Sumário

1. OBJETIVO

Uma vez que falhas nos serviços de TIC impactam diretamente a continuidade da prestação dos serviços de Tecnologia da Informação e Comunicações (TIC) dentro do Humap-UFMS, almeja-se com este plano prover medidas de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes graves ou desastres a partir da especificação das ameaças e riscos identificáveis na organização e análise de seus impactos, caso essas ameaças se concretizem. O plano de continuidade atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos.

2. PLANO DE AÇÃO PARA ATENDIMENTO DOS OBJETIVOS

2.1 ESCOPO

O Plano de Continuidade de TIC (PCTIC) está baseado em três vértices: pessoas, tecnologia e organização; abrange as estratégias necessárias à continuidade dos serviços de TI essenciais, tendo como escopo o seguinte:

- Plano de Continuidade Operacional;
- Plano de Administração de Crises;
- Plano de Recuperação de Desastres;
- Plano de Contingência em Período de Ameaça Biológica.

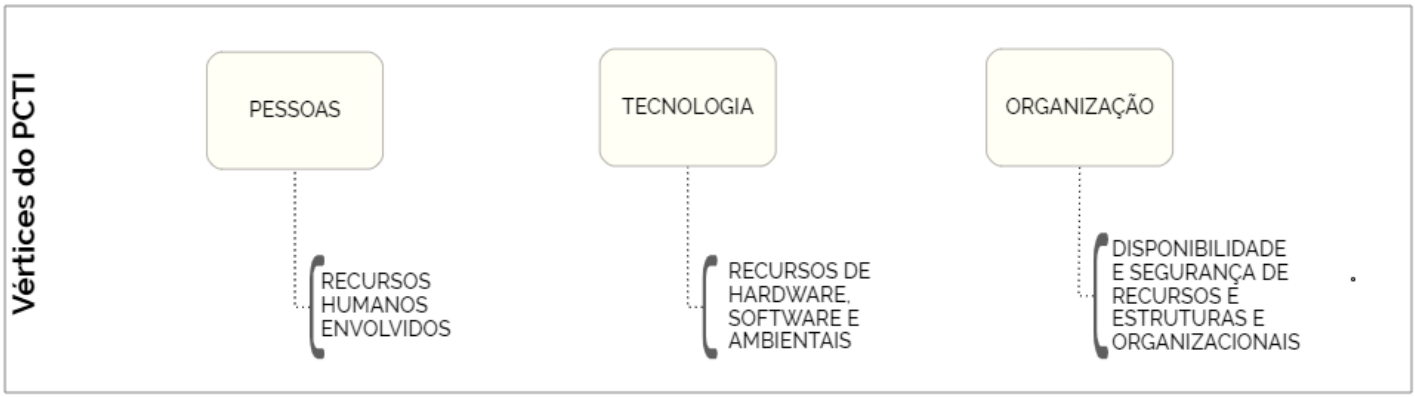


Figura 1 - Vértice do plano de Contingência

Estes planos podem ser executados tanto no âmbito do SGPTI, isoladamente, como parte do Plano de Continuidade de Negócio (PCN) do Humap-UFMS. O PCTIC está voltado a promover a continuidade dos processos definidos como críticos para a TI do Humap-UFMS e que impactam nos seus objetivos.

2.2 GRUPOS DO PCTIC

Este plano envolve basicamente quatro grupos:

- Contingência de Infraestruturas Físicas: assim compreendidas as situações de catástrofes naturais ou não, tais como inundações, incêndios, desabamentos, entre outros. No geral ocorrências que impeçam o acesso e/ou utilização das instalações do Humap-UFMS, como também danos físicos relevantes a instalações e/ou equipamentos, intencionais ou não, incluindo até mesmo falhas no fornecimento de energia elétrica;
- Contingência de Pessoas: aquelas onde os colaboradores chave não estão presentes por motivos de greves, doença, licenças e etc;
- Contingência de Infraestruturas Tecnológicas: compreendidas as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, telecomunicações, rede e segurança;
- Contingência de Serviços Externos - compreendidas as situações de não prestação de serviço contratado considerado crítico aos processos do Humap-UFMS.

