ATO N° 28/2018/SGP – Manaus, 10 de abril de 2018

Aprova o Processo de Gestão de Riscos de Tecnologia da Informação e Comunicação do TRT 11ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 11ª REGIÃO, Desembargadora do Trabalho ELEONORA DE SOUZA SAUNIER, no uso de suas atribuições legais e regimentais,

CONSIDERANDO que constitui iniciativa estratégica da Justiça do Trabalho da 11ª Região estabelecer a gestão de riscos, com base na implantação de metodologia, capacitação e da cultura do gerenciamento de riscos, de modo a promover ações práticas relativas ao tratamento de riscos inerentes às atividades institucionais, contribuindo para a redução da materialização de eventos que impactem negativamente seus objetivos;

CONSIDERANDO a Norma da ABNT NBR ISO 31000:2009 que estabelece princípios e diretrizes para a gestão de riscos;

CONSIDERANDO os macrodesafios do Poder Judiciário para o período 2015-2020, em especial o que trata da "Melhoria da infraestrutura e governança de TIC";

CONSIDERANDO a importância de estabelecer diretrizes, papéis e responsabilidades, práticas e processos de trabalho compatíveis com os modelos de referência reconhecidos mundialmente;

CONSIDERANDO a série de normas ABNT NBR ISO/IEC 27.000, que versam sobre a criação, funcionamento, manutenção e melhoria do Sistema de Segurança da Informação (SGSI);

CONSIDERANDO o referencial de boas práticas para o Gerenciamento de Serviços de TIC definido na biblioteca Information Technology Infrastructure Library (ITIL);

CONSIDERANDO as diretrizes básicas para a implantação da política de projetos no âmbito da Justiça do Trabalho de 1º e 2º graus traçadas pela Resolução CSJT nº 97, de 23 de março de 2013;

CONSIDERANDO o referencial de boas práticas para o gerenciamento de projetos definido no Project Management Body of Knowledge (PMBOK);

CONSIDERANDO a importância de estabelecer processos de trabalho, responsabilidades e práticas compatíveis com os modelos de excelência reconhecidos mundialmente, como a norma NBR ISO/IEC 38500:2009, o Control Objectives for Information and Related Technologies (Cobit), a Information Technology Infrastructure Library (ITIL) e a série de normas NBR ISO/IEC 20000:2008; e

CONSIDERANDO as informações constantes do DP-4394/2018 (e-SAP),

RESOLVE:

Art. 1º Aprovar o Processo de Gestão de Riscos de Tecnologia da Informação e Comunicação do Tribunal Regional do Trabalho da 11ª Região, nos termos constantes do anexo deste Ato.

Art. 2º Este Ato entra em vigor na data de sua publicação.

Assinado Eletronicamente
ELEONORA DE SOUZA SAUNIER
Presidente do TRT da 11ª Região

Processo de Gestão de Riscos de TIC

Sumário

Controle de Versões

Versão	Descrição	Data
01	Emissão inicial	10/04/2018

• FINALIDADE / CONTEXTO

Estabelecer o processo de gestão integrada de riscos de Tecnologia da Informação e Comunicações (TIC) no âmbito do Tribunal Regional do Trabalho da 11ª Região (TRT11), descrevendo as atividades de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos de TIC inerentes às atividades do Tribunal, incorporando a visão de riscos à tomada de decisões estratégicas e em conformidade com as melhores práticas de mercado

e regulamentações pertinentes.

• CAMPO DE APLICAÇÃO

Área de Tecnologia da Informação e Comunicação (TIC) do TRT da 11ª Região e suas Unidades Organizacionais, cujo trabalho seja influenciado pelos riscos de TIC.

• DEFINIÇÕES

- **Aceitar (ou assumir) o risco** – Uma forma de tratamento de risco na qual a organização decide realizar a atividade, assumindo as consequências caso o risco identificado se concretize.

- **Ameaça** – Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

- **Análise de riscos –** Processo de compreender a natureza do risco 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.

- **Apetite de risco** - Nível de risco que uma organização está disposta a aceitar para cumprir sua missão.

- **Atitude perante o risco** - Abordagem da organização para avaliar e eventualmente aceitar, mitigar, evitar ou transferir o risco.

- **Ativo** – Qualquer coisa que tenha valor para a organização. No contexto deste documento, ATIVO pode ser um processo de trabalho, um equipamento de tecnologia da informação e comunicações, uma área física, um grupo de pessoas, entre outros.

- **Avaliação de riscos** – Processo que define quais os riscos identificados no processo de análise serão aceitos ou tratados, bem como priorizar o tratamento dos mesmos.

- **Comunicação do risco** – Troca ou compartilhamento de informação sobre o risco entre o proprietário do risco e outras partes interessadas.

- **Contexto externo** - É o ambiente externo no qual o TRT11 busca atingir seus objetivos, podendo incluir:

• o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local;

• os fatores–chave e as tendências que tenham impacto sobre os objetivos da

organização;

- as relações com partes interessadas externas e suas percepções e valores.

- **Contexto interno** - O contexto interno é o ambiente interno no qual o TRT11 busca atingir seus objetivos, podendo incluir:

- governança, estrutura organizacional, funções e responsabilidades;
- políticas, objetivos e estratégias implementadas para atingi-los;
- capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);
- sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais como informais);
- relações com partes interessadas internas, e suas percepções e valores;
- cultura da organização;
- normas, diretrizes e modelos adotados pela organização;
- forma e extensão das relações contratuais.

- **Critérios de risco** - Termos de referência contra os quais a significância de um risco é avaliada. Os critérios de risco são baseados nos objetivos organizacionais e no contexto externo e contexto interno. Os critérios de risco podem ser derivados de normas, leis, políticas e outros requisitos.

- **Estimativa de riscos** – Processo utilizado para atribuir valores à probabilidade e impactos de um risco.

- **Evento** - Ocorrência ou mudança em um conjunto específico de circunstâncias.

- **Evitar o risco** – Decisão de não se envolver ou agir de forma a se retirar de uma situação de risco.

- **Gestão de Riscos** – Conjunto de processos que permite identificar e implementar medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de uma organização e equilibrá-los com os custos operacionais e financeiros envolvidos.

- **Identificação de riscos** – Processo para localizar, listar e caracterizar elementos do risco.

- **Incerteza** - Estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

- **Impacto (ou consequência)** - Resultado de um evento que afeta os objetivos.

- **Mapa de riscos** – Documento que relaciona os riscos identificados, sua origem, natureza e tipo.

- **Matriz de riscos (ou Matriz de Probabilidade x Impacto)** – Documento que especifica combinações de probabilidade de ocorrência de um risco e do impacto causado por sua ocorrência, permitindo assim calcular o nível de risco a partir da multiplicação dos valores atribuídos à probabilidade e ao impacto. Por exemplo:

Exemplo de Matriz de Riscos

Probabilidade	1 - Muito Baixo	2 - Baixo	3 - Médio	4 - Alto	5 - Muito Alto
5 - Muito alta (Probabilidade de ocorrência > 90%)	5	10	15	20	25
4 - Alta (Probabilidade de ocorrência ≥ 65% e < 90%)	4	8	12	16	20
3 - Média (Probabilidade de ocorrência ≥ 35% e < 65%)	3	6	9	12	15
2 - Baixa (Probabilidade de ocorrência ≥ 10% e < 35%)	2	4	6	8	10
1 - Muito Baixa (Probabilidade de ocorrência < 10%)	1	2	3	4	5

Impacto

- **Mitigar o risco** – Ações tomadas para reduzir a probabilidade, os impactos negativos, ou ambas, associadas a um risco.

- **Nível de risco** - Magnitude de um risco ou combinação de riscos, expressa em termos da combinação dos impactos e de suas probabilidades.

- **Parte interessada** - Pessoa ou grupo que tem um interesse no desempenho ou no sucesso de uma organização.

- **Plano de contingência de riscos** – Plano que descreve ações que devem ser tomadas caso o evento se concretize, identificando os responsáveis.

- **Plano de gestão de riscos** - Esquema dentro da estrutura da gestão de riscos que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos. Os componentes de gestão tipicamente incluem procedimentos, práticas, atribuição de responsabilidades, seqüência e cronologia das atividades. O plano de gestão de riscos pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização.

