PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO

PROCESSO DE GESTÃO DE RISCO DE TIC

SUMÁRIO

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

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 tem aplicabilidade na Secretaria de Tecnologia da Informação e Comunicação e estruturas organizacionais subordinadas a ela.

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;
- **Controle 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

6. CRITÉRIOS DE RISCOS

Os critérios de riscos são parâmetros estabelecidos para avaliar a magnitude dos riscos, a fim de que seja possível quantificar o nível de risco na busca da obtenção de resultados esperados pelo TRT16 em sua missão institucional.

Para efeito deste processo, definiu-se como metodologia para a análise de risco a forma proposta pela norma ABNT NBR ISO 31000:2018, a qual define o nível do risco em termos da combinação dos impactos e de suas probabilidades. Serão utilizadas escalas qualitativas para estimar a probabilidade e o impacto.

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%)

Tabela 2: Critérios de Probabilidade

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

Tabela 3: Critérios de Severidade

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 de forma do negócios e os prejuízos serão baixos
1	Muito Baixa	Compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado

Tabela 4: Critérios de Relevância

Para o cálculo do nível de risco pode-se adotar um modelo tridimensional denominado PSR ou um modelo bidimensional denominado PI. A tabela abaixo apresenta o nível de risco, a interpretação deste nível e os valores possíveis usando o modelo PSR e o modelo PI.

Nível de Risco	Interpretação	Valores possíveis do PSR	Valores possíveis do PI
Muito Alto	São riscos que, se houver recursos, devem ser eliminados, pois comprometem diretamente a continuidade do negócio	60,64,75,80,100,125	25
Alto	São riscos que podem não ser eliminados mas devem, ao menos, ser controlados em cada ciclo, pois comprometem indiretamente a continuidade do negócio e podem vir a se tornar riscos muito altos	32,36,40,45,48,50	15,16,20
Médio	São riscos que devem ser monitorados, mas não precisam ser tratados quando houver riscos de nível alto existentes	18,20,24,25,27,30	8,9,10,12
Baixo	São riscos que podem ser aceitos se houver riscos com nível médio existentes	8,9,10,12,15,16	3,4,5,6
Muito baixo	São riscos aceitáveis que devem ser informados e tratados e seu tratamento é absolutamente opcional	1,2,3,4,5,6	1,2

Tabela 5: Nível de risco com base no PSR e no PI.

Muito Baixo	Baixo	Médio	Alto	Muito Alto

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													

Tabela 6: Distribuição do nível de risco com base no PSR.

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				

Tabela 7: Distribuição do nível de risco com base no PI.

7. NÍVEL DE RISCO RESIDUAL

A análise de riscos só se completa quando as ações que a gestão adota para respondê-los são também avaliadas, chegando-se ao nível de risco residual, o risco que ainda permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e o impacto dos riscos, incluindo controles internos e outras ações. Formas de resposta a riscos podem variar entre aceitar, reduzir, evitar ou compartilhar o risco, incluindo o estabelecimento de atividades de controle para assegurar que as respostas definidas sejam efetivamente aplicadas.

Os controles existentes são controles estabelecidos por meio de políticas e procedimentos, desempenhadas em todos os níveis da organização, em vários estágios dentro do processo organizacional e no ambiente tecnológico, que ajudam a garantir o cumprimento das diretrizes determinadas pela Administração para mitigar os riscos à realização dos objetivos.

Uma forma de avaliar o efeito dos controles internos na mitigação de riscos consiste em estimar a eficácia de cada controle e

determinar um nível de confiança (NC), mediante análise dos atributos do desenho e da implementação do controle, conforme apresentado a seguir.

Nível de Confiança (NC)	Avaliação do Desenho e Implementação dos Controles (Atributos do Controle)	Risco do Controle (RC)
Inexistente NC = 0% (0,0	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	Muito Alto 1,0
Fraco NC = 20% (0,2)	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	Alto 0,8
Mediano NC = 40% (0,4)	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	Médio 0,6
Satisfatório NC = 60% (0,6)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Baixo 0,4
Forte NC = 80% (0,8)	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	Muito Baixo 0,2

Tabela 8: Níveis de confiança.

Uma vez determinado o nível de confiança (NC), pode-se determinar o risco de controle (RC), isto é, a possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência de eventos que possam afetar adversamente a realização de objetivos. O RC é definido como complementar ao NC: Risco de controle = 1 - Nível de confiança.

Pela fórmula é possível deduzir que quanto mais eficaz for o projeto e a implementação dos controles, ou seja, quanto maior for o NC, menor será o RC e vice-versa, porém este nunca será “zero”, uma vez que aquele nunca poderá ser 100%.

Uma vez estabelecido o RC, é possível estimar o nível de risco residual (NRR) que permanece depois de considerado o efeito das respostas adotadas pela gestão. Para isso, deduz-se do nível de risco inerente (NRI) o percentual de confiança (NC) atribuído ao controle, o que equivale a multiplicar o NRI pelo RC, utilizando a seguinte fórmula.

