Processo de Gerenciamento de Riscos de TIC

SETIC - Secretaria de Tecnologia da Informação e Comunicação

Gestor do Processo: Chefe da Divisão de Segurança da Informação
Área responsável: Divisão de Segurança da Informação - SETIC

JOENIR JOSE DELLA FLORA
06/07/2023 13:58

OBJETIVO

Estabelecer o Processo de Gerenciamento de Riscos de TIC no âmbito do Tribunal Regional do Trabalho da 14ª Região (TRT14), definindo papéis e responsabilidades, procedimentos a serem adotados, documentos relacionados e indicadores do processo.

DEFINIÇÕES GERAIS PARA A ADEQUADA EXECUÇÃO DESTE PROCESSO

1. **Papéis e Responsabilidades**
   - **Gestores das unidades da SETIC -** Representa os chefes das unidades administrativas internas da SETIC - Secretaria de Tecnologia da Informação e Comunicação. São responsáveis por identificar, analisar, propor tratamento e acompanhar o tratamento dos riscos.
   - **Comitê de Segurança da Informação** - Responsável pela avaliação das proposições de tratamento de riscos produzidas, chancelando a validade, momento e modo de implementação de cada tratamento.
   - **Responsáveis pelo tratamento do risco -** Servidores designados da SETIC com aptidão para implantar as medidas definidas no plano de tratamento de riscos.

2. **Ferramenta de gerenciamento de risco**

A adequada execução deste processo tem como premissa a existência de ferramenta de gestão de riscos que permita o registro de riscos individuais e o acompanhamento de seu ciclo de vida. A ferramenta deve permitir adicionar, para cada um dos riscos, pelo menos as seguintes informações: risco identificado, proponente do risco, probabilidade do risco, impacto do risco, grau (calculado ou não) do risco, consequências do risco, categoria do risco (conforme item 4 deste tópico), tipo do tratamento (conforme item 5 deste tópico), área e responsável pelo tratamento, cronograma de tratamento.

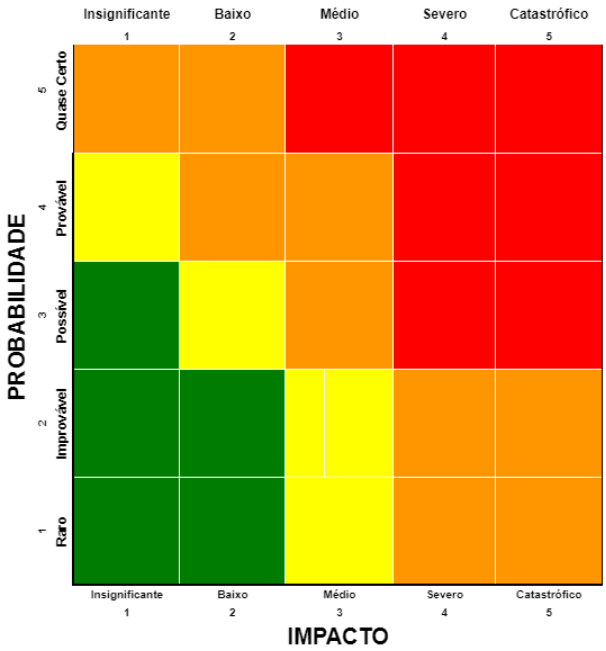
Inexistindo ferramenta especializada de gestão de riscos, é possível executar este processo utilizando-se de uma planilha eletrônica para registrar os riscos e os desdobramentos dos seus ciclos de vida. Recomenda-se, neste caso, a adoção de uma solução de planilha online (em nuvem), para permitir facilidades de consulta e edição.

Desde a primeira versão deste processo a SETIC realiza o registro e o acompanhamento centralizado dos riscos em planilha eletrônica. O acesso ao documento pode ser solicitado à Seção de Governança de TIC.

