PORTARIA-TJ - 35272023
Código de validação: 440B7F2922
(relativo ao Processo 385222023)

Aprova o Plano de Gestão de Riscos de Tecnologia da Informação do Poder Judiciário do Maranhão.

O **DESEMBARGADOR PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO MARANHÃO**, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução CNJ nº 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a aprovação da minuta do Plano de Gestão de Risco de TIC pelo Comitê de Governança de TIC, em reunião realizada em 22 de maio de 2023, conforme Ata da 7ª Reunião do CgovTIC, Tema 6;

R E S O L V E,

Art. 1. Aprovar o Plano de Gestão de Riscos de Tecnologia da Informação, conforme descrito no Anexo I;

Art. 2. Esta Portaria entra em vigor na data da sua publicação.

DÊ-SE CIÊNCIA, PUBLIQUE-SE E CUMPRA-SE.

PALÁCIO DA JUSTIÇA “CLÓVIS BEVILÁCQUA” DO ESTADO DO MARANHÃO

Anexo I
Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação
Diretoria de Informática e Automação

Data	Versão	Descrição	Autor	Aprovador
22/05/2023	V1	Emissão Inicial	Diretoria de Informática	Comitê de Governança de TIC

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor	Aprovador

1. INTRODUÇÃO

O Plano de Gestão de Riscos de TIC do Poder Judiciário do Estado do Maranhão (PGRTIC-PJMA) foi concebido com o intuito de internalizar práticas de gestão de riscos nas atividades conduzidas pelas equipes técnicas da Diretoria de Informática e Automação (DIA). A perspectiva de riscos é de suma importância no processo de tomada de decisões de maneira racional e fundamentada, contribuindo para aumentar a capacidade da organização em lidar com eventos inesperados que possam afetar negativamente os objetivos planejados.

A gestão de riscos não deve ser considerada apenas como uma tarefa burocrática, mas sim como um instrumento de tomada de decisão essencial que deve ser integrado aos processos de planejamento e execução dos trabalhos relevantes da DIA. É importante destacar que, por meio do PGRTIC-PJMA, esta Diretoria busca, através de procedimentos e processos de controle, minimizar a exposição a riscos, promover a conformidade regulatória, auxiliar a garantia da segurança e da privacidade das informações.

Dessa forma, as atividades de administração, avaliação e revisão periódica do PGRTIC-PJMA ficarão sob a responsabilidade desta diretoria, a fim de garantir que as práticas de gestão de riscos de TIC mantenham-se atualizadas e alinhadas com as necessidades do PJMA. Além disso, a DIA também empreenderá esforços para disseminar a cultura de gestão de riscos em todas as suas coordenadorias, a fim de que a perspectiva de riscos seja amplamente compreendida e considerada no processo decisório.

2. ESCOPO

O escopo do Plano de Gestão de Riscos de Tecnologia da Informação do PJMA inclui a identificação, avaliação, priorização, tratamento e monitoramento dos riscos associados às atividades operacionais, táticas e estratégicas da DIA, bem como aos projetos, iniciativas estratégicas, ativos de TI e processo de contratação.

3. DOCUMENTOS DE REFERÊNCIA

Os seguintes documentos de referência foram empregados na elaboração deste plano:

- Resolução CNJ 370/2021;
- Resolução CNJ 396/2021;
- Portaria CNJ 162/2021;
- ABNT NBR ISO/IEC 27005:2019;
- ABNT NBR ISO 31000:2018;
- Manual de Gestão de Riscos do Tribunal de Contas da União (TCU);
- Política de Gestão de Riscos do Tribunal de Justiça do Maranhão (TJMA).

4. APETITE AOS RISCOS

O apetite a riscos na TIC do PJMA está associado ao nível de risco que a organização está disposta a aceitar na busca e realização de sua missão quando relacionado às competências da DIA. O apetite é estabelecido pela alta administração e serve como ponto de referência para o planejamento das estratégias e objetivos da TI.

Com base nas discussões realizadas e apresentadas na Política de Riscos do TJMA, considera-se que esta diretoria deve manter o nível de apetite a riscos compatível com a organização em que está inserida, qual seja, o perfil conservador. Sendo assim, após a identificação dos riscos, a Diretoria de Informática e Automação estabelecerá maior nível de controle e contramedidas aos riscos identificados, optando pelo convívio com um baixo patamar de risco. À medida que a maturidade na Gestão de Riscos do TJMA, assim como da DIA for evoluindo, o apetite a riscos será revisado.

5. PROCESSO DE GESTÃO DE RISCOS

O processo de gestão de riscos da Tecnologia da Informação baseia-se em fundamentos de normas reconhecidas internacionalmente, como as normas ISO 31.000 e 27.001, no Manual do TCU e, em especial, na Política de Riscos do TJMA.

O processo de gestão de riscos da TI adotado por esta Diretoria segue o processo estabelecido pela alta administração, onde o processo é melhor detalhado na Política de Riscos do TJMA (Capítulo 6. PROCESSO DE GESTÃO DE RISCOS) e envolve as seguintes etapas: estabelecimento do contexto; avaliação de risco, que engloba a identificação, a análise e a avaliação de riscos; tratamento de risco e monitoramento dos riscos e controles. É fundamental destacar que todas as etapas devem conter processos de comunicação sobre riscos com as partes interessadas, tanto internas quanto externas.

A gestão de riscos da TI é um processo contínuo e dinâmico que deve ser revisado e atualizado periodicamente, a fim de garantir sua eficácia e eficiência na gestão dos riscos que a área de TI possa enfrentar.

5.1. Estabelecimento do Contexto

O estabelecimento do contexto se refere ao entendimento do ambiente em que a área de TI está inserida e seus objetivos estratégicos. Nesta etapa, é importante captar uma visão abrangente dos fatores e ameaças potenciais que podem afetar a capacidade da área de TI atingir seus objetivos.

5.2. Avaliação do Risco

O processo de avaliação de risco é composto por três subprocessos: identificação, análise e avaliação de risco. O objetivo do processo de avaliação de riscos é identificar os riscos a partir do contexto estabelecido; em seguida, determinar as suas probabilidades de ocorrência e os impactos que teriam caso venham a acontecer e, por fim, usar estas informações para estabelecer priorização e criticidade, além de orientar a escolha das estratégias de tratamento mais adequadas para cada risco identificado.

5.3. Tratamento do Risco

O tratamento de cada risco envolve a escolha das estratégias mais adequadas para evitar, reduzir, compartilhar ou aceitar os riscos identificados. Nesta etapa, deverá ser definida a resposta ao risco com estabelecimento de ação mitigatória, controles primários, indicadores, prazos e responsável.

5.4. Monitoramento dos Risco

O monitoramento dos riscos e controles consiste na verificação contínua da eficácia das ações implementadas para gerenciar os riscos identificados. Além disso, deverá ser realizado análises periódicas de eventos e fatores de risco para identificar preventivamente riscos novos ou emergentes.

5.5. Comunicação Sobre os Riscos

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

5.6. MATRIZ DE RISCOS DE TI

A primeira versão da matriz contém os riscos identificados a partir do trabalho realizado a nível institucional e que são de responsabilidade da Diretoria de Informática e Automação.

Desembargador RICARDO TADEU BUGARIN DUAILIBE
1º Vice-Presidente do Tribunal de Justiça
Matrícula 176362

Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 10/08/2023 14:03 (RICARDO TADEU BUGARIN DUAILIBE)