IMEI Instituto Mariano de Estudos e Inovação

PLANO DE CONTINGÊNCIA TECNOLÓGICA DA INFORMAÇÃO (TI)

Aracaju, 2026

SUMÁRIO

1. Objetivo
2. Aplicação e Escopo
2.1 Infraestrutura Física
2.2 Hardware
2.3 Software e Sistemas
2.4 Serviços de Rede
2.5 Dados e Informações
3. Diretrizes Gerais
4. Gestão de Riscos
5. Procedimentos de Resposta a Incidentes
6. Plano de Recuperação
7. Comunicação e Notificação
8. Treinamento e Conscientização
9. Manutenção e Atualização do Plano
10. Anexos

PLANO DE CONTINGÊNCIA TECNOLÓGICA DA INFORMAÇÃO (TI)

1. OBJETIVO

A operacionalidade contínua e eficiente dos serviços de Tecnologia da Informação (TI) constitui um pilar fundamental para o desenvolvimento e a excelência das atividades-fim e atividades-meio, abrangendo tanto os setores administrativos quanto os acadêmicos desta Instituição de Ensino Superior. Em plena conformidade com as diretrizes que estabelece a infraestrutura tecnológica como um componente essencial da qualidade educacional, este documento tem por objetivo precípuo instituir e formalizar os procedimentos, as ações e os métodos para a gestão de ocorrências, contingências e situações de emergência que possam impactar os serviços de TI.

O presente plano visa assegurar a resiliência e a alta disponibilidade dos serviços tecnológicos essenciais, garantindo que, diante de eventos adversos que possam ocorrer durante as atividades no campus ou que afetem sistemas acessados remotamente, as ações necessárias sejam aplicadas de forma coordenada, ágil e eficaz para a célere correção, mitigação dos impactos e o pleno restabelecimento da normalidade operacional.

2. APLICAÇÃO E ESCOPO

Este documento e seus procedimentos associados aplicam-se a todos os ativos de tecnologia da informação sob a gestão e responsabilidade do Instituto Mariano de Estudos e Inovação – IMEI. O escopo deste plano abrange, de forma não exaustiva:

- **Infraestrutura Física:** Servidores, *data centers* (locais ou em nuvem), equipamentos de rede (roteadores, *switches*, pontos de acesso), sistemas de cabeamento estruturado e fontes de energia ininterrupta (*Nobreaks*).
- **Hardware:** Computadores de mesa (*desktops*), *notebooks*, impressoras, projetores multimídia, e outros periféricos utilizados por colaboradores, docentes e discentes.

- **Software e Sistemas:** Sistemas de gestão acadêmica e administrativa (ERP), plataformas de ensino a distância (EAD), sistemas de bibliotecas, softwares de produtividade, aplicações departamentais e sistemas operacionais.
- **Serviços de Rede:** Conectividade com a internet, redes locais (LAN), redes sem fio (Wi-Fi), e serviços de segurança de perímetro, como o *Firewall*.
- **Dados e Informações:** Todos os dados institucionais, acadêmicos e administrativos, independentemente de seu formato ou meio de armazenamento.

Todos os colaboradores, docentes, discentes e prestadores de serviço que fazem uso da infraestrutura de TI da instituição são partes interessadas e devem observar as diretrizes aqui estabelecidas.

3. DEFINIÇÕES E TERMINOLOGIA

Para a correta interpretação e aplicação deste plano, adotam-se as seguintes definições, alinhadas às melhores práticas de mercado:

- **Acionamento:** Processo formal de ativação do plano de contingência e comunicação de uma situação de emergência à equipe designada para a resolução do incidente.
- **Contingência:** Estado de prontidão que envolve um conjunto de recursos, planos e procedimentos previamente definidos, destinados a garantir a continuidade dos serviços essenciais quando da ocorrência de um incidente disruptivo.
- **Incidente:** Qualquer evento não planejado que cause, ou tenha o potencial de causar, uma interrupção ou redução na qualidade de um serviço de TI, alterando a sua operação normal. A severidade de um incidente pode variar, podendo causar desde um pequeno transtorno até danos graves aos serviços institucionais.
- **Sistema de Chamados de Suporte Técnico:** Plataforma digital centralizada (software de *help desk*) para o registro, categorização, priorização, atribuição e acompanhamento de todas as solicitações de suporte técnico, garantindo a organização do fluxo de trabalho e a

comunicação transparente com o solicitante.

