INSTITUTO IMAEP

PLANO DE CONTINGÊNCIAS

Biblioteca Virtual

Nova Mutum - MT
2024

1. INTRODUÇÃO

O Plano de Contingências da Biblioteca Virtual do Instituto IMAEP estabelece procedimentos e ações a serem adotadas em situações de falhas técnicas, incidentes de segurança ou quaisquer eventos que possam comprometer a disponibilidade e o funcionamento normal dos serviços.

Este documento tem como finalidade garantir a continuidade das atividades educacionais, minimizar impactos aos usuários e assegurar a rápida recuperação dos serviços em situações adversas.

2. OBJETIVOS DO PLANO DE CONTINGÊNCIAS

- Garantir a continuidade dos serviços da Biblioteca Virtual;
- Minimizar o tempo de indisponibilidade em caso de falhas;
- Proteger a integridade dos dados e do acervo digital;
- Estabelecer responsabilidades e fluxos de comunicação;
- Assegurar a satisfação e a segurança dos usuários;
- Cumprir compromissos institucionais e normativos.

3. ABRANGÊNCIA E APLICAÇÃO

Este Plano de Contingências aplica-se a todos os componentes da infraestrutura tecnológica da Biblioteca Virtual do Instituto IMAEP, incluindo:

- Servidores e infraestrutura de hospedagem;
- Plataforma de gerenciamento da biblioteca;
- Sistema de autenticação e controle de acesso;
- Banco de dados e arquivos do acervo digital;
- Conexões de rede e internet;
- Recursos de backup e recuperação.

4. CLASSIFICAÇÃO DE INCIDENTES

Os incidentes são classificados conforme sua gravidade e impacto nos serviços:

4.1 CRÍTICO (Nível 1)

Indisponibilidade total da Biblioteca Virtual ou comprometimento grave de segurança.

- Exemplos: servidor fora do ar, ataque cibernético, perda de dados, violação de segurança;
- Prazo de resposta: IMEDIATO;
- Prazo de resolução: até 4 horas.

4.2 ALTO (Nível 2)

Falhas que afetam funcionalidades essenciais ou grande número de usuários.

- Exemplos: lentidão extrema, erro no sistema de autenticação, indisponibilidade parcial;
- Prazo de resposta: até 1 hora;
- Prazo de resolução: até 8 horas.

4.3 MÉDIO (Nível 3)

Problemas que afetam funcionalidades específicas ou número limitado de usuários.

- Exemplos: erro em recurso específico, problema de visualização em dispositivo específico;
- Prazo de resposta: até 4 horas;
- Prazo de resolução: até 24 horas.

4.4 BAIXO (Nível 4)

Problemas menores que não comprometem a operação principal.

- Exemplos: erro de exibição, link quebrado, ajuste de layout;
- Prazo de resposta: até 8 horas;
- Prazo de resolução: até 48 horas.

5. EQUIPE DE RESPOSTA A INCIDENTES

5.1 Composição da Equipe

- Coordenador de TI: responsável pela gestão técnica e tomada de decisões;
- Técnico de Suporte: execução de procedimentos técnicos e troubleshooting;
- Direção Acadêmica: comunicação institucional e decisões estratégicas;
- Fornecedor de Hospedagem: suporte externo para infraestrutura de servidores.

5.2 Responsabilidades

Coordenador de TI:

- Avaliar gravidade e classificar o incidente;
- Acionar equipe e recursos necessários;
- Coordenar ações de recuperação;
- Comunicar status à Direção e usuários.

Técnico de Suporte:

- Executar diagnóstico técnico;
- Implementar soluções corretivas;
- Documentar ações realizadas;
- Monitorar recuperação dos serviços.

Direção Acadêmica:

- Autorizar acionamento de recursos extraordinários;
- Comunicar situação à comunidade acadêmica;
- Avaliar impactos pedagógicos;
- Decidir sobre medidas compensatórias.

6. PROCEDIMENTOS POR TIPO DE INCIDENTE

6.1 INDISPONIBILIDADE TOTAL DO SERVIDOR

Situação: Servidor fora do ar, impossibilidade de acesso à Biblioteca Virtual.

