GABINETE DA PROCURADORIA-GERAL DE JUSTIÇA
Endereço: Rua do Araxá ,nº S/N - Araxá. CEP: 68903-883. Macapá. - Amapá.
Email: procuradoria@mpap.mp.br Tel.: (96) 3198-1625

Ato Normativo Nº 0000014/2025-GAB/PGJ

Institui a Política de Gestão de Continuidade de Serviços de TI no âmbito do Ministério Público do Estado do Amapá.

O **PROCURADOR-GERAL DE JUSTIÇA** do Ministério Público do Estado do Amapá, no uso das atribuições que lhe confere o art. 127, § 2º, da Constituição Federal, e o art. 4º, inciso II, da Lei Complementar Estadual nº 0079/2013;

CONSIDERANDO a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP), disciplinada pela Resolução n. 171, de 27 de junho de 2017, do Conselho Nacional do Ministério Público;

CONSIDERANDO a norma internacional ABNT/NBR ISO 22.301:2020 que especifica os requisitos para planejar, estabelecer, implementar, monitorar e melhorar continuamente um Sistema de Gestão de Continuidade de Negócio (SGCN) e a norma ABNT/NBR ISO 22.313:2020 que estabelece as orientações, recomendações e permissões para aplicação desses requisitos.

RESOLVE:

CAPÍTULO I

Das Disposições Preliminares

Art. 1º. Fica instituída a Política de Gestão de Continuidade de Serviços de TI - TICon no âmbito do Ministério Público do Estado do Amapá (MPAP), que estabelece objetivos, princípios, diretrizes, responsabilidades relacionadas ao processo de Gestão da Continuidade dos Serviços de TI do MPAP de forma eficiente, segura e em conformidade com as obrigações legais e regulatórias aplicáveis, nos termos deste Ato Normativo.

Parágrafo único. Esta política e as eventuais normas, metodologias, manuais e procedimentos dela decorrentes aplicam-se a todo o Departamento de Tecnologia da Informação (DTI) e a outras unidades que utilizem os serviços de TI para a execução de suas atividades, inclusive as unidades do Centro Integrado de Inteligência e Investigação (CIII), englobando, direta ou indiretamente, colaboradores e prestadores de serviços que utilizem os serviços de TI do MPAP.

Art. 2º. Para os fins deste ato, consideram-se os termos e as definições constantes no Glossário das Políticas de TI do MPAP.

CAPÍTULO II

Dos Objetivos, Princípios e Diretrizes

Art. 3º. São objetivos da TICon:

I - Declarar formalmente o comprometimento do MPAP no cumprimento das melhores práticas em Gestão de Continuidade na área de Tecnologia da Informação, visando mitigar os riscos de interrupções indesejadas nos serviços críticos de TI;

II - Desenvolver resiliência tecnológica, salvaguardar interesses e a reputação do MPAP diante de incidentes que provoquem a indisponibilidade de seus serviços de TI, reduzindo o tempo de resposta aos incidentes;

III - Preparar o MPAP para continuar a entregar seus serviços de TI em um nível aceitável com capacidade predefinida mesmo durante um incidente crítico;

IV - Promover a transparência e a comunicação eficaz entre todas as partes interessadas, facilitando o acompanhamento do progresso e o relatório de resultados de cada projeto;

V - Disponibilizar a metodologia de avaliação da criticidade dos serviços de TI para desenvolvimento e implantação dos Planos de Continuidade de TI (PCTI), identificando procedimentos e infraestrutura alternativa para manter a continuidade dos serviços;

VI - Assegurar a utilização eficiente e eficaz dos recursos disponíveis, incluindo financeiros, humanos e tecnológicos, a fim de garantir o melhor custo x benefício para o MPAP;

VII - Implementar práticas eficazes de identificação, avaliação e mitigação de riscos para minimizar impactos adversos na disponibilidade dos serviços de TI.