- **TI (Tecnologia da Informação):** Área estratégica responsável pela provisão, gestão, segurança e suporte de todos os recursos tecnológicos, sistemas e infraestrutura computacional da instituição.
- **Backup (Cópia de Segurança):** Processo de criação de cópias de dados de um sistema ou arquivos específicos, armazenadas em um local seguro e distinto do original, com o propósito fundamental de permitir a restauração da informação em caso de perda, corrupção ou desastre.
- **Intervenção:** Conjunto de ações táticas executadas durante uma emergência, em conformidade com os planos preestabelecidos, visando diagnosticar, conter, erradicar e recuperar os serviços afetados, minimizando os danos aos ativos de TI e o impacto nas operações da instituição.
- **Firewall:** Solução de segurança de perímetro de rede, baseada em hardware ou software, que monitora e filtra o tráfego de entrada e saída com base em um conjunto de regras de segurança, atuando como uma barreira de proteção entre a rede interna confiável e redes externas não confiáveis, como a Internet.
- **Situação de Emergência:** Condição crítica, desencadeada por um incidente, que resulta ou possui o potencial iminente de resultar em danos significativos aos sistemas, equipamentos, dados ou ao desempenho das atividades acadêmicas e administrativas da instituição.

4. RESPONSABILIDADES

4.1. Setor de Tecnologia da Informação (TI)

O Setor de TI é o guardião e principal executor deste plano. Suas atribuições incluem:

- Planejar, implementar, manter e aprimorar continuamente a infraestrutura de TI para garantir sua resiliência.
- Executar as ações de mitigação, contenção e recuperação descritas neste documento.
- Coordenar as equipes de resposta a incidentes, internas ou externas.
- Manter a comunicação clara e transparente com todas as partes

interessadas sobre o status dos incidentes.

- Revisar e atualizar este plano anualmente ou sempre que ocorrerem mudanças significativas no ambiente tecnológico.

4.2. Comunidade Acadêmica e Administrativa (Colaboradores, Docentes e Discentes).

Todos os usuários dos recursos de TI compartilham a responsabilidade de zelar pela segurança e estabilidade do ambiente tecnológico, devendo:

- Informar imediatamente ao Setor de TI sobre qualquer anomalia, falha, comportamento inesperado ou suspeita de incidente de segurança, utilizando os canais de comunicação oficiais.
- Adotar as boas práticas e políticas de uso dos recursos tecnológicos.
- Cooperar ativamente com o Setor de TI durante os processos de diagnóstico e resolução de incidentes.

5. CLASSIFICAÇÃO DE NÍVEIS DE INCIDENTES

Os incidentes serão classificados com base em seu impacto e urgência para priorizar a alocação de recursos e o tempo de resposta.

- **Nível I – Baixo Impacto:** Incidente que afeta um único usuário ou um serviço não crítico, sem impedir o andamento geral das atividades.
  - *Exemplo:* Problemas com periféricos (mouse, teclado), dificuldades de uso de um software específico que não paralise a função principal do colaborador.
- **Nível II – Médio Impacto:** Incidente que causa a interrupção parcial de um serviço ou impede a continuidade do trabalho de um colaborador, de um pequeno grupo ou afeta atividades acadêmicas isoladas.
  - *Exemplo:* Falha em um computador que impede sua utilização, indisponibilidade de um sistema departamental não essencial para toda a instituição.
- **Nível III – Alto Impacto (Crítico):** Incidente que causa a interrupção total de um serviço essencial, afetando um grande número de usuários, um setor inteiro ou toda a instituição, com potencial para paralisar as atividades acadêmicas e/ou administrativas.

- *Exemplo:* Indisponibilidade total da conexão com a internet, falha no servidor principal de arquivos, queda de energia elétrica geral no campus, indisponibilidade do sistema acadêmico principal.

