Portaria (Presidência) Nº 2126/2022 - PJPI/TJPI/SECPRE, de 30 de setembro de 2022

Dispõe sobre a instituição do Processo de Gestão de Riscos de Segurança da Informação no Âmbito do Poder Judiciário do Estado do Piauí.

O **PRESIDENTE DO EGRÉGIO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ**, Desembargador JOSÉ RIBAMAR OLIVEIRA, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução Nº 370 do Conselho Nacional de Justiça, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);

CONSIDERANDO a Resolução Nº 232/2021, de 05 de julho de 2021, que dispõe, no âmbito do Tribunal de Justiça do Estado do Piauí - TJPI, sobre o Sistema de Gestão de Segurança da Informação - SGSI e a Política de Segurança da Informação – PSI;

CONSIDERANDO a Tecnologia de Informação (TIC) como ferramenta indispensável à realização as funções institucionais do TJPI e como instrumento para viabilizar soluções que conduzam ao alcance dos objetivos estratégicos do Tribunal;

CONSIDERANDO o disposto nos itens 3.5 e 24, do Levantamento iGovTIC-Jud-2021 do CNJ, referente à formalização e cumprimento do processo de Plano de Gestão de Riscos de TIC;

CONSIDERANDO as recomendações das boas práticas de gerenciamento de Gestão de Riscos contidos nas Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação, Norma Técnica ABNT NBR ISO 31000:2018, que fornece princípios e diretrizes genéricas para a gestão de riscos, Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação, Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização e Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos à gestão de riscos.

R E S O L V E:

Art. 1º Fica instituído o processo de Gestão de Riscos de Segurança da Informação no Âmbito do Poder Judiciário do Estado do Piauí.

Art. 2º Para os fins deste Ato, entende-se como:

I - Ameaça – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização;

II - Análise de riscos – uso sistemático de informações para identificar fontes e estimar o risco;

III - Análise/avaliação de riscos – processo completo de análise e avaliação de riscos;

IV - Ativos de Informação – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

V - Avaliação de riscos – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

VI - Comunicação do risco – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas;

VII - Estimativa de riscos – processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

VIII - 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;

IX - Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC–TJPI) – conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

X - Gestão de Riscos em Projetos de TIC – conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.

XI - Gestão de Riscos em Processos de TIC – conjunto de atividades estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.

XII - Identificação de riscos – processo para localizar, listar e caracterizar elementos do risco.

XIII - 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;

XIV - Reter risco – forma de tratamento de risco pela qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

XV - 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;

XVI - Transferir risco – uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

XVII - Tratamento dos riscos – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

XVIII - Vulnerabilidade – conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de Segurança da Informação.

Art. 3º O processo definido visa atingir os seguintes objetivos:

I - Estabelecer as diretrizes da gestão de riscos relacionada ao ambiente tecnológico no âmbito deste Tribunal, aos projetos e processos de Tecnologia da Informação e Comunicações;

II - Definir o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações do TJPI (GRSIC-TJPI).

Art. 4º O processo de Gestão de Riscos de Segurança da Informação observará o manual do processo, constante no Anexo Único desta Portaria e dela parte integrante.

Art. 5º Os fluxos, o manual, a documentação e as demais informações sobre o processo estão disponíveis no Portal da Governança de TIC, na página do TJPI.

Art. 6º Os papéis definidos no manual do processo, relativos aos servidores da STIC, serão designados pelo Secretário da unidade.

Art. 7º Esta Portaria entra em vigor na data de sua publicação.

REGISTRE-SE, PUBLIQUE-SE e CUMPRA-SE.

GABINETE DA PRESIÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ, em Teresina-PI, 30 de setembro de 2022.