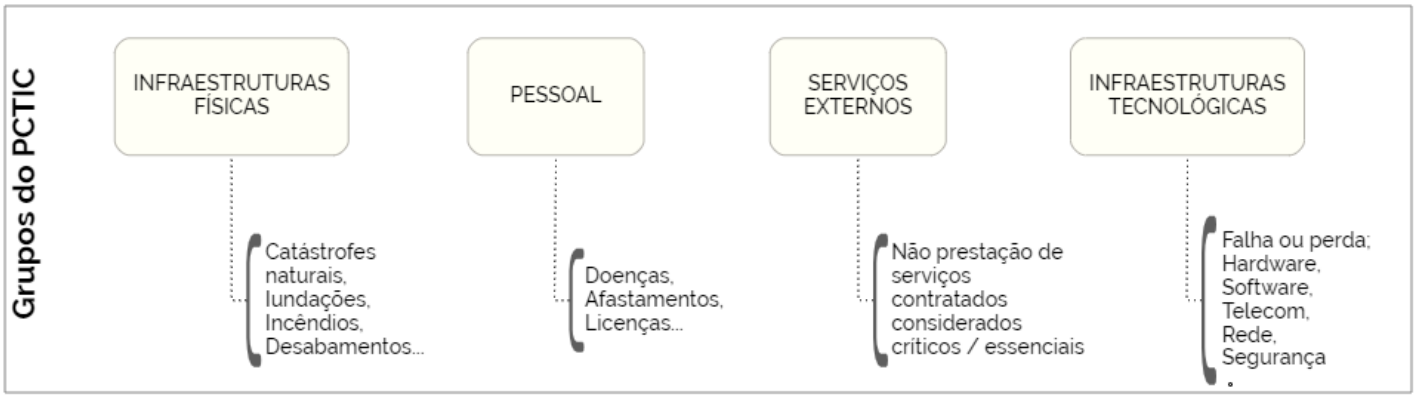


Figura 2 - Grupos do PCTIC

2.3 ÁREA

O PCTIC será administrado, avaliado e acionado no âmbito do Setor de Gestão de Processos e Tecnologia da Informação do Humap-UFMS tendo sua manutenção, organização e melhoria revistas e atualizadas periodicamente pelo Comitê de Governança de Tecnologia da Informação e Comunicações do Humap-UFMS.

Áreas cobertas:

SUPERINTENDÊNCIA
SETOR JURÍDICO
SETOR DE GESTÃO DE PROCESSOS E TECNOLOGIA DA INFORMAÇÃO
Unidade De Apoio Corporativo
Ouvidoria
Unidade De Planejamento
Unidade De Comunicação

GERÊNCIA DE ATENÇÃO À SAÚDE
Divisão de Gestão do Cuidado
Divisão Médica
Divisão de Enfermagem
SETOR MATERNO INFANTIL
Unidade De Cabeça E Pescoço
Unidade De Especialidades Clínicas
Unidade De Cuidados Intensivos E Semi Intensivos
Unidade De Clínica Cirúrgica
Unidade De Cuidados Intensivos E Semi intensivos Pediátricos
Unidade De Urgência E Emergência
Unidade De Hematologia, Oncologia E Radioterapia
Unidade De Clínica Médica
Unidade Do Sistema Musculoesquelético
Unidade De Doenças Infecciosas E Parasitarias.
Unidade Do Sistema Urinário
Unidade De Atenção À Saúde Da Criança E Do Adolescente
Unidade Do Sistema Cardiovascular
Unidade De Atenção Psicossocial
Unidade De Enfermagem Assistencial
Divisão De Apoio Diagnóstico E Terapêutico
SETOR DE APOIO DIAGNÓSTICO E TERAPÊUTICO
Unidade Laboratório De Anatomia Patológica
Unidade De Reabilitação
Unidade De Nutrição Clínica
Unidade Laboratório De Análises Clínicas
Unidade De Diagnóstico Por Imagem E Métodos Gráficos
Unidade De Cirurgia/RPA/CMF
SETOR DE FARMACIA HOSPITALAR
Unidade De Abastecimento.
Unidade De Farmácia Clinica E Dispensação.
SETOR DE VIGILANCIA EM SAUDE
SETOR DE REGULAÇÃO E AVALIAÇÃO EM SAÚDE
Unidade De Regulação Assistencial
Unidade De Processamento De Informação Assistencial

