PORTARIA N.º 1.110/2017-TJ, DE 18 DE JULHO DE 2017

Regulamenta a Política de Gestão de Riscos do Poder Judiciário do Estado do Rio Grande do Norte - PJRN.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO NORTE, no uso das suas atribuições legais e,

CONSIDERANDO que todos têm o direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado, nos termos do inciso XXXIII do art. 5º da Constituição Federal;

CONSIDERANDO que é dever de todo servidor público prestar as informações requeridas pelo público em geral, ressalvadas as protegidas por sigilo, bem como guardar sigilo sobre assuntos institucionais, nos termos do art. 116 da Lei nº 8.112, de 11 de dezembro de 1990;

CONSIDERANDO, finalmente, a legislação pertinente à matéria, notadamente o Decreto nº 7.845/2012, a Instrução Normativa GSI nº 1/2008, a Norma Complementar nº 04/IN01/DSIC/GSIPR, de 30 de junho de 2009, a Norma Complementar nº 05/IN01/DSIC/GSICPR, de 14 de agosto de 2009, a Norma Complementar nº 06/IN01/DSIC/GSICPR, de 11 de novembro de 2009, e Normas ABNT NBR ISO/IEC 27002, ABNT NBR ISO/IEC 27031 e Normas ABNT NBR ISO/IEC 22313, que instituem os códigos de melhores práticas para Gestão de Sistemas de Continuidade de Negócio e a Resolução CNJ nº 182 de 17 de outubro de 2013 e Resolução CNJ nº 211 de 15 de dezembro de 2015;

RESOLVE:

Art. 1º A presente Portaria rege a Política de Gestão de Riscos (PGR) do Poder Judiciário do Estado do Rio Grande do Norte (PJRN) que descreve as diretrizes, os processos, as responsabilidades e a estrutura da gestão de riscos.
Parágrafo único. A Política deve ser divulgada e adotada por todas as unidades do PJRN em todos os níveis, aplicáveis aos processos, às iniciativas estratégicas, táticas e operacionais.

Art. 2º Para fins desta Política considera-se:
I - Controle: qualquer processo, política, dispositivo, prática ou ação que modifique o risco;
II - Criticidade: magnitude do risco de ocorrência de um evento, obtido por meio do produto entre a probabilidade de ocorrência e o impacto dele decorrente;
III - Evento: ocorrência causada por fontes internas ou externas que geram um impacto negativo ou positivo;
IV - Gestão de Riscos: conjunto de ações para identificar, analisar, avaliar, priorizar, tratar e monitorar eventos em potencial que podem afetar o cumprimento dos objetivos organizacionais;
V - Impacto: efeito positivo ou negativo resultante da ocorrência de um evento;
VI - Probabilidade de um evento: chance de um evento ocorrer em um determinado período de tempo;
VII - Risco: todo evento que possua probabilidade de ocorrer e impacto sensíveis aos objetivos organizacionais do PJRN;
VIII - Risco inerente: risco existente sem a aplicação de controles;
IX - Risco residual: risco existente após a aplicação de controles; e
X - Tolerância a risco: nível de criticidade razoável que o PJRN está disposto a se submeter.

Art. 3º A Gestão de Riscos do PJRN obedecerá aos seguintes princípios:
I - Proteção dos valores organizacionais;
II - Melhoria contínua da organização e dos processos;
III - Qualidade e tempestividade das informações;
IV - Transparência; e
V - Alinhamento à gestão estratégica.

Art. 4º A PGR abrange as seguintes categorias de riscos:
I - Estratégicos: riscos associados à tomada de decisões que afetam o alcance dos objetivos da organização;
II - Operacionais: resultantes de falhas decorrentes de deficiências ou inadequações de processos internos, estrutura, pessoas, sistemas tecnologias, ou ainda de eventos externos (catástrofes naturais, greves, fraudes) que causem perda de produtividade, de ativos ou de orçamento;
III - De comunicação: riscos resultantes de eventos que impeçam ou dificultem a disponibilidade de troca de informações para a tomada de decisões e para o cumprimento das obrigações de transparência e prestação de contas; e
IV - De conformidade: riscos associados ao não cumprimento das normas e procedimentos internos, bem como dos princípios constitucionais, legislações ou regulamentações externas aplicáveis ao negócio.

Art. 5º O impacto gerado por um evento pode ser classificado como: pequeno, razoável, grande e extremo (Anexo II).
Parágrafo único. Dentre os aspectos envolvidos na classificação do impacto causado devem ser levadas em consideração, primordialmente, as dimensões: prazo, custo e qualidade.