DESEMBARGADOR JOSÉ RIBAMAR OLIVEIRA
PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ

ANEXO ÚNICO
PORTARIA (PRESIDÊNCIA) Nº 2126/2022 - PJPI/TJPI/SECPRE
PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO DO TJPI

VERSÃO 1.0.0

PROCESSO SEI Nº 22.0.000070110-0

Histórico de Versões

Versão	Descrição	Data	Responsável	Local
1.0.0	Criação do documento	09/2022	Gildean Alves / Enani Moura	INFRA/SEGINFO

Gestão de Riscos de Segurança da Informação e Comunicações

1. Objetivos

1.1. Estabelecer as diretrizes da gestão de riscos relacionadas ao ambiente tecnológico no âmbito deste Tribunal, aos projetos e processos de Tecnologia da Informação e Comunicações, e definir o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações do TJPI (GRSIC-TJPI).

2. Aplicabilidade

2.1. Este documento aplica-se a todas as unidades pertencentes à Secretaria de Tecnologia da Informação e Comunicações, responsáveis por gerenciar, manipular e operar informações, projetos, processos, produtos e serviços relacionados à área de TIC no âmbito do TJPI.

3. Motivações

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

3.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos.

3.3. Conformidade com normatizações e regulamentações relacionadas ao assunto.

4. Referências normativas

4.1. Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

4.2. Norma Técnica ABNT NBR ISO 31000:2018, que fornece princípios e diretrizes genéricas para a gestão de riscos.

4.3. Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação.

4.4. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

4.5. Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos à gestão de riscos.

4. Conceitos e definições

4.1. Ameaça – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização;

4.2. Análise de riscos – uso sistemático de informações para identificar fontes e estimar o risco;

4.3. Análise/avaliação de riscos – processo completo de análise e avaliação de riscos;

4.4. Ativos de Informação – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

4.5. Avaliação de riscos – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

4.6. Comunicação do risco – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas;

4.7. Estimativa de riscos – processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

4.8. 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;

4.9. Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC–TJPI) – conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

4.10. Gestão de Riscos em Projetos de TIC – conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.

4.11. Gestão de Riscos em Processos de TIC – conjunto de atividades, estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.

4.12. Identificação de riscos – processo para localizar, listar e caracterizar elementos do risco.

4.13. 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;

4.14. Reter risco – forma de tratamento de risco pela qual se decide realizar a

atividade, assumindo as responsabilidades caso ocorra o risco identificado;

4.15. 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;

4.16. Transferir risco – uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

4.17. Tratamento dos riscos – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

4.18. Vulnerabilidade – conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de Segurança da Informação.

5. Escopo

5.1. A Gestão de Riscos, definida por esta Norma, tem seu escopo limitado às medidas protetivas dos ativos de informação, bem como dos projetos e processos relacionados à área de TIC, que suportam os principais processos de negócio do TJPI.

6. Diretrizes

6.1. A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TIC e está alinhada à Política de Segurança da Informação deste Tribunal.

6.2. Gestão de Riscos é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis para cada projeto, processo e/ou serviço analisado.

6.3. Os riscos são analisados e avaliados em função de sua relevância para os principais processos de negócio deste Tribunal e são tratados de forma a assegurar respostas tempestivas e efetivas.

7. Gestão de riscos em projetos de TIC

7.1. As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos adotada pela Secretaria de Tecnologia da Informação de Comunicações.

8. Gestão de riscos em processos de TIC

8.1. A gestão e comunicação de riscos em processos de TIC são definidas na especificação de cada processo e visam à identificação e ao controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria.

8.1.1. As atividades inerentes à gestão de riscos nos processos de TIC devem observar as diretrizes desta norma e outras específicas relacionadas ao processo.

8.2. A gestão de riscos em processos de TIC é monitorada pelo Escritório de Processos de TIC.

9. Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC-TJPI)

9.1. O processo de GRSIC-TJPI é contínuo, fornecendo subsídios e integrando-se à implantação e operação do Sistema de Gestão de Segurança da Informação e da Gestão de Continuidade de Negócios.

