EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES
SCS Quadra 9, Edifício Parque Cidade Corporate, Torre C, 1° ao 3° andares - Bairro Asa Sul
Brasília-DF, CEP 70308-200
(61) 3255-8900 - http://www.ebserh.gov.br

Norma Operacional - SEI nº 4/2022/SGTI/DTI-EBSERH

Brasília, *data da assinatura eletrônica*.

Norma Operacional de Contingência de Serviços de Tecnologia da Informação

A **DIRETORA DE TECNOLOGIA DA INFORMAÇÃO** da Empresa Brasileira de Serviços Hospitalares (Ebserh), no uso de suas atribuições legais, de acordo com as competências que lhe foram conferidas pelo artigo 103 do Regimento Interno atualizado em 21 de junho de 2022, e considerando a necessidade de normatização dos procedimentos para elaboração dos Planos de Contingência de Serviços de Tecnologia da Informação para Administração Central e Hospitais Universitários da Rede Ebserh, resolve:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Esta Norma Operacional de Contingência de Serviços de Tecnologia da Informação (TI) apresenta um roteiro compreendendo instruções, recomendações e considerações necessárias para elaboração do Plano de Contingência de um Serviço de TI, com vistas a garantir a segurança na disponibilidade, integridade, confidencialidade e autenticidade.

Art. 2º O Plano de Contingência de Serviços de TI visa à disponibilidade e à continuidade dos serviços quanto ao escopo da Tecnologia da Informação.

Parágrafo Único. O conjunto dos Planos de Contingência dos Serviços de TI constitue o Plano de Continuidade de TI.

Art. 3º O objetivo geral de um Plano de Contingência para cada Serviço de TI é habilitar a organização a recuperar o serviço após um incidente crítico que venha caracterizar uma crise, causando indisponibilidade ou degradação grave à operação padrão, possibilitando ainda:

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

II - Mitigar a possibilidade de um incidente causar a indisponibilidade do serviço; e

III - Responder de forma adequada, reduzindo os danos potenciais do incidente.

Art. 4º O Plano de Contingência é constituído por quatro fases, Ativar, Desenvolver, Implantar e Manter, que serão conduzidas de forma progressiva e incremental, constituindo um ciclo de vida que manterá a qualidade do Plano de Contingência.

CAPÍTULO II
DOS CONCEITOS

Art. 5º Para os fins desta norma consideram-se os seguintes conceitos:

I - Ativos: aquilo que tem valor tangível ou intangível para a organização, tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional;

II - Desastre: evento, ação ou omissão, repentino e não planejado que permita acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, causando perda para toda ou parte da organização e gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

III - Gestão de Continuidade de Negócio: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso as ameaças se concretizem. Esse processo fornece estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes, a reputação, a marca da organização e suas atividades de valor agregado;

IV - Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum avo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

V - Plano de *Backup*: documento formal onde são definidos os responsáveis pela cópia dos dados, o que será armazenado, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da Política de *Backup*;

VI - Plano de Contingência de Serviços de TI: documento que habilita a organização a recuperar um processo de negócio sustentado pela TI, após um incidente crítico que venha caracterizar uma crise, causando indisponibilidade ou degradação grave à operação padrão do processo de negócio;

VII - Plano de Continuidade de Serviços de TI: conjunto dos Planos de *Backup* e dos Planos de Contingência de Serviço de TI, possibilitando respostas imediatas a incidentes graves, permitindo a continuidade de determinado Processo de Negócio;

VIII - Prazo Máximo de Interrupção Tolerável (PMIT): prazo máximo que um serviço pode ficar fora de operação;

IX - *Recovery Point Objective* (RPO): ponto no tempo em que os dados devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

X - *Recovery Time Objective* (RTO): tempo estimado para restaurar os dados e tornar os clientes de backup novamente operacionais, correspondendo ao prazo máximo em que se admite manter os clientes de backup inoperantes até a restauração de seus dados após um incidente;

XI - Serviço de TI: qualquer provimento de serviços de desenvolvimento, implantação, manutenção, armazenamento e recuperação de dados e operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação, que sustentem um processo de negócio essencial;

XII - Unidade Gestora do Serviço de TI: Unidade da Ebserh responsável pelo provimento do serviço de TI;

XIII - Unidade Gestora do Negócio: Unidade da Ebserh responsável pela definição de processos de trabalho, requisitos, regras de negócio e níveis de serviço aplicáveis ao serviço de TI.

CAPÍTULO III
Das Fases de Elaboração e Manutenção

Art. 6º O roteiro de criação do Plano de Contingência de Serviço de TI compreende as seguintes fases e etapas:

I - Fase 1 – Ativar:

a) Etapa 1 - Análise de impacto; e

b) Etapa 2 – Planejamento do escopo.

II - Fase 2 – Desenvolver:

a) Etapa 3 - Criar estratégia; e

b) Etapa 4 – Elaborar plano.

III - Fase 3 – Implantar:

a) Etapa 5 - Integrar a estratégia na arquitetura; e

b) Etapa 6 - Treinar, exercitar e testar o plano.

IV - Fase 4 – Manter:

a) Etapa 7 - Assegurar a manutenção do plano; e

b) Etapa 8 – Controlar as mudanças e atualizar.

CAPÍTULO IV
DA FASE ATIVAR

Art. 7º A fase 1 - Ativar estabelece os fundamentos do Plano de Contingência de Serviços de TI que sustentam sua elaboração, através das etapas análise de impacto e planejamento do escopo do Plano no respectivo serviço.

Parágrafo Único. O objetivo desta fase é minimizar a perda de dados e manter o serviço em operação, analisando três objetivos de segurança:

I - Confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizados não tenham conhecimento da informação, de forma proposital ou acidental;

II - Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental; e

III - Disponibilidade: garantir que as informações estejam disponíveis para as partes autorizadas sempre que necessário, com acesso oportuno e confiável ao uso das informações.

SEÇÃO I – Da Análise de Impacto

Art. 8º Deverá ser determinada a criticidade de recuperação por meio da identificação dos impactos de interrupção e tempo de inatividade máxima do serviço de TI em relação à área de negócio por ele apoiada, observando-se os seguintes critérios:

§ 1º Prazo Máximo de Interrupção Tolerável (PMIT): representa a quantidade total de tempo que o responsável pelo processo considera aceitável, se o serviço de TI ou dados específicos ficarem indisponíveis, requerendo método de recuperação apropriado, com o nível de detalhes necessários, para desenvolver procedimentos operacionais e técnicos de suporte para a Recuperação; e

§ 2º *Recovery Point Objective* (RPO): representa a perda máxima de dados tolerada quando houver a ativação da contingência.