- **Plano de tratamento de riscos –** Plano que descreve as ações de

tratamento do risco, identificando os responsáveis, com o objetivo de reduzir o risco a um nível aceitável (risco residual).

- **Probabilidade** – Chance de algo acontecer.

- **Processo de avaliação de riscos -** processo completo de **análise** e **avaliação** de riscos**.**

- **Processo de trabalho -** Conjunto de atividades interrelacionadas que transforma insumos em produtos, agregando valor e atendendo à demanda do cliente**.**

- **Proprietário do risco** - Pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco.

- **Risco** – Efeito da incerteza na realização dos objetivos da organização. O risco é muitas vezes expresso em termos de uma combinação de impactos de um evento (incluindo mudanças nas circunstâncias) e a probabilidade de ocorrência associada.

- **Risco residual** - Risco remanescente após o tratamento do risco.

- **Transferir risco** – Compartilhamento com uma outra parte do ônus da perda ou do benefício do ganho associado a um risco. A transferência do risco pode ser efetuada por meio de seguro ou outros acordos. A transferência do risco pode gerar novos riscos ou modificar o risco existente.

- **Tratamento dos riscos** – Processo e implementação de ações e controles para aceitar, evitar, mitigar ou transferir um risco. Essas medidas normalmente visam trazer os níveis de risco para patamares aceitáveis, previamente estabelecidos através do critério do risco.

- **Vulnerabilidade** – Conjunto de fatores internos ou causa potencial de um evento indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de controle.

- **PAPÉIS E RESPONSABILIDADES**

- **Comitê Gestor de Segurança da Informação - CGSI**
  - Definir a Política de Gestão de Riscos e encaminhar para aprovação;
  - Elaborar o plano institucional de gestão de riscos, incluindo a definição do Processo de Gestão de Riscos;
  - Atuar como proprietário do Processo de Gestão de Riscos;
  - Monitorar, analisar criticamente e revisar a Política de Gestão de Riscos

(melhoria contínua);

- Fomentar práticas de Gestão de Risco.

• Proprietário dos processos de trabalho

- Definir quais dos seus processos de trabalho devem ser submetidos ao processo de gestão de riscos;
- Definir as diretrizes de gestão de riscos específicas de seus processos de trabalho (escopo, periodicidade/obrigatoriedade, critérios de risco, apetite de risco e designação dos papéis de gestão de riscos nos termos do processo em questão), em alinhamento com as diretrizes do Comitê Gestor de Riscos.
- Definir o contexto da análise de riscos em sua área de atuação, definindo os critérios da análise de riscos, a Matriz de Riscos (Probabilidade x Impacto) e os níveis de risco aceitáveis relevante para o contexto em análise.

• Proprietário dos riscos

- Avaliar os riscos encontrados no escopo definido;
- Revisar e aprovar o Plano de Tratamento de Riscos;
- Encaminhar o Plano de Tratamento de Riscos para o responsável pelo tratamento dos riscos;
- Auxiliar o responsável pelo tratamento dos riscos na solução de impedimentos ou dificuldades na implementação das ações de tratamento de riscos, quando necessário.
- Comunicar os riscos e o andamento das ações de tratamento às partes interessadas;
- Monitorar o Plano de Tratamentos dos Riscos.

• Analistas de Riscos

- Identificar os riscos no escopo estabelecido;
- Analisar e estimar o valor dos riscos identificados;
- Sugerir Plano de Tratamentos dos Riscos, se possível.

• Responsável pelo tratamento dos riscos

- Implementar o Plano de Tratamentos dos Riscos;
- Informar o Proprietário dos Riscos qualquer dificuldade durante a implementação das ações de tratamento de riscos;
- Informar o Proprietário dos Riscos sobre o surgimento de novos riscos a partir da implementação das ações de tratamento.

4.4. Partes Interessadas

- Manter-se informada sobre os riscos.

- **Matriz RACI**

Atividades	Comitê Gestor de Segurança da Informação	Proprietário dos processos de trabalho	Analistas de Riscos	Proprietários dos Riscos	Responsável pelo tratamento dos riscos	Partes Interessadas
Definira Política de Gestão de Riscos e encaminhar para aprovação	R/A	I		I		C
Elaborar o plano institucional de gestão de riscos, incluindo a definição do Processo de Gestão de Riscos	R/A	C		I		I
Monitorar, analisar criticamente e revisar a Política de Gestão de Riscos (melhoria contínua)	R/A	C		C		I
Definir quais dos seus processos de trabalho devem ser submetidos ao processo de gestão de riscos		R/A		C		C
Definir as diretrizes de gestão de riscos específicas de seus processos de trabalho (escopo, periodicidade/obrigatoriedade, critérios de risco, apetite de risco e designação dos papéis de gestão de riscos nos termos do processo em questão)		R/A		C		C
Definir o contexto da análise de riscos em sua área de atuação		R/A		C		C
Estabelecer o plano de gestão de riscos, definindo os critérios da análise de riscos, a Matriz de Riscos (Probabilidade x Impacto) e os níveis de risco aceitáveis e inaceitáveis relevante para o contexto em análise		R/A		C		

Identificar os riscos no escopo estabelecido		C	R/A	C		
Analisar e estimar o valor dos riscos identificados no escopo estabelecido		C	R/A	C		
Avaliar os riscos encontrados no escopo definido			C	R/A		
Elaborar o Plano de Tratamentos dos Riscos			R	R/A	I	
Comunicar os riscos às partes interessadas				R/A		I
Monitorar o Plano de Tratamento dos Riscos				R/A	C	I
Implementar o Plano de Tratamentos dos Riscos				A	R	

Legenda: A – Aprova; R – Responsável pela execução; I – Informado; C – Consultado

- **PROCESSO DE GESTÃO DE RISCOS DE TIC**

- **Considerações gerais**

- A Gestão de Riscos de TIC no TRT11 deve considerar os seguintes princípios estabelecidos pela norma ABNT NBR ISO31000:2009:

  - A gestão de riscos de TIC cria e protege valor.

  A gestão de riscos contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho referente, por exemplo, à segurança da informação, à conformidade legal e regulatória, ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação.

  - A gestão de riscos de TIC é parte integrante de todos os processos organizacionais.

  A gestão de riscos de TIC não é uma atividade autônoma separada das principais atividades e processos da organização. A gestão de riscos de TIC faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças.

  - A gestão de riscos de TIC é parte da tomada de decisões.

  A gestão de riscos auxilia os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação.

- A gestão de riscos de TIC aborda explicitamente a incerteza.

A gestão de riscos explicitamente leva em consideração a incerteza, a natureza dessa incerteza, e como ela pode ser tratada.

- A gestão de riscos de TIC é sistemática, estruturada e oportuna.

Uma abordagem sistemática, oportuna e estruturada para a gestão de riscos de TIC contribui para a eficiência e para os resultados consistentes, comparáveis e confiáveis.

- A gestão de riscos de TIC baseia-se nas melhores informações disponíveis.

As entradas para o processo de gerenciar riscos são baseadas em fontes de informação, tais como dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões, e opiniões de especialistas. Entretanto, convém que os tomadores de decisão se informem e levem em consideração quaisquer limitações dos dados ou modelagem utilizados, ou a possibilidade de divergências entre especialistas.

- A gestão de riscos de TIC é feita sob medida.

A gestão de riscos está alinhada com o contexto interno e externo do TRT11 e com o perfil do risco.

- A gestão de riscos de TIC considera fatores humanos e culturais.

A gestão de riscos de TIC reconhece as capacidades, percepções e intenções do pessoal interno e externo que podem facilitar ou dificultar a realização dos objetivos do TRT11.

- A gestão de riscos de TIC é transparente e inclusiva.

O envolvimento apropriado e oportuno de partes interessadas e, em particular, dos tomadores de decisão em todos os níveis da organização assegura que a gestão de riscos permaneça pertinente e atualizada. O envolvimento também permite que as partes interessadas sejam devidamente representadas e terem suas opiniões levadas em consideração na determinação dos critérios de risco.