Unidade De Monitoramento E Avaliação

GERÊNCIA DE ENSINO E PESQUISA
Unidade de Web saúde
SETOR DE GESTÃO DA PESQUISA E INOVAÇÃO TECNOLÓGICA
SETOR DE GESTÃO DO ENSINO
Unidade de Gerenciamento de Atividades de Graduação e Ensino Técnico
Unidade de Gerenciamento de Atividades de Pós Graduação

GERÊNCIA ADMINISTRATIVA
Divisão Administrativa Financeira
SETOR DE ORÇAMENTO E FINANÇAS
Unidade De Programação Orçamentária E Financeira
Unidade De Pagamento Da Despesa
Unidade De Liquidação Da Despesa
SETOR DE AVALIAÇÃO E CONTROLADORIA
UNIDADE DE CONTABILIDADE FISCAL
UNIDADE DE CONTABILIDADE DE CUSTOS
SETOR DE ADMINISTRAÇÃO
Unidade De Compras
Unidade De Contratos
Unidade De Apoio Operacional
Unidade De Patrimônio
Unidade De Licitações
Divisão De Gestão De Pessoas
Divisão De Logística E Infraestrutura Hospitalar
SETOR DE ENGENHARIA CLÍNICA
SETOR DE INFRAESTRUTURA FÍSICA
SETOR DE HOTELARIA HOSPITALAR
SETOR DE SUPRIMENTOS
Unidade De Produtos Para Saúde
Unidade De Almoxarifado

2.4 TERMOS E DEFINIÇÕES

Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para a organização;

Ativo: qualquer recurso que tenha valor para a organização e cujo risco precisa ser controlado;

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

BPMN: Acrônimo de Business Process Modeling Notation. Notação gráfica que descreve a lógica dos passos de um processo de negócio. É um padrão internacional de modelagem que permite modelar o processo de uma maneira unificada e padronizada;

Probabilidade do risco: possibilidade de concretização de uma ameaça;

Nível de risco: magnitude do risco, expressa em termos da combinação das consequências e de suas probabilidades.

Evento de Segurança da Informação: ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Risco de segurança da informação: possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos. É medido em função da combinação da probabilidade de um evento e de sua consequência;

Risco Residual: Risco remanescente após o tratamento de risco ter sido implementado. O risco residual pode conter riscos não identificados;

Contexto Externo: é o ambiente externo no qual a organização se situa e busca atingir seus objetivos (ambiente cultural, financeiro, regulatório, econômico, entre outros);

Contexto Interno: é o ambiente interno no qual a organização busca atingir seus objetivos (governança, estrutura organizacional, políticas, normas, objetivos, diretrizes, cultura organizacional, entre outros);

TIC: Tecnologia da Informação e Comunicações;

Impacto (ou consequência): uma das consequências da ocorrência de um evento. Ocasiona mudança adversa no nível obtido dos objetivos.

2.5 CRITÉRIOS PARA AVALIAÇÃO DE RISCO

Os critérios de riscos são parâmetros estabelecidos para avaliar a magnitude dos riscos, a fim de seja possível quantificar o impacto negativo na busca da obtenção de resultados esperados pelo Humap-UFMS em sua missão institucional.

Para efeito deste processo, definiu-se como metodologia para a análise de risco a forma proposta pela norma ABNT NBR ISO 31000:2009, a qual define o nível do risco em termos da combinação dos impactos e de suas probabilidades.