Art. 9º As prioridades de recuperação dos serviços de TI deverão ser identificadas quanto ao objetivo do tempo de recuperação.

§ 1º *Recovery Time Objective* (RTO): define a quantidade máxima de tempo que um componente do serviço de TI pode permanecer indisponível antes que ocorra um impacto inaceitável em outros componentes que também apoiem na sustentação. Quando não é possível atender imediatamente ao RTO e o PMIT é inflexível, deve-se documentar a situação e ativar um Plano de Ação para sua mitigação.

§ 2º A Etapa de análise de impacto deve seguir o modelo constante no *Tamplate* A no Modelo do Plano de Contingência, anexo a esta norma.

Art. 10 A alocação de recursos financeiros e humanos eficaz requer a definição do grau de criticidade do serviço de TI.

Art. 11 O grau de criticidade do serviço de TI será definido a partir da análise de impacto que uma possível paralisação no serviço causaria, aplicando-se a seguinte metodologia:

I - Quanto ao impacto legal ou regulatório:

a) 0 ponto – não traz sanção legal, somente advertência;

b) 1 pontos – existe sanção legal corretiva, mas contornável legalmente;

c) 2 pontos – existe sanção legal punitiva, gerando multa e processo judicial;

d) 3 pontos - existe sanção legal punitiva, gerando multa e processo judicial grave, com prejuízos à organização; e

e) 4 pontos - existe sanção legal punitiva, gerando multa e processo judicial grave, com demissão de executivos, desapropriação de bem patrimonial e fechamento da organização.

II - Quanto ao impacto de imagem:

a) 0 ponto – não há impacto comprometedor de imagem;

b) 1 pontos – existe impacto interno à área responsável pelo processo de negócios;

c) 2 pontos – existe impacto interno às áreas da organização;

d) 3 pontos – existe impacto interno e externo à organização; e

e) 4 pontos – existe impacto, comprometendo a imagem pública da organização, inviabilizando a retomada do processo de negócio.

III - Quanto ao impacto operacional:

a) 0 ponto - não gera impacto operacional;

b) 1 pontos – existe impacto operacional razoável, mas contornável com aplicação de contingência;

c) 2 pontos – existe impacto operacional, comprometendo atividades não-chave, mas contornável com aplicação de contingências;

d) 3 pontos – existe impacto operacional, comprometendo atividades-chave, mas contornável com aplicação de contingências; e

e) 4 pontos – existe impacto operacional, impossibilitando a continuidade dos negócios da organização.

IV - Quanto ao impacto financeiro:

a) 0 ponto – não há impacto razoável financeiro;

b) 1 pontos – existe impacto financeiro, mas contornável;

c) 2 pontos – existe impacto financeiro, contornável com esforço razoável;

d) 3 pontos – existe impacto financeiro, contornável com grande esforço; e

e) 4 pontos – existe impacto financeiro não contornável, inviabilizando a retomada do processo de negócio.

V - Quanto ao impacto relacionado à saúde e à vida:

a) 0 ponto – Não há impacto direto à saúde ou à vida;

b) 1 pontos – Existe impacto nos processos, com baixo risco à saúde;

c) 2 pontos – Existe impacto indireto, com risco moderado à saúde ou a agravamento de um estado físico do indivíduo;

d) 3 pontos – Existe impacto direto à saúde, podendo gerar danos graves; e

e) 4 pontos – Existe impacto direto à vida, podendo gerar óbito do indivíduo.

Art. 12 O grau de criticidade do serviço de TI será o somatório da pontuação referida no artigo anterior, considerado como:

I - Baixo, caso a somatório esteja entre 0 e 8, cuja indisponibilidade não afeta a organização;

II - Médio, caso a somatório esteja entre 9 e 12, cuja indisponibilidade afeta a organização causando impactos reparáveis; e

III - Alto, caso o somatório esteja entre 13 e 20, cuja indisponibilidade afeta muito a organização, causando impacto de difícil reparação.

Art. 13 A Administração Central e os Hospitais Universitários deverão elaborar, no mínimo, Plano de Contingência dos serviços de TI classificados com criticidade alta.

Art. 14 Deverá ser considerada a pontuação do grau de criticidade para priorizar a elaboração dos Planos de Contingência, conforme anexo II - Planilha de Criticidade de Serviços de TI.

SEÇÃO II – Da Atuação do Plano

Art. 15 Para a aplicabilidade do Plano de Contingência deverão ser definidos ambiente principal e alternativo em que o serviço de TI será hospedado, com as seguintes informações:

I - Localidade e região onde o respectivo serviço de TI está instalado;

II - Caso exista um contrato válido com algum ambiente alternativo, informações relevantes sobre o contrato, ponto focal, contato do serviço de suporte e onde eles se localizam de acordo com as premissas a seguir:

a) A Ebserh poderá usar o ambiente alternativo e os recursos definidos para recuperar o serviço de TI durante a ocorrência de um desastre; e

b) O ambiente alternativo pode ser utilizado para sustentar o serviço de TI durante todo o período de interrupção, até que haja o retorno ao funcionamento no ambiente principal.

Art. 16 O Plano de Contingência será acionado quando ocorrerem cenários de desastre que apresentem risco à continuidade do respectivo serviço de TI.

§ 1º Deve-se mapear os principais eventos de desastre juntamente com suas possíveis causas, sendo a listagem extensiva, mas não definitiva, cabendo revisão sempre que for necessário.

§ 2º Para a etapa de definição do escopo de atuação do Plano de Contingência, foi criado o *Tamplate B* no Modelo de Plano de Contingência, anexo a esta norma.

CAPÍTULO V
DA FASE DESENVOLVER

Art. 17 A fase 2 - Desenvolver estabelece a estratégia de contingência e organiza a elaboração do Plano de Contingência.

SEÇÃO I – Criação da Estratégia de Contingência

Art. 18 A estratégia de contingência é criada para mitigar as ameaças apresentadas na fase Ativar e abrange o planejamento da recuperação do serviço de TI diante de um desastre.

Art. 19 Os métodos e estratégias devem abordar os impactos de interrupção e os períodos de inatividade aceitáveis identificados na análise de impacto e devem ser integrados à arquitetura do sistema de contingência durante a fase de desenvolvimento e aquisição do Ciclo de Vida do Plano de Contingência.

Art. 20 Para composição da estratégia, devem ser levantadas as informações sistêmicas e tecnológicas do serviço de TI, incluindo, pelo menos, os seguintes itens:

I - Planilha de Ativos, com os seguintes dados:

a) Atributos;

b) Relacionamento de dependência; e

c) Mapeamento dos nomes dos *hosts* e dos ativos.