- A gestão de riscos de TIC é dinâmica, iterativa e capaz de reagir a mudanças.

A gestão de riscos de TIC continuamente percebe e reage às mudanças. Na medida em que acontecem eventos externos e internos, o contexto e o

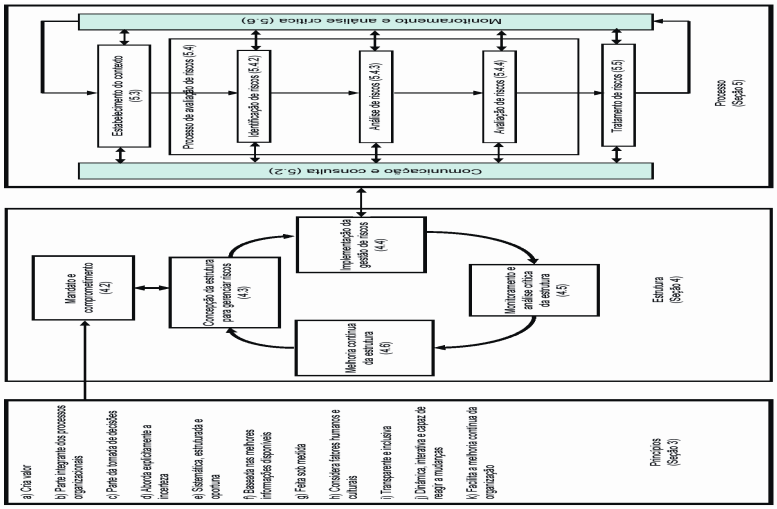
conhecimento modificam-se, o monitoramento e a análise crítica de riscos são realizados, novos riscos surgem, alguns se modificam e outros desaparecem.

- A gestão de riscos de TIC facilita a melhoria contínua da organização.

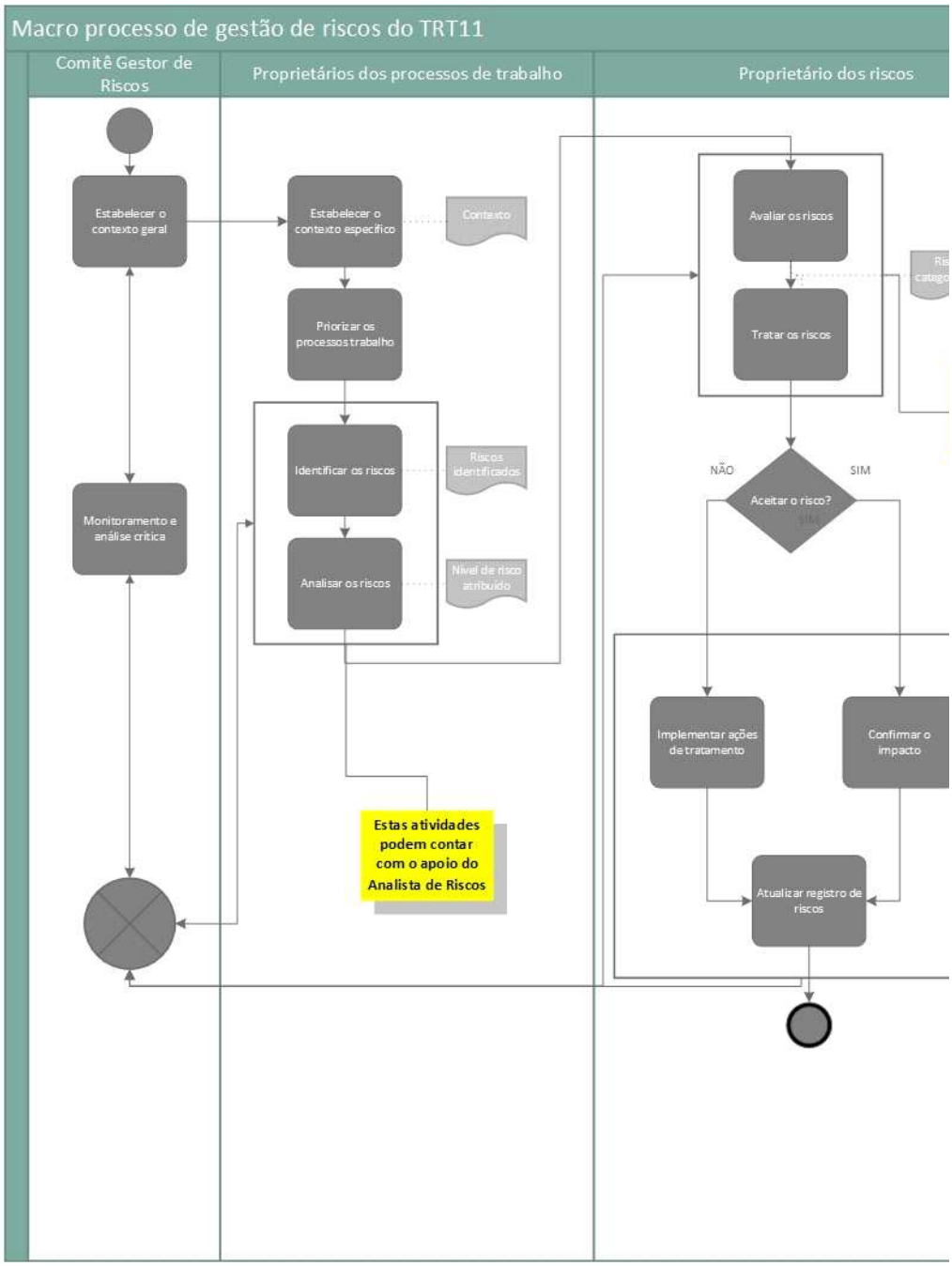
Convém que as organizações desenvolvam e implementem estratégias para melhorar a sua maturidade na gestão de riscos de TIC juntamente com todos os demais aspectos da sua organização.

- **Descrição do Processo**

- O processo gestão de riscos de TIC do TRT11 é composto pelas seguintes etapas:
  - Estabelecimento do contexto de riscos;
  - Avaliação de riscos (Subdividido em identificação, análise e avaliação de riscos);
  - Tratamento de riscos;
  - Comunicação e consulta;
  - Monitoramento e análise crítica.
- Este modelo está formalizado na norma brasileira ABNT NBR ISO 31000:2009, conforme o diagrama abaixo:



- O macro fluxo do processo de gestão de riscos de TIC do TRT11 está apresentado na figura abaixo:



- **Estabelecimento do contexto de riscos**

  - O estabelecimento do contexto inclui a definição do contexto externo, interno e de gestão de riscos e a classificação dos critérios de risco:

• Estabelecer o contexto externo envolve a familiarização com o ambiente em que o TRT11 opera, incluindo:

  - os fatores culturais, políticos, legais, regulatórios, financeiros, econômicos e ambientais competitivos, seja em nível internacional, nacional, regional ou local;
  - fatores–chave e tendências que tenham impacto sobre os

objetivos da organização;

- percepções e valores das partes interessadas externas.

- Estabelecer o contexto interno envolve o entendimento:
    - dos objetivos e das estratégias que estão em vigor a fim de atingi–los;
    - das capacidades do TRT11 em termos de recursos e conhecimento;
    - dos fluxos de informação e processos de tomada de decisão;
    - das partes interessadas internas;
    - das percepções, valores e cultura;
    - das políticas e processos;
    - de normas e modelos de referência adotados pelo TRT11;
    - das estruturas (por exemplo, governança, papéis e responsabilizações).
- Estabelecer o contexto do processo de gestão de riscos inclui:
    - a definição de responsabilizações e responsabilidades;
    - a definição da extensão das atividades de gestão de riscos a serem conduzidas, contemplando inclusões e exclusões específicas;
    - a definição da extensão do projeto, processo, função ou atividade em termos de tempo e local;
    - a definição das relações entre um projeto ou atividade específicos e outros projetos ou atividades da organização;
    - a definição das metodologias do processo de avaliação de riscos;
    - a definição dos critérios de risco;
    - a definição de como o desempenho na gestão de riscos é avaliado;
    - a identificação e a especificação das decisões e ações que precisam ser tomadas;
    - identificação dos estudos necessários para escopo ou enquadramento, sua extensão e objetivos;
    - os recursos requeridos para tais estudos.
- Definir os critérios de risco envolve decidir:
    - a natureza e os tipos de consequências a serem incluídos e como eles serão medidos;
    - a forma como as probabilidades devem ser expressas;

- como um nível de risco será determinado;
- os critérios pelos quais será decidido quando um risco necessita de tratamento;
- os critérios para decidir quando um risco é aceitável e/ou tolerável;
- se e como as combinações de riscos serão levadas em consideração.

