HOSPITAL DE CLÍNICAS DA UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Avenida Pará, nº 1720 - Bairro Umuarama
Uberlândia-MG, CEP 38405-320

Plano - SEI nº 2/2023/SETISD/SUP/HC-UFU-EBSERH

Uberlandia, 1 de Março de 2023.

PLANO DE TRABALHO À IMPLANTAÇÃO DA CONTINUIDADE DE TIC

1. **INTRODUÇÃO**

1.1. **Objetivo do Projeto**

1.1.1. Implantar **Continuidade de Tecnologia da Informação e Comunicação - TIC** através da construção, preparo e implementação do conjunto de planos de contingência dos seus principais serviços, conforme **Relação de Sistemas Críticos de TIC 28316803**, de forma a habilitar a instituição a recuperá-los após incidentes críticos que venham a caracterizar crises, causando indisponibilidades ou degradações graves à operação padrão.

1.2. **Diretrizes e Referências Institucionais**

1.2.1. **Norma Operacional SEI nº 4/2022/SGTI/DTI-EBSERH 26419477**;

1.2.2. **Modelo de Plano de Contingência de Serviços Críticos de TIC 26420424**;

1.2.3. **Relação de Sistemas Críticos de TIC 28316803**.

2. **JUSTIFICATIVA DO PROJETO**

2.1. **Garantir** que o **processo de serviço possa ser retomado dentro dos requisitos e prazos adequados** conforme a necessidade do negócio;

2.2. **Mitigar** a possibilidade de um **incidente causar a indisponibilidade do serviço**; e

2.3. **Responder** de forma adequada, **reduzindo os danos potenciais** do incidente.

3. **ESCOPO PRELIMINAR DO PROJETO E DO SEU PRODUTO**

3.1. A **construção** e **implementação** de cada **plano de contingência dos serviços críticos de TIC**, conforme **Relação de Sistemas Críticos de TIC 28316803**, que serão constituídas por **quatro (04) etapas - ATIVAÇÃO, DESENVOLVIMENTO, IMPLANTAÇÃO e MANUTENÇÃO -** a serem pragmaticamente conduzidas de forma **progressiva** e **incremental**, estabelecendo um **ciclo de vida que manterá a qualidade do Plano de Contingência da TIC**.

3.2. **Unidades Gestoras**

3.2.1. **Unidade Gestora do Serviço de TIC**

3.2.1.1. Gerir e coordenar o Plano de Contingência de Serviços de TIC;

3.2.1.2. Reunir com as áreas de negócio para definir os parâmetros do Plano de Contingência de Serviços de TIC;

3.2.1.3. Supervisionar todo o processo de recuperação e restauração, sendo a primeira que terá de tomar medidas em caso de um evento que caracterize uma crise;

3.2.1.4. Definir as equipes técnicas necessárias para gerenciar a contingência.

3.2.2. **Unidade Gestora do Negócio**

3.2.2.1. Apoiar na elaboração do Plano de Contingência de Serviços de TIC;

3.2.2.2. Propor soluções de melhoria ou alteração

3.2.2.3. Promover a integração com o Unidade Gestora do Serviço de TIC;

3.2.2.4. Acompanhar e avaliar a efetividade na utilização do Plano de Contingência do Serviço de TIC;

3.2.2.5. Propor à Unidade Gestora do Serviço de TIC prioridades de atendimento às demandas;

3.2.2.6. Reavaliar, periodicamente, os benefícios, a necessidade, a utilidade e o uso do serviço de TIC.

4. **PRAZO DO PROJETO**

Descrição das Atividades	Prazo
• Abertura de Processo SEI, com a inserção da Planilha de Criticidade preenchida, contendo a definição dos Serviços Críticos de TI e identificação das Unidades Gestoras dos respectivos serviços, conforme metodologia contida na Norma Operacional de Contingência de Serviços de TI.	**até 03/02/2023**
• Anexo, no mesmo Processo SEI, do cronograma de elaboração dos Planos de Contingência dos Serviços Críticos de TI.	
• Encaminhamento do Processo SEI para acompanhamento do Serviço de Governança de TI (SGTI/DTI).	
• No mesmo Processo SEI, deverão ser registrado todos os Planos de Contingência dos Serviços Críticos de TI, sendo que, pelo menos, a cada quatro meses deverá ser elaborado um Plano de Contingência.	Entrega de todos os planos, **até 31/12/2023**