3. Cálculo do grau de ameaça e matriz de prioridade dos riscos

A avaliação do grau de ameaça dos riscos é obtido por meio do produto entre o valor da probabilidade e o valor do impacto que cada risco representa. Como há 5 valores possíveis para a probabilidade e 5 para o impacto, o grau do risco pode variar entre 1 e 25, e este valor ajuda a indicar quão prioritário deve ser o tratamento do risco.

Além do grau de ameaça dos riscos é possível classificá-los em 4 níveis de prioridade. Estes níveis permitem agrupamento e melhor tratamento em função da probabilidade e impacto de um deles. Para calcular o nível de prioridade, basta localizar a probabilidade e o impacto de cada risco na matriz abaixo. O cruzamento de linha e coluna indicará o nível (cor) de prioridade resultante.



Localizado o nível (cor), recomenda-se a adoção da postura de tratamento sugerida na tabela a seguir:

Nível	Postura de Tratamento Sugerida
I	Riscos pouco significantes. Não são exigidas ações imediatas
B	Riscos não graves. Sugere-se apenas monitoramento regular
M	Riscos de média prioridade. Requerem a definição e execução de ações corretivas para reduzir sua ameaça potencial
A	Riscos prioritários. Exigem a definição e implantação imediata de ações corretivas

4. **Categorias de riscos**
    - **Estratégico:** Estão associados à tomada de decisão que pode afetar negativamente o alcance dos objetivos da organização.
    - **Operacional:** Riscos que afetam o desempenho e a qualidade das atividades operacionais de TI. Os riscos devem ser mitigados, transferidos, eliminados ou explorados, pois não poderão ser aceitos.
    - **Reputação ou Imagem:** Riscos que podem afetar a imagem da SETIC ou da organização. Os riscos devem ser mitigados, transferidos, eliminados ou explorados, pois não poderão ser aceitos.
    - **Financeiro:** Estão associados ao não cumprimento de princípios constitucionais, legislações específicas ou regulamentações externas aplicáveis ao negócio, bem como de normas e procedimentos internos.
    - **Conformidade:** Riscos externos ao controle direto do TRT14, mas que ainda assim podem afetar o sucesso das metas e ações. Os riscos externos podem ser aceitos, pois independem de ação direta do TRT14.
    - **Tecnologias:** Riscos relacionados a problemas técnicos em hardware, software ou outra solução de informática (apontamento genérico).
    - **Infraestrutura de TI:** Riscos relacionados a problemas técnicos em hardware, software, ou demais equipamentos de TI (exige conhecimento técnico para definir esta categoria).
    - **Software:** Riscos relacionados a problemas técnicos em um software específico (exige conhecimento técnico para definir esta categoria).
    - **Escopo:** Riscos relacionados ao assunto escopo de um projeto, exemplo: indefinições, alterações constantes, sem validação.
    - **Cliente / Usuário:** Riscos relacionados a clientes ou usuários de algum projeto, por exemplo: indefinição, representante ausente, sem comprometimento.

5. **Tipos de tratamento dos riscos**
    - **Modificar (diminuir) o risco** – opção mais comum, inclui a implementação de salvaguardas (controles), como sistemas de supressão de incêndio etc.
    - **Evitar o risco** – significa evitar realizar tarefas ou processos se eles incorrerem em riscos que são simplesmente muito grandes/custosos para mitigar com quaisquer outras opções (por exemplo, banir o uso de laptops fora das instalações da empresa se o risco de acesso não autorizado para estes laptops for muito alto).
    - **Transferir o risco** – significa transferir o risco para outra parte (por exemplo, adquirir um seguro predial para transferir parte do risco financeiro para uma companhia de seguro). Esta opção não influencia o incidente em si.
    - **Aceitar o risco** – significa aceitar o risco sem fazer nada a respeito. Opção comumente usada quando os custos de mitigação são maiores do que os prejuízos provocados pelo incidente.
      Ao avaliar a aceitação de um risco de TIC, geralmente são considerados vários critérios para tomar uma decisão informada. Os critérios que podem ser usados para aceitar um risco de TIC são:
        - Probabilidade: Avalia a possibilidade de um evento indesejado ocorrer. É importante considerar a probabilidade de o risco se concretizar, levando em conta fatores como histórico de incidentes, vulnerabilidades conhecidas, ameaças ativas e mudanças no ambiente.
        - Impacto: Analisa a extensão do dano potencial caso o evento ocorra. O