- Os critérios podem ser baseados em fontes tais como
    - objetivos acordados do processo;
    - critérios identificados em especificações;
    - fontes gerais de dados;
    - critérios setoriais geralmente aceitos, tais como os níveis de integridade de segurança;
    - apetite ao risco do TRT11;
    - requisitos legais e outros requisitos para equipamentos ou aplicações específicos.
- Cabe ao Proprietário dos Processos de Trabalho descrever o contexto de gestão de riscos dentro do seu âmbito de atuação de acordo com os requisitos anteriores.
- A descrição do contexto de gestão de riscos deve conter, no mínimo:

- O propósito da análise de riscos;
- Identificação do ativo objeto da análise de riscos que pode ser, por exemplo, entre outros:
- Uma aplicação de TI;
- Planos estratégicos de TIC;
- Contratações de TIC;
- Projetos médios ou grandes
- A infraestrutura de TI;
- Um processo de trabalho;
- Um setor ou área física;
- Um grupo de servidores que efetuam atendimento ao público.
- Os critérios de risco a considerar, que incluem:
- Os pontos de vista das partes interessadas;
- O nível aceitável de risco;
- A periodicidade ou obrigatoriedade da análise (anual, semestral, etc.);
- A Matriz de Risco.
- A designação dos papéis e responsabilidades para a gestão de riscos.

- Opcionalmente também podem ser identificados:

• O valor estratégico do ativo analisado;

• A criticidade do ativo;

• O histórico de ocorrência de eventos de risco com o ativo;

• Avaliação do contexto interno e externo que influenciam ou podem ser influenciados pelo ativo analisado;

• Informações históricas relevantes no escopo a analisar (por exemplo, sobre vulnerabilidades ou falhas conhecidas).

- **Processo de Avaliação de Riscos**

  - Identificação dos riscos de TIC

• As atividades da fase de identificação dos riscos são executadas pelo analista de risco e compreendem:

  - Identificar os ativos de TIC e seus respectivos responsáveis dentro do contexto estabelecido;

• Identificar os riscos associados aos ativos no contexto definido, considerando:

• As ameaças ou fontes de risco envolvidas;

• As vulnerabilidades existentes nos ativos;

• As ações de segurança e controle já adotadas.

• Elaborar um Registro do Risco descrevendo qual é o risco, uma descrição do risco e quais vulnerabilidade e/ou ameaças relacionadas ao risco.

• O Anexo 1 ilustra exemplos genéricos de tipos de riscos dentro dos contextos externos e internos de uma organização.

• O Anexo 2 ilustra exemplos de técnicas de identificação de riscos.

  - Análise de riscos

• Nesta fase o analista de risco atribui um nível (ou valor) para os riscos encontrados durante a fase de *Identificação dos Riscos*.

• O nível do risco é calculado pela fórmula *Risco = Probabilidade x Impacto*, com os valores de Probabilidade e Impacto obtidos na Matriz de Risco estabelecida para a análise.

• Opcionalmente o analista de risco pode sugerir a avaliação dos riscos analisados e um Plano de Tratamentos desses riscos;

• O analista de risco deve atualizar o formulário de registro e análise de riscos de cada risco, indicando o valor de cada risco relacionado.

- Avaliação de riscos

- A avaliação dos riscos é executada pelo Proprietário dos Riscos que deve:
    - Avaliar os riscos em função do valor obtido para cada risco durante a fase de *Análise de riscos*, determinando se são aceitáveis ou se requerem tratamento;
      Nota: Caso o analista de riscos já tenha sugerido uma avaliação e um plano de tratamento, o Proprietário dos Riscos deve validar/revisar a sugestão do analista.

- Relacionar os riscos que necessitam de tratamento, priorizando-os de acordo com o apetite para o risco estabelecido no contexto de gestão de riscos;
    - Definir e justificar sua atitude perante o risco (aceitar, evitar, mitigar ou transferir);
    - Elaborar um plano de tratamento dos riscos e um plano de contingência, observando:

- A eficácia das ações de segurança e de controle já existentes;
- As restrições organizacionais, técnicas e estruturais;
- Os requisitos legais;
- A análise custo/benefício.
    - Encaminhar os riscos que devem ser tratados para o responsável pelo tratamento dos riscos.

- O plano de tratamento dos riscos deve conter:
- Ação de tratamento;
- Responsável;
- Prazo;
- Monitoramento.
- O plano de tratamento dos riscos pode conter, opcionalmente:
- Por quê? – a importância da implementação do controle;
- Como? – a descrição de como implementar o controle;
- Onde? – o local para implementação do controle;
    - Quanto custa? – o valor em reais ou em H/H (homem hora) para a implementação do controle (opcional).

- **Tratamento de riscos**

- O responsável pelo tratamento de riscos deve implementar as ações de

tratamento estabelecidas no Plano de Tratamento de Riscos.

• O Proprietário do Risco deve monitorar as atividades de tratamento de riscos, garantindo a tempestiva implementação das ações de tratamento e atuando de forma a resolver impedimentos ou dificuldades que possam impactar a implementação por parte do responsável.

- **Comunicação e consulta**

• O Proprietário do Risco deve manter as partes interessadas informadas a respeito de todas as fases da gestão de risco, compartilhando informações relevantes com essas partes.

• O responsável pelo tratamento dos riscos deve informar o Proprietário do Risco sobre qualquer dificuldade que possa interferir na implementação das ações de tratamento dos riscos.

• Deve-se realizar a divulgação de informações sobre os riscos que foram identificados tenham eles sido tratados ou não, a todas as partes interessadas que precisem ter conhecimento a respeito deles.

- **Monitoramento e análise crítica**

• O monitoramento e análise crítica tratam da revisão e análise periódica da gestão de riscos, objetivando o aprimoramento contínuo do processo no TRT11.

• A atividade de monitoramento deve ser efetuada por meio da verificação regular, no mínimo, dos seguintes fatores:

• As respostas ao risco estão sendo implementadas como planejadas;

• As ações de respostas ao risco estão eficazes como esperadas ou se novas respostas devem ser desenvolvidas;

• Surgimento de riscos que não foram identificados anteriormente;

• Riscos que deixaram de existir;

• Se o risco residual está dentro do apetite de risco do TRT11;

• Mudanças no contexto interno ou externo que podem gerar mudanças no contexto de riscos;

• Mudanças nos fatores de risco (ameaça, vulnerabilidade, probabilidade e impacto).

• A análise crítica do processo de gestão de riscos será feita no contexto de melhoria contínua dos processos do TRT11 e deve ser efetuada por meio de reuniões periódicas dos responsáveis pelo processo onde são avaliados:

• Resultados de indicadores;

• Mudanças no contexto interno e externo que possam influenciar nos critérios de gestão de risco estabelecidos;

• Resultados obtidos com a implementação de ações de tratamento de riscos.