6. MAPEAMENTO DE RISCOS E AÇÕES DE MITIGAÇÃO

Este plano foi desenvolvido para ser ativado em resposta a emergências que apresentem riscos à continuidade dos serviços. O Quadro 1 detalha os principais riscos identificados, suas descrições e as respectivas ações de mitigação.

Quadro 1 – Matriz de Riscos e Mitigação

Risco	Descrição Detalhada	Ações de Mitigação e Prevenção
Interrupção de Energia Elétrica	Perda de fornecimento elétrico por fatores externos (concessionária) ou internos (curto-circuito, falha em disjuntores), comprometendo todos os equipamentos eletrônicos.	Utilização de *Nobreaks* com autonomia adequada em servidores, equipamentos de rede e computadores críticos. Manutenção preventiva periódica da rede elétrica interna. Procedimentos para desligamento seguro (*shutdown*) dos sistemas em caso de falha prolongada.
Indisponibilidade de Rede/Circuitos	Falha na conectividade interna ou externa, causada por rompimento de cabos, defeito em equipamentos ativos de rede ou falha no serviço da operadora de internet.	Monitoramento ativo e contínuo da saúde dos equipamentos de rede. Contratos de Nível de Serviço (SLA) com a operadora de internet. Manutenção de inventário de equipamentos de rede para substituição rápida. Inspeção periódica da infraestrutura de cabeamento.
Falha em Equipamentos Gerais	Mau funcionamento ou parada total de equipamentos, decorrente de obsolescência, desgaste de componentes ou necessidade de intervenção de software.	Inspeções periódicas e manutenções preventivas. Política de atualização e ciclo de vida do parque tecnológico. Climatização adequada das salas de equipamentos e servidores. Manutenção de um estoque mínimo de equipamentos de reposição (*spare parts*).
Falha Humana (Acidental ou por Imperícia)	Ações não intencionais de usuários que resultam em exclusão de dados, configuração incorreta de sistemas ou danos físicos a equipamentos, por falta de atenção ou conhecimento técnico.	Programas contínuos de capacitação e treinamento em segurança da informação e uso de sistemas. Implementação do princípio do menor privilégio no controle de acesso. Criação e divulgação d e manuais de boas práticas. Auditoria regular dos acessos e permissões

Indisponibilidade de Sistemas	Impossibilidade de acesso a sistemas críticos (acadêmicos, administrativos), causada por falhas de software, hardware do servidor, ou problemas com serviços em nuvem.	Monitoramento constante da saúde dos servidores e aplicações. Rotinas de backup automatizadas e testes periódicos de restauração. Contratos de suporte técnico com os fornecedores dos sistemas. Arquitetura de sistemas que priorize a alta disponibilidade.
Ataques Cibernéticos Externos	Tentativas ou sucessos de ataques (ex: *Ransomware*, *Phishing*, DDoS) originados de fora da rede, visando o roubo de informações, a interrupção de serviços ou a extorsão.	Gerenciamento de *Firewall* de Próxima Geração (NGFW). Utilização de solução de antivírus/antimalware corporativa. Política de gestão de atualizações de segurança (*patch management*). Sistema de Detecção e Prevenção de Intrusão (IDS/IPS). Campanhas de conscientização dos usuários sobre segurança.
Ataques Cibernéticos Internos	Ações maliciosas ou negligentes por parte de usuários legítimos, que tentam acessar dados não autorizados ou deliberadamente causar a indisponibilidade de um serviço.	Segmentação da rede para isolar sistemas críticos. Monitoramento e registro (*logging*) de eventos de segurança. Gerenciamento de identidade e controle de acesso rigoroso. Políticas de uso aceitável claras e com consequências definidas.

7. ESTRATÉGIAS E PROCEDIMENTOS DE RESPOSTA A INCIDENTES

A seguir, são detalhados os fluxos de ação a serem seguidos para cada tipo de emergência identificada.

7.1. Interrupção de Energia Elétrica

1. **Identificação:** Constatação da falta de energia no campus.
2. **Ação Imediata:** O departamento de manutenção deve ser imediatamente acionado para verificar a causa e tomar as providências cabíveis.
3. **Contingência de TI:**

- Sistemas hospedados em nuvem permanecerão operacionais e acessíveis externamente.
- Equipamentos críticos (servidores, rede) e computadores administrativos continuarão funcionando com a energia dos *Nobreaks*. O Setor de TI monitorará a carga e iniciará o desligamento

seguro antes do esgotamento total.