Nível de risco residual = Nível de risco inerente x Risco do controle

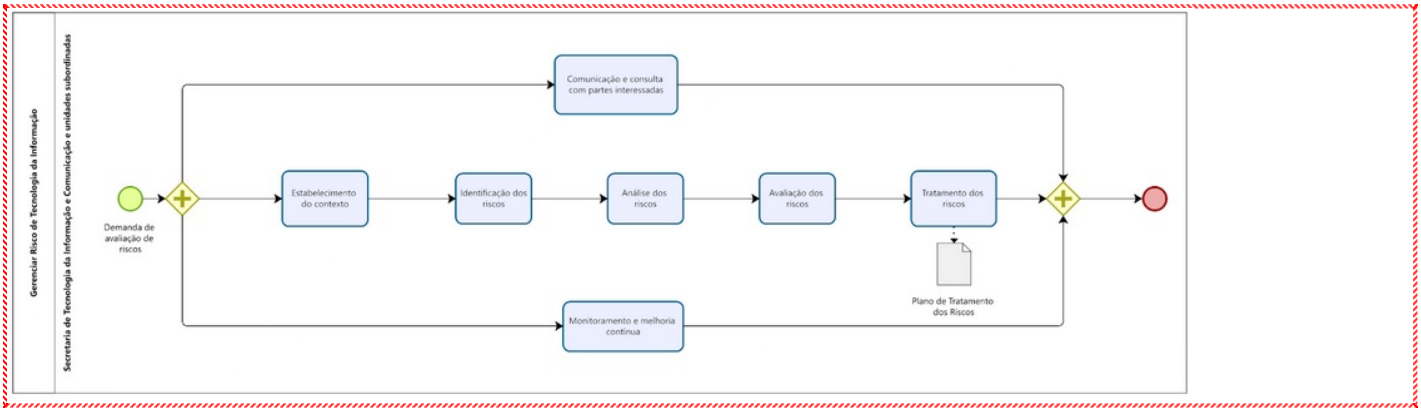
O apetite ao risco de TIC é definido como nível médio, isto é, o Tribunal envidará esforços no sentido de que o nível dos riscos de TIC seja limitado ao nível médio, subordinando-se a relação custo benefício das ações de controle dos riscos, que deve ser sempre positiva.

8. 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:



9. DESCRIÇÃO DAS ATIVIDADES

ATIVIDADE	OBJETIVO	RESPONSÁVEL	
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 • Estipular os objetivos a serem alcançados. Por exemplo: conformidade legal, preparação de um plano de resposta a incident • 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 necessár • Identificação de ameaças - realizar o levantamento das ameaças que tem potencial de comprometer ativos, identificando as • Identificação de controles existentes - realizar o levantamento dos mecanismos administrativos, físicos ou operacionais capa • Identificação de vulnerabilidades - realizar o levantamento das vulnerabilidades que podem ser exploradas por ameaças par • Identificação das consequências - realizar o levantamento do prejuízo ou das consequências para o TRT16 que podem decor **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 **Descrição**: • Avaliação das consequências - avaliar os impactos sobre os negócios do TRT16 levando-se em conta as consequências, por e • Avaliação da probabilidade dos incidentes - avaliar a probabilidade de ocorrência de incidentes em cada cenário e seus impa • Determinação do nível de risco - realizar a mensuração do nível de risco para todos os incidentes considerados com o uso do **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 **Saídas**: Lista de riscos priorizados, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que po
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 **Descrição**: Selecionar as opções de tratamento para os riscos selecionados considerando o resultado da análise/avaliação de risco • Evitar o risco - ação para evitar totalmente o risco; • Transferir o risco - compartilhar ou transferir uma parte do risco a terceiros; • Mitigar o risco - reduzir o impacto ou a probabilidade de ocorrência do risco; • Aceitar o risco - aceitar ou tolerar o risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considera **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 **Descrição**: • Monitoramento e análise crítica dos fatores de risco - assegurar o controle do risco, monitorando riscos residuais e identifica • Monitoramento, análise crítica e melhoria do processo de gestão de risco - garantir que o processo de gestão de riscos esteja **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 **Descrição**: • Realizar a comunicação das informações produzidas ao longo da execução do processo de gestão de riscos, bem como dispo **Saídas:** Entendimento contínuo do Processo de Gestão de Riscos de TIC e dos resultados obtidos.

10. 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					MONITORAMENTO			
ID	ATIVO	CAUSAS	EVENTOS	CONSEQUÊNCIAS	PROBABILIDADE	SEVERIDADE	RELEVÂNCIA	NRI	NÍVEL DE RISCO INERENTE	CONTROLES	EFICÁCIA	RISCO RESIDUAL	TIPO DE RESPOSTA	CONTROLES PROPOSTOS	RESPONSÁVEL	DATA INÍCIO	DATA FIM	DATA	STATUS	OCORREU?	COMENTÁRIO

Documento assinado eletronicamente por **RAFAEL ROBINSON DE SOUSA NETO**, **Secretário de Tecnologia da Informação e Comunicação**, em 21/03/2024, às 09:24, 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 **0114286** e o código CRC **71C4EF00**.