Ações imediatas:

1. Verificar status do servidor no painel de controle da hospedagem;
2. Acionar suporte técnico do fornecedor de hospedagem;
3. Verificar logs de erro para identificar causa;
4. Executar procedimento de reinicialização se necessário;
5. Comunicar usuários sobre a situação via e-mail e site institucional.

Ações de recuperação:

6. Se servidor comprometido: restaurar backup mais recente;
7. Verificar integridade dos dados após restauração;
8. Realizar testes de funcionamento de todas as funcionalidades;
9. Liberar acesso aos usuários;
10. Comunicar normalização dos serviços.

Tempo estimado de recuperação: até 4 horas.

6.2 FALHA DE CONEXÃO DE INTERNET

Situação: Problema no link de internet do data center ou da instituição.

Ações:

11. Verificar status da conexão com provedor de internet;
12. Acionar link de internet secundário (redundância);
13. Contatar provedor para resolução do problema;
14. Se problema for local: verificar equipamentos de rede (roteadores, switches);
15. Comunicar aos usuários se indisponibilidade prolongada.

Tempo estimado de recuperação: até 2 horas.

6.3 ATAQUE CIBERNÉTICO OU INVASÃO

Situação: Detecção de tentativa de invasão, vírus, ransomware ou ataque DDoS.

Ações imediatas:

16. ISOLAR IMEDIATAMENTE o sistema comprometido;

17. Bloquear acesso externo até resolução;
18. Acionar fornecedor de segurança/hospedagem;
19. Preservar logs e evidências para análise forense;
20. Alterar todas as senhas de acesso administrativo.

Ações de recuperação:

21. Realizar varredura completa de segurança;
22. Corrigir vulnerabilidades identificadas;
23. Restaurar sistema a partir de backup seguro;
24. Implementar medidas de segurança adicionais;
25. Notificar usuários caso dados tenham sido comprometidos (LGPD).

Tempo estimado de recuperação: até 8 horas.

6.4 PERDA OU CORRUPÇÃO DE DADOS

Situação: Dados do acervo ou banco de dados corrompidos ou perdidos.

Ações:

26. Identificar extensão da perda ou corrupção;
27. Isolar causa do problema (falha de hardware, erro humano, ataque);
28. Restaurar dados do backup mais recente;
29. Verificar integridade dos dados restaurados;
30. Implementar medidas para evitar recorrência.

Tempo estimado de recuperação: até 6 horas.

6.5 FALHA NO SISTEMA DE AUTENTICAÇÃO

Situação: Usuários impossibilitados de fazer login.

Ações:

31. Verificar logs de erro do sistema de autenticação;
32. Verificar conexão com banco de dados de usuários;
33. Reiniciar serviço de autenticação se necessário;
34. Testar login com diferentes perfis de usuário;
35. Se problema persistir: acionar fornecedor da plataforma.

Tempo estimado de recuperação: até 2 horas.

6.6 LENTIDÃO OU DEGRADAÇÃO DE PERFORMANCE

Situação: Sistema acessível mas com performance abaixo do aceitável.

Ações:

36. Monitorar uso de recursos do servidor (CPU, memória, disco);
37. Verificar número de acessos simultâneos;
38. Identificar processos ou consultas lentas;

39. Otimizar banco de dados se necessário;
40. Aumentar recursos do servidor temporária ou permanentemente.

Tempo estimado de recuperação: até 4 horas.

7. PLANO DE COMUNICAÇÃO

7.1 Comunicação Interna

- Coordenador de TI comunica imediatamente à Direção sobre incidentes críticos;
- Equipe técnica mantém registro detalhado de todas as ações;
- Reuniões de acompanhamento a cada 2 horas em incidentes críticos.

7.2 Comunicação Externa (Usuários)

Canais de comunicação:

- E-mail institucional para todos os usuários cadastrados;
- Aviso na página inicial do site institucional;
- Mensagem na tela de login da Biblioteca Virtual;
- WhatsApp institucional (casos críticos).

