PDTIC 2024/2027

ANEXO V – Plano de Gestão de Riscos de TIC

DIRETORIA DE
TECNOLOGIA DA INFORMAÇÃO

INSS
INSTITUTO NACIONAL DO SEGURO SOCIAL

Março, 2024 | versão 1.0

PLANO DE GESTÃO DE RISCOS DE TIC

Este plano tem por objetivo apresentar a identificação e a análise dos principais riscos associados ao planejamento e à execução do PDTIC 2024/2027 e atingimento dos seus resultados.

Fundamenta-se no Artigo 6º, Inciso III da Portaria SGD/ME nº 778, de 04 de abril de 2019:

"Art. 6º O PDTIC é o instrumento de alinhamento entre as estratégias e os planos de TIC e as estratégias organizacionais, e deverá:
...
III - conter, no mínimo:
a) inventário de necessidades priorizado;
b) plano de metas e ações;
c) plano de gestão de pessoas;
d) plano orçamentário; e
e) plano de gestão de riscos;"

A Gestão de Riscos do INSS é o conjunto de princípios, alçadas, processos e atividades coordenadas para dirigir, controlar e monitorar a organização no que se refere a riscos. Estruturada em pilares fundamentais para sua implementação, a gestão de riscos do INSS é composta por normativos de base legal como a **Resolução CEGOV/INSS nº 5, de 28/05/2020 (alterada pela Resolução CEGOV/INSS nº 19, de 20/05/2022)** que instituiu a Política de Gestão de Riscos do INSS e a **Portaria Conjunta DIGOV/DTI/INSS nº 1, de 28/03/2023** que instituiu o Sistema de Gerenciamento de Riscos – SISGR/INSS como ferramenta oficial para identificação, análise, avaliação, comunicação e acompanhamento dos riscos mapeados no âmbito do INSS, sendo composta, também, por documentos de referência como a **Metodologia de Gerenciamento de Riscos do INSS** (Resolução CEGOV/INSS nº 20, de 20/05/2022), os quais direcionam a atuação finalística e de apoio à governança e gestão do INSS.

A Figura 01 ilustra os pilares da Gestão de Riscos do Instituto Nacional do Seguro Social – INSS:

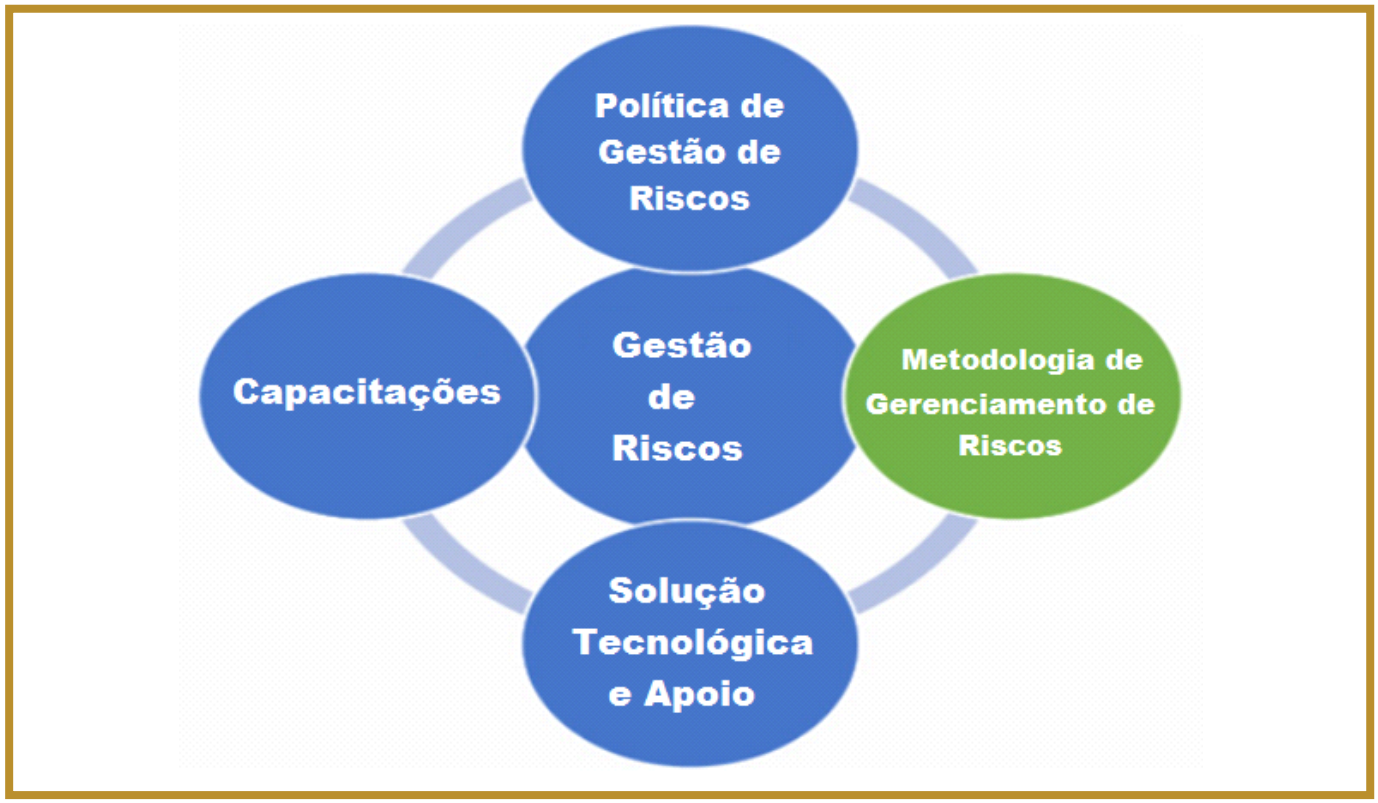

Figura 01 – Pilares da Gestão de Riscos do INSS

Procedimentos Gerenciais

Por meio de atuação integrada com assessoramento das funções de governança da Diretoria de Tecnologia da Informação – DTI e da Diretoria de Governança, Planejamento e Inovação – DIGOV, os coordenadores setoriais devem promover a gestão de riscos de TIC para que seja objeto de acompanhamento pelo Comitê Temático de Governança Digital (CTGD) e, sempre que cabível, pelo Comitê Estratégico de Governança (CEGOV) do Instituto.

As funções de governança atuam em conjunto para disponibilizar orientação do processo e da ferramenta de suporte (solução tecnológica) para o registro e gerenciamento dos riscos de TIC, de acordo com o preconizado nos instrumentos que compõem os pilares fundamentais da gestão de riscos do INSS. A visão básica do processo de gerenciamento de riscos pode ser identificada no macroprocesso representado na Figura 02:

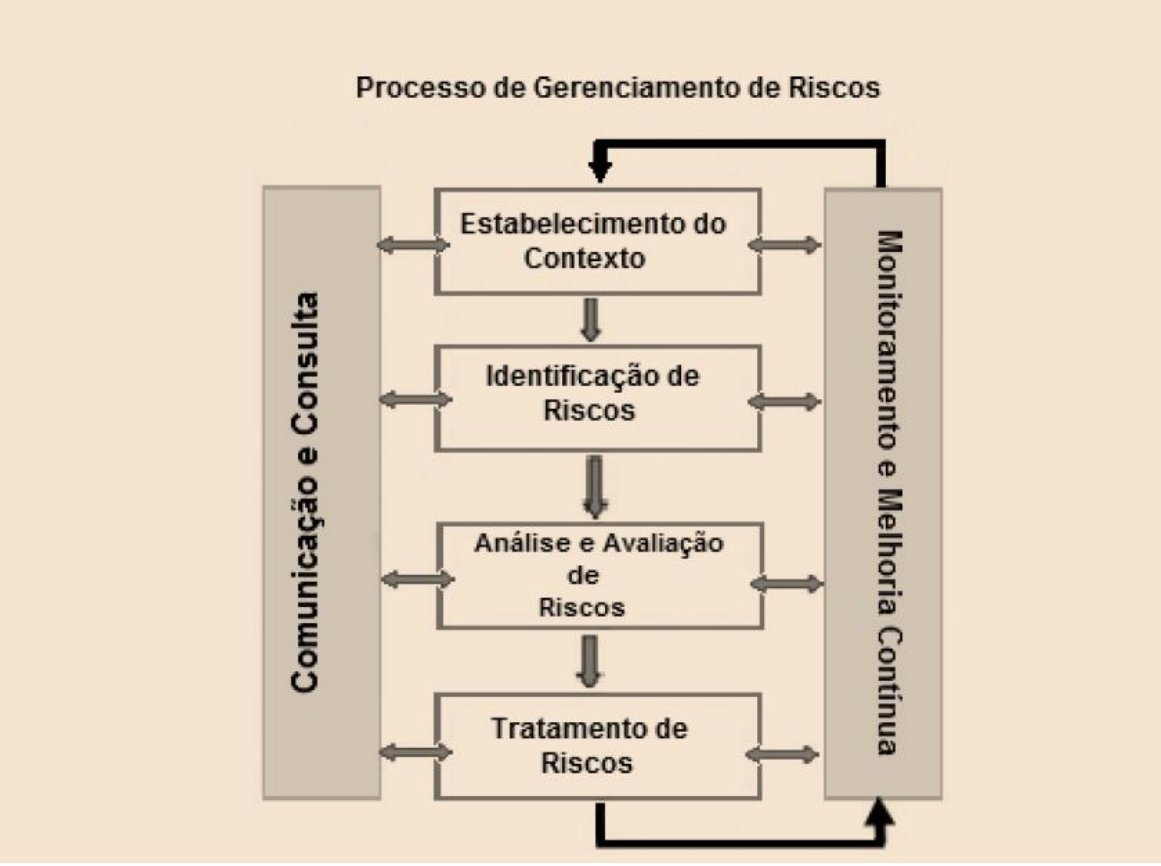

Figura 02 – Processo de Gerenciamento de Riscos (Fonte: Norma ABNT NBR ISO 31000:2009 – adaptado)

Inventário Preliminar de Riscos Corporativos de TIC

R1. Indisponibilidade dos responsáveis indicados para o planejamento ou execução do PDTIC
R2. Desalinhamento entre o resultado da Análise SWOT na etapa de planejamento do PDTIC (diagnóstico do ambiente) e a realidade
R3. Descontinuidade de iniciativas de TIC (ações e projetos)
R4. Baixa execução das iniciativas de TIC planejadas
R5. Falha no monitoramento do PDTIC

Protocolo PIV para análise de Riscos

De acordo com a metodologia são apresentadas as escalas de Probabilidade, Impacto e Nível de Risco / Vulnerabilidade para análise dos riscos:

Probabilidade

A probabilidade de um evento ocorrerá e será medida analisando as causas ou o evento de risco, considerando aspectos como a frequência observada ou esperada.

A probabilidade (P) é pontuada de 1 a 5, conforme demonstrado na tabela a seguir:

Probabilidade	Descrições de suporte à análise
5 – Muito Alta (quase certo ou muito provável)	Pela análise do histórico, evento deve ocorrer em mais de 90% dos ciclos do processo/ação/sistema *(na maioria das circunstâncias)*
4 – Alta (provável)	Pela análise do histórico, evento deve ocorrer de 50% a 90% dos ciclos do processo/ação/sistema *(provavelmente na maioria das circunstâncias)*
3 – Média (possível)	Pela análise do histórico, evento deve ocorrer de 30% a 50% dos ciclos do processo/ação/sistema *(em algum momento)*
2 – Baixa (improvável)	Pela análise do histórico, evento deve ocorrer de 10% a 30% dos ciclos do processo/ação/sistema *(em algum momento)*
1 – Muito Baixa (rara)	Pela análise do histórico, evento deve ocorrer em menos de 10% dos ciclos do processo/ação/sistema *(em ciscunstâncias excepcionais)*

Tabela 01 – Escala de Probabilidade de Riscos de TIC

Impacto

O impacto será mensurado em função da análise das consequências de um evento de risco com relação às dimensões (custo, prazo, escopo e qualidade) no caso de projetos/processos/iniciativas e com relação à severidade que avalia o comprometimento do desempenho, confiabilidade ou qualidade do processo de trabalho ou do serviço provido tanto para o público interno quanto para o externo.