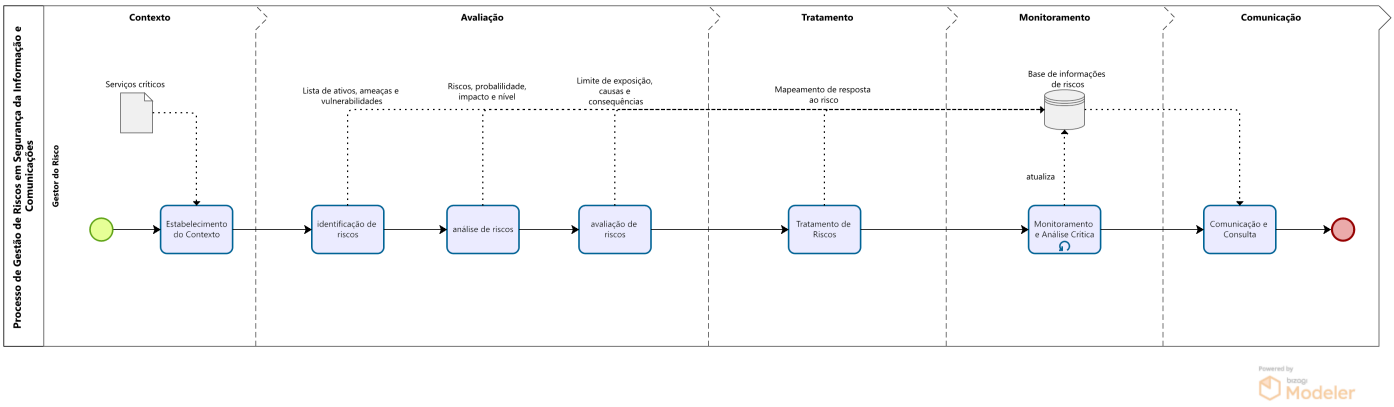
9.2. O processo de GRSIC-TJPI está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2011 e ABNT NBR ISO/IEC 31000:2018;

9.4. O tratamento dos riscos será definido de acordo com as necessidades levantadas pelas partes interessadas, regulamentações e legislações vigentes, avaliação técnica e análise custo/benefício.

9.5. Considerando as políticas praticadas pelo TJPI, não há riscos passíveis de serem tratados através da estratégia de transferência de riscos.

10. Processo da Gestão de Riscos de Segurança da Informação e Comunicação

O processo de Gestão de Riscos do TJPI possui as seguintes etapas: Estabelecimento do Contexto, Processo de Avaliação de Riscos, Tratamento de Riscos, Monitoramento e Análise Crítica e Comunicação e Consulta.



10.1 Estabelecimento do Contexto

Ao iniciar as atividades para a elaboração do plano de gestão de riscos, a primeira tarefa consiste em compreender o ambiente no qual o trabalho será desenvolvido, definir o escopo e critérios a serem considerados no processo de gestão de riscos. Nesta etapa, a equipe que realiza a gestão de risco deve identificar todos os processos e atividades críticas sujeitas a vulnerabilidades de forma que os riscos possam ser gerenciados.

Nesse sentido, a Resolução 370 do CNJ, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) 20212026, define o Índice de Serviços Críticos com Gestão de Risco como um dos indicadores do objetivo estratégico “Aprimorar Segurança da Informação e a Gestão de Dados”. A intenção é avaliar se os serviços identificados como críticos possuem gestão de risco e se são aplicados.

10.2 Avaliação de Riscos

O processo de Avaliação de Riscos de Tecnologia da Informação possui as seguintes etapas: identificação de riscos, análise de riscos e avaliação de riscos.

11.2.1 Identificação de Riscos

Uma vez definidos os serviços críticos para a estratégia do Tribunal, a ação prática do gestor do ativo nesta etapa deve ser identificar os ativos de TI que suportam a execução desses serviços críticos. Tal atividade dá início a etapa de identificação dos riscos de TI. As ameaças e as vulnerabilidades associadas a cada ativo que suporta um serviço crítico devem ser levantadas conforme o estabelecido na norma ISO 27005, permitindo, assim, uma identificação mais apropriada dos riscos de TI.

11.2.2 Análise de Riscos

Na análise de riscos, para cada um dos riscos identificados na etapa anterior, a ação prática do gestor de risco deve ser definir os seguintes passos: avaliar a probabilidade e o impacto do risco e definir o nível desse risco.

