)**	**Moderado (3)**	**Alto (4)**	**Muito Alto (5)**
		Impacto = Severidade				

8. NÍVEL DE RISCO RESIDUAL

O nível de risco residual corresponde ao risco que permanece após a consideração dos controles existentes e das medidas de tratamento adotadas.

A avaliação do risco residual permite verificar se os controles implementados são suficientes para reduzir o risco a níveis aceitáveis, observando o apetite ao risco definido pelo TRT16.

Para essa avaliação, deve ser considerado o nível de confiança dos controles existentes, que representa o grau de eficácia dos controles na mitigação dos riscos.

Quanto maior a eficácia dos controles, maior será o nível de confiança e, consequentemente, menor será o risco residual.

O nível de confiança deverá ser definido com base na análise do desenho e da implementação dos controles existentes, observando se os controles:

Nível de Confiança (NC)	**Avaliação do Desenho e Implementação dos Controles (Atributos do Controle)**	**Risco do Controle (RC)**
Inexistente NC = 0% (0,0)	Controles inexistem ou são ineficazes, mal desenhados ou mal implementados, isto é, não funcionais	Muito Alto 1,0

Fraco NC = 20% (0,2)	Controles possuem aplicação limitada ou informal, tendem a ser aplicados caso a caso, a responsabilidade é individual e há elevado grau de dependência do conhecimento das pessoas.	Alto 0,8
Mediano NC = 40% (0,4)	Controles mitigam parcialmente o risco, mas não contemplam todos os aspectos relevantes em razão de deficiências no desenho ou nas ferramentas utilizadas.	Médio 0,6
Satisfatório NC = 60% (0,6)	Controles mitigam o risco de forma satisfatória, são sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, reduzem adequadamente os riscos identificados.	Baixo 0,4
Forte NC = 80% (0,8)	Controles representam boas práticas consolidadas, mitigando todos os aspectos relevantes do risco.	Muito Baixo 0,2

O risco de controle corresponde à possibilidade de que os controles adotados não sejam suficientes para prevenir, detectar ou corrigir, em tempo hábil, eventos que possam afetar os objetivos institucionais.

O risco de controle é calculado como complemento do nível de confiança, conforme a fórmula:

Risco de Controle = 1 – Nível de Confiança

Após a definição do risco de controle, o nível de risco residual deverá ser calculado conforme a seguinte fórmula:

Nível de Risco Residual = Nível de Risco Inerente x Risco de Controle

O apetite ao risco de TIC é definido como nível médio, isto é, o Tribunal envidará esforços no sentido de que o PSR dos riscos de TIC seja limitado ao nível médio, subordinando-se à relação custo-benefício das ações de controle dos riscos, que deve ser sempre positiva.

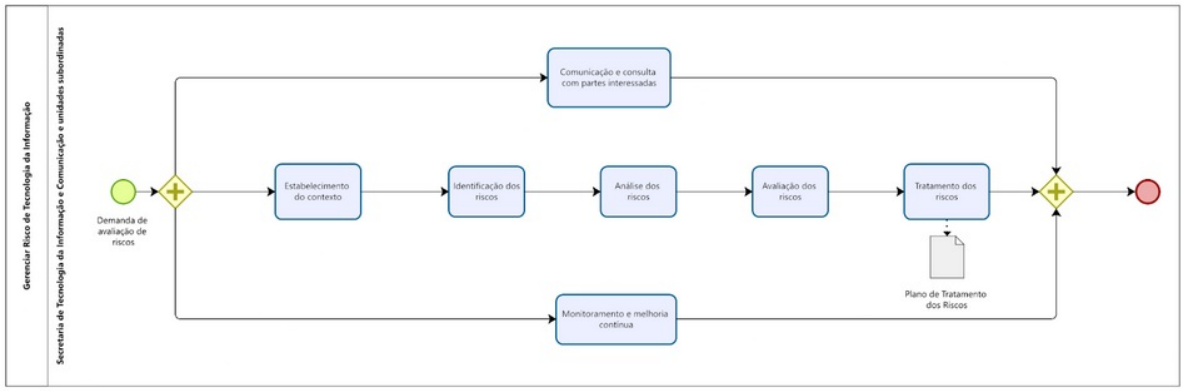
As situações em que o risco residual permanecer acima do apetite ao risco deverão ser justificadas e acompanhadas por plano de tratamento, contendo responsáveis, prazos e medidas mitigatórias.