II - Topologia física e lógica.

SEÇÃO II – Elaboração do Plano de Contingência

Art. 21 O Plano de Contingência é constituído dos seguintes documentos:

I - Planejamento da Recuperação;

II - Plano de Recuperação/Restauração Operacional;

III - Guia de Equipes e Fornecedores; e

IV - Plano de Teste e Manutenção.

Art. 22 O Planejamento da Recuperação contempla os artefatos criados nas etapas de análise de impacto, escopo do plano de contingência, topologia física e lógica e lista de ativos.

Art. 23 A partir da estratégia de continuidade é criado o Plano de Recuperação/Restauração Operacional, que corresponde às ações associadas aos Ciclos de Ativação e Notificação, Recuperação e Restauração.

Art. 24 O Ciclo de Ativação e Notificação relata as ações a partir de um incidente crítico que possa paralisar o respectivo serviço de TI.

§ 1º A ativação do Plano de Contingência ocorrerá após uma interrupção ou falha que possa vir a se estender além do PMIT estabelecido para o serviço de TI;

§ 2º A partir da identificação deverá se iniciar os procedimentos de notificação e de escalada, para conscientização e comunicação do estado de recuperação às partes interessadas;

§ 3º Ao ser ativado o Plano de Contingência, os responsáveis pelos componentes do respectivo serviço (conectividade, *hardware*, *software*, entre outros) e os usuários, devem ser notificados de uma possível interrupção de longo prazo, bem como uma avaliação completa dos agentes causadores da interrupção.

§ 4º As informações de avaliação devem ser apresentadas pelos responsáveis dos componentes do serviço e podem ser usadas para modificar os procedimentos específicos de recuperação, conforme a causa da interrupção;

§ 5º Durante este ciclo será contado o tempo relativo ao RTO.

§ 6º Toda operacionalização da ativação e notificação deverá ser descrita conforme modelo em anexo a esta norma, com o propósito de garantir o início das atividades para o restabelecimento da continuidade dos processos e atividades no *site* alternativo.

Art. 25 O Ciclo de Recuperação tem como objetivo reestabelecer o serviço de TI no ambiente alternativo.

§ 1º Deverão ser detalhadas as atividades e os procedimentos para a recuperação do serviço de TI, de modo que uma equipe técnica qualificada possa reestabelecer o serviço.

§ 2º Este ciclo é entendido como uma Mudança Emergencial do ambiente principal para o alternativo.

§ 3º Durante este ciclo está sendo contado o tempo relativo ao RTO restante e ao *Work Recovery Time* (WRT).

§ 4º A recuperação do serviço de TI tem como requisito o RPO especificado na análise de impacto.

§ 5º Toda operacionalização da recuperação deverá ser apresentada no modelo em anexo, cujo propósito é o de garantir o restabelecimento da disponibilidade das funcionalidades do serviço de TI no site alternativo.

Art. 26 O ciclo de restauração é utilizado pelo plano de contingência e aplica-se à restauração do serviço de TI no ambiente principal.

§ 1º Deverão ser detalhadas as ações a serem tomadas em duas etapas: validar a Restauração no ambiente principal e desativar o serviço do ambiente alternativo.

I - Validar a Restauração no ambiente principal:

a) O Plano de Contingência é testado e validado quanto à sua operacionalidade no ambiente principal;

b) Procedimentos de validação incluem testes de funcionalidade, processamento simultâneo e ou validação de dados; e

c) O Plano de Contingência é declarado operacional pelos responsáveis após a conclusão do teste de validação.

II - Desativar o Plano de Contingência no ambiente alternativo:

a) Inclui notificação aos usuários sobre o status operacional do Plano de Contingência;

b) Devem ser realizadas atividades de *clean-up* no serviço de TI instalado no ambiente alternativo; e

c) Inclui a documentação sobre o esforço de recuperação, registro de atividades, incorporação das lições aprendidas em atualizações do Plano de Contingência e preparação dos recursos para incidentes críticos futuros.

§ 2º. Toda operacionalização deverá estar em conformidade com os procedimentos do modelo em anexo, com o propósito de garantir o restabelecimento da disponibilidade das funcionalidades do serviço de TI.

Art. 27 Para operacionalização do Plano de Contingência do Serviço de TI deverá ser criado o guia de equipes para estabelecer os papeis atribuídos no Plano de Contingência.

§ 1º. Todos os profissionais constantes no guia de equipes devem estar preparados para responder a um evento de contingência que afete o serviço de TI.

§ 2º. As listas dos papéis e responsabilidades deverão refletir a realidade da organização quanto à especialização do usuário dentro do ambiente do serviço de TI, conforme as ações a serem executadas.

§ 3º. Os membros da equipe serão responsáveis pelas tarefas relacionadas ao Plano de Contingência e, em algumas situações, poderão ser convidados outros profissionais.

Art. 28 Para execução do Plano de Contingência, deverá ser criado o guia de fornecedores para relacionar equipamentos aos respectivos fornecedores e garantias, caso haja necessidade de acioná-los em uma crise.

Art. 29 Para criação do Guia de Equipe e Fornecedores deve ser observado o **Template C** do anexo desta norma.

CAPÍTULO VI
DA FASE IMPLANTAR

Art. 30 A fase 3 - Implantar orienta as etapas de Integrar à Arquitetura e de Treinar, Exercitar e Testar.

SEÇÃO I – Integrar à Arquitetura

Art. 31 Deverá ser desenvolvida a estrutura necessária para suportar o Serviço de TI no ambiente alternativo.

Art. 32 Todos os procedimentos operacionais de recuperação e restauração devem ser listados e descritos passo a passo nesta fase, de forma a documentar as ações técnicas necessárias para que o Plano de Recuperação/Restauração Operacional seja executado.

SEÇÃO II – Treinar, Exercitar e Testar

Art. 33 Para garantir que as equipes envolvidas no Plano de Contingência estejam conscientes e capacitadas a executar o plano, deverá ser realizado um teste real de recuperação e restauração, a fim de validar o Plano de Contingência elaborado.

Art. 34 Para os treinamentos deverão ser considerados os seguintes itens:

I - Informar os indivíduos sobre seus papéis e responsabilidades e validar se possuem as habilidades relacionadas, preparando-os para a participação em exercícios, testes e situações de emergência reais;

II - Realizar atividades que permitem que a equipe demonstre sua compreensão do assunto e conscientização quanto aos papéis e responsabilidades, promovendo, para os indivíduos que irão cumprir os papéis designados nas equipes, as respectivas responsabilidades definidas pelo Plano de Contingência, através da familiarização com seus papéis definidos;

III - Realizar o treinamento pelo menos uma vez por ano e, em qualquer tempo, para todo indivíduo recém designado; e

IV - Treinar os profissionais nos respectivos papéis, tendo como meta que os papéis e responsabilidades de recuperação possam ser adequadamente executados.