Art. 4º. A TICon fundamenta-se nos seguintes princípios:

I - Resiliência Tecnológica: assegura que o MPAP seja capaz de resistir e se adaptar a interrupções, mantendo a continuidade de seus serviços de TI críticos, mesmo diante de incidentes significativos;

II - Proteção dos Serviços de TI: visa proteger os serviços críticos de TI do MPAP contra ameaças e interrupções;

III - Disponibilidade de Serviços: busca garantir que os serviços de TI estejam disponíveis quando necessários, de acordo com os níveis de serviço acordados;

IV - Cultura de Continuidade: visa promover uma cultura organizacional que valorize a continuidade de serviços de TI e a preparação para emergências em todos os níveis;

V - Conformidade Normativa: visa garantir que a TICon esteja em conformidade com as normas do CNMP, com as melhores práticas de mercado e com outras regulamentações aplicáveis.

Art. 5º. As diretrizes para execução TICon compreendem:

I - Análise de Impacto nos Serviços de TI (ITSIA): é o processo de identificação e avaliação dos impactos que a indisponibilidade de serviços de Tecnologia da Informação pode causar nas operações críticas do MPAP;

II - Avaliação de Riscos: avaliações de riscos periódicas, visando identificar ameaças potenciais e vulnerabilidades que possam afetar a continuidade dos serviços de TI do MPAP;

III - Desenvolvimento de Estratégias de Continuidade: desenvolver e implementar estratégias eficazes para mitigar riscos e garantir a continuidade dos serviços críticos de TI;

IV - Elaboração de Planos de Continuidade de TI (PCTI): estabelecer, documentar e manter os Planos de Continuidade de Serviços de TI abrangentes que detalham as ações a serem tomadas em caso de interrupções provenientes de incidentes críticos que afetem os serviços de TI;

V - Treinamento e Conscientização Contínua: sugerir programas de treinamento e conscientização para garantir que todos os colaboradores do MPAP compreendam suas responsabilidades em relação à continuidade dos serviços de TI;

VI - Realização de Testes e Exercícios de Contingência: realizar testes e exercícios regulares dos PCTI para validar sua eficácia e identificar áreas de melhoria;

VII - Monitoramento e Revisão: implementar um processo contínuo de monitoramento e revisão da TICon para garantir sua relevância e eficácia, incorporando lições aprendidas e melhorias contínuas;

VIII - Comunicação e Relacionamento com Partes Interessadas: estabelecer canais de comunicação claros e eficazes com todas as partes interessadas internas e externas para garantir uma resposta coordenada a interrupções nos serviços de TI.

CAPÍTULO III

Do Sistema de Gestão de Continuidade de Serviços de TI

Art. 6º. O Sistema de Gestão de Continuidade de Serviços de TI trata da capacidade estratégica e tática da área de Tecnologia da Informação em planejar e responder a incidentes e interrupções, assegurando a continuidade dos serviços de TI em um nível previamente definido pelos gestores da área.

§ 1º. As etapas do Ciclo de Gestão de Continuidade de Serviços de TI devem estar integradas ao ciclo de vida dos serviços críticos de tecnologia da informação.

§ 2º. A gestão de crises tecnológicas, a continuidade de serviços de TI e os planos de recuperação de desastres são partes integrantes da governança de TI, sendo de responsabilidade da Diretoria de Tecnologia da Informação e dos gestores de sistemas.

Art. 7º. O Ciclo de Gestão de Continuidade de TI no MPAP tem duração de 1 (um) ano e é dividido em 4 (quatro) etapas:

I - Avaliação dos Serviços de TI;

II - Elaboração dos Planos de Continuidade de TI (PCTI);

III - Realização dos Testes de Contingência e Recuperação;

IV - Melhoria Contínua.

§ 1º. No primeiro semestre devem ser realizadas as atividades de identificação, revisão e avaliação dos serviços de TI, incluindo a Análise de Impacto nos Serviços de TI (ITSIA), o mapeamento de dependências tecnológicas e a definição das estratégias de continuidade para os cenários de falha mais relevantes.

§ 2º. No segundo semestre devem ser elaborados os Planos de Continuidade de TI (PCTI), bem como o agendamento e a execução dos testes de contingência, incluindo a elaboração dos respectivos relatórios técnicos de validação.

