ANEXO XV
NORMA DE GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução nº 44/2022-GP	

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	14/08/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A gestão de riscos é uma metodologia contínua, que consiste no conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos que poderão afetar as rotinas do Poder Judiciário do Estado do Maranhão (PJMA) nos níveis estratégico, tático e operacional.

Esta norma obedecerá ao escopo definido na Política de Segurança da Informação (PSI) e deverá observar, no que couber, as diretrizes que constam na Resolução GP nº 44/2022 ou posterior que a substitua.

Para fins desta norma, aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I da PSI.

2. OBJETIVOS

Contextualizar e identificar os riscos.

Analisar e estabelecer ordem prioritária dos riscos.

Avaliar e priorizar as ações para reduzir a ocorrência dos riscos.

Tratar periodicamente os riscos.

Monitorar os riscos.

Comunicar os riscos aos responsáveis.

Envolver as partes interessadas nas decisões de gestão de riscos.

Coletar informações de forma a melhorar a abordagem da gestão de riscos.

3. DIRETRIZES

Sugere-se que o processo de gestão de riscos de segurança da informação observe as seguintes diretrizes:

I - ser parte integrante dos processos organizacionais de Tecnologia da Informação e Comunicação (TIC);

II - ser parte da tomada de decisões;

III - ser sistemático, estruturado e oportuno;

IV - ser baseado nas melhores informações disponíveis;

V - considerar fatores humanos e culturais;

VI - ser transparente e inclusivo;

VII - ser dinâmico, interativo e capaz de reagir às mudanças tempestivamente;

VIII - contribuir para a melhoria contínua do PJMA.

O processo de gestão de riscos será baseado nos conceitos de governança corporativa, na norma ABNT NBR ISO/IEC 27005 e alinhado ao modelo denominado PDCA (Plan-Do-Check-Act).

4. GESTÃO DE RISCO

A gestão de riscos de segurança da informação deverá apoiar as unidades administrativas e/ou judiciais (organizacionais) do PJMA no sentido de:

I - aprimorar o processo de tomada de decisão, com o propósito de incorporar a visão de riscos em conformidade com as melhores práticas de mercado;

II - melhorar a alocação de recursos;

III - aprimorar os controles internos;

IV - alinhar a tolerância aos riscos e à estratégia adotada;

V - resguardar a alta administração e os(as) gestores(as) quanto à tomada de decisão e à prestação de contas;

VI - identificar, avaliar e reagir às oportunidades e ameaças; e

VII - melhorar a eficiência operacional por meio do gerenciamento de riscos.

4.1 Avaliação de Risco

O processo de avaliação de risco será coordenado pelo(a) gestor(a) de risco, sendo necessário que o(a) mesmo(a) tenha responsabilidade e autoridade compatíveis com a execução das atividades relativas à gestão de risco.

O primeiro passo será estabelecer o contexto no que se refere ao entendimento do ambiente em que o(a) gestor(a) de risco estará inserido(a). Em seguida, o(a) gestor(a) deverá identificar os ativos e/ou processos que poderão ter os princípios da segurança da informação afetados no âmbito do PJMA e associá-los aos seus respectivos riscos.

No passo seguinte, o(a) gestor(a) de risco associará as ameaças e vulnerabilidades para cada identificação realizada. Todo ativo e/ou processo poderá estar associado a várias ameaças e cada ameaça poderá estar relacionada a várias vulnerabilidades. Existem exemplos de ameaças e vulnerabilidades disponíveis na norma ABNT NBR ISO/IEC 27005, porém o(a) gestor(a) de risco terá a flexibilidade de associar os ativos e/ou processos com outras ameaças e vulnerabilidades identificadas e não catalogadas.

Em seguida, o(a) gestor(a) de risco deverá analisar os impactos (Quadro 1) decorrentes de cada combinação das ameaças e vulnerabilidades, as quais estarão associadas a cada mapeamento realizado, caso o risco identificável se concretize:

Insignificante	**1**	Impacto mínimo nos objetivos do processo.
Menor	**2**	Impacto pequeno nos objetivos do processo.
Moderado	**3**	Impacto moderado nos objetivos do processo, porém recuperável.
Significativo	**4**	Impacto significativo nos objetivos do processo, de difícil reversão.
Forte	**5**	Impacto catastrófico nos objetivos do processo, de forma irreversível.

Quadro 1: Escala de impacto

Após a avaliação do impacto, é necessário avaliar a probabilidade (Quadro 2) de ocorrência de tal risco, ou seja, a probabilidade de uma ameaça explorar a vulnerabilidade:

Raro	**1**	Em situações excepcionais o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.
Improvável	**2**	De forma inesperada ou casual o evento poderá ocorrer, pois as circunstâncias indicam pouca possibilidade.

Possível	**3**	De alguma forma o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.
Provável	**4**	De forma esperada o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.
Quase certo	**5**	De forma garantida o evento ocorrerá, pois as circunstâncias indicam claramente essa possibilidade.

Quadro 2: Escala de probabilidade

Ao inserir os valores de impacto (I) e probabilidade (P), o nível de risco (R) será calculado automaticamente multiplicando os dois valores (P x I). Os controles de segurança já existentes deverão ser levados em consideração no processo de avaliação de risco.