Art. 35 Para os exercícios deverão ser considerados os seguintes itens:

I - Simular uma emergência projetada para validar a viabilidade de um ou mais aspectos do Plano de Contingência;

II - Validar o conteúdo do Plano de Contingência por meio da discussão de suas funções, atividades e respostas a situações de emergência em um ambiente simulado ou outros meios de validação de respostas que não envolva o uso do ambiente real; e

III - Os exercícios são orientados a cenários, como uma falha de energia ou um incêndio, causando danos, com situações adicionais sendo apresentadas durante o exercício.

Art. 36 Para os testes deverão ser considerados os seguintes itens:

I - Definir ferramentas de avaliação que usem métricas quantificáveis para validar a operabilidade de um serviço de TI ou componente do serviço em um ambiente operacional recuperado;

II - O escopo do teste pode variar de componentes ou de todo o serviço de TI; e

III - Realizar o teste real dos componentes ou de todo o serviço de TI.

CAPÍTULO VII
DA FASE MANTER

Art. 37 A fase 4 - Manter prevê a revisão frequente do plano, ou sempre que se fizer necessário, para refletir possíveis mudanças ou atualizações tecnológicas no serviço de TI.

Art. 38 Deverão ser revisados:

I - Procedimentos técnicos;

II - *Hardware, software* e outros equipamentos (tipos, especificações e quantidades);

III - Nomes e informações de contato dos membros da equipe;

IV - Listas de fornecedores internos e externos;

V - Requisitos de instalações alternativas e externas; e

VI - Registros vitais do serviço de TI.

Art. 39 O Plano de Contingência contém informações operacionais e pessoais potencialmente confidenciais, não devendo ser seu conteúdo publicado.

Art. 40 Na ocorrência de uma mudança significativa, a análise de impacto deve ser refeita e atualizada com as novas informações, para identificar novos requisitos ou parâmetros orientadores de contingência.

Art. 41 A manutenção do Plano deve continuar à medida que o serviço de TI passa pela fase de Descarte, e sua distribuição deve ser controlada, visando:

I - Manter um registro das cópias do Plano e para quem foram distribuídas;

II - Coordenar as mudanças feitas no Plano, estratégias e comunicar as mudanças aos envolvidos, conforme necessário;

III - Registrar as modificações do Plano usando um registro de mudanças, que lista o número da página, o comentário e a data da mudança; e

IV - Atualizar todos os documentos pertinentes ao Anexo – Modelo do Plano de Contingência.

Art. 42 Esta norma guiará a elaboração do Plano de Contingência de Serviço de TI, a partir do preenchimento do modelo em anexo.

CAPÍTULO VIII
DAS RESPONSABILIDADES

Art. 43 Os Planos de Contingência de Serviços de TI serão assinados pelos responsáveis da Unidade Gestora do Serviço de TI e da Unidade Gestora do Negócio, no âmbito da Administração Central e dos Hospitais Universitários, conforme norma específica.

Art. 44 São atribuições da Unidade Gestora do Serviço de TI:

I - Gerir e coordenar o Plano de Contingência;

II - Reunir com as áreas de negócio para definir os parâmetros do Plano de Contingência;

III - Supervisionar todo o processo de recuperação e restauração, sendo a primeiro que terá de tomar medidas em caso de um evento que caracterize uma crise; e

IV - Definir as equipes técnicas necessárias para gerenciar a contingência.

Art. 45 São atribuições da Unidade Gestora do Negócio:

I - Apoiar na elaboração do Plano de Contingência;

III - propor soluções de melhoria ou alteração;

III - promover a integração com o Unidade Gestora do Serviço de TI;

XIII - acompanhar e avaliar a eficiência e a efetividade na utilização do Plano de Contingência do Serviço de TI;

XIV - propor à Unidade Gestora do Serviço de TI prioridades de atendimento às demandas; e

XX - reavaliar, periodicamente, os benefícios, a necessidade, a utilidade e o uso do serviço de TI.

Art. 46 As equipes técnicas serão orientadas pela Unidade Gestora do Serviço de TI executando todas as ações previstas no Plano de Contingência.

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 47 Casos não contemplados nesta norma serão deliberados pela DTI.

Art. 48 Esta norma será atualizada a cada dois anos ou a qualquer tempo, conforme necessidade.

Art. 49 O não atendimento a esta norma ensejará apuração de responsabilidade nos termos da Norma Operacional de Controle Disciplinar (link).

Art. 50 Esta norma entra em vigor na data de sua publicação.

(assinado eletronicamente)

SIMONE HENRIQUETA COSSETIN SCHOLZE

Diretora de Tecnologia da Informação

Documento assinado eletronicamente por **Simone Henriqueta Cossetin Scholze**, **Diretor(a)**, em 20/10/2022, às 16:48, 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 **24763853** e o código CRC **3B8495FA**.

Referência: Processo nº 23477.013525/2021-47 SEI nº 24763853

Anexo – Modelo de Plano de Contingência

As seções abaixo descrevem o modelo a ser utilizado para preencher o Plano de Contingência.

Aprovação do Plano

Com a responsabilidade designada, certificamos que este documento identifica a criticidade no que se refere à missão do serviço de TI *"...nome do serviço de TI..."* e que a estratégia de recuperação identificada fornece a capacidade de recuperar a funcionalidade que automatiza as atividades de forma adequada e a um custo benefício em acordo com o seu grau de criticidade.

Informo também que é previsto que este Plano de Contingência do *"...serviço de TI..."* será testado pelo menos uma vez anualmente e o resultado dos testes podem ser encontrados na pasta de documentação apropriada.

Este documento será modificado à medida que ocorrerem alterações e permanecerá sob controle de versão.

_____

Data

_____

"Responsável pela Unidade Gestora do Negócio"

_____

"Responsável pela Unidade Gestora do TI"

1. Introdução

O *"...Serviço de TI..."* atende às demandas de informação, tanto da própria Ebserh quanto de órgãos de controle, governos e cidadãos e dá suporte para que a Ebserh viabilize a *"...informar a finalidade do serviço de TI..."*.

É, portanto, fundamental à Ebserh, para apoiar nos processos, sendo considerado o *"Serviço de TI"* um processo de Alta Criticidade para o cumprimento da missão da Ebserh e para a transparência de suas ações institucionais.