• **ENTRADAS / SAÍDAS**

Atividade	Quem executa	Entradas	Saídas
6.2.4. Estabelecimento do contexto de riscos	Proprietário dos processos de negócio	Informações sobre o contexto interno e externo do TRT11; Objetivos estratégicos do TRT11; Objetivos acordados do processo; Critérios identificados em especificações; Fontes gerais de dados; Critérios setoriais geralmente aceitos, tais como os níveis de integridade de segurança; Apetite ao risco do TRT11; Requisitos legais e outros requisitos para equipamentos ou aplicações específicos.	Contexto de gestão de riscos.
6.2.5. Processo de Avaliação de Riscos			

Identificação dos riscos	Analista de riscos	Contexto de gestão de riscos.	Riscos identificados; Formulários para registro e análise de riscos preenchido com lista de riscos no escopo.
Análise de riscos	Analista de riscos	Formulários para registro e análise de riscos preenchido com lista de riscos no escopo.	Nível de risco estabelecido; Formulário para registro e análise de riscos atualizado.
Avaliação de riscos	Proprietário dos riscos	Formulário para registro e análise de riscos atualizado.	Riscos aceitos; Riscos a tratar; Plano de tratamento de riscos.
6.2.6. Tratamento de riscos	Responsável pelo tratamento dos riscos	Plano de Tratamento de Riscos.	Situação das ações de tratamento de riscos; Riscos tratados.
6.2.7. Comunicação e consulta	Proprietário dos riscos	Plano de Tratamento de Riscos; Situação das ações de tratamento de risco oriundas do Responsável pelo tratamento de riscos.	Atas de reunião; Situação das ações de tratamento de riscos para partes interessadas.

6.2.8. Monitoramento e análise crítica	Comitê Gestor de Segurança da Informação	Informações sobre ações de tratamento de risco implementadas; Surgimento de riscos que não foram identificados anteriormente; Riscos que deixaram de existir; Mudanças no contexto interno ou externo que podem gerar mudanças no contexto de riscos; Mudanças nos fatores de risco (ameaça, vulnerabilidade, probabilidade e impacto); Informações sobre indicadores do processo de gestão de risco.	Atas de reuniões de análise crítica; Recomendações de melhoria do processo de gestão de riscos.

- **DOCUMENTOS DE REFERÊNCIA**

  - ABNT NBR ISO 31000:2009 - Gestão de riscos - Princípios e diretrizes
  - ABNT NBR ISO 31010:2012 – Gestão de riscos – Técnicas para o processo de avaliação de riscos

- Norma Complementar nº 04/IN01/DSIC/GSIPR - GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, Revisão 01, de 15 de fevereiro de 2013.

- Política de Segurança da Informação do TRT da 11ª Região

- **ANEXOS**

- **Anexo 1 - Exemplos genéricos de tipos de riscos**

Tipos de Riscos	
Contexto Externo	**Contexto Interno**

Econômicos Disponibilidade de capital Emissões de crédito, inadimplência Concentração Liquidez Mercados financeiros Desemprego Concorrência Fusões / aquisições **Socioambientais** Emissões e dejetos Energia Desenvolvimento sustentável **Sociais** Características demográficas Comportamento do consumidor Cidadania corporativa Privacidade Terrorismo **Tecnológicos** Interrupções Comércio eletrônico Dados externos Tecnologias emergentes **Naturais** Desastres naturais **Legal/Regulatório** Multas, sanções aplicadas por órgãos reguladores	**Riscos Estratégicos** Visão estratégica mal compreendida Plano estratégico não definido Estrutura organizacional inapropriada Falta de integração entre processos organizacionais Partes interessadas não identificadas Falta de apoio da alta direção Ausência do Plano de continuidade de negócios **Riscos de TI** Requisitos de Segurança da Informação não definidos Falta de integração dos Sistemas de TI Ausência do controle de acesso aos Sistemas de TI Obsolescência dos Sistemas de TI Sistemas de TI não escalonáveis Falhas nos projetos de TI **Riscos Físicos e Ambientais** Falta de manutenção da estrutura física Ataques terroristas Desastres naturais **Riscos de Conformidade e Contratuais** Ausência de legislação interna Desconformidade com a legislação externa Existência de cláusulas contratuais exorbitantes Mudanças nos requisitos de entrega dos serviços Entrega dos serviços em desconformidade com os requisitos Ingerência das relações com fornecedores **Riscos Operacionais e de Recursos Humanos** Responsáveis por atividades operacionais não definidos Falta de execução dos testes do plano de recuperação de desastres Funções e responsabilidades não segregadas

- **Anexo 2 - Exemplos de técnicas de identificação de riscos**

A metodologia de identificação de riscos emprega uma combinação de técnicas como ferramentas de apoio. Por exemplo, a administração do TRT11 poderá utilizar seminários interativos em grupo como parte de seu método de identificação de riscos, com um facilitador utilizando alguma ferramenta para assessorar os participantes.

As técnicas de identificação de eventos de risco examinam tanto o passado quanto o futuro e apresentam grande variação quanto à sofisticação; enquanto muitas das técnicas mais sofisticadas são específicas ao próprio ramo de atividades das organizações, a maior parte é obtida mediante uma abordagem simples.

Por exemplo, tanto as indústrias de serviços financeiros, de saúde e de segurança empregam técnicas de rastreamento de eventos de perda. Essas técnicas iniciam-se com foco no histórico de eventos comuns para, então, alimentar esses dados em modelos de projeção mais sofisticados. As organizações mais avançadas em termos de gerenciamento de riscos corporativos utilizam uma combinação de técnicas que aliam eventos passados e potenciais eventos futuros. As técnicas também variam de acordo com o nível onde são utilizadas na organização.

Apresentamos abaixo exemplos de técnicas de identificação de riscos.

Técnica	Descrição

Brainstorming	Técnica de geração de idéias em grupo dividida em duas fases: 1) fase criativa, onde os participantes apresentam o maior número possível de idéias; 2)fase crítica, onde cada participante defende sua idéia com o objetivo de convencer os demais membros do grupo. Na segunda fase são filtradas as melhores idéias, permanecendo somente aquelas aprovadas pelo grupo. A técnica é composta de quatro regras básicas: 1) As críticas devem ser banidas – a avaliação das idéias deve ser guardada para momentos posteriores; 2) A geração livre de idéias deve ser encorajada; 3) Foco na quantidade – quanto maior o número de idéias, maiores as chances de se ter idéias válidas; 4) Combinação e aperfeiçoamento de idéias geradas pelo grupo.
Técnica Delphi	Esta técnica de criação de consenso utiliza respostas escritas ao invés de reunir pessoalmente os membros do grupo, ou ainda método para a sistemática coleta e comparação crítica de julgamentos, de participantes anonimamente isolados, sobre um tópico, através de um conjunto de questionários cuidadosamente desenvolvidos, intercalados com informações sumarizadas e "feedback" das opiniões, derivadas das respostas anteriores.
Entrevista/Julgamento de Especialistas	Entrevistas livres, semi-estruturadas ou estruturadas conduzidas individualmente ou em grupo com especialistas no assunto em questão.
Identificação de Causa	Processo desenhado usado na investigação e categorização das causas essenciais de um risco, sendo dividida em quatro etapas, a saber: coleta de dados; diagramação do fator de causa; identificação da causa raiz e geração da recomendação e implementação.

Análise SWOT (“strengths”, “weaknesses”, “opportunities”, “threats”)	Acrônimo para “Strengths, Weakness, Opportunities and Threats”, que em português podemos traduzir como Forças, Fraquezas, Oportunidades e Ameaças. É uma ferramenta de planejamento estratégico, utilizada para análise de projetos e/ou negócios, ou em qualquer outra situação que envolva uma decisão. A aplicação da técnica consiste na avaliação do projeto sob cada uma das quatro perspectivas - forças, fraquezas, oportunidades e ameaças - geralmente apresentadas em forma de quadrantes.
“Checklist”	Consiste em uma lista de itens, que vão sendo marcados como sim ou não, podendo ser utilizada por um membro da equipe, em grupo ou em uma entrevista.
Diagrama de Causa e Efeito	O Diagrama de Causa e Efeito é também conhecido como Diagrama de Ishikawa ou Espinha-de-peixe, e é útil para a identificação da causa dos riscos. O diagrama é montado organizando o efeito à direita e as causas à esquerda. Para cada efeito existem categorias de causas. As causas principais podem ser agrupadas por estas categorias.
Fluxograma	Representação gráfica que apresenta os passos de um processo. Assim, esta técnica é aplicada para compreender como os riscos, ou os elementos de um sistema se inter-relacionam.
Diagrama de Influência	Representação gráfica contendo nós que representam as variáveis da decisão de um problema. Um diagrama de influência tradicional é composto por três tipos de nós: decisão, incerteza, resultado; e por dois tipos de relação entre os nós: relação causal e relação de precedência. A relação causal ocorre entre os elementos de resultado e de incerteza e indica uma dependência probabilística. A relação de precedência ocorre entre elementos de decisão e representam precedência de tempo.