- Os equipamentos em laboratórios e áreas acadêmicas serão religados de forma controlada após o restabelecimento da energia.

7.2. Problemas com Nobreak

1. **Identificação:** Alarme sonoro/visual do equipamento ou constatação de falha.
2. **Ação Imediata:** O colaborador deve desconectar os equipamentos do *Nobreak* defeituoso e conectá-los a um *Nobreak* de reserva ou a uma tomada estabilizada, comunicando o fato ao Setor de TI.
3. **Resolução:** O Setor de TI providenciará o envio do equipamento para assistência técnica especializada e, após o retorno, o testará e o designará como reserva.

7.3. Problemas de Conexão com a Internet

1. **Comunicação:** Qualquer colaborador deve notificar o Setor de TI por telefone em caso de indisponibilidade geral.
2. **Diagnóstico:** O Setor de TI realizará uma análise técnica preliminar.
3. **Escalonamento:** Se o problema for interno, a empresa de infraestrutura será acionada. Se for externo, a provedora de internet será contatada, registrando-se o protocolo de atendimento.

7.4. Problemas com Equipamentos de Rede

1. **Identificação:** Falha de conectividade setorial ou alerta de monitoramento.
2. **Ação:** O Setor de TI acionará a empresa responsável pela infraestrutura para diagnóstico e manutenção. Se o reparo não for viável, a substituição do equipamento será providenciada com urgência.

7.5. Problemas Físicos com Cabeamento de Rede

1. **Diagnóstico:** O Setor de TI verificará a integridade dos cabos e conectores com ferramentas adequadas.
2. **Resolução:**

   - Falha no conector: A troca e crimpagem serão realizadas imediatamente.
   - Rompimento do cabo: A substituição do lance de cabo será realizada

o mais rápido possível.

- Rompimento de fibra óptica: A provedora de internet ou empresa especializada será acionada.

7.6. Problemas com Computadores nos Laboratórios de Informática

1. **Comunicação:** O docente responsável deve abrir um chamado via Sistema de Suporte Técnico, detalhando o problema.
2. **Priorização:** Se o incidente impedir o andamento da aula, o atendimento será imediato. Caso contrário, será agendado.
3. **Resolução e Feedback:** Após a intervenção, o chamado será atualizado com a solução e o solicitante notificado.

7.7. Problemas com Computadores Administrativos

1. **Comunicação:** O colaborador deve registrar a ocorrência no Sistema de Chamados. Em caso de indisponibilidade do sistema, o contato telefônico é o canal alternativo.
2. **Priorização:** Incidentes que paralisem totalmente o trabalho do colaborador terão prioridade máxima.
3. **Resolução e Feedback:** O Setor de TI realizará o atendimento e informará o usuário sobre a conclusão através do sistema.

7.8. Problemas com Equipamentos Gerais (Impressoras, Projetores) O procedimento segue o mesmo fluxo do item 7.7, com comunicação via Sistema de Chamados e priorização baseada no impacto da falha.

7.9. Incidentes Causados por Falha Humana

1. **Comunicação:** O colaborador deve reportar o incidente ao Setor de TI via Sistema de Chamados. Alunos devem comunicar a um colaborador para que esta abra o chamado.
2. **Resolução:** O Setor de TI agendará o atendimento para reverter a ação (ex: restaurar um arquivo de backup) ou corrigir o problema.
3. **Ação Educativa:** O Setor de TI fornecerá ao usuário orientações para evitar a reincidência, reforçando as boas práticas.

7.10. Problemas de Acesso aos Sistemas

1. **Comunicação:** O colaborador deve reportar o problema via Sistema de Chamados.
2. **Análise e Escalonamento:** O Setor de TI realizará uma análise

inicial. Caso seja uma falha no software, o chamado será escalonado para o desenvolvedor ou para o suporte técnico do fornecedor.

3. **Resolução e Feedback:** O solicitante será mantido informado sobre o andamento e a conclusão.