Serão utilizadas escalas quantitativas para estimar a probabilidade e o impacto. Tais escalas encontram-se representadas nas Tabela 1 e Tabela 2

Peso	Critérios	Probabilidade
5	Muito Alta	50% < Probabilidade <= 100%
4	Alta	20% < Probabilidade <= 50%
3	Média	8% < Probabilidade <= 20%
2	Baixa	2% < Probabilidade <= 8%
1	Muito Baixa	0% < Probabilidade <= 2%

Tabela 1- Critérios de Probabilidade

Peso	Impacto	Descrição
5	Catastrófico	Impacto máximo nos objetivos do processo avaliado, sem possibilidade de recuperação.
4	Muito Relevante	Impacto significante nos objetivos do processo avaliado, com possibilidade remota de recuperação.
3	Relevante	Impacto mediano nos objetivos do processo avaliado, com possibilidade de recuperação.
2	Pouco Relevante	Impacto mínimo aos objetivos do processo avaliado. São facilmente remediáveis.
1	Insignificante	Impacto insignificante nos objetivos do processo avaliado. Dispensa qualquer medida de reparação.

Tabela 2- Critérios de Impacto

O nível do risco é calculado pelo produto entre a probabilidade e o impacto. A Tabela 3 apresenta a matriz de risco, ferramenta utilizada para a classificação dos níveis de risco.

Extremo Elevado Médio Baixo		PROBABILIDADE				
		Muito baixa (1)	Baixa (2)	Média (3)	Alta (4)	Muito Alta (5)
IMPACTO	Catastrófico (5)	5	10	15	20	25
	Muito relevante (4)	4	8	12	16	30
	Relevante (3)	3	6	9	12	15
	Pouco relevante (2)	2	4	6	8	10
	Insignificante (1)	1	2	3	4	5

Tabela 3- Matriz de Risco

2.6 PROCESSO DE GESTÃO DE RISCOS

O modelo adotado pelo SGPTI para o gerenciamento de riscos pautou-se na norma ISO 31000:2018 Diretrizes. A seguir será feita uma breve abordagem sobre o gerenciamento de riscos abordado na referida norma.

2.6.1 GESTÃO DE RISCOS: Introdução

O gerenciamento de riscos é um processo repetitivo e não-exaustivo, que auxilia as organizações quanto ao alcance de objetivos, tomada de decisões e estabelecimento de estratégias. Para se fazer um bom gerenciamento de riscos é necessário que se considere os contextos internos e externos da organização, incluindo fatores humanos e culturais. A Figura 1 apresenta a os princípios, estrutura e processos em que devem se basear o gerenciamento de riscos dentro de uma organização.