O Impacto (I) é pontuado de 1 a 5, conforme demonstrado na tabela abaixo:

Impacto	Descrições de suporte à análise
5 – Catastrófico (extremo)	Evento prejudica o alcance da missão institucional
4 – Grande	Evento prejudica o alcance do objetivo estratégico ao qual está vinculado
3 – Moderado	Evento prejudica o alcance dos objetivos do processo organizacional
2 – Pequeno	Evento prejudica o alcance das metas do processo organizacional
1 – Insignificante (incidental ou inexistente)	Evento causa pouco ou nenhum impacto nas metas do processo organizacional

Tabela 02 – Escala de Impacto de Riscos de TIC

Nível de Risco / Vulnerabilidade

O nível de risco corresponde a combinação do impacto e de suas probabilidades que possam comprometer a efetividade da gestão de TIC, bem como o alcance dos resultados pretendidos no Plano Diretor de TIC.

A tabela de níveis de risco define a Vulnerabilidade (V) ou grau de risco para avaliação da intensidade a qual uma instituição está exposta.

Nível de Risco / *Vulnerabilidade*	Pontuação	Descrições do nível de risco para suporte à análise	Tipo de Resposta	Ação de Controle
Risco Crítico / *Muito Alta*	13 a 25	Nível de risco muito além do apetite a riscos. Indica que nenhuma opção de resposta foi identificada para reduzir a probabilidade e o impacto a nível aceitável *(nenhum tipo de ação preventiva ou de controle)*	Evitar / Prevenir	Promover ações que evitem / eliminem as causas e efeitos
Risco Alto / *Alta*	07 a 12	Nível de risco além do apetite a riscos. Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos *(ações preventivas ou de controle insuficientes)*	Tratar / Reduzir (mitigar)	Adotar medidas para reduzir a probabilidade ou impacto dos riscos, ou ambos
Risco Moderado / *Média*	04 a 06	Nível de risco dentro do apetite a riscos. Indica que o risco residual requer atividades de monitoramento específicas, visando a manutenção de resposta e controles para manter o risco neste nível ou reduzi-lo sem custos adicionais *(ações preventivas ou de controle parcialmente suficientes)*	Compartilhar / Transferir	Reduzir a probabilidade ou impacto pela transferência ou compartilhamento de parte do risco: (seguro, transações de hedge, terceirização da atividade)
Risco Pequeno / *Baixa*	01 a 03	Nível de risco dentro do apetite a riscos. Indica que o risco inerente já está dentro da tolerância a risco *(ações preventivas ou de controle suficientes)*	Aceitar	Conviver com o evento de risco, mantendo práticas e procedimentos existentes

Tabela 03 – Escala de Níveis de Riscos de TIC

Matriz de Riscos

A seguir é apresentada a matriz de riscos, composta pelos elementos referentes às escalas de probabilidade e impacto com os correspondentes níveis de risco.