A matriz de risco (Quadro 3), representa os possíveis resultados da combinação das escalas de probabilidade e impacto (P x I), determinando o nível de risco (R):

		PROBABILIDADE x IMPACTO (P x I)				
PROBABILIDADE	Quase certo (5)					
	Provável (4)					
	Possível (3)					
	Improvável (2)					
	Raro (1)					
		Insignificante (1)	Menor (2)	Moderado (3)	Principal (4)	Forte (5)
		IMPACTO				

Quadro 3: Matriz de riscos

Vale destacar que quanto maior a probabilidade e o impacto, maior será a medida de risco. Desse modo, com base nos níveis de impacto e probabilidade será estabelecido o nível de criticidade (Quadro 4) dos riscos identificados:

CRITICIDADE
Menor
Moderada
Maior
Severa

Quadro 4: Criticidade do risco

Diante disso, o(a) gestor(a) de risco deverá avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento. Os riscos classificados com as criticidades “menor” e “moderada” serão considerados aceitáveis e deverão ser monitorados constantemente pelo(a) gestor(a). Enquanto os riscos classificados com as criticidades “maior” e “severa” serão considerados inaceitáveis e deverão ser tomadas ações para tratá-los.

4.2 Tratamento de Risco

O tratamento de risco envolverá a escolha de estratégias para alterar o nível de cada risco identificado, bem como o desenvolvimento de planos de tratamento que, uma vez executados, resultarão na implementação de novos controles internos ou na modificação dos controles existentes.

As opções de tratamento de riscos incluem evitar, reduzir ou mitigar, transferir ou compartilhar e aceitar ou tolerar o risco. Uma ou mais opções de tratamento deverão ser selecionadas para riscos classificados com criticidade “maior” e/ou “severa”. São elas:

I - evitar o risco: decide-se não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

II - reduzir ou mitigar o risco: adotar ações para reduzir a probabilidade ou a consequência negativa associada a um risco. Exemplo: adoção de controles de segurança;

III - transferir ou compartilhar os riscos: o ônus associado a um risco é compartilhado com outra entidade. Exemplo: contratação de seguros, terceirização de atividades, etc.;

IV - aceitar ou tolerar o risco: assumem-se as responsabilidades caso o risco se materialize. Esse item só será permitido se outras opções de tratamento tiverem custo maior do que o impacto potencial.

Deve-se entender, que o apetite pelo risco, definido como a quantidade de risco que uma organização está disposta a buscar ou aceitar, poderá variar de organização para organização. São fatores que afetam o apetite pelo risco de uma organização: tamanho, complexidade e setor. Convém que o apetite pelo risco seja definido e regularmente analisado, criticamente, pela Alta Administração do PJMA.

Diante disso, o(a) gestor(a) de risco deverá avaliar o custo-benefício de cada opção de tratamento e definir as ações prioritárias a serem implementadas, bem como, o prazo de execução e avaliação dos resultados obtidos.

No caso da opção pelo item II acima, poderá ser necessário avaliar o novo valor de impacto e probabilidade no processo de tratamento de risco, a fim de avaliar a eficácia dos controles implementados.

O tratamento de risco relacionado aos processos terceirizados deverá ser abordado por meio dos contratos estabelecidos juntos às partes interessadas.

4.3 Monitoramento dos Riscos

O(A) gestor(a) de risco deverá monitorar, detectar falhas, rever e atualizar os processos de avaliação e tratamento de risco. Cada gestor(a) estabelecerá indicadores de acompanhamento e informes dos planos de ação instituídos. Após concretizados, os riscos e controles deverão ser reavaliados e revistos ao longo do tempo para identificar preventivamente o surgimento de riscos novos ou emergentes.

Os riscos deverão ser monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças:

a) nos critérios de avaliação e aceitação dos riscos;

b) no ambiente;

c) nos ativos e/ou processos;

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

A revisão será realizada pelo menos uma vez por ano, ou com maior frequência no caso de mudanças organizacionais significativas, nas tecnologias utilizadas, nos objetivos de negócio ou no ambiente de negócios do PJMA.

4.4 Registro e Comunicação

O(A) gestor(a) de risco deverá registrar os resultados da avaliação e tratamento de risco dos ativos sob sua responsabilidade e todas as revisões ou evoluções subsequentes.

A comunicação sobre os riscos deverá ser realizada de forma clara, objetiva e eficiente, garantindo que as informações sejam compartilhadas com as partes envolvidas e interessadas.

5. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

5.1 Gestor(a) de Risco

Compete ao(à) gestor(a) de risco:

I - realizar a escolha dos ativos e/ou processos que terão os riscos gerenciados e tratados;

II - propor os níveis aceitáveis de exposição ao risco;

III - definir as ações de tratamento a serem implementadas, bem como o prazo de implementação e avaliação dos resultados obtidos;

IV - implementar o plano de ação definido para o tratamento de risco dos ativos e/ou processos mapeados;

V - realizar as atividades de identificação e avaliação de riscos dos ativos e/ou processos sob sua responsabilidade;

VI - gerenciar os riscos inerentes dos ativos e/ou processos, de forma a mantê-los em nível de exposição aceitável;

VII - comunicar novos riscos que não fazem parte da relação de riscos dos ativos e/ou processos já identificados.

6. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

7. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

8. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.