impacto pode incluir perda financeira, interrupção do negócio, danos à reputação, violação de dados ou qualquer outro impacto negativo relevante. Quanto maior o impacto, maior a necessidade de considerar a aceitação do risco.

- Custo-benefício: Avalia se o custo de implementar medidas de mitigação do risco é justificável em relação ao benefício esperado. Em alguns casos, pode ser mais econômico aceitar o risco e estar preparado para lidar com suas consequências do que investir recursos significativos em medidas de proteção.
- Disponibilidade de recursos: Avalia se o Tribunal possui os recursos necessários para implementar medidas de mitigação adequadas. Às vezes, a aceitação do risco pode ser uma opção quando não há recursos suficientes disponíveis para implementar as contramedidas apropriadas.

No entanto, é importante ressaltar que a aceitação do risco não significa negligenciá-lo ou ignorá-lo, e sim, envolve uma análise criteriosa e com uma decisão consciente de assumir determinados riscos com base em uma compreensão clara dos impactos potenciais e na capacidade de lidar com eles.

A diferença entre **evitar** e **aceitar** o risco é que, ao reter, a organização continua realizando as rotinas que podem provocar os riscos, ao evitar, a organização deixa de executar as rotinas/processos que podem vir a provocar o risco no ambiente.

5.1 Assunção de riscos

Assunção de Riscos consiste na aceitação do nível de exposição a um risco, considerando não ser viável estabelecer ações para sua mitigação e, assim, aceitando as possíveis consequências.

Essa decisão sempre está associada ao apetite a risco da organização e aos benefícios esperados pelas ações a serem implementadas. Devendo sempre a solicitação partir dos responsáveis pelo risco a ser assumido.

Todas decisões de assunção de riscos deverão ser deliberadas pelo Comitê de Gestão TIC e comunicadas periodicamente junto ao comitê de riscos institucional.

6. Estabelecimento do contexto

O contexto de risco é a circunstância onde aparecem os eventos de riscos, mediante essa situação, a gestão de riscos deverá considerar o ambiente ou a situação delimitada nesta fase.