9. FLUXO DO PROCESSO

Para realizar a gestão de riscos de quaisquer objetos, as seguintes etapas devem ser seguidas:

- estabelecimento do contexto;
- identificação dos riscos;
- análise dos riscos;
- avaliação dos riscos;
- tratamento dos riscos;
- comunicação e consulta com partes interessadas;
- monitoramento e melhoria contínua.

O processo de gestão de riscos pode ser visualizado na figura a seguir:



10. DESCRIÇÃO DAS ATIVIDADES

ATIVIDADE	OBJETIVO	RESPONSÁVEL	DETALHAMENTO
Estabelecimento do contexto	Consiste em compreender o ambiente externo e interno no qual o objeto de gestão de riscos se encontra inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.	Servidor da SETIC responsável pelo contexto analisado	Entradas: Todas as informações relevantes sobre a organização para a definição do contexto da gestão de riscos. Descrição: - Definir os critérios básicos para a gestão de riscos, tais como critério de avaliação de riscos, critério de impacto e critérios de aceitação do risco; - Estipular os objetivos a serem alcançados. Por exemplo: conformidade legal, preparação de um plano de resposta a incidentes, etc.; - Definir o escopo - descrição dos limites do projeto, sua abrangência, seus resultados e entregas. Saídas: Especificação dos critérios básicos, o escopo e os limites do processo de gestão de riscos.

Identificação dos riscos	Compreende o reconhecimento e a descrição dos riscos relacionados aos objetivos/resultados de um objeto de gestão de riscos, envolvendo a identificação de possíveis fontes de riscos.	Servidor da SETIC responsável pelo contexto analisado	Entradas: - Contexto dos riscos (critérios básicos, o escopo e os limites, e a organização do processo de gestão de riscos); - Lista dos ativos relacionados aos riscos; - Informações do histórico e de incidentes ou eventos passados; - Documentação dos controles, planos de implementação do tratamento do risco. Descrição: - Identificação de ativos - realizar o levantamento dos ativos que estão dentro do escopo estabelecido. Além disso, é necessário listar os serviços/sistemas relacionados aos ativos identificados; - Identificação de ameaças - realizar o levantamento das ameaças que tem potencial de comprometer ativos, identificando as suas fontes; - Identificação de controles existentes - realizar o levantamento dos mecanismos administrativos, físicos ou operacionais capazes de tratar a ocorrência de um incidente de segurança existentes no TRT16; - Identificação de vulnerabilidades - realizar o levantamento das vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos ou a organização. Essas vulnerabilidades podem ser das seguintes áreas: organização; processos e procedimento; rotinas de gestão; recursos humanos; ambiente físico; configuração do sistema de informação; hardware, software ou equipamento de comunicação; dependência de entidades externas; - Identificação das consequências - realizar o levantamento do prejuízo ou das consequências para o TRT16 que podem decorrer de um cenário de incidente. Um cenário de incidente é a descrição de uma ameaça explorando as vulnerabilidades. Saídas: - Lista de ativos cujos riscos precisam ser controlados; - Lista de processos de negócios relacionados aos ativos; - Lista de ameaças com a identificação do tipo e da fonte das ameaças; - Lista de todos os controles existentes; - Lista de vulnerabilidades associadas aos ativos, ameaças e controles; - Lista de cenários de incidentes com suas consequências.
Análise dos riscos	A análise do risco se refere ao desenvolvimento da compreensão sobre o risco e à determinação do nível de risco.	Servidor da SETIC responsável pelo contexto analisado	Entradas: Lista de cenários de incidentes com suas consequências, incluindo a identificação de ameaças, vulnerabilidades, ativos afetados e consequências para os ativos e processos do negócio. Descrição: - Avaliação das consequências - avaliar os impactos sobre os negócios do TRT16 levando-se em conta as consequências, por exemplo, de uma violação de segurança da informação. As consequências poderão ser expressas em função de critérios financeiros, técnicos, humanos, do impacto nos negócios, dentre outros; - Avaliação da probabilidade dos incidentes - avaliar a probabilidade de ocorrência de incidentes em cada cenário e seus impactos; - Determinação do nível de risco - realizar a mensuração do nível de risco para todos os incidentes considerados com o uso dos resultados obtidos pela avaliação das consequências e avaliação de probabilidade. Saídas: - Lista de consequências avaliadas referente a um cenário de incidente; - Probabilidade dos cenários de incidentes; - Lista de riscos com níveis de valores designados.
Avaliação dos riscos	A avaliação do risco envolve a comparação do seu nível com o limite de exposição a riscos, a fim de determinar se o risco é aceitável.	Servidor da SETIC responsável pelo contexto analisado	Entradas: Lista de riscos com níveis de valores designados e critérios para a avaliação de riscos. Descrição: - Consiste em comparar os níveis de riscos estimados com critérios de riscos definidos pelo TRT16, a fim de determinar a ação mais adequada a ser tomada em relação ao risco, identificando quais riscos necessitam ser tratados e quais terão prioridade no tratamento. Saídas: Lista de riscos priorizados, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.
Tratamento dos riscos	Compreende o planejamento e a realização de ações para modificar o nível de risco	Servidor da SETIC responsável pelo contexto analisado	Entradas: Lista de riscos priorizados, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos. Descrição: Selecionar as opções de tratamento para os riscos selecionados considerando o resultado da análise/avaliação de riscos, custo esperado para implementação e benefícios previstos. Deve-se identificar a ordem de prioridade, bem como os prazos de execução. As respostas aos riscos podem envolver uma ou mais das seguintes opções de tratamento: - Evitar o risco - ação para eliminar totalmente o risco; - Transferir o risco -compartilhar ou transferir parte do risco a terceiros; - Mitigar o risco - reduzir o impacto e/ou a probabilidade de ocorrência do risco; - Aceitar o risco -aceitar ou tolerar o risco sem que nenhuma ação específica seja tomada, quando o nível do risco for considerado aceitável, a capacidade da organização para tratá-lo for limitada ou o custo da mitigação for desproporcional ao benefício esperado. Saídas: Mapa de Risco. Modelo no Anexo I.