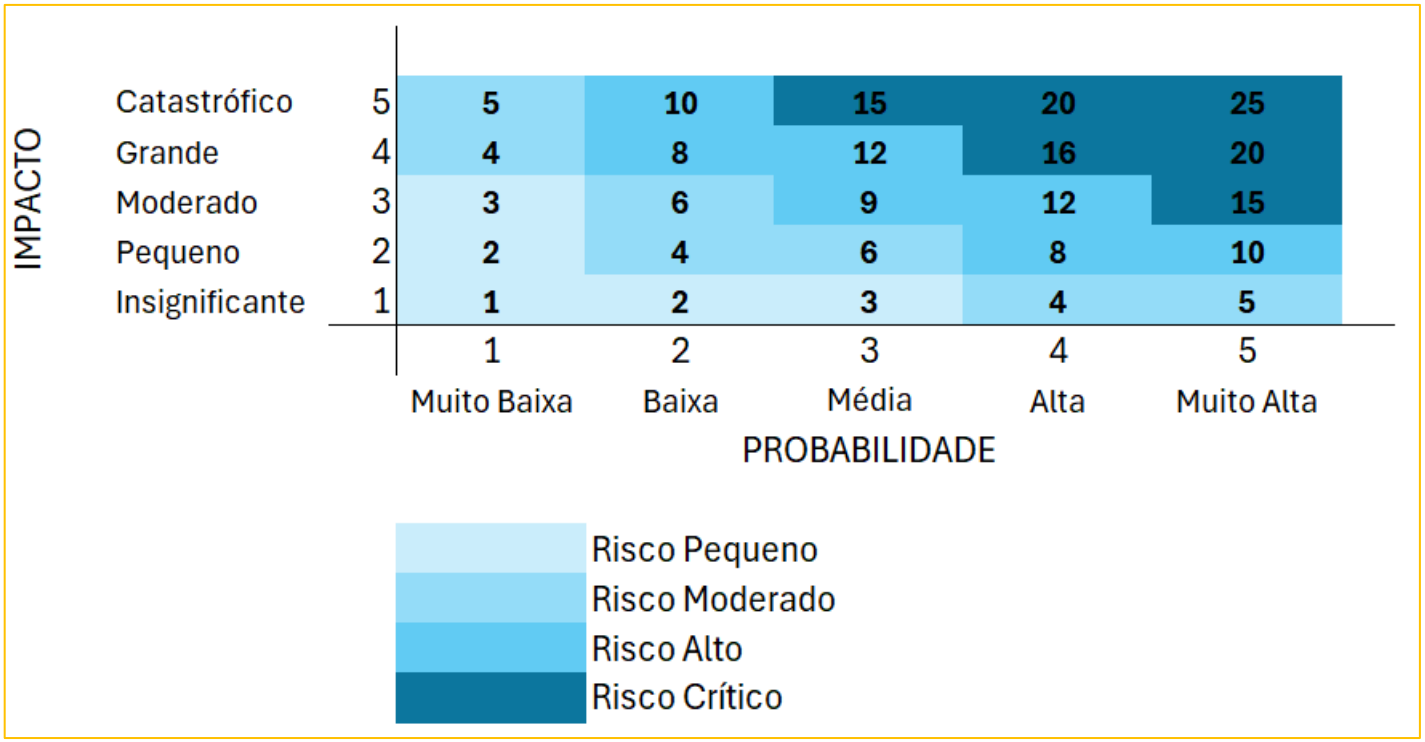

Figura 03 – Matriz de Riscos

Avaliação / Controle dos Riscos e Classificação no Diagrama de Riscos por Nível

Risco	Categoria do Risco	Aval. Risco Residual		Pontuação	Diagrama de Riscos (Nível)	Resposta ao Risco
		P	I			
R1. Indisponibilidade dos responsáveis indicados para o planejamento ou execução do PDTIC	Estratégico	2	3	6	Moderado	**Mitigar:** Sensibilização dos gestores sobre o planejamento a ser executado; substituir atores envolvidos no processo;
R2. Desalinhamento entre o resultado da Análise SWOT na etapa de planejamento do PDTIC (diagnóstico do ambiente) e a realidade	Operacional	2	3	6	Moderado	**Mitigar:** Adotar ações de apoio ao desenvolvimento das atividades junto aos gestores e indicados; realizar a adequação das iniciativas propostas com equívoco.
R3. Descontinuidade de iniciativas de TIC (ações e projetos)	Estratégico	2	4	8	Alto	**Mitigar:** Instar as instâncias de Governança para comunicação, acompanhamento e prestação de contas; acompanhar a atualização das normas para identificação dos possíveis impactos na execução do PDTIC.
R4. Baixa execução das iniciativas de TIC planejadas	Operacional	2	3	6	Moderado	**Mitigar:** Estabelecer o monitoramento contínuo do PDTIC; estabelecer um Plano de Contingência.
R5. Falha no monitoramento do PDTIC	Operacional	2	3	6	Moderado	**Mitigar:** Planejamento adequado das ações visando a melhoria do processo de monitoramento;