Art. 6º As probabilidades dos eventos a serem considerados na análise de riscos são: raro, incomum, comum e quase certo (Anexo II).
§1º Em casos onde o impacto é sensível e haja dados suficientes para análise, devem ser usadas probabilidades quantitativas para um melhor detalhamento do evento.
§2º Para definição da probabilidade qualitativa, considera-se:
I - Raro: eventos que podem ocorrer em circunstâncias excepcionais;
II - Incomum: já houve histórico de ocorrência em organizações semelhantes;
III - Comum: histórico de ocorrências frequentes em organizações semelhantes; e
IV - Quase certo: histórico de ocorrências na organização e já se espera que aconteça.

Art. 7º Os níveis de risco considerados para gestão de riscos podem ser classificados como: baixo, moderado, alto e extremo (Anexo II).
Parágrafo único. Com relação à classificação para aceitação dos riscos, considera-se:
I - Baixo: risco aceitável que deve ser monitorado e revisado periodicamente;
II - Moderado: risco aceitável que necessita do desenvolvimento de um plano de tratamento além do monitoramento e revisão periódica;
III - Alto: geralmente não aceitável que exige o monitoramento e desenvolvimento de plano de tratamento detalhado desenvolvido por especialista; e
IV - Extremo: não aceitável.

Art. 8º As ações para tratamento dos riscos identificados deverão estar alinhadas aos seguintes conceitos:
I - Aceitar: assumir o risco por escolha consciente e justificada;
II - Reduzir: aplicar controles que diminuam a probabilidade de ocorrência ou o impacto do risco;
III - Transferir: compartilhar o risco com outra parte interessada em aceitar parte do risco; e
IV - Evitar: descontinuar ou não iniciar uma atividade que dá origem ao risco.
§1º As ações de tratamento deverão explicitar as iniciativas propostas, os responsáveis pela implementação, os recursos requeridos e o cronograma sugerido, exceto para os casos de aceitação do risco.
§2º Todas as ações de tratamento serão monitoradas continuamente, a fim de avaliar o risco residual, aceitabilidade do risco, impacto, probabilidade e a implantação de novos controles.

Art. 9º São objetivos específicos da PGR do PJRN:
I - Integrar a análise de riscos às tomadas de decisões;
II - Aplicar as melhores práticas adotadas no setor público;
III - Orientar, identificar, avaliar, tratar, monitorar e comunicar os riscos que afetem a consecução dos objetivos institucionais;
IV - Alinhar a tolerância ao risco às estratégias adotadas; e
V - Aprimorar os controles internos.

Art. 10. O processo adotado no PJRN para gestão dos riscos seguirá a seguinte sequência:
I - Estabelecimento do contexto;
II - Identificação dos riscos;
III - Análise dos riscos;
IV - Avaliação dos riscos;
V - Tratamento dos riscos;
VI - Monitoramento; e
VII - Comunicação.
§1º A fase de estabelecimento do contexto é composta pelo levantamento dos parâmetros externos e internos relevantes para a gestão de risco e essenciais à estratégia do PJRN.
§2º A identificação dos riscos envolve o inventário e a descrição dos eventos, suas probabilidades e respectivos impactos nos objetivos do PJRN.
§3º A análise dos riscos é a compreensão da natureza e da classificação do risco, resultante do produto da probabilidade de sua ocorrência com o respectivo impacto (Anexo II).
§4º A avaliação dos riscos trata da comparação dos resultados da análise de riscos com os critérios limites adotados para determinar a aceitabilidade do risco.
§5º O tratamento do risco consiste na seleção e aplicação de um ou mais controles em resposta aos riscos.
§6º O monitoramento é o acompanhamento e análise crítica da efetividade de todas as fases do processo.
§7º A comunicação é a manutenção de fluxo constante de informações entre as partes interessadas durante as fases do processo.

Art. 11. A gestão de riscos será realizada em intervalos de pelo menos um ano, para reavaliação do contexto, riscos, controles e respostas ao risco.

Art. 12. A estrutura de Gestão de Riscos do PJRN é composta pelo Núcleo de Governança Estratégica (Resolução nº 01/2017-TJ), pelo Comitê de Segurança da Informação - CSI (Portaria nº 007/2017-TJ-SETIC) e pelos Gestores de Risco.

Parágrafo único. São considerados Gestores de Riscos, em seus respectivos âmbitos de atuação, todos os ocupantes de cargo em comissão ou função de confiança de liderança, titulares e substitutos, bem como os responsáveis pelos processos de trabalho, projetos e ações nos níveis estratégicos, tático ou operacional do PJRN.