Técnica de Grupo Nominal	A técnica o grupo nominal foi elaborada para ser utilizada na área de planejamento, com o objetivo de ampliar a produção criativa do grupo, facilitar as decisões em equipe, estimular a geração de ideias críticas e servir como instrumento de agrupamento de ideias. Assim sendo, esta técnica corresponde na geração silenciosa de ideias escritas; Exposição das ideias geradas ao grupo na forma de frases simples em cartões ou tiras de papel; Discussão de cada ideia registrada para esclarecimento e avaliação; Votação individual das ideias em ordem de prioridade, com a decisão do grupo sendo trabalhada matematicamente através da classificação por quantidade de votos obtidos ou ordenação por ordem de prioridade.
"Pondering"	Abordagem simples e muito básica, que envolve uma só pessoa para identificar os riscos, e pode servir como uma opção padrão quando nenhuma outra abordagem é possível. Entretanto, faz-se necessário que a pessoa tenha vivência e experiência na área onde estão sendo identificados os riscos. Na aplicação desta técnica a pessoa sozinha reflete, pondera ou considera o problema, gerando a lista de opções.

- **Anexo 3 – Análise de risco com o Módulo Risk Manager®**

A ferramenta utilizada para análise de risco no TRT11 é o Módulo Risk Manager®. Esta contém uma metodologia de cálculo de Risco aderente à norma ABNT NBR ISO 31000:2009 - Gestão de riscos - Princípios e diretrizes. A metodologia utilizada no Módulo Risk Manager® permite que o cálculo do risco seja aplicável a elementos tecnológicos, processuais e comportamentais da instituição.

O Módulo Risk Manager® utiliza um método de Análise de Riscos qualitativa que calcula um índice ("rating") denominado **PSR**® (**P**robabilidade, **S**everidade e **R**elevância). Este índice define o Risco para cada Controle ausente encontrado na Análise. Da fórmula do Risco:

RISCO = PROBABILIDADE X IMPACTO

No Módulo Risk Manager®, o valor do impacto no negócio é atendido pelas duas variáveis S e R, Severidade e Relevância respectivamente, e esta

fórmula do Risco é calculada então pela seguinte equação:

RISCO = PROBABILIDADE X SEVERIDADE X RELEVÂNCIA

PSR®

Em conformidade com a ISO Guide 73, que define o risco como "a combinação da probabilidade de um evento e sua consequência", o Módulo Risk Manager® considera para cálculo do risco um índice (PSR®) que representa a estimativa destes fatores.

Este valor PSR® representa o grau de risco associado à ausência de um controle, sendo calculado pela equação Risco = Probabilidade x Severidade x Relevância, onde os fatores da Probabilidade e Severidade são pontuados durante as análises técnicas, e a Relevância pontuada considerando-se a visão do negócio, em termos da relevância do ativo para a organização.

Assim, o Risco associado a cada Controle ausente é calculado multiplicando-se os três fatores básicos, e o resultado é um valor numérico entre 1 e 125, com seu nível variando conforme o resultado desta multiplicação:

Nível de Risco	Valores Possíveis PSR®
Muito Baixo	1, 2, 3, 4, 5,6
Baixo	8, 9, 10, 12, 15,16
Médio	18, 20, 24, 25, 27,30
Alto	32, 36, 40, 45, 48,50
Muito Alto	60, 64, 75, 80, 100,125

O PSR® representa o índice para o cálculo do Risco no Módulo Risk Manager®. Para os ativos, o seu índice de Risco é o resultado da soma algébrica do PSR® dos Controles ausentes em seus componentes.

O PSR® de um ativo é o resultado da soma dos PSR® de seus Controles não implementados.

Apesar de o risco técnico (binômio Probabilidade e Severidade) da ausência do Controle ser importante para os gestores de tecnologia, para a Análise de Riscos e, consequentemente, para a Segurança da Informação, o que importa é considerar o Risco ao negócio como fator de priorização de ações (pois considera o fator Relevância do Ativo).

A Matriz a seguir segue como referência para se estabelecer uma pontuação adequada para cada um dos fatores do PSR®. É importante frisar que esta matriz serve como instrumento de sintonia do senso comum, de forma a substituir avaliações subjetivas por critérios mais objetivos para cada um dos fatores do PSR®, transformando-os em valores de 1 a 5.

	PSR			
	Probabilidade A ocorrência da vulnerabilidade ser explorada pelas ameaças	**Severidade** A consequência de a vulnerabilidade ser explorada pelas ameaças	**Relevância** O comprometimento da segurança dos ativos	
5	É quase certa (> 95%)	Afetará extremamente a segurança	Pode afetar todo a instituição	Muito Alta
4	É muito provável (65% ≤ P < 95%)	Afetará muito gravemente a segurança	Pode afetar um ou mais negócios da instituição e os prejuízos serão muito altos	Alta
3	É provável (35% ≤ P < 65%)	Afetará gravemente a segurança	Pode afetar uma parte do negócio da instituição e os prejuízos serão razoáveis	Média
2	É improvável (5% ≤ P < 35%)	Afetará pouco a segurança	Pode afetar uma parte pequena e localizada do negócio da instituição e os prejuízos serão baixos	Baixa
1	É muito improvável (< 5%)	Quase não afetará a segurança	Pode afetar uma parte muito pequena do negócio da instituição e os prejuízos serão desprezíveis	Muito Baixa

A somatória de todos os PSRs dos controles não implementados, divididos pelo total dos PSRs dos controles aplicáveis e multiplicados por 100, nos fornece o índice risco (Risk Index).

No que se refere a Conformidade, e de forma análoga, o total de controles implementados dividido pelo total de controles aplicáveis, multiplicado por 100, nos fornece o índice de conformidade (Compliance Index).

- **ANEXO 4 - Interpretação do PSR para o Tratamento dos Riscos**

O TRT11 utiliza a seguinte interpretação dos resultados do PSR® para o Tratamento dos Riscos

Nível de Risco do Controle PSR®	Interpretação
Muito Alto	São Riscos inaceitáveis, e os gestores dos ativos devem ser orientados para que os tratem imediatamente.
Alto	São Riscos inaceitáveis e os gestores dos ativos devem ser orientados para, ao menos, controlá-los.

Médio	São Riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos, contudo a aceitação do Risco deve ser feita por meios formais.
Baixo	São Riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos.
Muito Baixo	São Riscos aceitáveis e devem ser informados para os Gestores dos ativos.

- **Anexo 5 - Indicadores de Gestão de Riscos propostos para o TRT11**

Abaixo são apresentadas sugestões de indicadores para monitoramento e avaliação do desempenho do processo de gestão de riscos. Essas sugestões devem ser avaliadas pelo TRT11 para definição dos indicadores que serão implementados.

Risk Index Consolidado	
Itens	**Detalhes**
Objetivo Estratégico	Permitir ao CGR visualizar o nível consolidado de riscos de todos os ativos, sistemas e processos de negócio do TRT11, incluídos no escopo da análise de riscos.
Métrica (s)	Percentual (%) de PSR dos controles não implementados dos ativos do escopo da análise de riscos.
Frequência de Medição	Anual.
Meta (s)	Deverá ser definida pelo CGR. **Sugestão: 50%.**
Fórmula (s)	Este indicador é calculado dividindo-se o total de riscos dos controles não implementados (PSR existente) pelo total de riscos dos controles aplicáveis (PSR total).
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager.

Risk Index por Área de Negócio	
Itens	**Detalhes**
Objetivo Estratégico	Permitir ao CGR visualizar os níveis de risco de todos os ativos, sistemas e processos de negócio incluídos no escopo da análise de riscos, totalizados por área.
Métrica (s)	Percentual (%) de PSR dos controles não implementados dos ativos do escopo da análise de riscos, agrupados por área.
Frequência de Medição	Anual.

Meta (s)	Deverá ser definida pelo CGR. **Sugestão: 50%.**
Fórmula (s)	Este indicador é calculado dividindo-se o total de riscos dos controles não implementados (PSR existente) pelo total de riscos dos controles aplicáveis (PSR total).
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager.