Art. 8º. As normas, procedimentos, manuais e metodologias de Gestão de Continuidade de Serviços de TI do MPAP devem considerar como referência, além dos normativos internos vigentes, as melhores práticas estabelecidas pelas normas ABNT/NBR ISO 22301:2020 e ABNT/NBR ISO 22313:2020.

Parágrafo único. A TICon, suas atualizações, bem como eventuais diretrizes complementares devem ser amplamente divulgadas a todos os colaboradores da área de TI, a fim de promover sua observância, assimilação e o fortalecimento da cultura de continuidade e resiliência tecnológica.

Da Avaliação dos Serviços de TI

Art. 9º. A identificação e o cadastramento dos serviços de TI devem ser baseados nas funções institucionais da área de Tecnologia da Informação, conforme descrito na lei e regimentos internos, considerando as responsabilidades essenciais e específicas atribuídas ao Departamento de Tecnologia da Informação (DTI).

§ 1º. A identificação dos serviços de TI deve conter, no mínimo, as seguintes informações:

I - Nome do serviço de TI (iniciando com verbo de ação, exemplo: "Gerenciar acesso de usuários", "Monitorar infraestrutura de rede");

II - Descrição resumida do serviço;

III - Entradas (todos os elementos que um serviço de TI necessita para funcionar adequadamente: documentos, dados, informações, integrações, etc.);

IV - Sistemas e outros serviços de TI vinculados, quando aplicável;

V - Recursos vinculados (infraestrutura, pessoas, sistemas, contratos e empresas terceirizadas);

VI - Análise de Impacto nos Serviços de TI - ITSIA;

VII - Tempo de Recuperação Esperado (RTO - Recovery Time Objective): tempo máximo aceitável entre a interrupção do serviço e a retomada das operações, com base nas estratégias definidas;

VIII - Saídas (todos os resultados, entregas ou funcionalidades geradas pelo serviço de TI)

Art. 10. A avaliação da criticidade dos serviços de TI será realizada por meio de um questionário de risco e impacto, aplicado pela equipe responsável pela continuidade de serviços de TI.

§ 1º. Ao final da avaliação, cada serviço avaliado será classificado nos seguintes níveis de criticidade: Baixo, Médio ou Alto.

§ 2º. Os serviços relacionados a sistemas críticos de TI, por suas características de alta disponibilidade e impacto direto nas operações institucionais, serão automaticamente classificados como de criticidade Alta.

Art. 11. O nível de criticidade dos serviços de TI será utilizado como um dos principais critérios para tomada de decisão nas seguintes situações:

I - Priorização na retomada de sistemas e serviços em ambientes de produção pelo DTI;

II - Definição e acionamento das estratégias de recuperação de desastres (Disaster Recovery);

III - Priorização na proteção da infraestrutura de TI que suporta serviços críticos.

Dos Cenários

Art. 12. Os principais cenários analisados pelo DTI para elaboração dos Planos de Continuidade de TI (PCTI), são:

I - Desastre em TI: situação de comprometimento total ou significativo e prolongado do ambiente central de TI do MPAP.

§ 1º. As estratégias de continuidade a serem adotadas devem levar em consideração os possíveis fatores: falha em procedimentos, problemas de infraestrutura, ataques cibernéticos e quaisquer outros eventos externos que venham impactar o processamento, armazenamento e comunicações e afetem os serviços de TI.

§ 2º. Neste cenário recomenda-se a adoção de estratégias que envolvam:

a) Definição de ambientes de processamento distribuídos em outros locais (cidades e/ou estados);

b) Redundância e espelhamento de recursos/equipamentos de processamento, armazenamento e comunicação de dados em outros locais.

II - Indisponibilidade de Infraestrutura de TI: situação de interrupção e/ou queda de desempenho dos serviços de TI devido a falhas em equipamentos e/ou sistemas de um dos ambientes centrais de TI, provocados por quaisquer fatores tais como: falha em procedimentos, problemas de infraestrutura, eventos externos e ataques cibernéticos.