O *"...serviço de TI..."* deve ser capaz de operar de forma eficaz, sem interrupção, ou com o mínimo de tempo de interrupção de modo a não se prolongar por tempo excessivo, pois poderá comprometer os objetivos de negócios da Ebserh.

Em eventual situação, em que venha a ocorrer interrupção não prevista ao ..."*serviço de TI...*", deve haver alternativa de contingência à execução do respectivo sistema em outro ambiente de processamento de dados, isto é, um ambiente alternativo, que mantenha as funcionalidades e níveis de desempenho, de modo a premitir a continuidade do processo de negócio.

2. Análise de impacto

Template A

A análise de impacto identifica os parâmetros de sustentação em caso de uma eventual indisponibilidade, habilitando a priorização da ativação dos serviços de TI e componentes críticos.

1 – Serviço de TI

Descrição do Serviço de TI e os Processos sustentados por ele

2 – Detalhar o Impacto da interrupção do serviço de TI que o suporta, identificando e avaliando os potenciais impactos.

Potencial Impactos	Descrição	Avaliação do Impacto
Ex SEI "tramitação de documento"	*Não haver possibilidade de tramitar documento eletronicamente enquanto o sistema estiver paralisado*	*Alto*
Ex Mentorh "Contabilização de horas extras"	*Impossibilidade de lançar as horas extras e faltas dos funcionários.*	*Médio*
Ex AGHU "Evolução do paciente de forma manual"	*Pacientes serem evoluídos nos hospitais de forma manual,*	*Alto*
"item n"		

3 – Identificar o grau de impacto

Grau de Criticidade	

Classificação	Gravidade	Descrição
Baixa Criticidade	**1 a 8**	**Pouco importante**, cuja indisponibilidade não afeta a organização
Média Criticidade	**9 a 12**	**Importante**, cuja indisponibilidade afeta a organização, causando impactos reparáveis
Alta Criticidade	**13 a 20**	**Muito importante**, cuja indisponibilidade afeta muito a organização, causando impacto de reparação difícil.

4 - Determine os valores dos Parâmetros Técnicos

PMIT (Em Horas)	RPO (Em Minutos)	RTO(Minutos)

3. Escopo de Atuação do Plano de Contingência do "...serviço de TI..."

Template B

1 Ambiente Principal e Alternativos do Serviço de TI:

Nome	Cidade Estado	Empresa presta Suporte	Contato do Suporte	Endereço
"Principal"				
"Alternativo 1"				
"Alternativo 2"				

2 Ameaças

Listagem exaustiva, mas não definitiva, dos possíveis eventos de desastre que acionam o Plano de Contingência do Serviço de TI.

Potencial Ameaça	Descrição	Probabilidade
Ex "Desabamento do CDC"	*De origem Natural, ocorrer chuva ou terremoto de forma a parar o funcionamento do CDC*	*BAIXA*
"item 2"		
"item 3"		
"item n"		

4. Estratégia de Continuidade do "...serviço de TI..."

A Estratégia de contingência é criada para mitigar as potenciais ameaças apresentadas e abrange o planejamento da recuperação.

Os métodos e estratégias devem abordar os impactos de interrupção e os períodos de inatividade permitidos identificados na análise de impacto e devem ser integrados à arquitetura do sistema de contingência durante a fase de desenvolvimento e aquisição do Ciclo de Vida do Plano de Contingência.

Dados de Infraestrutura do *"...serviço de TI..."*

Para tanto, devem ser levantadas as informações sistêmicas e tecnológicas do serviço de TI, incluindo, de forma não conclusiva, mas exaustiva, pelo menos os seguintes itens:

I. Planilha de Ativos:
   - Atributos, Relacionamento de dependência, Mapeamento host e ativos;

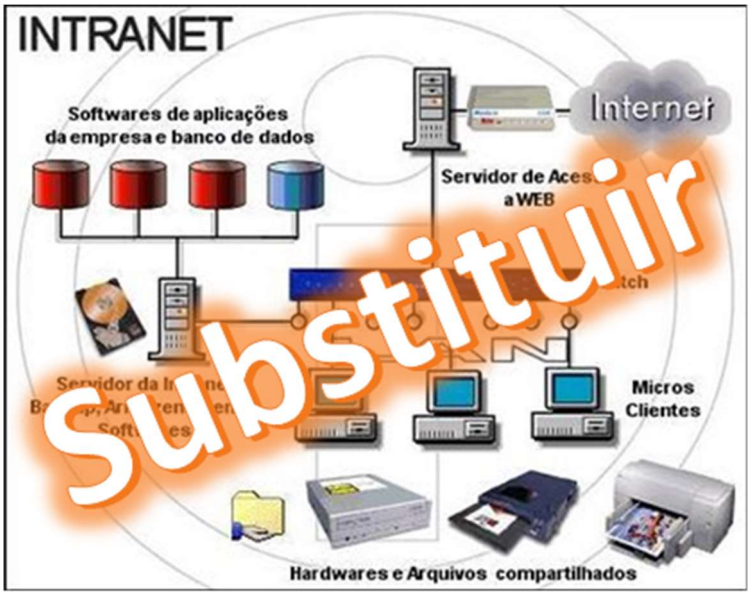
II. Topologia física e lógica;

a. Planilha de Ativos

Nome Ativo	Tipo do IC	Função	Localização	Marca/modelo	Em Garantia
Item 1					
Item 2					
Item n					

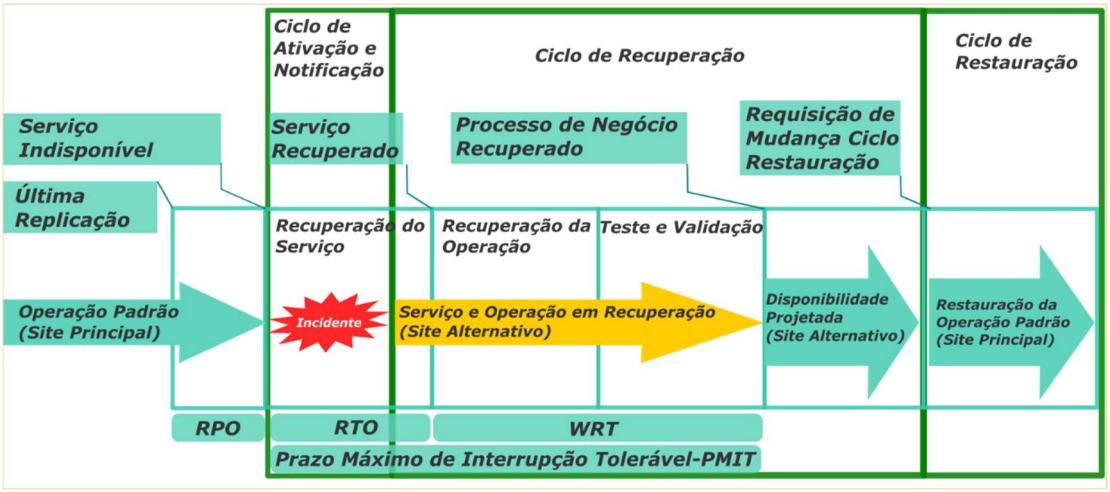
b. Topologia física e lógica

"...inserir imagem real..."