Risk Index por Processo de Negócio	
Itens	**Detalhes**
Objetivo Estratégico	Permitir às áreas de negócio visualizarem os níveis de risco de todos os processos de negócio incluídos no escopo da análise de risco, permitindo priorizar as ações de segurança de forma alinhada aos negócios.
Métrica (s)	Percentual (%) de PSR dos controles não implementados dos ativos do escopo da análise de riscos, agrupados por processo de negócio.
Frequência de Medição	Semestral.
Meta (s)	Deverá ser definida pelas áreas de negócio. **Sugestão: 60%.**
Fórmula (s)	Este indicador é calculado dividindo-se o total de riscos dos controles não implementados (PSR existente) pelo total de riscos dos controles aplicáveis (PSR total).
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager,

Risk Index por Sistema/Serviço	
Itens	**Detalhes**
Objetivo Estratégico	Permitir à SETIC visualizar os níveis de risco de todos os sistemas e serviços incluídos no escopo da análise de risco, permitindo combater vulnerabilidades de forma proativa.
Métrica (s)	Percentual (%) de PSR dos controles não implementados dos ativos do escopo da análise de riscos, agrupados por sistema ou serviço.
Frequência de Medição	Semestral.
Meta (s)	Deverá ser definida pela SETIC. **Sugestão: 60%.**
Fórmula (s)	Este indicador é calculado dividindo-se o total de riscos dos controles não implementados (PSR existente) pelo total de riscos dos controles aplicáveis (PSR total).
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager,

Risk Index por Ativo

Itens	Detalhes
Objetivo Estratégico	Permitir à SETIC visualizar os níveis de risco de todos os ativos incluídos no escopo da análise de risco, permitindo combater vulnerabilidades de forma proativa em ativos de tecnologia, ambientes, processos e pessoas.
Métrica (s)	Percentual (%) de PSR dos controles não implementados de cada ativo do escopo da análise de riscos.
Frequência de Medição	Semestral.
Meta (s)	Deverá ser definida pela SETIC. **Sugestão: 60%.**
Fórmula (s)	Este indicador é calculado dividindo-se o total de riscos dos controles não implementados (PSR existente) pelo total de riscos dos controles aplicáveis (PSR total).
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager,

Compliance Index Consolidado	
Itens	**Detalhes**
Objetivo Estratégico	Permitir ao CGR visualizar o nível consolidado de conformidade de todos os ativos, sistemas e processos de negócio do TRT11, incluídos no escopo da análise de riscos.
Métrica (s)	Percentual (%) de controles implementados dos ativos do escopo da análise de riscos.
Frequência de Medição	Anual.
Meta (s)	Deverá ser definida pelo CGR. **Sugestão: 50%.**
Fórmula (s)	Este indicador é calculado dividindo-se a quantidade total de controles implementados pela quantidade total de controles aplicáveis.
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager,

Compliance Index por Área de Negócio	
Itens	**Detalhes**
Objetivo Estratégico	Permitir ao CGR visualizar o nível consolidado de conformidade de todos os ativos, sistemas e processos das áreas de negócio do TRT11, incluídos no escopo da análise de riscos.
Métrica (s)	Percentual (%) de controles implementados dos ativos do escopo da análise de riscos, agrupados por área de negócio.
Frequência de Medição	Anual.
Meta (s)	Deverá ser definida pelo CGR. **Sugestão: 50%.**

Fórmula (s)	Este indicador é calculado dividindo-se a quantidade total de controles implementados pela quantidade total de controles aplicáveis.
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager,

Compliance Index por processo de negócio	
Itens	**Detalhes**
Objetivo Estratégico	Permitir ao CGR visualizar o nível consolidado de conformidade de todos os ativos e sistemas agrupados por processos das áreas de negócio, incluídos no escopo da análise de riscos.
Métrica (s)	Percentual (%) de controles implementados dos ativos do escopo da análise de riscos, agrupados por processo de negócio.
Frequência de Medição	Semestral.
Meta (s)	Deverá ser definida pela Gestão da área de negócio em conjunto com o CGR. **Sugestão: 60%.**
Fórmula (s)	Este indicador é calculado dividindo-se a quantidade total de controles implementados pela quantidade total de controles aplicáveis.
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager,

Compliance Index por sistema/serviço	
Itens	**Detalhes**
Objetivo Estratégico	Permitir à SETIC visualizar o nível consolidado de conformidade de todos os ativos agrupados por sistemas ou serviços incluídos no escopo da análise de risco (tecnologia, ambientes, processos e pessoas).
Métrica (s)	Percentual (%) de controles implementados dos ativos do escopo da análise de riscos, agrupados por sistema ou serviço.
Frequência de Medição	Semestral.
Meta (s)	Deverá ser definida pela SETIC. **Sugestão: 60%.**
Fórmula (s)	Este indicador é calculado dividindo-se a quantidade total de controles implementados pela quantidade total de controles aplicáveis.
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager,

Compliance Index por ativo	
Itens	**Detalhes**

Objetivo Estratégico	Permitir à SETIC visualizar os níveis de conformidade de todos os ativos incluídos no escopo da análise de risco (tecnologia, ambientes, processos e pessoas).
Métrica (s)	Percentual (%) de controles implementados dos ativos do escopo da análise de riscos, agrupados por ativo.
Frequência de Medição	Semestral.
Meta (s)	Deverá ser definida pela SETIC. **Sugestão de 60%**
Fórmula (s)	Este indicador é calculado dividindo-se a quantidade total de controles implementados pela quantidade total de controles aplicáveis.
Fonte de Informação	Relatório de Análise de Riscos – RAR, Modulo Risk Manager,

- **Anexo 6 – Estabelecimento do contexto geral de gestão de riscos do TRT11**

O estabelecimento do contexto tem como propósito definir os fatores, internos e externos, e os critérios de riscos para os quais os riscos deverão ser geridos. A definição desses fatores parametrizará a atuação das demais atividades que compõem o processo de gestão de riscos do TRT11. As informações abaixo podem servir de base para criação do Plano de Gestão de Riscos do TRT11 pelo Comitê Gestor de Riscos.

- **Fatores internos e externos**

Ficam definidas as seguintes categorias de eventos: Conformidade e Fiscalização, Regulamentação, Recursos Humanos, Fornecedores, Tecnologia da Informação, Desastres, Controles Físicos, Reputação, Cultura Organizacional, Ambiente Cultural, Social e Político e Econômicos. Tais categorias estão distribuídas pelos contextos externo e interno, conforme tabela abaixo.

Contexto Interno	Contexto Externo
Conformidade e Fiscalização: • Normatização, controle e fiscalização interna; • Gestão dos elementos que influenciam o alcance dos objetivos estratégicos.	**Regulamentação:** • Ambiente regulatório; • Aderência aos principais requisitos regulatórios externos.
Recursos Humanos: • Carga de trabalho; • Segregação de funções; • Clima organizacional.	**Fornecedores:** • Relação com os fornecedores; • Sanções ao contratado; • Cláusulas contratuais sobre a entrega do objeto contratado.

Tecnologia da Informação: • Abrangência dos benefícios da TI; • Demanda interna por recursos de TI; • Alinhamento da TI ao plano corporativo de continuidade de negócios; • Definição de parâmetros mínimos de qualidade e eficiência dos serviços prestados pela TI.	**Desastres:** • Inundação, incêndio, etc.; • Vandalismo, terrorismo.
Controles Físicos: • Controles de segurança física; • Alinhamento entre os controles de segurança física e lógica; • Existência do Plano de Continuidade de Negócios ou Plano de Recuperação de Desastres.	**Reputação:** • Percepção da sociedade.
Cultura Organizacional: • Adaptação da cultura organizacional às mudanças no contexto interno.	**Ambiente Cultural, Social e Político:** • Mudanças de governo.
Econômicos: • Disponibilidade financeiro-orçamentária.	

Ao estabelecer o contexto específico, o proprietário do processo de trabalho deverá ajustar as categorias de eventos, excluindo as que não se aplicam ao processo de trabalho e incluindo as que não estejam previstas.