Conteúdo da comunicação:

- Informar sobre a situação de forma clara e objetiva;
- Indicar prazo estimado de normalização;
- Orientar sobre alternativas temporárias (se houver);
- Comunicar quando serviços forem normalizados.

7.3 Modelo de Comunicação - Indisponibilidade

Assunto: [URGENTE] Biblioteca Virtual temporariamente indisponível

Prezados alunos e professores, informamos que a Biblioteca Virtual está temporariamente indisponível devido a [motivo]. Nossa equipe técnica está trabalhando para resolver o problema. Previsão de normalização: [horário]. Pedimos desculpas pelo transtorno. Equipe IMAEP.

8. RECURSOS ALTERNATIVOS E SOLUÇÕES TEMPORÁRIAS

8.1 Em Caso de Indisponibilidade Prolongada

- Disponibilização de acervo físico na biblioteca local (se disponível);
- Solicitação de prorrogação de prazos de trabalhos e atividades;
- Orientação aos professores para flexibilização de bibliografias;
- Comunicação com fornecedor para acesso via plataforma alternativa (se existente).

8.2 Compensação aos Usuários

- Extensão de prazos acadêmicos proporcionalmente ao tempo de indisponibilidade;
- Comunicação transparente sobre as causas e medidas adotadas;
- Implementação de melhorias para evitar recorrência.

9. MEDIDAS PREVENTIVAS

Para minimizar a ocorrência de incidentes, o Instituto IMAEP adota:

- Monitoramento 24/7 de disponibilidade dos servidores;
- Backup automático diário de todos os dados;
- Atualização regular de sistemas operacionais e softwares;
- Aplicação imediata de patches de segurança críticos;
- Testes periódicos de restauração de backup;
- Redundância de conexão de internet;
- Firewall e sistemas de detecção de intrusão ativos;
- Treinamento contínuo da equipe técnica;
- Revisão semestral deste Plano de Contingências.

10. TESTES E SIMULAÇÕES

O Instituto IMAEP realiza periodicamente:

- Teste de restauração de backup: mensalmente;
- Simulação de indisponibilidade: semestralmente;
- Revisão de procedimentos: anualmente;
- Atualização de contatos de emergência: semestralmente.

11. REGISTRO E DOCUMENTAÇÃO DE INCIDENTES

Todos os incidentes devem ser documentados em formulário específico contendo:

- Data e hora de detecção do incidente;
- Classificação de gravidade;
- Descrição detalhada do problema;
- Ações tomadas e responsáveis;
- Tempo de resolução;
- Causa raiz identificada;
- Medidas preventivas implementadas.

Objetivo: Aprendizado organizacional e melhoria contínua dos processos.

12. INDICADORES DE DESEMPENHO

Métricas acompanhadas mensalmente:

- Disponibilidade do sistema (meta: 99,9%);
- Tempo médio de resposta a incidentes críticos (meta: < 30 minutos);
- Tempo médio de resolução de incidentes críticos (meta: < 4 horas);
- Número de incidentes por categoria;
- Taxa de sucesso de restauração de backup (meta: 100%).

13. REVISÃO E ATUALIZAÇÃO DO PLANO

Este Plano de Contingências será revisado e atualizado:

- Anualmente, de forma programada;
- Após cada incidente crítico;
- Quando houver mudanças significativas na infraestrutura;
- Quando houver alterações na equipe técnica.

14. CONSIDERAÇÕES FINAIS

O Plano de Contingências da Biblioteca Virtual do Instituto IMAEP demonstra o compromisso institucional com a continuidade dos serviços educacionais e a satisfação dos usuários.

A existência de procedimentos estruturados e equipe capacitada garante resposta rápida e eficiente a situações adversas, minimizando impactos e assegurando a qualidade dos serviços prestados.

O Instituto IMAEP reafirma seu compromisso com a excelência educacional e a melhoria contínua de seus processos e infraestrutura tecnológica.

Nova Mutum - MT, _____ de _____ de 20____.

_____

Direção do Instituto IMAEP

_____

Coordenação de Tecnologia da Informação