Probabilidade - é a chance de um evento ocorrer dentro do prazo previsto para se alcançar o resultado ou objetivo. Por exemplo, se o objeto da gestão de riscos é um projeto, estima-se a probabilidade da ocorrência do risco durante o prazo previsto para entrega do seu produto final. Para estimar a probabilidade será usada uma escala qualitativa de cinco níveis, conforme a seguir.

	Escala de Probabilidade
Muito baixa	Acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.
Baixa	o histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo

Média	Repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte
Alta	Repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerão nesse horizonte.
Muito alta	Ocorrência quase garantida no prazo associado ao objetivo

Impacto - o impacto mede o potencial comprometimento do objetivo ou resultado. Por exemplo, um risco com potencial para comprometer um objetivo na sua totalidade ou na sua quase totalidade é considerado um risco de alto impacto. Segue abaixo a escala para impacto.

	Escala de Impacto
Muito baixo	Compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado.
Baixo	Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado.
Médio	Compromete razoavelmente o alcance do objetivo/resultado.
Alto	Compromete a maior parte do atingimento do objetivo/resultado
Muito alto	Compromete totalmente ou quase totalmente o atingimento do objetivo/resultado.

Nível de Risco - O nível de risco é calculado a partir da combinação das escalas de probabilidade e de impacto. Para definir o nível de risco, deve ser usada a matriz abaixo.

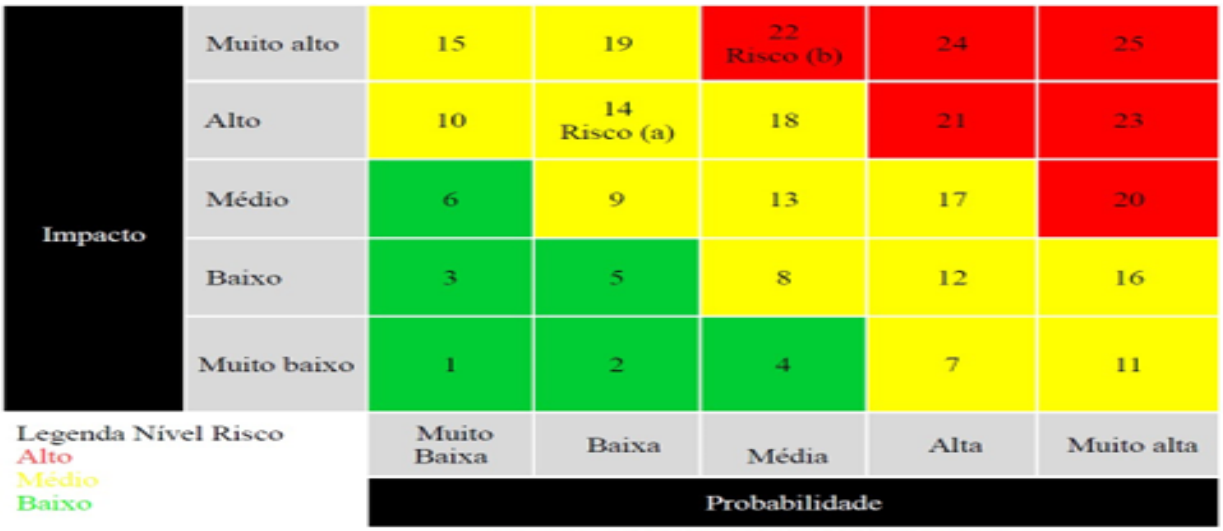


Figura 1: Matriz probabilidade e impacto

Apresentaremos uma análise de risco exemplificativa. Consideraremos os seguintes eventos de riscos que poderiam afetar os sistemas essenciais:

Indisponibilidade da rede de dados;

- Impacto: alto
- Probabilidade: baixa

Perda da base de dados, sem possibilidade de recuperação.