Planejamento da Recuperação

O Modelo de Plano de Contingência foi desenvolvido para recuperar um serviço de TI usando uma abordagem em três fases, Fase Ativação e Notificação, Fase de Recuperação e Fase de Restauração, conforme mostrado na figura abaixo.



Esta abordagem assegura que os esforços de recuperação do serviço sejam realizados em uma sequência de atividades para maximizar a eficácia do esforço de recuperação e minimizar o tempo de interrupção.

Cada fase apresentada no modelo é sustentada pelo Plano de Recuperação/Restauração Operacional apresentados neste anexo.

5. Guia de Equipes e Fornecedores

Template C

O Plano de Contingência estabelece diversas responsabilidades, atribuídas a papéis definidos nas equipes, para suportar a Contingência, realizando as Fases Ativação e Notificação, Recuperação e Restauração do *"...serviço de TI..."*.

5.1 Equipes

O Guia de Equipes estabelece os papeis atribuídos ao Plano de Contingência. As equipes com papéis atribuídos devem estar preparadas para responder a um evento de contingência que afete ao Serviço de TI e tem as responsabilidades definidas, categorizadas através de camadas hierárquicas, isto é, estratégica, tática e operacional.

As listas dos papéis e responsabilidades nesta seção foram criadas para refletir possíveis tarefas que os membros da equipe terão de executar, devendo ser adaptada à realidade da organização.

Os membros da equipe são responsáveis pela execução de todas as tarefas. Em algumas situações de Contingência, membros da equipe podem ser chamados a desempenhar tarefas não descritas nesta seção, devido a situações incomuns.

As Equipes definidas neste modelo deverão ser usadas como exemplos, devendo ser adaptada conforme a realidade da unidade e do serviço de TI no momento de criação do respectivo Plano de Contingência.

Guia de Equipe

Papel	Indivíduo	Cargo na Ebserh	Telefone

Exemplo de Possíveis Papeis:

Coordenação da Contingência

A Coordenação da Contingência irá supervisionar todo o processo de recuperação e restauração, sendo a primeira equipe que terá de tomar medidas em caso de um evento que caracterize uma Crise, avaliando o evento e determinando que medidas devem ser tomadas para a organização retomar o processo de negócio Gestão de Processos Administrativos Eletrônicos como previsto.

Liderança Operacional da Contingência

A Liderança Operacional da Contingência é responsável por executar todas as decisões relacionadas com os esforços de recuperação e restauração. A principal função será orientar durante o processo de recuperação e restauração todas as equipes envolvidas.

Equipe de Instalações

A Equipe de Instalações é responsável por todas as questões relacionadas com as instalações físicas que abrigam os serviços de TI no ambiente principal e alternativo. Esta equipe assegura que as instalações do Ambiente Alternativo são mantidas de forma adequada, avalia os danos e supervisiona os reparos no Ambiente Principal em caso de destruição ou danificação.

Equipe de Banco de Dados

A Equipe de Banco de Dados é responsável pelo o gerenciamento do Sistema Gerenciador de Banco de Dados, incluindo a estruturação e a administração.

Equipe de Conectividade

A Equipe de Conectividade é a responsável pela avaliação do dano específico para qualquer infraestrutura de conectividade, incluindo WAN e LAN, e quaisquer conexões internas. Esta Equipe é a principal responsável por fornecer a funcionalidade da conectividade de referência e pode ajudar outras equipes do Plano de Contingência, conforme necessário.

Equipe de Hardware e Software

A Equipe de Hardware e Software é responsável por manter toda infraestrutura de processamento e armazenamento, garantindo a funcionalidade de referência.

Equipe de Aplicação

A Equipe de Aplicação é responsável por garantir que todos os componentes do serviço contingenciado executem ações conforme necessário para cumprir os objetivos em caso de recuperação ou restauração, garantindo e validando o desempenho apropriado da aplicação e pode ajudar outras equipes, conforme necessário.

Equipe de Monitoramento

A Equipe de Monitoramento tem o objetivo de manter o monitoramento do Ambiente Alternativo exatamente conforme é realizado para o Ambiente Principal.

Equipe de Comunicação Institucional

A Equipe de Comunicação é a equipe responsável por toda a comunicação durante a ativação da Contingência, seja, uma recuperação ou restauração.

5.2 Fornecedores

A lista de Fornecedores deve relacionar o equipamento ao contato de suporte, caso haja:

Função	Equipamento/Serviço	Contato	Suporte	Garantia	Atendimento
Conectividade					
Armazenamento					
Banco de Dados					
Sistemas Operacionais					
Segurança					
Infraestrutura Predial					
Backup & Retrieve					
Virtualização					
Customizações e melhorias no ambiente					
Aplicação					

6. Plano de Recuperação/Restauração Operacional

Ciclo de Ativação Notificação

O Plano de Gerenciamento de Incidentes Críticos documenta as informações necessárias para gerir eficazmente as atividades de registro, identificação, tratamento, relativas aos Incidentes Críticos, a serem conduzidas em todos os ativos do ambiente do Ambiente Principal, físico e lógico, que sustenta o Serviço de TI.

A Atividade Caracterizar e Monitorar o Chamado é realizada através da Matriz GUT abaixo:

	Não há 1	Pouco 2	Considerável 3	Muito 4	Extremamente 5
Gravidade					
Urgência					
Tendência					
Nível de Criticidade (G x U x T)					

Nível de Criticidade	Atividade	Responsável
Menor ou igual a 32	Não informar à Coordenação de Contingência, mas manter o acompanhamento da evolução quanto à criticidade, até quando houver o encerramento do Chamado.	Liderança Operacional da Contingência
Acima de 32	Informar imediatamente à Coordenação de Contingência.	Liderança Operacional da Contingência

Caso seja necessária a aplicação da contingência, deverá proceder a notificação à Liderança Operacional da Contingência e esta ativará o Plano de Recuperação Operacional.