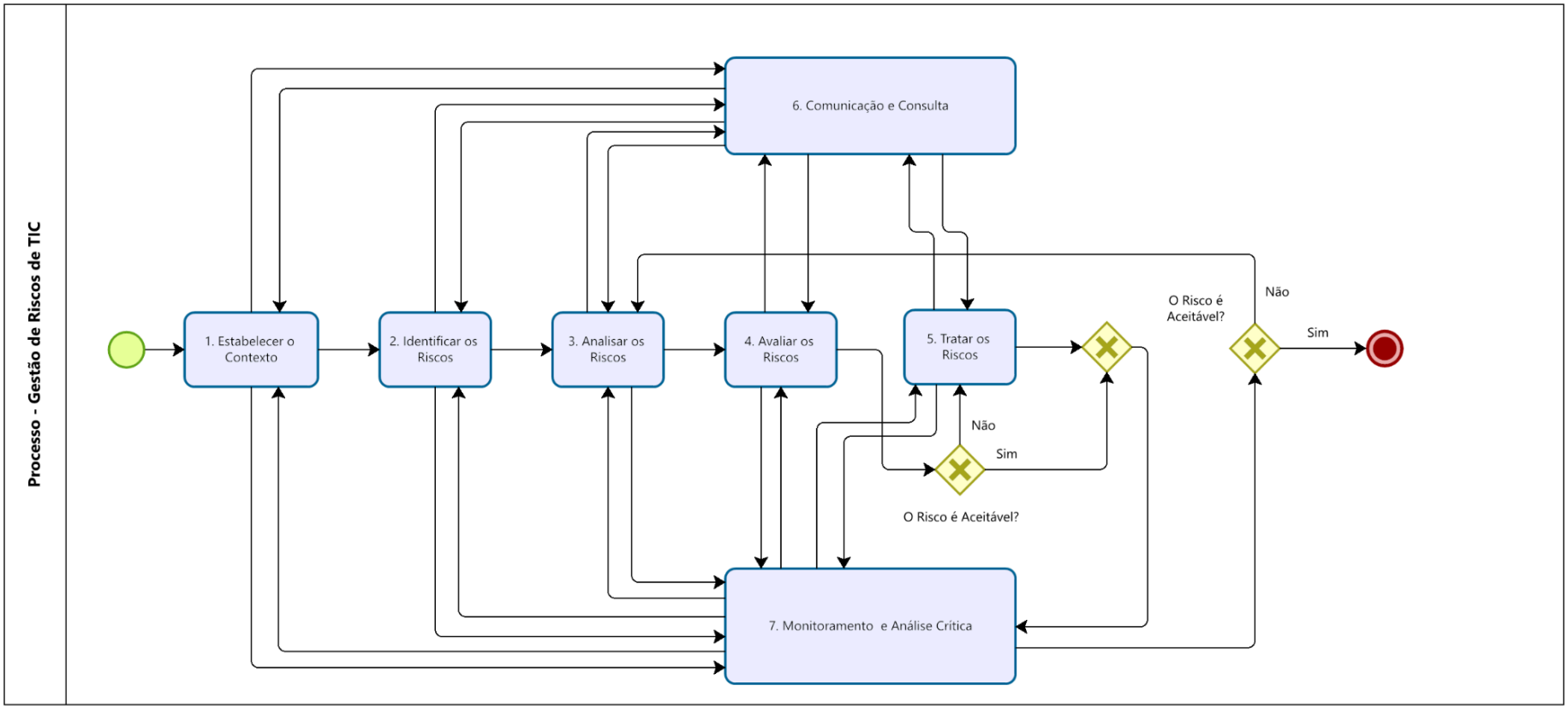
Antes da realização da etapa de Identificar e Registrar os Riscos, deve ser realizado o levantamento dos contextos interno e externo, as leituras de cenário atual e, também, a avaliação dos objetivos estratégicos da organização. O Contexto do Processo de

Gerenciamento de Riscos de TIC delimita o escopo no que se refere à abrangência das partes da organização envolvidas e aos critérios gerais para as atividades da gestão de riscos.

Juntamente com os objetivos estratégicos e táticos estabelecidos pelo TRT14, o entendimento desses contextos é de suma importância para que os diversos riscos sejam identificados.