- **Critérios de Riscos**

A seguir, encontram-se definidos os critérios de riscos, que compõem o contexto geral de gestão de riscos do TRT11. Cabe ao proprietário dos processos de trabalho avaliar e redefinir tais critérios, de acordo com as necessidades específicas de seu âmbito e escopo de atuação.

- **Escala de probabilidade**

A tabela abaixo define a escala de probabilidade a ser utilizada no processo de gestão de riscos. O proprietário dos processos de trabalho pode, quando necessário, adequar somente os quantitativos da coluna "Ocorrências". A probabilidade está associada às chances de o evento ocorrer.

Escala de Probabilidade			
Descritor	**Descrição**	**Ocorrências**	**Nível**
Muito Baixa	Evento extraordinário, sem histórico de ocorrência.	Até 5	1

Baixa	Evento casual e inesperado, sem histórico de ocorrência.	>5 até 10	2
Média	Evento esperado, de frequência reduzida, e com histórico de ocorrência parcialmente conhecido.	>10 até 15	3
Alta	Evento usual, com histórico de ocorrência amplamente conhecido.	>15 até 20	4
Muito Alta	Evento repetitivo e constante.	>20	5

- **Escala de impacto**

Para que o nível de impacto seja definido, é necessário considerar quais são as dimensões (custo, prazo, escopo e qualidade) do objetivo do processo de trabalho avaliado que serão influenciadas direta ou indiretamente. O impacto está associado às consequências do evento ocorrido.

Impacto nas dimensões do objetivo				
Custo (aumento %)	**Prazo (atraso %)**	**Escopo (afetação)**	**Qualidade (degradação)**	**Nível**
Até 5	Até 5	Insignificante	Irrisória	1
>5 até 10	>5 até 10	Pouco	Pouco	2
>10 até 15	>10 até 15	Significativa	Relevante	3
>15 até 20	>15 até 20	Muito significativa	Muito relevante	4
>20	>20	Ampla	Grave	5

Vale salientar que nem sempre o nível será o mesmo para todas as dimensões. Caso isso aconteça, considerar-se-á o nível mais alto.

Após considerar o impacto nas dimensões do objetivo, chega-se aos níveis de impacto:

Escala de impacto		
Descritor	**Descrição**	**Nível**
Muito Baixo	Impacto insignificante nos objetivos.	1
Baixo	Impacto mínimo nos objetivos.	2
Médio	Impacto mediano nos objetivos, com possibilidade de recuperação.	3
Alto	Impacto significante nos objetivos, com possibilidade remota de recuperação.	4
Muito Alto	Impacto máximo nos objetivos, sem possibilidade de recuperação.	5

O proprietário dos processes de trabalho pode, quando necessário, adequar somente os quantitativos das colunas “Custo” e “Prazo”.

- **Escala de relevância**

A relevância indica o grau em que o comprometimento da segurança do objeto em análise, seja ele um ativo, um processo de trabalho, um ambiente, etc., pode afetar as atividades do TRT11 caso o risco se realize, impedindo o Tribunal de atingir seus objetivos e cumprir sua missão. A relevância é utilizada pelo Módulo Risk Manager® para cálculo do PSR® (ver anexo 9.3. Anexo 3 – Análise de risco com o Módulo Risk Manager®).

A tabela abaixo define a escala de relevância a ser utilizada no processo de gestão de riscos com apoio do Módulo Risk Manager®.

Escala de relevância		
Descritor	**Descrição**	**Nível**
Muito Baixa	Pode afetar uma parte muito pequena do negócio da instituição e os prejuízos serão desprezíveis.	1
Baixa	Pode afetar uma parte pequena e localizada do negócio da instituição e os prejuízos serão baixos.	2
Média	Pode afetar uma parte do negócio da instituição e os prejuízos serão razoáveis.	3
Alta	Pode afetar um ou mais negócios da instituição e os prejuízos serão muito altos.	4
Muito Alta	Pode afetar todo a instituição.	5

O proprietário dos processes de trabalho não pode fazer adequações nesta matriz.

- **Índice de risco**

A tabela abaixo tem por finalidade relacionar os níveis de probabilidade e impacto permitindo, então, definir o Nível de Risco.

O proprietário dos processes de trabalho não pode fazer adequações nesta matriz.

		Probabilidade				
		1 – Muito Baixa	**2 - Baixa**	**3 - Média**	**4 – Alta**	**5 – Muito Alta**
Impa	**5 – Muito Alto**	5	10	15	20	25
	4 – Alto	4	8	12	16	20

	3 – Médio	3	6	9	12	15
	2 – Baixo	2	4	6	8	10
	1 – Muito Baixo	1	2	3	4	5

Legenda Nível de Risco:

BAIXO	**MÉDIO**	**ALTO**	**EXTREMO**

Se consideramos no cálculo do índice de risco a relevância do objeto da análise, obteremos os seguintes valores de PSR®:

Nível de Risco	Valores Possíveis PSR®
Muito Baixo	1, 2, 3, 4, 5,6
Baixo	8, 9, 10, 12, 15,16
Médio	18, 20, 24, 25, 27,30
Alto	32, 36, 40, 45, 48,50
Muito Alto	60, 64, 75, 80, 100,125

- **Matriz "Apetite a Risco"**

O apetite a risco é a quantidade de risco, em sentindo mais abrangente, que o Tribunal se dispõe a aceitar na busca por agregar valor aos serviços prestados para a sociedade. O apetite a risco está diretamente associado à estratégia da instituição e deve ser considerado no momento de definir as estratégias, pois estas expõem o TRT11 a diferentes riscos.

O apetite a riscos do TRT11 está definido na tabela abaixo.

Os proprietários dos processos de trabalho não podem fazer adequações neste critério de riscos.

		Probabilidade				
		1 – Muito Baixa	**2 - Baixa**	**3 - Média**	**4 – Alta**	**6 – Muito Alta**
Impacto	5 – Muito Alto					
	4 – Alto				**ABSOLUTAMENTE INACEITÁVEL**	
	3 – Médio			**INACEITÁVEL**		
	2 – Baixo	**OPORTUNIDADE**		**ACEITÁVEL**		

	1 – Muito Baixo			

Legenda Apetite a Risco:

BAIXO	MÉDIO	ALTO	EXTREMO

Nível de Risco	Valores Possíveis PSR®	Apetite a Risco
Muito Baixo	1, 2, 3, 4, 5,6	Oportunidade
Baixo	8, 9, 10, 12, 15,16	
Médio	18, 20, 24, 25, 27,30	Aceitável
Alto	32, 36, 40, 45, 48,50	Inaceitável
Muito Alto	60, 64, 75, 80, 100,125	Absolutamente inaceitável

- **Diretrizes para priorização do tratamento de riscos**

Como último critério de riscos, encontram-se as diretrizes para priorização do tratamento de riscos cuja finalidade é auxiliar na avaliação da resposta mais adequada no tratamento dos riscos.

A tabela abaixo contém as diretrizes definidas pelo Comitê de Gestão de Riscos para o estabelecimento do contexto geral.

O proprietário dos processes de trabalho não pode fazer adequações nas diretrizes.

Nível de Risco	Descrição	Diretriz para Resposta
Extremo	Indica um nível de risco absolutamente inaceitável, muito além do apetite a risco do TRT11.	Qualquer risco encontrado nessa área deve ter uma resposta imediata. Admite-se postergar o tratamento somente mediante parecer do Diretor da Unidade, ou cargo equivalente.
Alto	Indica um nível de risco inaceitável, além do apetite a risco do TRT11	Qualquer risco encontrado nessa área deve ter uma resposta em um intervalo de tempo definido pelo Diretor da Unidade, ou cargo equivalente. Admite-se postergar o tratamento somente mediante parecer do Diretor da Unidade, ou cargo equivalente.

Médio	Indica um nível de risco aceitável, dentro do apetite a risco do TRT11.	Não se faz necessário adotar medidas especiais de tratamento, exceto manter os controles já existentes.
Baixo ou Muito Baixo	Indica um nível de risco baixo ou muito baixo, onde há possíveis oportunidades de maior retorno que podem ser exploradas.	Explorar as oportunidades, se determinado pelo Diretor da Unidade, ou cargo equivalente.