Poder Judiciário

Tribunal de Justiça da Paraíba

Diretoria de Tecnologia da Informação

DITEC

TRIBUNAL DE JUSTIÇA DA PARAÍBA

Plano de Gestão de Risco de TI

Agosto/2021

sumário

Índice de conteúdos

Histórico de Alterações

Versão	Descrição	Modelo	Período	Responsável	Local
1.0.0	**Elaboração do Modelo de Artefato (Designer do Processo de Gestão de Riscos de SI)**	**1.0.0**	**Agosto / 2021**	**Wandernedja Ferreira wanda@tjpb.jus.br**	**COGTI**
1.0.0	**Criação do Plano de Gestão de Riscos de TIC**	**1.0.0**	**Agosto / 2021**	**Francisco Magalhães maga@tjpb.jus.br**	**COSEI**

Histórico de Revisões

Versão	Revisor	Período da Revisão	Próxima Revisão	Local
1.0.0	Paulemir Soares - CODAC (Integrante da ETRI)	Agosto / 2021	Setembro / 2022	GEINF
1.0.0	Aerton Ferreira – COBAD (Integrante da ETRI)	Agosto / 2021	Setembro / 2022	GEINF
1.0.0	José Oliveira - CORED (Integrante da ETRI)	Agosto / 2021	Setembro / 2022	GEINF

Histórico de Aprovações

Versão	Aprovação	Data	Comitê
1.0.0	Ney Robson Medeiros (Diretor de Tecnologia da Informação)	Setembro / 2021	CGTI
1.0.0	José Djalma (Gerente da Gerência de Infraestrutura)	Setembro / 2021	CGTI
1.0.0	Marconi Edson (Gerente do Processo Judicial Eletrônico)	Setembro / 2021	CGTI
1.0.0	Júlio Paiva (Gerente da Gerência de Sistemas)	Setembro / 2021	CGTI
1.0.0	José Fábio Alencar (Gerente da Gerência de Atendimento)	Setembro / 2021	CGTI

1. APRESENTAÇÃO

A Estratégia Nacional de TIC para o Poder Judiciário (ENTIC-JUD), aprovada pela Resolução CNJ nº 370/2021, de 28 de janeiro de 2021, determina em seu art. 37 que cada órgão deve elaborar um Plano de Gestão de Riscos de TIC com foco na continuidade de negócios, manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, objetivando mitigar as ameaças mapeadas para atuar de forma preditiva e preventiva às possíveis incertezas.

O plano de gestão de riscos é um esquema dentro da estrutura de gestão de riscos que especifica a abordagem, os recursos a serem aplicados para gerenciar riscos e os componentes de gestão, incluindo procedimentos, práticas, sequência e cronologia das atividades e atribuição de responsabilidades.

1.1 Referências

As principais referências para a elaboração deste plano foram a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2021-2026, Portaria CNJ 162/2021, ISO/IEC 27005:2019, ISO/IEC 31000:2018, Processo de Gestão de Riscos e Manual de Gestão de Risco do TCU Versão 2.

1.2. Princípios da Gestão de Riscos

Os princípios da gestão de riscos fornecem orientações sobre as características de uma gestão de riscos eficaz e eficiente, comunicando seu valor e explicando sua intenção e propósito. Os princípios são a base para gerenciar riscos e convém que sejam considerados no Plano de Gestão de Riscos da organização. Os princípios direcionam uma abordagem: integrada; estruturada e abrangente; personalizada; inclusiva; dinâmica; baseada na melhor informação disponível; baseada em fatores humanos e culturais.

2. PROCESSO DA GESTÃO DE RISCOS

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

2.1 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) 2021-2026, 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.

2.2 Processo de 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.

2.2.1 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.

2.2.2 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.

Impacto	Muito alto	15	19	22 Risco (b)	24	25
	Alto	10	14 Risco (a)	18	21	23
	Médio	6	9	13	17	20
	Baixo	3	5	8	12	16
	Muito baixo	1	2	4	7	11
Legenda Nível Risco Alto Médio Baixo		Muito Baixa	Baixa	Média	Alta	Muito alta
		Probabilidade				

Figura 1: Matriz probabilidade e impacto

Segue uma análise de risco (meramente exemplificativa): o TJPB usa um sistema nacional de processamento de informações e prática de atos processuais que é de grande relevância para o cumprimento de metas do órgão. Em relação a esse sistema foram identificados os seguintes eventos de riscos que poderiam afetar o cumprimento dessas metas:

a) Indisponibilidade da rede de dados;
- Impacto: alto
- Probabilidade: baixa

b) 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 TJPB das matrizes de impacto e probabilidade:

1) 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.

2) 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.

3) Fazer a avaliação dos riscos considerando a situação real do TJPB (considerando os controles existentes e em funcionamento).

2.2.3 Avaliação de Riscos

A avaliação do risco envolve a comparação do nível de risco dos ativos do TJPB 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.