(Legenda: P – Probabilidade / I – Impacto)

Tabela 04 – Avaliação e Classificação dos Riscos em Inventário Preliminar

Diagrama de Riscos

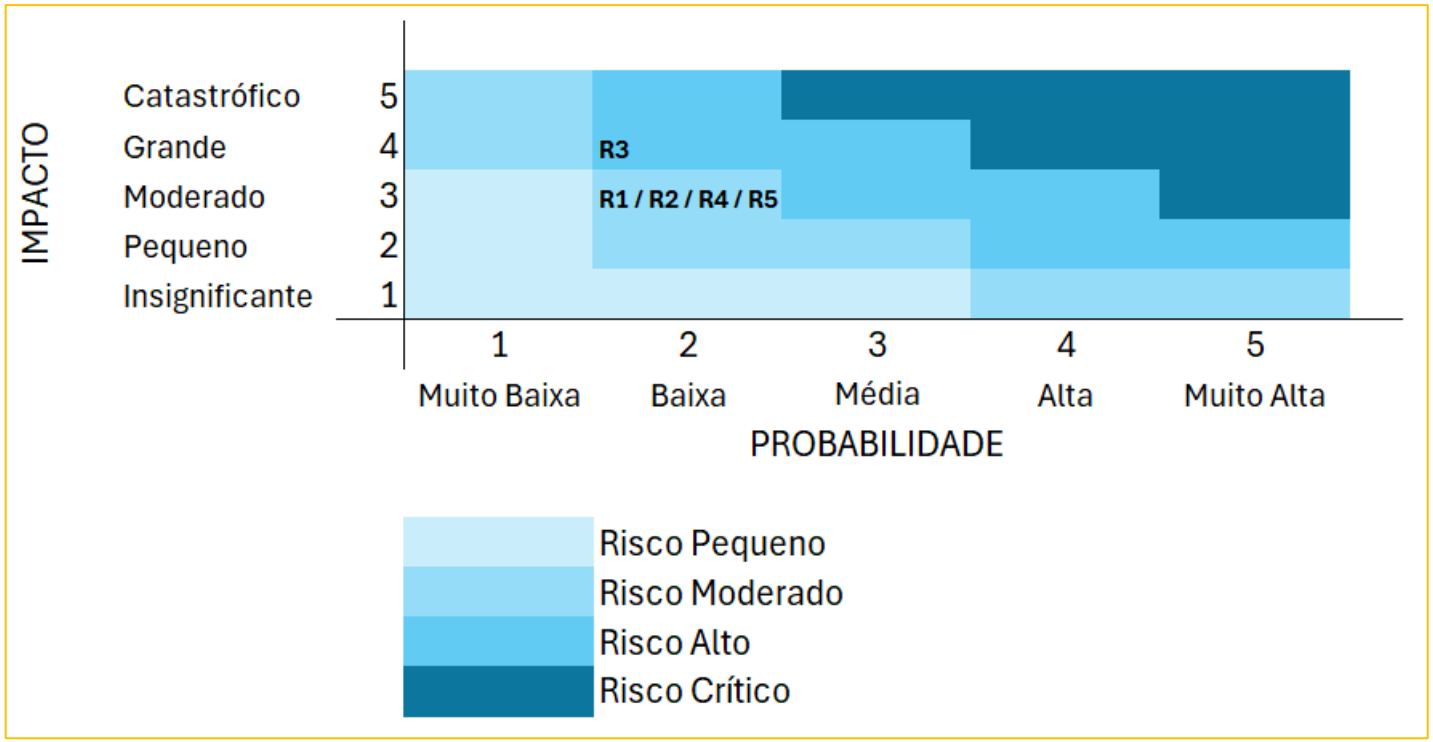

Figura 04 – Diagrama de Riscos