Se houver o entendimento que ainda não há necessidade de aplicação da contingência, deverá solicitar à Liderança Operacional da Contingência para categorizar como Incidente Crítico e Monitorar o Chamado.

Ciclo de Recuperação Operacional

O ciclo de recuperação operacional é utilizado pelo Plano de Contingência e se aplica a recuperar o Serviço de TI no Ambiente Alternativo.

Deverá ser descrito o passo a passo para cada item do Procedimentos Operacionais de Recuperação.

Procedimentos Operacionais de Recuperação

- **Avaliação do Incidente Crítico**
  - Acompanhar a Mudança Emergencial;
  - Comunicar ao Gestor do Processo que o Serviço de TI sustenta sobre os resultados da Mudança Emergencial.
- **Ativar a Contingência – Informar as equipes e os Gestores**
  - Realizar uma avaliação completa da interrupção para determinar a extensão da disruptividade ocorrida, incluindo os danos ocorridos e o tempo de recuperação esperado;
  - Mobilizar as equipes;
  - Informar o status operacional para cada equipe;
  - Fornecer os resultados da avaliação à Coordenação da Contingência para ajudá-la na coordenação da recuperação e na notificação adequada da Contingência às equipes de negócio;
  - Elaborar uma Requisição de Mudança Emergencial, tendo como base os procedimentos informados abaixo;
  - Submeter a Requisição de Mudança Emergencial ao Gerente de Mudanças;
  - Acompanhar a análise da RDM;
  - Comunicar o avanço da execução da Mudança Emergencial para a Coordenação Geral;
  - Colocar em produção o Serviço de TI no Ambiente Alternativo.
- **Realizar a Recuperação**
  - Comunicar as Partes Interessadas, utilizando a Lista de Contato Responsáveis pela Sustentação do serviço de TI, informada no documento Guia de Equipes e Fornecedores;
  - Informar o evento à comunidade usuária, divulgando o novo Acordo de Nível de Serviço – Disponibilidade Projetada de Serviço.
  - Comunicar à Liderança da Contingência sobre os resultados da notificação.
- **Notificar a Contingência**
  - Validar o funcionamento de comunicação de acesso ao Ambiente Alternativo;
  - Realizar alterações do roteamento do Ambiente Principal para o Ambiente Alternativo;
  - Comunicar à Liderança da Contingência sobre os resultados da ativação.
- **Ativar o Ambiente Alternativo**
  - Verificar o funcionamento das bases de dados dos serviços no Ambiente Alternativo;
  - Documentar as informações, referente às capacidades, configurações, hierarquia de acesso, etc., referentes aos bancos de dados, mantendo-os atualizados;
  - Manter a biblioteca sobre às informações de uso, como manuais, tutoriais, etc, atualizada;
  - Atuar em conjunto com as equipes responsáveis, para garantir a execução da replicação íntegra do banco de dados;
  - Validar as configurações do banco de dados no Ambiente Alternativo sempre que novos equipamentos forem incorporados ou alterados no Ambiente Principal;
  - Acompanhar toda mudança dos ativos que sustentam o serviço de TI no Ambiente Alternativo;
  - Garantir de forma segura o conjunto de credenciais para acesso aos bancos de dados, para uso nos Ambientes Principal e Alternativo;
  - Desenvolver e testar os procedimentos operacionais de baixar (“shutdown”) e reiniciar (“start”) os bancos de dados nos Ambientes Principal e Alternativo;

- Desenvolver e testar os Procedimentos Técnicos de Suporte de Administração (gerenciamento dos ativos), de Atendimento (reação a Incidentes Críticos) e Monitoramento (verificação proativa) para os ativos de hardware e software que sustentam os serviços de TI instalados nos Ambientes Principal e Alternativo;
- Revisar e manter atualizadas as informações e procedimentos operacionais definidos nos Planos relacionados à recuperação e restauração;
- Executar as respectivas ações definidas no Plano de Manutenção da Contingência, validando a sequência e procedimentos definidos, corrigindo as não conformidades.
- Comunicar à Liderança da Contingência sobre os resultados da verificação.

- **Validar o Banco de Dados**
  - Verificar o funcionamento dos ativos de hardware e software no Ambiente Alternativo;
  - Comunicar à Liderança da Contingência sobre os resultados da verificação.
- **Validar a Operação dos Ativos de Hardware e Software**
  - Verificar o funcionamento dos ativos de hardware e software no Ambiente Alternativo;
    Comunicar à Liderança da Contingência sobre os resultados da verificação
- **Validar a Aplicação**
  - Validar a integridade dos dados e funcionalidades do Serviços de TI, conforme Teste e Validação de Dados e Funcionalidade;
  - Comunicar à Liderança da Contingência sobre os resultados da verificação.
- **Monitorar a Aplicação no Ambiente Alternativo**
  - Ativar o monitoramento da aplicação no Ambiente Alternativo;
  - Comunicar à Liderança da Contingência sobre os resultados da ativação
- **Comunicar a Recuperação**
  - Comunicar as Partes Interessadas e Comunidade Usuária sobre a Recuperação realizada.

Ciclo de Restauração Operacional

O ciclo de restauração operacional é utilizado pelo Plano de Contingência e se aplica a restaurar o Serviço de TI no Ambiente Principal.

Deverá ser descrito o passo a passo para cada item do Procedimentos Operacionais de Restauração.

Procedimentos Operacionais de Restauração

- **Ativar a Restauração**
  - Mobilizar e coletar o status operacional de cada equipe;
  - Validar o checklist da ativação da restauração;
  - Fornecer os resultados da avaliação à Coordenação da Contingência;
  - Projetar o orçamento de Restauração;
  - Elaborar uma Requisição de Mudança, conforme as atividades previstas para os Procedimentos Operacionais de Restauração;
  - Submeter a Requisição de Mudança ao Gerente de Mudanças;
  - Acompanhar a evolução da Mudança;
  - Comunicar o avanço da Mudança para a Coordenação da Contingência

- **Restaurar as Instalações de Operação**
  - Adequar a infraestrutura de operação para hospedar o serviço de TI;
  - Identificar os ativos (processamento, armazenamento e comunicação) que estão em estado de falha e devem ser substituídos;
  - Se houver ativos em estado de falha corrigi-los.
  - Energizar todos os ativos;
  - Validar as infraestruturas;
  - Comunicar à Liderança da Contingência sobre os resultados da restauração.