5. **CRONOGRAMA PRELIMINAR DO PROJETO**

5.1. Levantamento dos serviços

5.2. Descrever segurança referente ao fornecimento de energia eletrica (nobreak, etc)

5.3. Seguranca referente a refrigeração (ar condicionado)

5.4. Segurança referente ao storage

5.5. Segurança referente ao Switch SAN

5.6. Segurança referente ao link de internet

5.7. Segurança referente ao backup (ferramenta bacula, nuvem)

5.8. Segurança referente ao PACs

5.9. Segurança referente ao jboss

5.10. Segurança referente ao banco de dados DB2

5.11. Segurança referente ao file server

5.12. Segurança referente ao firewall

5.13. Segurança referente a prevenção de invasões

6. ESCOPO

Tarefa	Responsável	Prazo
Identificação dos serviços e matriz de risco	SETISD	02/2023
Descrever segurança referente ao fornecimento de energia eletrica	SETISD/UISTI	05/2023
Seguranca referente a refrigeração (ar condicionado)	UISTI	05/2023
Segurança referente ao storage	UISTI	05/2023
Segurança referente ao Switch SAN	UISTI	07/2023
Segurança referente ao link de internet	UISTI	07/2023
Segurança referente ao backup (ferramenta bacula, nuvem)	UISTI/USID	07/2023
Segurança referente ao PACs	USID	09/2023
Segurança referente ao jboss	USID	09/2023
Segurança referente ao banco de dados DB2	USID	12/2023
Segurança referente ao file server	UISTI	12/2023
Segurança referente ao firewall	UISTI	12/2023
Segurança referente a prevenção de invasões	ETIR	12/2023