§ 1º. Neste cenário recomenda-se a adoção de estratégias que envolvam:

a) Definição de ambientes de processamento distribuídos em diferentes locais;

b) Redundância e espelhamento de recursos/equipamentos de processamento, armazenamento e comunicação de dados;

c) Sistemas de backup em nuvem ou armazenamento off-site com replicação geográfica;

d) Soluções de disaster recovery automatizadas com sincronização em tempo real.

III - Indisponibilidade de Serviços Terceirizados de TI: interrupção dos serviços prestados por empresas contratadas pelo MPAP que afetam diretamente os serviços de TI.

§ 1º. É recomendável ao DTI observar:

a) Manifestações de categorias profissionais ou movimentos sociais que envolvam empregados de empresas fornecedoras de serviços de TI;

b) Problemas legais ou financeiros (insolvência, falência, concordata, etc.) envolvendo as empresas contratadas;

c) Outros problemas que afetem diretamente os empregados das empresas contratadas de forma a prejudicar a prestação dos serviços de TI.

§ 2º. Neste cenário recomenda-se a adoção de estratégias que envolvam:

a) Utilização dos serviços de outra empresa do mesmo ramo;

b) Absorção temporária dos serviços por servidores do MPAP;

c) Contratação emergencial de outras empresas;

d) Negociação de prazos com usuários;

e) Acionamento de fluxo de comunicação.

IV - Ataque Cibernético: incidente gerado a partir de qualquer tentativa de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado, ou fazer uso não autorizado dos sistemas e infraestrutura de TI.

§ 1º. Neste cenário recomenda-se a adoção de estratégias que envolvam:

a) Redundância de ambientes, equipamentos e empresas fornecedoras de circuitos de comunicação;

b) Testes periódicos dos procedimentos de preparação e resposta;

c) Fluxos de comunicação e acionamento;

d) Integração com a Política de Segurança Cibernética do MPAP, observando as medidas preventivas, de detecção, resposta e recuperação nela descritas;

Da Elaboração dos Planos de Continuidade de TI (PCTI)

Art. 13. A elaboração dos Planos de Continuidade de TI (PCTI) é obrigatória para os serviços de criticidade Alta.

Parágrafo único: Para os serviços de criticidade Média e Baixa a elaboração é facultativa, cabendo ao DTI avaliar o risco da não elaboração frente a possíveis perdas com interrupção.

Art. 14. O PCTI abrange as etapas de planejamento (antes do incidente), resposta (durante) e retorno (depois) para o enfrentamento de interrupções para os cenários definidos pelo DTI.

Art. 15. Os PCTIs devem ser atualizados e testados ao menos uma vez ao ano, conforme o cronograma do ciclo de avaliação de Gestão de Continuidade de TI definido pelo DTI.

Art. 16. O PCTI deve descrever de forma clara e objetiva:

I - Estratégias de atuação para cada cenário, visando garantir a continuidade dos serviços de TI em situações de contingência;

II - Critérios mensuráveis para avaliar a eficácia dos procedimentos estabelecidos para atuação em situação de crise.

Parágrafo único: É recomendável que o DTI mantenha cópia em meio eletrônico de seus PCTIs, em local seguro e de acordo com a Política de Segurança da Informação e a Norma de Backup do MPAP.

Da Realização dos Testes de Contingência

Art. 17. Todos os PCTIs, após aprovados, devem ser testados ao menos uma vez ao ano, independentemente do nível de criticidade dos serviços vinculados.

Parágrafo único: Cabe ao DTI avaliar a necessidade de realizar mais testes ao ano, considerando, por exemplo, a existência de:

I - Exigências normativas aplicáveis ao Ministério Público;

II - Recomendações específicas de órgãos de controle;

III - Requisitos de segurança definidos pelo Conselho Nacional do Ministério Público;

IV - Orientação da administração superior ou do Comitê Estratégico de TI;

V - Alterações significativas no ambiente ou nos recursos que compõem a estratégia contida no PCTI, inclusive pessoas;

VI - Quaisquer outros motivos que tornem necessário o aprimoramento da efetividade do PCTI.

Art. 18. Todo teste de contingência realizado deve ser evidenciado através do Relatório de Testes que deve descrever os resultados obtidos a partir dos critérios estabelecidos no PCTI.