Art. 13. A Gestão de Riscos no PJRN é de responsabilidade compartilhada de magistrados, servidores, estagiários e prestadores de serviço.

Art. 14. Compete ao Núcleo de Governança Estratégica aprovar e analisar o relatório de análise de risco e decidir sobre possíveis providências, e definir o grau de tolerância a riscos.

Art. 15. Cabe ao CSInfo e aos Gestores de Riscos o desenvolvimento de relatórios de análise e monitoramento de risco, bem como propor controles e ações de resposta.

Art. 16. Compete ao CSInfo:
I - Disseminar a Política de Gestão de Riscos;
II - Avaliar e divulgar as melhores práticas de gestão de riscos para utilização no âmbito do Tribunal;
III - Estimular e disseminar cultura de gestão de riscos para todo o Tribunal;
IV - Elaborar metodologia de gestão de riscos do Tribunal, bem como propor as atualizações necessárias;
V - Coordenar o processo de gestão de riscos no nível estratégico;
VI - Elaborar relatório de análise crítica e o mapa de riscos no nível estratégico;
VII - Prestar apoio técnico aos Gestores de Riscos para a utilização da metodologia de gestão de riscos de forma eficaz;
VIII - Monitorar o tratamento aos riscos no nível estratégico;
IX - Propor, disseminar e/ou realizar ações de sensibilização e capacitação sobre gestão de riscos para que sejam aplicadas em Planejamentos de Contratações, Novos Projetos e Documentos de Planejamento de TIC.

Art. 17. Compete aos Gestores de Riscos:
I - Conhecer e adotar a Política e os instrumentos de gestão de riscos, promovendo a efetividade dos controles dela decorrentes;
II - Fornecer subsídios para o acompanhamento, monitoramento e análise crítica do processo de gestão de riscos em sua área de atuação;
III - Estimular a cultura de gestão de riscos em sua equipe;
IV - Sugerir melhorias para a metodologia de gestão de riscos definida para o Tribunal;
V - Identificar, analisar, avaliar, tratar e monitorar risco sem sua área de atuação;
VI - Aplicar controles em sua área de atuação decorrentes da gestão de riscos;
VII - Elaborar e manter os respectivos planos de riscos de processos de trabalho e iniciativas estratégicas, táticas e operacionais;
VIII - Participar de ações de sensibilização e capacitação sobre gestão de riscos.

Art. 18. As Análises de Risco devem ser desenvolvidas pelos Gestores de Risco e analisadas pelo CSInfo, quando for da competência da Secretaria de Tecnologia da Informação e Comunicação (SETIC), e, nos demais casos, pelo Núcleo de Gestão Estratégica do PJRN.
Parágrafo único. As Análises de Risco devem seguir o padrão disposto no Anexo II, conforme art. 17 da Resolução CNJ nº 182 de 17 de outubro de 2013.

Art. 19. Esta Portaria entra em vigor na data de sua publicação.

Desembargador EXPEDITO FERREIRA
Presidente

Anexo I
Portaria nº 1.110/2017-TJ, de 18 de julho de 2017

Sugestão de Análise de Risco

Probabilidade					
20%	Quase Certo	0,2	1	1,8	4
10%	Comum	0,1	0,5	0,9	2
5%	Incomum	0,05	0,25	0,45	1
1%	Raro	0,01	0,05	0,09	0,2
		Pequeno	Razoável	Grande	Extremo
		1	5	9	20
		Impacto			

-

Níveis de Risco:

- Extremo (acima de 1,0);
- Alto (entre 0,1 e 0,9);
- Moderado (entre 0,05 e 0,09);
- Baixo (entre 0 e 0,05).

Anexo II
Portaria nº 1.110/2017-TJ, de 18 de julho de 2017

Formulário para Análise de Risco do Poder Judiciário do Rio Grande do Norte

Esse formulário tem como objetivo cadastrar requisições para Análise de Risco para tomada de decisões estratégicas do Poder Judiciário do Rio Grande do Norte.

*Obrigatório
Escopo*

Descrição das ameaças*

Probabilidade de cada ameaça*

(rara, incomum, comum, quase certa)

Impacto de cada ameaça*

(pequeno, razoável, grande ou extremo)

Descrição dos riscos que envolvem cada ameaça.*

(baixo, moderado, alto e extremo)

Sugestão de ações para tratamento dos riscos.*

(aceitar, reduzir, transferir, evitar)

Riscos residuais identificados.*

(aceitar, reduzir, transferir, evitar)