7. RECURSOS HUMANOS ENVOLVIDOS

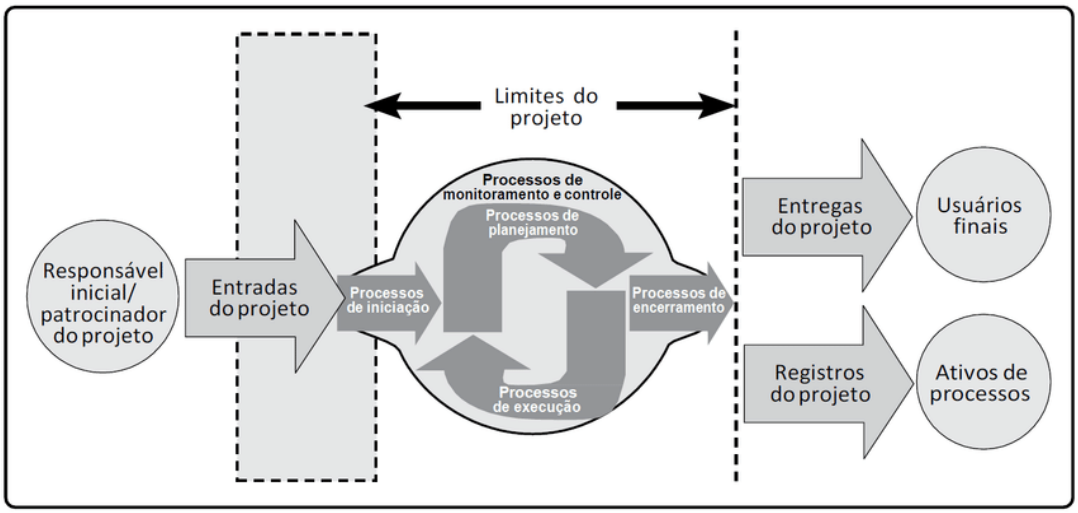
Chefe do Setor de TI e Saúde Digital

Chefe da Unidade de Sistemas de Informação da Informação e Inteligência de Dados

Chefe da Unidade de Infraestrutura, Suporte e Tecnologia da Infomração

Estrutura organizacional do SETISD

8. METODOLOGIA BÁSICA DE GESTÃO DO PROJETO



Grupo de processos de gerenciamento de projetos conforme PMBoK - PMI

8.1. **Metodologia básica do ciclo iterativo de gerenciamento do projeto**

8.1.1. **Processos de Iniciação (IN)**

8.1.1.1. Elaborar o **Termo de Abertura do Projeto (TAP)**;

8.1.1.2. Identificar as principais partes interessadas.

8.1.2. **Processos de Planejamento (PL)**

8.1.2.1. Elaborar o **Plano de Trabalho**

8.1.2.2. Construir o **Plano de Gerenciamento do Projeto (PGP)**

8.1.3. **Processos de Execução (EX)**

8.1.3.1. Executar atividades conforme o **PGP**

8.1.3.2. Reportar regularmente evolução das atividades e dos resultados gerados

8.1.4. **Processos de Monitoramento e Controle (M/C)**

8.1.4.1. Monitorar e controlar desvios processuais em nível operacional regularmente apresentados pelos *reports* conforme o **PGP**

8.1.4.2. Demandar, quando necessário, acertos e melhorias em nível tático ao planejamento para atualização do **PGP**

8.1.4.3. Demandar - se for real, inevitável, extremamente necessário - reestruturação do **TAP**

8.1.5. **Processos de Encerramento (EN)**

8.1.5.1. Encerrar gradativamente fases ou projeto

9. **MACROATIVIDADES OPERACIONAIS**

9.1. A criação de cada Plano de Contingência de Serviço Críticos de TIC compreenderá as seguintes etapas e respectivas macroatividades, cujos detalhamentos encontram-se na **Norma Operacional SEI nº 4/2022/SGTI/DTI-EBSERH 26419477**:

9.1.1. **Ativação**: estabelecer os fundamentos dos Planos de Contingência de Serviços de TIC, que sustentarão sua elaboração, através das etapas análise de impacto e planejamento do escopo do Plano no respectivo serviço.

9.1.1.1. **Analisar impacto**: Determinar criticidade de recuperação por meio da identificação dos impactos de interrupção e tempo de inatividade máxima do serviço crítico de TIC em relação à área de negócio por ele apoiada.

9.1.1.2. **Planejar escopo**: Definir ambiente principal e alternativo em que o serviço de TIC será hospedado.

Etapa Ativação

9.1.2. **Desenvolvimento**: estabelecer a estratégia de contingência e organiza a elaboração dos Planos de Contingência.

9.1.2.1. **Criar estratégia da contingência**: Mitigar as ameaças apresentadas na etapa de ativação, abrangendo o planejamento da recuperação do serviço de TIC diante a um desastre.

9.1.2.2. **Elaborar planos**: Construir os planos de contingência constituídos pelos seguintes documentos:

- Plano de Recuperação/Restauração Operacional;
- Guia de Equipes e Fornecedores; e
- Plano de Teste Manutenção.

Etapa Desenvolvimento

9.1.3. **Implantação**: orientar as etapas de Integrar à Arquitetura e de Treinar, Exercitar e Testar.

9.1.3.1. **Integrar estratégia na arquitetura**: Desenvolver a estrutura necessária para suportar o serviço crítico de TIC no ambiente alternativo.

9.1.3.2. **Treinar, exercitar e testar planos**: Promover treinamento para conscientização e capacitação das equipes envolvidas nos planos de contingência, documentando as ações técnicas necessárias para que o plano de recuperação/restauração operacional seja executado.

Etapa Implantação

9.1.4. **Manutenção**: prever a revisão frequente do plano ou sempre que se fizer necessário, para refletir possíveis mudanças ou atualizações tecnológicas no serviço de TIC.

9.1.4.1. **Assegurar manutenção dos planos**: Revisar frequentemente o plano, sempre que se fizer necessário.

9.1.4.2. **Controlar e atualizar mudanças**: Refletir mudanças ou atualizações tecnológicas necessárias ao serviço crítico de TIC.

Etapa Manutenção

Gerente do Projeto
(assinado eletronicamente) **Marcos Alexandre Lemos Rodrigues** Setor de Tecnologia da Informação e Saúde Digital Portaria-SEI nº 489, de 26 de maio de 2020

Documento assinado eletronicamente por **Marcos Alexandre Lemos Rodrigues**, **Chefe de Setor**, em 24/03/2023, às 10:23, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ebserh.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **28316894** e o código CRC **D0AFC726**.

Referência: Processo nº 23860.003419/2023-93 SEI nº 28316894