Parágrafo único: O relatório deve conter evidências da realização do teste e ser assinado pelo Diretor de TI, em até 20 dias após sua realização ou dentro do prazo final do ciclo de Gestão de Continuidade de TI, o que ocorrer primeiro.

Art. 19. No caso dos testes com resultado "não satisfatório" cabe ao DTI:

I - Indicar no relatório as ações de melhoria;

II - Providenciar a realização das ações de melhoria, atualizando o PCTI;

III - Realizar novo teste em até 30 dias corridos, para avaliar a correção das deficiências detectadas.

Art. 20. Caso o teste de contingência gere algum risco de provocar interrupção real ou seja considerado de elevada complexidade para simular o cenário, o DTI deve comunicar o fato à alta administração, via e-mail corporativo, contendo a justificativa da impossibilidade do teste e a data provável do novo teste.

Da Melhoria Contínua

Art. 21. O processo de Gestão da Continuidade de TI do MPAP tem como objetivo principal permitir que a área de TI possa prover o nível mínimo de serviço acordado, minimizando o risco para um nível aceitável e planejado, recuperando os serviços essenciais de TI dentro dos requisitos e prazos adequados à necessidade das demais áreas do MPAP.

Parágrafo único: O processo de melhoria contínua visa:

I - Manter um conjunto de Planos e/ou procedimentos que suportem a Gestão de Continuidade de TI sempre atualizados e operacionais;

II - Assegurar que as estratégias de continuidade e recuperação sejam eficientes de modo a garantir a resiliência tecnológica do MPAP;

III - Definir mecanismos de monitoramento, através de indicadores e relatórios gerenciais periódicos para realizar proativamente os ajustes necessários.

Art. 22. Os procedimentos de recuperação de serviços de TI abrangem as atividades a serem realizadas para restaurar os serviços de TI em caso de ameaças de interrupção.

Art. 23. Os testes dos procedimentos de recuperação dos serviços de TI têm como objetivo:

I - Validar planos, roteiros, mapas de topologia e procedimentos, modificando e/ou acrescentando dados e informações quando necessário;

II - Manter e elevar a capacidade técnica e operacional dos profissionais do suporte, visando a manutenção dos níveis de qualidade, disponibilidade, operacionalidade, suporte e controle requeridos na prestação dos serviços de TI;

III - Acompanhar, verificar, validar e certificar o comportamento da infraestrutura de TI em situações de indisponibilidade parcial ou total.

Art. 24. Os Relatórios de Testes devem ser acompanhados de evidências que comprovem a realização do teste, visando validar a efetividade das estratégias adotadas.

Art. 25. Todos os procedimentos de recuperação de serviços de TI contidos nos PCTIs devem ser testados, no mínimo, uma vez por ano.

Art. 26. As equipes participantes do teste devem:

I - Registrar ou solicitar registro, na ferramenta de Gestão de Serviços de TI, de todo incidente ocorrido durante a realização dos testes de continuidade;

II - Receber, dar andamento/atendimento e controlar as ações decorrentes dos problemas ocorridos durante a realização de testes;

III - Propor alterações nos roteiros dos testes de continuidade.

Art. 27. Após a realização dos testes são realizadas reuniões de avaliação para verificação, análise e registro, previamente à elaboração do relatório final, dos problemas ocorridos, dos procedimentos executados e da necessidade de ações de melhoria.

Parágrafo único: Os testes classificados como "não satisfatórios" devem ser repetidos durante o mesmo ciclo de Gestão de Continuidade de TI, após solucionadas as pendências que comprometeram o resultado do teste anterior.

Art. 28. Após a elaboração do relatório final, eventuais ações de melhoria devem ser acompanhadas até a sua resolução, visando assegurar que os incidentes, problemas e outras falhas identificadas nos testes de continuidade de serviços de TI sejam tratados.