7.11. Problemas com Acesso a um Site Específico

1. **Comunicação:** O usuário deve abrir um chamado informando a URL e a mensagem de erro.
2. **Análise:** O Setor de TI investigará se o bloqueio é justificado pelas regras do *Firewall*.
3. **Resolução:** Caso seja um bloqueio indevido para um site pertinente, a liberação será efetuada e o usuário informado.

7.12. Incidentes de Segurança (Ataques Externos)

1. **Detecção e Contenção:** Ao detectar um ataque, o Setor de TI tomará medidas imediatas de bloqueio para isolar o impacto.
2. **Erradicação e Recuperação:** Em caso de ataque bem-sucedido, os sistemas afetados serão restaurados a partir de backups confiáveis. Computadores infectados serão obrigatoriamente formatados.
3. **Análise Pós-Incidente:** Relatórios e logs serão preservados para investigação. Medidas de segurança adicionais serão implementadas para prevenir futuros incidentes.

7.13. Incidentes de Segurança (Ataques Internos)

1. **Investigação:** O Setor de TI investigará a origem e a natureza do incidente.
2. **Remediação:** O serviço ou equipamento afetado será restaurado.
3. **Ação Disciplinar e Prevenção:** O usuário responsável será identificado e o caso encaminhado aos gestores competentes. Medidas de controle de acesso serão reavaliadas.

7.14. Outros Problemas Para todas as outras solicitações de TI, o canal padrão é o Sistema de Chamados de Suporte, seguindo o fluxo padrão de atendimento.

8. CONTROLES PREVENTIVOS E ESTRATÉGIA DE RECUPERAÇÃO

O Setor de TI adotará as seguintes estratégias proativas:

- **Gestão de Backups:** Implementar e manter uma rotina de backups periódicos dos dados críticos, seguindo a regra 3-2-1 (três cópias, em duas mídias diferentes, com uma cópia off-site/nuvem). Testes de restauração serão realizados semestralmente.
- **Retenção de Dados:** Manter cópias de segurança de e-mails de colaboradores desligados, conforme a política de retenção de dados da instituição.
- **Inventário de Contingência:** Manter um estoque mínimo de equipamentos de reserva (*standby*), incluindo computadores/notebooks, *Nobreaks* e projetores, para substituição imediata em caso de falha.

9. MANUTENÇÕES PREVENTIVAS

A manutenção preventiva é crucial para minimizar a ocorrência de incidentes.

Quadro 2 – Cronograma de Manutenção Preventiva

Equipamento	Frequência	Responsável	Ações Detalhadas
Nobreaks	Anualmente	Assistência Especializada	Teste de baterias, calibração e limpeza interna.
Computadores / Notebooks	Semestralmente	Setor de TI	Atualização do sistema operacional e softwares. Verificação de segurança (antivírus). Troca de senhas de contas de administrador local. Limpeza de arquivos temporários e otimização de disco. Limpeza física dos componentes (se fora da garantia). Verificação de logs do sistema.
Projetores	Anualmente	Assistência Especializada	Limpeza de lentes e filtros, verificação da vida útil da lâmpada.
Sistema de Climatização (Servidores)	Semestralmente	Empresa Especializada	Verificação de gás, limpeza de filtros e manutenção geral.

10. PLANO DE COMUNICAÇÃO

A comunicação eficaz durante um incidente é vital.

10.1. A Quem Comunicar O ponto central de contato para reportar qualquer incidente de TI é o **Setor de TI da Instituto Mariano de Estudos e Inovação – IMEI**.

10.2. Como Comunicar

- Canal Preferencial: Sistema de Chamados de Suporte Técnico.
- Canais Alternativos (em caso de indisponibilidade do sistema):
- E-mail: suporte@imei.edu.br
- Telefone: (79) 99876-9884

Para incidentes de Nível III (Alto Impacto), o Setor de TI será responsável por comunicar proativamente os gestores da instituição e, se necessário, emitir comunicados gerais para a comunidade acadêmica sobre a natureza do problema e a previsão de normalização.

Este é um documento dinâmico e é revisado anualmente ou sempre que uma mudança significativa na infraestrutura de TI ocorrer, garantindo sua relevância e eficácia contínuas.