- Impacto: muito alto
- Probabilidade: média

Olhando para a tabela acima é possível deduzir o nível de risco de cada um dos dois eventos: o nível de risco de (a) é 14 e o de (b) é 22. O nível de risco é dado pelo número inscrito em cada célula da matriz, não sendo obtido por qualquer fórmula matemática. São 25 possíveis níveis de risco, em que cada nível está associado a uma estimativa de probabilidade e de impacto. A matriz ordena os possíveis níveis de risco, desde o mais baixo, ao qual é atribuído o nível 1 (evento muito raro, de impacto muito baixo), até o mais elevado, ao qual se atribui o nível 25 (probabilidade muito alta, evento praticamente certo, e de impacto muito alto)

Algumas considerações importantes sobre o uso no TJPI das matrizes de impacto e probabilidade:

- O impacto é a dimensão mais importante: um evento de impacto muito alto e de probabilidade de ocorrência muito baixa deve preocupar o gestor muito mais do que o oposto, um evento de probabilidade muito alta e impacto muito baixo – se o impacto é mínimo, logo a preocupação deve ser menor.
- Atribuição de valores arbitrários: deve-se evitar o uso de matrizes que "calculam" o nível do risco pela soma ou multiplicação desses valores, dado o risco de distorção trazido por matrizes simétricas, que consideraram como do mesmo nível os riscos descritos no item anterior. Na matriz acima apresentada, um risco com probabilidade muito baixa e impacto muito alto é classificado como de nível 15, enquanto outro risco de probabilidade muito alta e impacto muito baixo é considerado de nível 11, ou seja, é bem menos prioritário para a ação do gestor do que o de nível 15.
- Fazer a avaliação dos riscos considerando a situação real do TJPI (considerando os controles existentes e em funcionamento).

10.2.1 Categorias de riscos

- **Estratégico:** Estão associados à tomada de decisão que pode afetar negativamente o alcance dos objetivos da organização. o **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 STIC ou do Tribunal. Os riscos **devem** ser mitigados, transferidos, eliminados ou explorados, pois não poderão ser aceitos. o **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 TJPI, mas que ainda assim podem afetar o sucesso das metas e ações. Os riscos externos podem ser aceitos, pois independem de ação direta do TJPI. o **Tecnologias:** Riscos relacionados a problemas técnicos em hardware, software ou outra solução de informática.
  o **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). o **Escopo:** Riscos relacionados ao assunto escopo de um projeto, exemplo: indefinições, alterações constantes, sem validação. o **Cliente / Usuário:** Riscos relacionados a clientes ou usuários de algum projeto, por exemplo: indefinição, representante ausente, sem comprometimento.

10.2.2 Avaliação de Riscos

A avaliação do risco envolve a comparação do nível de risco dos ativos do TJPI com o limite de exposição a riscos, a fim de determinar que riscos o Tribunal está disposto a aceitar. O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco. Espera-se que com os resultados do tratamento o nível de risco real fique abaixo do limite de exposição tolerável.

A ação prática do gestor de risco nesta fase deve ser: identificar, na matriz probabilidade e impacto, os riscos cujos níveis estão acima do limite de exposição a riscos (faixa vermelha) e, para esses riscos, identificar as respectivas fontes, causas e consequências; os riscos que estão na faixa amarela, abaixo do limite de exposição a riscos, deverão ser monitorados os riscos que estão na faixa verde, também abaixo do limite de exposição, podem ser aceitos sem que nenhuma providência tenha que ser tomada.

Para retratar o exposto neste parágrafo, segue uma tabela na sequência.

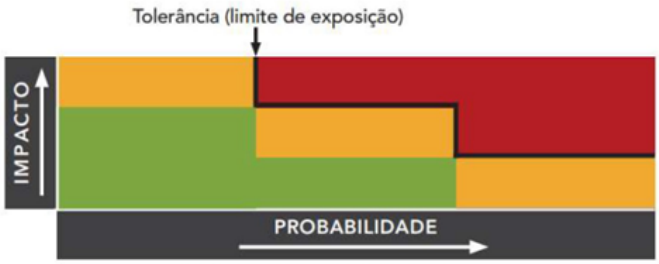


Figura 2: Matriz de avaliação dos riscos

10.3 Tratamento de Riscos

O tratamento de riscos está relacionado à resposta a riscos encontrados. Envolve decidir se o risco vai ser tratado ou não, promovendo a priorização de tratamento dos riscos. A estratégia de tratamento de risco adotada pelo TJPI é composta pelas opções: modificar o risco, aceitar o risco, evitar o risco e compartilhar o risco, conforme descrito na tabela a seguir.