CAPÍTULO IV

Das Responsabilidades

Art. 29. Cabe ao Comitê Estratégico de TI do MPAP, como órgão máximo de governança de TI, as seguintes atribuições:

I - Aprovar a Política de Gestão de Continuidade de Serviços de TI, suas atualizações e normas complementares;

II - Aprovar e revisar, anualmente, a lista de serviços críticos de TI e seus respectivos níveis de criticidade;

III - Deliberar sobre os recursos necessários para implementação e manutenção das estratégias de continuidade dos serviços críticos de TI;

IV - Deliberar sobre os casos omissos desta Política e suas normas complementares;

V - Avaliar e decidir sobre riscos residuais identificados nos Planos de Continuidade de TI, quando os mesmos forem considerados de alto impacto institucional.

Art. 30. Cabe à Divisão de Governança de TI do MPAP as seguintes atribuições:

I - Coordenar a implementação e manutenção do Sistema de Gestão de Continuidade de Serviços de TI;

II - Prospectar normas externas que possam influenciar no Sistema de Gestão de Continuidade de Serviços de TI do MPAP;

III - Desenvolver e/ou ajustar políticas, estratégias, normas, metodologias e padrões para Gestão de Continuidade de TI;

IV - Definir e manter a metodologia de Análise de Impacto nos Serviços de TI (ITSIA);

V - Realizar análises periódicas da maturidade do processo de Gestão de Continuidade de TI;

VI - Coordenar a elaboração e revisão do Plano de Comunicação para situações de crise que afetem os serviços de TI;

VII - Propor ações de capacitação para os colaboradores diretamente envolvidos no processo de Gestão de Continuidade de TI;

VIII - Preparar relatórios gerenciais sobre o desempenho do Sistema de Gestão de Continuidade de Serviços de TI para o CETI;

IX - Coordenar a revisão anual dos níveis de criticidade dos serviços de TI.

Art. 31. Cabe à Divisão de Infraestrutura de TI do MPAP as seguintes atribuições:

I - Elaborar e manter atualizados os Planos de Continuidade de TI (PCTI) relacionados à infraestrutura tecnológica (data centers, servidores, redes, armazenamento, backup, entre outros);

II - Implementar e manter as estratégias de redundância e alta disponibilidade dos ambientes de infraestrutura que suportam os serviços críticos;

III - Planejar e executar os testes de continuidade relacionados à infraestrutura de TI;

IV - Elaborar os relatórios de resultados dos testes de continuidade sob sua responsabilidade;

V - Monitorar o ambiente de infraestrutura para detectar precocemente possíveis falhas que possam afetar a continuidade dos serviços;

VI - Implementar controles para mitigar riscos de segurança cibernética que possam afetar a continuidade dos serviços de TI;

VII - Manter documentado o mapeamento de dependências da infraestrutura tecnológica que suporta os serviços críticos;

VIII - Elaborar relatórios técnicos sobre incidentes que afetem a infraestrutura e impactem na continuidade dos serviços de TI.

Art. 32. Cabe à Divisão de Sistemas de TI do MPAP as seguintes atribuições:

I - Elaborar e manter atualizados os Planos de Continuidade de TI (PCTI) relacionados aos sistemas e aplicações críticas;

II - Implementar recursos de resiliência nas aplicações críticas, como mecanismos de tratamento de erros, retomada automática e otimização de desempenho;

III - Planejar e executar os testes de continuidade relacionados aos sistemas e aplicações;

IV - Elaborar os relatórios de resultados dos testes de continuidade sob sua responsabilidade;

V - Implementar mecanismos de auditoria e rastreabilidade nas aplicações para facilitar a recuperação em caso de falhas;

VI - Manter documentado o mapeamento de dependências entre sistemas, bancos de dados e serviços;

VII - Assegurar que o processo de desenvolvimento de software incorpore requisitos de continuidade de serviços;

VIII - Elaborar relatórios técnicos sobre incidentes que afetem os sistemas e impactem na continuidade dos serviços de TI.