FLUXOGRAMAS DESTE PROCESSO

Fluxograma: Processo de Gerenciamento de Riscos de TIC



DESCRIÇÃO DAS ATIVIDADES DO FLUXOGRAMA: Processo de Gerenciamento de Riscos de TIC			
Nome da atividade	**Objetivo**	**Responsável**	**Tarefas / Ações**
1. Estabelecer o Contexto	Compreender o ambiente externo e interno no qual o objeto de gestão de riscos de TIC encontra-se inserido e em identificar parâmetros e critérios a serem considerados neste processo.	Gestores das unidades da SETIC e Secretário de TIC	**Entrada:** Planos, Processos e outros documentos relacionados à TIC. **Tarefas:** ● Propor o objeto da gestão de riscos; ● Aprovar o objeto da gestão de riscos; ● Definir a equipe responsável pela gestão de riscos do objeto; ● Identificar quais objetivos ou resultados devem ser alcançados pelo objeto; ● Identificar as partes interessadas do objeto e do resultado; ● Identificar os fatores do ambiente que podem afetar o alcance dos objetivos ou dos resultados; ● Identificar os ativos que suportam o objeto; ● Estabelecer critérios para analisar e avaliar os níveis de risco ● do objeto; ● Aprovar o contexto. **Saída:** Contexto estabelecido
2. Identificar os riscos	Levantar possíveis ameaças que possam afetar o negócio, registrando-os na ferramenta de gestão de riscos. O Levantamento pode ser feito individualmente ou em grupo.	Gestores das unidades da SETIC	**Entrada:** Contexto estabelecido **Tarefas:** ● Identificar eventos ou ameaças com potencial de impactar negativamente o ambiente, imediata ou futuramente; ● Registrar os riscos encontrados no software de gestão de riscos. ● Definir, no mínimo: a) Categoria do risco; b) Área responsável; c) Risco (ameaça) identificado; d) Consequências do risco; e) partes interessadas. A informação de “categoria do risco” pode assumir um dos valores sugeridos no item 4 das informações gerais deste processo.

			OBS: Esta atividade pode ser realizada individualmente (quando um chefe de seção decide verificar riscos em sua unidade) ou em grupo (quando a SETIC promove, por exemplo, uma oficina de identificação de riscos com todas as suas unidades internas). Em ambos os casos os chefes acessam diretamente a ferramenta de gestão de riscos e registram os seus riscos. Caso o levantamento seja feito em grupo e a ferramenta não permita acesso multiusuário, os riscos são levantados pelos chefes da SETIC e registrados na ferramenta pelo Chefe da Seção de Governança de TIC. **Saída:** Lista de riscos identificados e registrados na ferramenta de gestão de riscos
3. Analisar os riscos	Avaliar o grau de ameaça dos riscos de acordo com a probabilidade e o impacto de cada um	Gestores das unidades da SETIC	**Entrada:** Riscos catalogados na ferramenta de gestão de riscos. **Tarefas:** ● Definir, para cada risco levantado na atividade anterior, a probabilidade de sua ocorrência e o impacto potencial que ele pode provocar no ambiente. A probabilidade pode assumir um dos seguintes valores: 1 - Raro 2 - Improvável 3 - Possível 4 - Provável 5 - Quase Certo O impacto pode assumir um dos seguinte valores: 1 - Insignificante 2 - Baixo 3 - Médio 4 - Severo 5 - Catastrófico O grau do risco será calculado pelo produto entre a probabilidade e o impacto. Sua prioridade será definida conforme a matriz de avaliação de prioridade. **Saída:** Riscos catalogados na ferramenta de gestão de riscos com grau de ameaça definido.
4. Avaliar os riscos	Planejar tratamento individual dos riscos, definindo	Gestores das unidades da SETIC	**Entrada:** Riscos com grau de ameaça definido. **Tarefas:** ● Avaliar os riscos, definindo, para cada um, o tipo de

	procedimentos de tratamento, responsabilidades e prazos		tratamento a ser adotado (conforme detalhado no item 5 das definições gerais para execução deste processo). O tipo de tratamento pode ser: ○ Diminuir (modificar) o risco; ○ Evitar o risco; ○ Transferir o risco; ○ Aceitar o risco. ● Dependendo do tratamento definido, definir ainda: ○ procedimentos de implementação ○ responsável pela implementação ○ prazo de execução. A escolha pela retenção de um risco exige justificativa. **Saída:** Propostas de Tratamento dos Riscos definidas na ferramenta de gestão de riscos.
5. Tratar os riscos	Implementar as ações de tratamento definidas nas propostas de tratamento.	Responsável pelo tratamento do risco	**Entrada:** Propostas de tratamento de riscos aprovadas pelo CSI. **Tarefas:** ● Os responsáveis pela execução das ações de tratamento de cada um dos riscos devem implementar cada uma das ações de tratamento conforme as orientações das PTRs aprovadas no CSI. **Saída:** Riscos tratados conforme definições da PTRs.
6. Comunicação e Consulta	Informar às partes interessadas sobre os riscos e detalhes de tratamento de cada um deles	CSI, CGesTIC e/ou CGTIC	**Entrada:** Proposta de tratamento de riscos aprovada **Tarefas:** ● Avaliar as partes interessadas em cada risco constante da PTR. ● Comunicar às partes interessadas (preferencialmente por e-mail) as ações de tratamento dos riscos que serão realizadas, com seus respectivos prazos de execução. **Saída:** Riscos comunicados às partes interessadas.