RESPOSTA AO RISCO	**DESCRIÇÃO**
Modificar	O risco precisa ser gerenciado pela inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e considerado aceitável.
Aceitar	O objetivo dessa resposta é avaliar se os demais tipos de respostas ao risco são viáveis. Em algumas situações, como: risco de baixo nível ou custo desproporcional ao benefício do tratamento, a opção mais adequada é aceitar ou reter o risco.
Evitar	Inclui basicamente a descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de um software, a alienação de um equipamento ou a extinção de uma divisão ou processo de trabalho.
Compartilhar	Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a terceirização de uma atividade e outras.

Conhecendo os riscos envolvidos em suas áreas de atuação e o resultado de suas análises, cada gestor deve levar em consideração o nível de tolerância ao risco e com isso tomar sua decisão sobre o tratamento dos riscos.

No Tratamento de Risco, a ação prática do gestor de risco é prover ações (respostas) para reduzir o nível de risco mapeado nos passos anteriores. Essas ações podem envolver controles, capacitação, redesenho de processo, realocação de pessoas, aperfeiçoamento de soluções de TI, etc. que, ao final, irão modificar, evitar, aceitar ou compartilhar os riscos.

10.4 Monitoramento e Análise Crítica

O monitoramento trata da revisão e avaliação periódica da gestão de riscos, objetivando aprimorar continuamente a instituição. O monitoramento tem finalidade de:

- Garantir que os controles sejam eficazes e eficientes no projeto e na operação.
- Obter informações adicionais para melhorar a avaliação dos riscos.

- Analisar os eventos, as mudanças e aprender com o sucesso ou fracasso do tratamento dos riscos.
- Detectar mudanças nos contextos externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que poderão exigir a revisão da forma de tratar os riscos e das prioridades.
- Identificar os riscos emergentes, que poderão surgir após o processo de análise crítica, reiniciando o ciclo do processo de gestão de riscos.

Convém que os resultados do monitoramento e da análise crítica sejam registrados e reportados periodicamente.

10.5 Comunicação e Consulta

A comunicação e a consulta constituem o fluxo de informações entre as partes envolvidas no processo de gestão de riscos a fim de assegurar a compreensão necessária à tomada de decisão, devendo durante todas as fases do processo de gestão de riscos. As informações devem estar consolidadas e organizadas de forma que seja fácil e inteligível o acompanhamento de todo o processo.

A consulta consiste na disponibilização das informações consolidadas em local de fácil acesso, como o portal corporativo do Tribunal. A comunicação consiste no envio periódico das informações disponibilizadas na consulta para todos os envolvidos.

11. Recursos

Faz-se necessário que o TJPI aloque recursos apropriados para a gestão de riscos. Tais recursos podem ser pessoas, processos, tecnologia da informação, comunicação e treinamento.

13. Papéis e responsabilidades

Para gerenciar o processo de gestão de riscos institucional, os integrantes de governança e gestão de riscos do TJPI serão as seguintes unidades organizacionais:

Gestores das unidades da STIC - representa os chefes das unidades administrativas internas da STIC - Secretaria de Tecnologia da Informação e Comunicação. São responsáveis por identificar, analisar, propor tratamento e

acompanhar o tratamento dos riscos.;

Comitê Gestor de Tecnologia da Informação (CGTI) - responsável pela avaliação das proposições de tratamento de riscos produzidas, chancelando a validade, momento e modo de implementação de cada tratamento.;

Gestores de risco - servidores designados da STIC com aptidão para implantar as medidas definidas no plano de tratamento de riscos.

14. Atualização da Norma

As diretrizes previstas na presente norma serão atualizadas na forma do art. 14 § 1º da Política de Segurança da Informação vigente, sempre que alterados os procedimentos de Gestão de Riscos de TIC, observada a periodicidade prevista para a Política de Segurança da Informação.