- **Restaurar a Conectividade**
  - Revisar a topologia de rede;
  - Revisar a documentação e procedimentos para restabelecer o serviço.
  - Configurar switch e servidor com as VLANs;
  - Configurar roteador de borda;
    - Restabelecer túneis (VPN);
    - Restabelecer outras conexões necessárias;
  - Realizar testes de conectividade;
  - Atualizar documentação de conectividade;
  - Deixar preparadas as alterações do roteamento do Ambiente Alternativo para o Ambiente Principal;
  - Validar a conectividade do Ambiente Principal com as localidades que terão usuários;
  - Comunicar à Liderança da Contingência sobre os resultados da restauração.

- **Restaurar a Operação dos Ativos de Hardware e Software**
  - Realizar as configurações de Segurança;
    a. Nos ativos: IPS, Firewall, Balanceamento de carga
    b. Nos softwares: AntiSpam, Antivírus.
  - Instalar e configurar os Sistemas Operacionais nos ativos de Processamento e Armazenamento
    a. Atualizar Sistema Operacional;
    b. Configurar virtualização;
    c. Validar as configurações;
    d. Instalar aplicativos (Apache, etc.);
    e. Configurar DNS interno;
    f. Ativar Licenças;
    g. Restaurar e homologar backup do sistema aplicativo;
    h. Realizar testes;
    i. Configurar DNS;
    j. Atualizar documentação;
    k. Verificar o funcionamento da Infraestrutura de Armazenamento;
    l. Criar volumes necessários;
    m. Configurar zonas no switch SAN para storage e servidor de backup;
    n. Preparar ativo de backup em fita;
    o. Configurar conexão com o ativo de backup em fita;
    p. Validar infraestrutura de armazenamento;
    q. Atualizar documentação;
    r. Realizar testes de segurança da nova infraestrutura;
    s. Validar o funcionamento dos ativos de hardware e software;
    t. Comunicar à Liderança da Contingência sobre os resultados da restauração.

- **Restaurar o Banco de Dados**
    - Ativar a Replicação do Banco de Dados do Ambiente Alternativo para o Ambiente Principal;
    - Verificar o funcionamento das bases de dados dos sistemas;
    - Comunicar à Liderança da Contingência sobre os resultados da verificação

- **Restaurar a Aplicação**
    - Ativar a Replicação da Aplicação do Ambiente Alternativo para o Ambiente Principal;
    - Realizar testes;
    - Realizar os testes de conectividade e segurança da aplicação;
    - Validar a integridade dos dados e funcionalidades do Serviço de TI, conforme o Plano de Teste e Validação de Dados e Funcionalidade;
    - Ativar o serviço do serviço de TI;
    - Comunicar à Liderança da Contingência sobre os resultados da restauração.

- **Restaurar o Monitoramento da Aplicação no Ambiente Principal**
    - Ajustar o monitoramento;
    - Testar o monitoramento;
    - Atualizar documentação;
    - Ativar o monitoramento da aplicação;
    - Comunicar à Liderança da Contingência sobre os resultados da restauração do monitoramento.

- **Ativar o Ambiente Principal**
    - Validar o funcionamento de comunicação do Ambiente Principal;
    - Ativar Replicação do Ambiente Principal para o Ambiente Alternativo;
    - Ativar o roteamento do Ambiente Alternativo para o Ambiente Principal;
    - Comunicar à Liderança da Contingência sobre os resultados da ativação.

- **Comunicar a Restauração**
    - Comunicar as Partes Interessadas e Comunidade Usuária sobre a Restauração realizada.

9. Plano de Teste e Manutenção

Embora os esforços sejam feitos para construir este plano de contingência de forma completa e mais precisa possível, é difícil contemplar todas as possíveis situações que podem ocorrer quando da decretação de uma Crise e ativação do Plano de Contingência.

Além disso, ao longo do tempo a necessidade de aplicar a Contingência pode mudar.

Como resultado desses dois fatores, o ambiente de produção do serviço de TI no Ambiente Alternativo deve ser testado periodicamente, visando descobrir erros e omissões e prover os ajustes necessários.

9.1 Testes

A Ebserh está empenhada em assegurar que este plano de contingência é funcionalmente eficaz e eficiente. O plano de contingência deve ser testado numa periodicidade a ser definida.

O plano de contingência pode ser testado por um dos métodos, em separado ou em conjunto:

1) Comparação dos tamanhos das bases de dados;
2) Teste das funcionalidades;
3) Verificar se os requisitos de software para execução do serviço de TI no Ambiente Alternativo estão de acordo com o ambiente de produção instalado no Ambiente Principal;
4) Análise dos logs da replicação do banco de dados e dos arquivos do repositório de dados.

Quaisquer situações de não conformidade serão abordadas pela Liderança Operacional da Contingência e corrigidas.

No quadro abaixo é sugerida uma Agenda de Testes, considerando o dia D para realizar efetivamente o teste.

Atividade	Data máxima	Responsável
Identificar o facilitador de teste.	D - 5 (dias) antes de começar o teste.	Liderança da Contingência
Determinar o escopo do Teste.	D - 4 (dias) antes de começar o teste.	Liderança da Contingência, Facilitador do Teste
Definir o Plano de Teste.	D - 4 (dias) antes de começar o teste.	Facilitador do Teste
Identificar e engajar os recursos, agendar o teste	D - 3 (dias) antes de começar o teste.	Facilitador do Teste
Executar o Plano de Teste	D = 0 (realizar o teste)	Facilitador do Teste, Liderança da Contingência.
Finalizar as atividades e relatar as lições aprendidas.	D + 5 (dias) após realizar o teste	Liderança da Contingência
Atualizar o plano de contingência baseado nas lições aprendidas.	D + 10 (dias) após realizar o teste	Liderança da Contingência

Aprovar e distribuir a versão atualizada do plano de contingência.	D + 15 (dias) após realizar o teste	Coordenação da Contingência, Liderança da Contingência

9.2 Manutenção

O plano de Contingência será atualizado com frequência de *"...inserir frequência..."*a ser definida ou a qualquer momento quando houver uma atualização do serviços de TI que o sustenta, através do controle do Gerenciamento de Mudanças.

CLASSIFICAÇÃO DE CRITICIDADE DE SERVIÇOS DE TI

Nº	SERVIÇOS DE TI	RESPONSÁVEIS		IMPACTO (de 0 a 4 ponto)					TOTAL
		UN. GESTORA DO NEGÓCIO	UN. GESTORA DO SERVIÇO DE TI	Legal ou Regulatório	de Imagem	Operacional	Financeiro	Relacionado à Saúde e à Vida	
1	<SERVIÇO 01>								0
2	<SERVIÇO 02>								0
3	<SERVIÇO 03>								0
									0
									0