Art. 33. Cabe à Divisão de Suporte e Serviços de TI do MPAP as seguintes atribuições:

I - Elaborar e manter atualizados os Planos de Continuidade de TI (PCTI) relacionados aos serviços de atendimento e suporte ao usuário;

II - Coordenar as comunicações com os usuários durante situações de crise que afetem os serviços de TI;

III - Planejar e executar os testes de continuidade relacionados aos serviços de suporte;

IV - Elaborar os relatórios de resultados dos testes de continuidade sob sua responsabilidade;

V - Manter equipes de atendimento treinadas para atuar conforme os procedimentos definidos nos PCTIs;

VI - Registrar e categorizar todos os incidentes relacionados à continuidade dos serviços de TI;

VII - Manter atualizadas as bases de conhecimento com soluções de contorno (workarounds) para incidentes recorrentes;

VIII - Elaborar relatórios estatísticos sobre incidentes que afetem a continuidade dos serviços de TI.

Art. 34. Cabe a todas as divisões do Departamento de Tecnologia da Informação (DTI) e as unidade do Centro Integrado de Inteligência e Investigação (CIII):

I - Identificar ameaças e adotar medidas para enfrentar situações adversas que afetem os serviços de TI sob sua responsabilidade;

II - Registrar no sistema de Gestão de Continuidade de TI todas as alterações no funcionamento normal dos serviços;

III - Cadastrar e manter atualizados os serviços de TI sob sua responsabilidade no catálogo de serviços;

IV - Comunicar, previamente, quaisquer eventos que possam causar interrupções aos serviços de TI;

V - Participar das avaliações de impacto da interrupção dos serviços de TI (ITSIA);

VI - Formalizar os PCTIs sob sua responsabilidade e apresentar os documentos relacionados à Gestão de Continuidade de TI aos órgãos internos e externos, quando solicitado;

VII - Realizar os testes dos PCTIs para avaliar a efetividade das estratégias adotadas e elaborar os respectivos relatórios;

VIII - Propor melhorias contínuas nos processos e procedimentos de continuidade de serviços de TI;

IX - Participar, ativamente, das situações de crise que afetem os serviços de TI, conforme os papéis e responsabilidades definidos nos PCTIs.

Do Comitê de Gestão de Crises de TI

Art. 35. Fica instituído o Comitê de Gestão de Crises de TI, composto pelo Diretor de TI, pelos chefes das divisões do DTI e por outros integrantes designados pelo Diretor de TI, com as seguintes atribuições:

I - Coordenar as ações de resposta a incidentes críticos que afetem múltiplos serviços de TI;

II - Declarar situação de crise de TI quando necessário, acionando os respectivos PCTIs;

III - Tomar decisões táticas e operacionais durante situações de crise;

IV - Realizar a comunicação com a alta administração e demais partes interessadas durante situações de crise;

V - Avaliar a efetividade das ações de resposta após a resolução de situações de crise;

VI - Propor melhorias nos PCTIs com base nas lições aprendidas.

Parágrafo único: O Comitê de Gestão de Crises de TI deve se reunir, no mínimo, uma vez por semestre para avaliar os planos de resposta a incidentes e, extraordinariamente, sempre que houver uma situação de crise que afete os serviços críticos de TI.

CAPÍTULO V

Das Disposições Finais

Art. 36. Esta Política será revisada periodicamente, pelo menos a cada ano, ou sempre que se entenda necessário, visando garantir que os Planos de Continuidade de Serviços de TI do MPAP estejam documentados e atualizados em conformidade às melhores práticas de Gestão da Continuidade de TI.

Art. 37. Casos omissos ou esclarecimentos desta Política de Gestão da Continuidade de Serviços de TI, Normas Complementares ou Procedimentos do MPAP são de exclusiva responsabilidade do Comitê Estratégico de TI (CETI) e passíveis de aprovação pela Procuradoria Geral de Justiça do Estado do Amapá, conforme o caso.

Art. 38. Este Ato entra em vigor na data de sua publicação e revogam-se as disposições em contrário.

Macapá, 03 de Outubro de 2025

{signatarios}

Assinado eletronicamente por **ALEXANDRE FLAVIO MEDEIROS MONTEIRO**, **PROCURADOR-GERAL DE JUSTIÇA**, em 03/10/2025, às 15:49, Ato Normativo Nº 004/2018-PGJ e Lei Federal nº. 11.419/2006