



SEÇÃO VII DA GESTÃO DA INFRAESTRUTURA DE TI

Art. 21. A regulamentação da gestão da infraestrutura de TI contemplará:

I - quanto às mudanças:

a) registro, avaliação e aprovação das mudanças;

b) prévia comunicação aos usuários impactados; II - controle e gestão dos itens de configuração e dos ativos de TI. Parágrafo único. Caberá ao CETI em conjunto com a DTI, aprovar e priorizar as mudanças de grande impacto nos serviços de TI, levando-se em consideração os riscos de TI identificados.

SEÇÃO VIII DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO NOS ATIVOS DE TI

Art. 22. A regulamentação da gestão de que trata o art. 18 buscará garantir que os ativos críticos, os riscos, as ameaças, as vulnerabilidades e os incidentes de segurança sejam identificados, monitorados e priorizados por meio de controles efetivos.

Art. 23. O macroprocesso de gestão da segurança da informação nos ativos de TI contemplará a continuidade dos serviços de TI e o uso dos ativos de TI.

CAPÍTULO VII DAS DISPOSIÇÕES FINAIS

Art. 24. O CETI em conjunto com a DTI promoverá ações e estratégias para:

I - sensibilização da instituição quanto à importância da governança e gestão do uso da TI, pela adoção de boas práticas de TI, para o alcance dos objetivos estratégicos, em parceria com a Diretoria Geral e demais setores das áreas finalísticas e estruturantes.

II - comunicação visando ampliar a participação e a transparência das diversas ações relacionadas à TI na instituição com o apoio da Diretoria de Comunicação Social.

III - treinamento contínuo dos usuários em serviços de TI em parceria com a Escola Superior do Ministério Público do Estado de Alagoas (ESMP/AL);

Gabinete do Procurador-Geral de Justiça, em Maceió, 10 de fevereiro de 2025.

LEAN ANTÔNIO FERREIRA DE ARAÚJO
Procurador-Geral de Justiça

ATO PGJ Nº 06/2025

Dispõe sobre a Política de Gestão de Riscos de Tecnologia da Informação Ministério Público do Estado de Alagoas (PGTI/MPAL)

Art. 1º Instituir a Política de Gestão de Riscos de Tecnologia da Informação – PGRTI no âmbito do Ministério Público do Estado de Alagoas - MPAL.

Art. 2º A PGRTI/MPAL observará conceitos, objetivos, princípios, diretrizes, papéis e responsabilidades estabelecidos neste ato, bem como as disposições constitucionais, legais e regimentais vigentes.

CAPÍTULO I DOS CONCEITOS



Art. 3º Para os efeitos do presente ato, considera-se:

- I – serviço de TI: uma ou mais soluções de TI que, em conjunto, habilitam um processo de negócio;
- II – catálogo de serviços de TI: banco de dados ou documento estruturado contendo informações sobre os serviços de TI ativos;
- III – risco de TI: efeito da incerteza em projetos, iniciativas ou serviços de TI caracterizado por uma possível alteração negativa em relação ao resultado esperado;
- IV – natureza do risco: tipo do risco (financeiro, patrimonial, ético, de imagem, de conformidade, etc);
- V – nível de risco: magnitude do risco, obtida a partir do produto da probabilidade de ocorrência do risco pelo seu impacto;
- VI – tolerância ao risco: nível de risco que a Instituição considera aceitável;
- VII - evento: ocorrência, interna ou externa, capaz, de causar impacto em objetivos estratégicos, programas, projetos, processos de trabalho ou iniciativas institucionais;
- VIII – processos críticos de trabalho: são aqueles sem os quais as funções essenciais do MPAL não podem ser exercidas;
- IX - serviços críticos de TI: são aqueles que dão suporte aos processos críticos de trabalho e constam no catálogo de serviços de TI.

CAPÍTULO II DOS OBJETIVOS

Art 4º A PGRTI/MPAL tem por objetivo geral:

- I – assegurar o alinhamento do processo de gestão de risco de TI com a gestão de risco da Instituição;
- II – identificar, avaliar e reduzir continuamente o risco relacionado à TI dentro dos níveis de tolerância estabelecidos pela alta administração da instituição;
- III – promover o balanceamento adequado entre os custos e os benefícios da gestão dos riscos de TI.