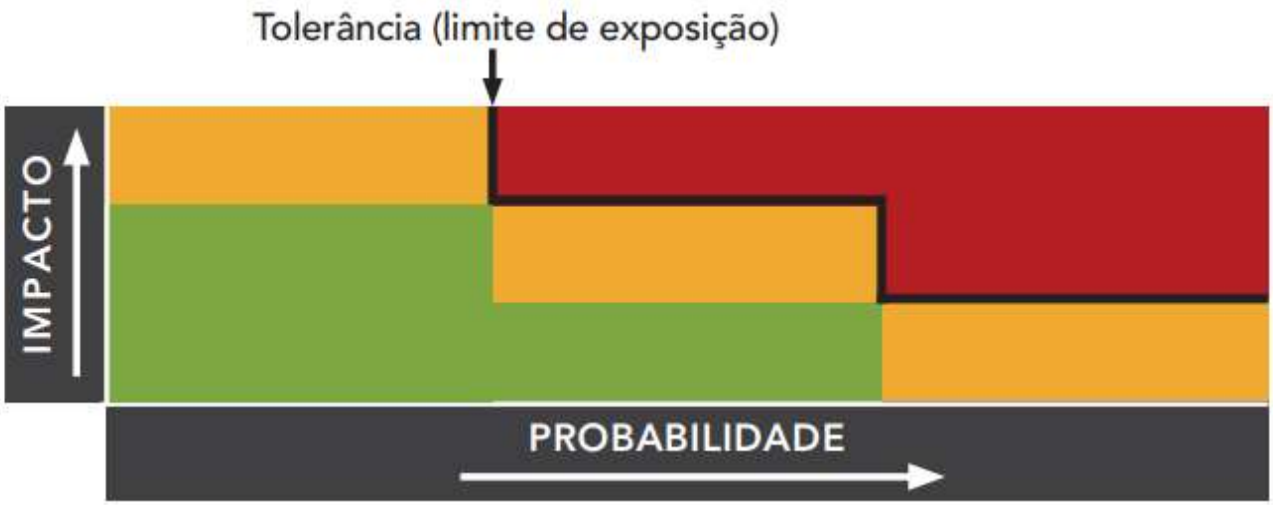

Figura 2: Matriz de avaliação dos riscos

2.3 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 TJPB 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. Para colocar em prática o tratamento de riscos, segue abaixo uma ferramenta chamada What If, que foi adaptada para este Plano. Ela não serve apenas para tratar os riscos, mas também permite tratar todas as etapas já discutidas anteriormente, como identificação, análise e avaliação dos riscos, podendo, portanto, ser usada pelo gestor para colocar tudo em prática a partir de um só lugar.

PROCESSO:	Gestão de Risco de TI no TJPB				DATA:	30/08/21							
Critérios:	de 1 a 6 = risco baixo			de 7 a 19 = risco médio			de 20 a 25 = risco alto						
Processo/Serviço /Sistema/Ação/ativo / Projeto/contratação	O QUE ACONTECERIA SE	EFEITO	Probabilidade	Impacto	RISCO	CONTROLES ATUAIS	AÇÕES RECOMENDADAS	RESP.	PRAZO	Implantado em	Nova Probabilidade	Novo Impacto	Risco residual
Base de dados Críticas	Houvesse perda de dados de sistemas críticos, sem possibilidade de recuperação	*Interrupção de serviços essenciais *Perda de dados críticos *Danos a reputação e imagem do TJPB	Média	Muito alta	22	*Realização de backup local *Teste de backup	*backup remotos e em s erviços de nuvem. *Backups protegidas por segurança física ou criptografia ao serem armazenados ou movidos pela rede	João	18/8/2021	SIM	Muito Baixa	Médio	6
Serviço de Internet	Houvesse indisponibilidade do serviço de Internet nos dois provedores	*Interrupção de serviços prestados	Baixa	alto	14	* Link redundante	*Contratação de um terceiro provedor	Beto	30/8/2021	SIM	Muito baixa	Baixo	3

Figura 3: Ferramenta What If adaptada

A ferramenta What If é genérica o que permite seu uso em diversas áreas: processos, etapas de processo, objetivos, resultados, produtos, serviços, sistemas, projetos, ações, etc. conforme foi descrito na primeira coluna da tabela acima. Nessa tabela foram colocados dois exemplos de serviços (nas duas primeiras linhas), meramente ilustrativos: Base de dados críticas e Serviço de Internet. Uma outra coluna interessante é a de risco (nível de risco). Por exemplo, para encontrá-la basta conferir a probabilidade e impacto do cenário “Houvesse perda de dados de sistemas críticos, sem possibilidade de recuperação” se materializar. A coluna “CONTROLES ATUAIS” refere-se a controles que foram implantados, ou seja, a realidade atual. A coluna “AÇÕES RECOMENDADAS” pode ser um ou alguns controles melhores ou simplesmente melhorias a serem implantadas no futuro e uma vez implantadas, deve nos levar a um novo nível de risco (Risco Residual), o que se espera que seja menor, já que novos controles foram colocados em prática.

2.4 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:

1. Garantir que os controles sejam eficazes e eficientes no projeto e na operação.
2. Obter informações adicionais para melhorar a avaliação dos riscos.
3. Analisar os eventos, as mudanças e aprender com o sucesso ou fracasso do tratamento dos riscos.
4. 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.
5. 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.

2.5 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.

3. RECURSOS

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

4. PAPÉIS E RESPONSABILIDADE

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

a) Comitê de Governança de Segurança da Informação (CGSI);
b) Comitê Gestor de Tecnologia da Informação (CGTI);
c) Unidade responsável pela Gestão de Segurança da Informação de TI do TJPB; e
d) Gestores de riscos.