7. Monitoramento e Análise Crítica	Acompanhamento da implementação adequada e oportuna das ações de tratamento dos riscos	Gestores das unidades da SETIC	**Entrada:** PTR com riscos pendentes de tratamento. **Tarefas:** - Avaliar se cada um dos riscos pendentes de tratamento em seu âmbito está sendo: ○ Tratado no prazo planejado; ○ Corretamente tratado, conforme especificações da PTR; ○ Corretamente documentado, conforme progridem as ações de tratamento. - Caso algum risco esteja descumprindo alguma das obrigações acima, comunicar-se com o responsável pela implementação do tratamento do risco para solicitar a correção o mais rápido possível. **Saída:** Comunicações às partes interessadas sobre o tratamento do(s) risco(s).

GLOSSÁRIO

Análise de riscos - processo para compreender a natureza do risco e determinar o nível de risco;
Assunção de riscos - situação na qual a organização se dispõe a manter-se exposta a um determinado risco, considerando o apetite a risco da organização.
Avaliação de riscos - processo de comparação dos resultados da análise de risco com critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis;
Comunicação do risco - conjunto de processos contínuos e iterativos que uma organização realiza para fornecer, compartilhar ou obter informações e para dialogar com as partes interessadas sobre o gerenciamento de riscos;
Evitar risco - forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;
Identificação de riscos - processo para localizar, listar e caracterizar elementos de risco.
Reduzir risco - forma de tratamento de risco pela qual se decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;
Riscos de Segurança da Informação e Comunicações - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
Tratamento dos riscos - processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

SIGLAS E ABREVIATURAS

CSI - Comitê de Segurança da Informação
CGesTIC - Comitê de Gestão de TIC
CGTIC - Comitê de Governança de TIC
PTR - Proposta de Tratamento dos Riscos
SETIC - Secretaria de Tecnologia da Informação e Comunicação
TI - Tecnologia da Informação
TIC - Tecnologia da Informação e Comunicação
TRT14 - Tribunal Regional do Trabalho da 14ª Região

REFERÊNCIAS

- Norma Complementar nº 04/IN01/DSIC/GSIPR
- Norma Técnica ABNT NBR ISO/IEC 27005:2019
- Norma Técnica ABNT NBR ISO 31000:2018
- Norma Técnica ABNT NBR ISO/IEC 27001:2013
- Norma Técnica ABNT ISO GUIA 73:2009

- Norma Técnica ISO/IEC 27000:2018
- Norma ABNT NBR ISO/IEC 27002:2013

DESTINAÇÃO DO PROCESSO

Usuários de serviços de Tecnologia do Tribunal Regional do Trabalho da 14ª Região e servidores da Secretaria de Tecnologia da Informação e Comunicação.

OUTRAS INFORMAÇÕES DESTE PROCESSO

Elaboração: Vinícius Vieira Marques	**Data:** 08/07/2021
Revisão: Vinícius Vieira Marques	**Data:** 12/07/2021
Data de aprovação formal:	16/07/2021

Histórico de Revisões

Data	Versão	Descrição	Responsável
12/07/2021	1.0	Versão inicial do documento	Vinícius Vieira Marques
08/06/2022	1.1	Revisão do processo	Joenir José Della Flora
29/05/2023	1.2	Revisão do processo	Wainner Brum Caetano