CAPÍTULO III DAS DIRETRIZES

Art 5º A gestão de risco de TI deve ser:

- I – aplicada a projetos, iniciativas e serviços críticos de TI;
- II – incorporada ao processo de tomada de decisões dentro da Diretoria de Tecnologia da Informação – DTI e ao Comitê Estratégico de Tecnologia da Informação – CETI;

CAPÍTULO IV DOS PAPÉIS E DAS RESPONSABILIDADES

Art 6º Serão responsáveis pela coordenação e gestão da PGRTI/MPAL, as seguintes instâncias institucionais, respectivamente:

- I - Comitê Estratégico de Tecnologia da Informação — CETI;
- II - Diretoria de Tecnologia da Informação em conjunto com as seções da DTI quanto às matérias inerentes a estas.

Art 7º A gestão de riscos de TI deverá:

- I – escolher, justificadamente, dentre os objetos sob sua responsabilidade previstos no art. 5º, quais terão os riscos gerenciados, considerando a dimensão dos prejuízos que possam causar;



II – assegurar que os riscos sejam gerenciados de acordo com os critérios estabelecidos neste documento;

III – monitorar informações adequadas sobre a gestão de riscos e reportá-las às partes interessadas.

CAPÍTULO V DA GESTÃO DE RISCO DE TI

Art. 8º A gestão de riscos de TI é um processo que deve ser executado considerando, no mínimo, as seguintes etapas:

I – identificar e descrever os riscos de TI: consiste na busca, no reconhecimento e na descrição de riscos, mediante a identificação de fontes, eventos, causas e potenciais consequências. Essa ação é validada mediante registro dos riscos identificados em documento, planilha ou sistema, sempre de forma padronizada e gerenciável;

II – avaliar os riscos de TI: compreender a natureza do risco e determinar o respectivo nível de risco mediante a combinação da probabilidade de sua ocorrência e dos possíveis impactos, observando os seguintes critérios:

a) o risco de TI deve ser classificado quanto a sua natureza: financeira, patrimonial, ética, de imagem ou de conformidade;

b) a probabilidade de o risco de TI ocorrer deverá ser classificada como baixa, média e alta;

c) o impacto deverá ser classificado como pequeno, intermediário ou grande;

d) os níveis de riscos devem ser classificados, após análise da combinação entre probabilidade e impacto, como sendo de baixa gravidade, média gravidade ou alta gravidade.

III – tratar os riscos de TI: consiste na seleção e na implementação de uma ou mais ações de tratamento, que terão o objetivo de evitar, mitigar, transferir ou aceitar o risco;

IV - as propostas de tratamento dos riscos de TI devem ser aprovadas pelo CETI, quando tratarem de projetos, iniciativas ou serviços que deem suporte aos processos críticos de trabalho, ou pelo Diretor de TI nos demais casos;

V – monitorar e comunicar: verificar continuamente se os riscos se concretizaram, se as ações de tratamento propostas foram executadas, se houve sucesso no tratamento ou na mitigação dos riscos de TI e comunicar os resultados às partes interessadas com base nos critérios a seguir:

a) a comunicação deve ser periódica e por meio da apresentação de relatório;

b) a frequência da comunicação deve ser definida junto com as partes interessadas.

VI – melhorar continuamente: a partir da análise dos resultados do monitoramento, propor, quando for necessário, melhorias para a gestão dos riscos, considerando que:

a) riscos antes aceitáveis, por exemplo, podem ser reclassificados e tratados com outras ações;

b) novos riscos podem ser identificados e gerenciados.

CAPÍTULO VI DAS DISPOSIÇÕES FINAIS

Art. 9º O CETI, em conjunto com a DTI, promoverá ações e estratégias para:

I - sensibilização da instituição quanto à importância da gestão de riscos de TI, pela adoção de boas práticas de TI, para o alcance dos objetivos estratégicos, em parceria com a Diretoria Geral e demais setores das áreas finalísticas e estruturantes;

II - comunicação visando ampliar a participação e a transparência das diversas ações relacionadas à TI na instituição com o apoio da Diretoria de Comunicação Social;

III - treinamento contínuo dos usuários em serviços de TI em parceria com a Escola Superior do Ministério Público do Estado de