Monitoramento e melhoria contínua	Compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse.	Servidor da SETIC responsável pelo contexto analisado	Entradas: Todas as informações sobre os riscos gerados ao longo da execução das atividades do Processo de Gestão de Riscos de TIC. Descrição: - Monitoramento e análise crítica dos fatores de risco - assegurar o controle do risco, monitorando riscos residuais e identificando novas ameaças e vulnerabilidades, assegurando a execução dos planos de tratamento dos risco e avaliando sua eficiência e eficácia na redução dos riscos; - Monitoramento, análise crítica e melhoria do processo de gestão de risco - garantir que o processo de gestão de riscos esteja realmente atendendo aos requisitos estratégicos do negócio. Saídas: Alinhamento contínuo da gestão de riscos.
Comunicação e consulta com partes interessadas	Refere-se à identificação das partes interessadas e ao compartilhamento de informações relativas à gestão de riscos sobre determinado objeto, observada a classificação da informação quanto ao sigilo.	Servidor da SETIC responsável pelo contexto analisado	Entradas: Todas as informações sobre os riscos gerados ao longo da execução das atividades do Processo de Gestão de Riscos de TIC. Descrição: - Realizar a comunicação das informações produzidas ao longo da execução do processo de gestão de riscos, bem como disponibilizar essas informações para consulta, a fim de assegurar a compreensão necessária à tomada de decisão envolvendo riscos. Saídas: Entendimento contínuo do Processo de Gestão de Riscos de TIC e dos resultados obtidos.

ANEXO I – MODELO DO MAPA DE RISCO

MAPA DE RISCO																
Histórico de Revisões																
DATA	VERSÃO	DESCRIÇÃO							AUTOR							
IDENTIFICAÇÃO DO ESCOPO																
Ativo/Processo/Projeto																
Objetivo do Ativo/Processo/Projeto																
IDENTIFICAÇÃO DO RISCO						ANÁLISE DO RISCO					CONTROLES EXISTENTES			TRATAMENTO DE RISCO		
ID	ATIVO	CAUSAS	EVENTOS	CONSEQUÊNCIAS		PROBABILIDADE	SEVERIDADE	RELEVÂNCIA	NRI	NÍVEL DE RISCO INERENTE	CONTROLES	EFICÁCIA	RISCO RESIDUAL	TIPO DE RESPOSTA	CONTROLES PROPOSTOS	RESPONSÁVEL

Documento assinado eletronicamente por **RAFAEL ROBINSON DE SOUSA NETO**, **Secretário de Tecnologia da Informação e Comunicação**, em 15/04/2026, às 15:57, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site Autenticar Documentos informando o código verificador **1146243** e o código CRC **9D6111DA**.

Referência: Processo nº 000004429/2018 SEI nº 1146243