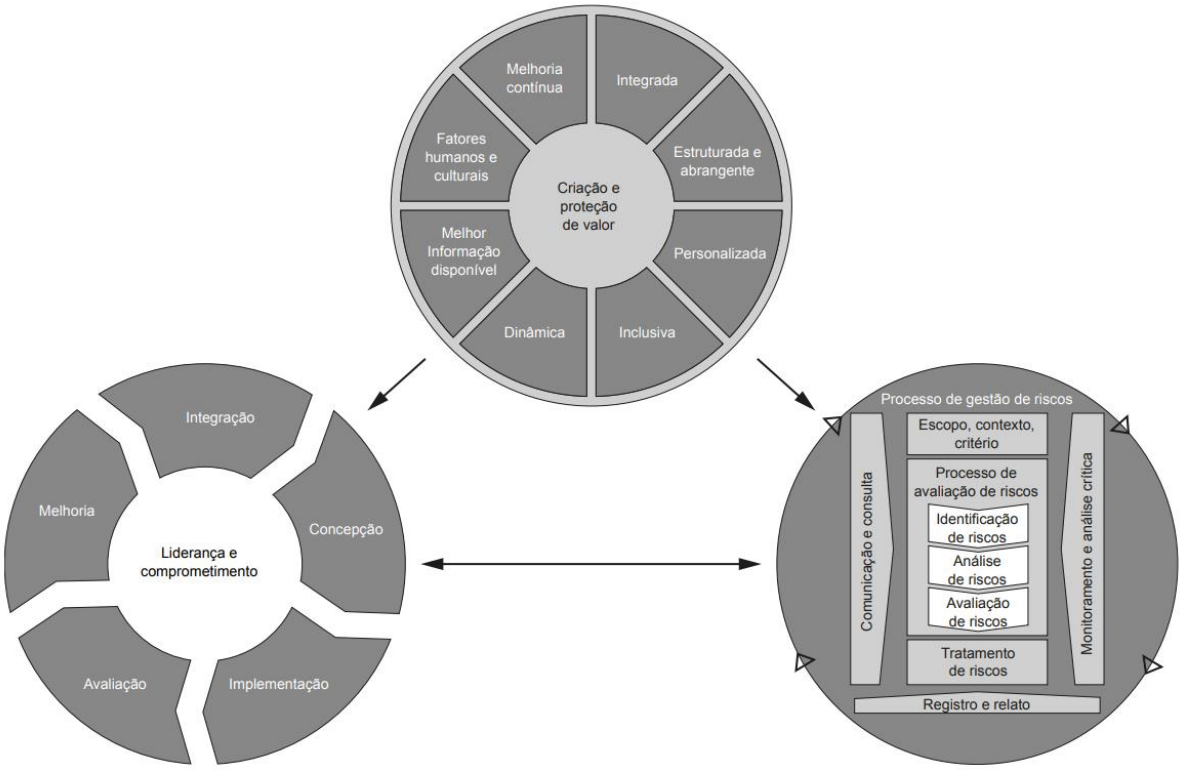


Figura 3 - Princípios, Estrutura e Processo de Gestão de Risco ABNT NBR ISO 31000:2018

2.6.2 GESTÃO DE RISCOS: Princípios

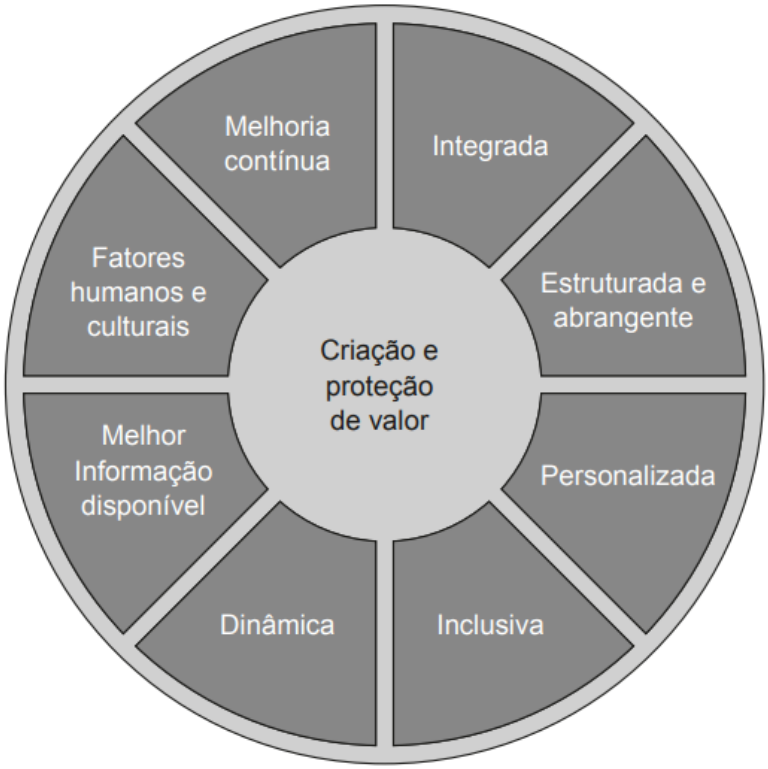


Figura 4 - Gestão de Riscos: Princípios

A gestão de riscos requer o uso dos seguintes princípios:

- Integrada: a gestão de riscos é parte integrante de todas as atividades organizacionais;
- Estruturada e abrangente: uma abordagem estruturada e abrangente para a gestão de riscos contribui para resultados consistentes e comparáveis;
- Personalizada: a estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos interno e externo da organização relacionados aos seus objetivos;
- Inclusiva: o envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada;
- Dinâmica: Riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna;

- Melhor informação disponível: as entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos explicitamente leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. Convém que a informação seja oportuna, clara e disponível para as partes interessadas pertinentes;
- Fatores humanos e culturais: o comportamento humano e a cultura influenciam significativamente todos os aspetos da gestão de riscos em cada nível e estágio;
- Melhoria contínua: a gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

2.6.3 GESTÃO DE RISCOS: Estrutura

Figura 5 - Gestão de Riscos: Estrutura

A estrutura da gestão de riscos busca apoiar a organização na integração da gestão de riscos em atividades significativas e funções. A sua eficácia depende da sua integração na governança e em todas as atividades na organização, requerendo assim apoio das partes interessadas, em particular da Alta Direção.

A gestão de riscos requer uma estrutura que engloba o seguinte:

- Liderança e comprometimento: convém que a alta direção e demais órgãos de supervisão assegurem que a gestão de riscos esteja integrada em toda a organização;
- Integração: o risco é gerenciado por todas as partes da estrutura da organização, sendo todos responsáveis pelo gerenciamento dos riscos;
- Concepção: ao conceber a estrutura para gerenciar riscos, convém que a organização examine e entenda seus contextos externos e internos;
- Implementação: convém que a organização implemente a estrutura de gestão de riscos por meio de um plano apropriado, com identificação dos diferentes tipos de decisões a serem tomadas, modificação dos processos, onde necessário, e garantia que os arranjos da organização sejam claramente compreendidos e praticados;
- Avaliação: a organização deve mensurar periodicamente a estrutura e determinar se a mesma permanece adequada para o alcance dos objetivos;
- Melhoria: a organização deve monitorar e adaptar continuamente a estrutura para abordar as mudanças internas e externas com a adoção da melhoria contínua.

2.6.4 GESTÃO DE RISCOS: Processos

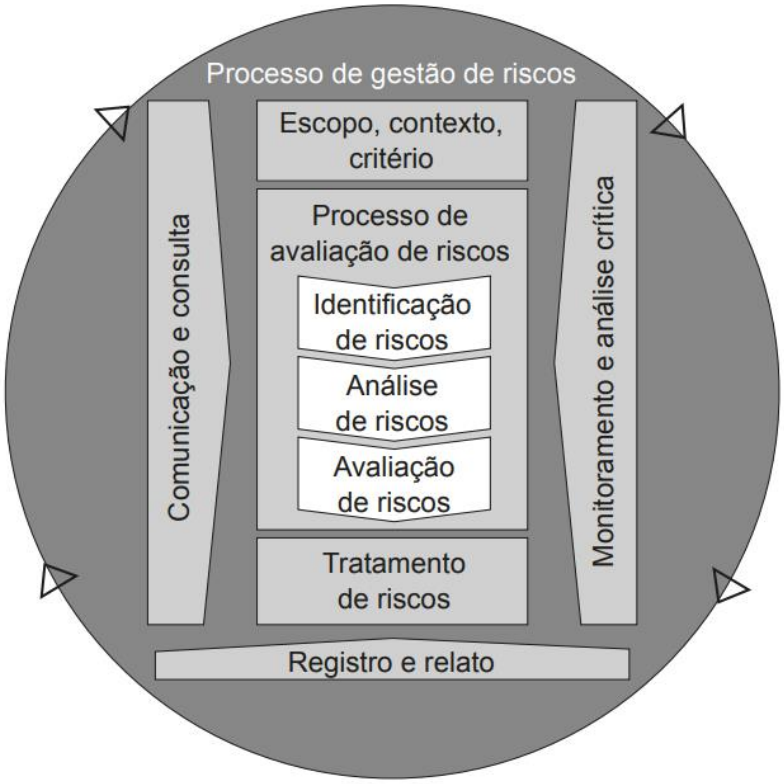


Figura 6 - GESTÃO DE RISCOS: Processo

O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as seguintes atividades:

- Comunicação e consulta: objetiva auxiliar as partes interessadas na compreensão do risco, sobre as decisões que são tomadas e as razões para tal;
- Escopo, contexto e critério: permite um processo de avaliação de riscos eficaz e um tratamento apropriado. Envolver a definição do escopo e compreensão dos contextos interno e externo;
- Processo de avaliação de riscos: permite a identificação, análise e avaliação de riscos;
- Tratamento de riscos: tem como objetivo selecionar e implementar opções para abordar os riscos;
- Monitoramento e análise crítica: visa assegurar e melhorar a qualidade e eficácia da concepção, implententação e resultados do processo;

- Registro e relato: visa fornecer informações ara a tomada de decisão, melhorar as atividades de gestão de riscos e auxiliar a interação com as partes interessadas.

O fluxo de processos de Gestão de Riscos do SGPTI/Humap-UFMS encontra-se desenhado em BPMN no Anexo I.

A definição do escopo das atividades do SGPTI/Humap-UFMS tarefas previstas pelo Processo de Gestão de Riscos do SGPTI/Humap-UFMS estão especificadas no Anexo II.

É importante destacar que embora todas as tarefas do processo sejam de responsabilidade do Setor de Gestão de Processos e Tecnologia da Informação, a participação de outras unidades da área de TIC (Desenvolvimento, Governança, Relacionamento com o Usuário e AGHU) e do Subcomitê Gestor de Segurança da Informação e Comunicações são indispensáveis para o sucesso na gestão dos riscos.

As unidades de TIC participarão das atividades sempre que os riscos envolverem as suas respectivas áreas de atuação. O Subcomitê Gestor de Segurança da Informação e Comunicações será instado a validar e aprovar os artefatos produzido ao longo do processo quando for necessário o estabelecimento de diretrizes com aplicabilidade em todo Hospital.

2.7 PRINCIPAIS RISCOS

O PCTIC foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam risco à continuidade dos serviços essenciais. O quadro disponível no Anexo III define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

2.8 NÍVEIS DE INCIDENTES

Nível I – Hipótese acidental que pode ser controlada pela equipe de TI do Humap-UFMS e que não afeta o andamento do trabalho do servidor.

Ex: Problemas com equipamentos periféricos de computadores.

Nível II – Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo servidor.

Ex: Problema com o funcionamento do Computador (não liga, travamento, etc) ou ainda sistemas offline impedindo o uso do mesmo.

Nível III – Hipótese acidental que impede o uso de sistemas ou equipamentos de todo Setor, impedindo o desenvolvimento do trabalho de uma área específica.

Ex: Falha de um Switch de rede do PAM.

Nível IV – Hipótese acidental que impede o uso de sistemas ou equipamentos de todo o Humap, impedindo assim o desenvolvimento do trabalho de todos os servidores do Hospital.

Ex: Falha na conexão com a internet, queda de energia elétrica no campus ou ainda problema técnico em algum servidor de rede que controla a conexão interna do Hospital, ou ainda, falha em sistemas críticos de uso dentro do hospital.

2.9 PRIORIDADES

A definição da prioridade no atendimento precisa ser técnica e pragmática, sendo assim a opção é seguir as boas práticas. O conjunto de boas práticas ITIL, utilizado pelas grandes corporações no mundo todo, é uma delas. Portanto, a PRIORIDADE é definida pela relação URGÊNCIA versus IMPACTO.

O número de usuários afetados por departamento, área ou atividade específica, define o impacto do incidente. Já a urgência pode levar em conta a característica da atividade e o quanto ela impacta, por exemplo, nas atividades que não podem ser interrompidas: cirurgias, exames, atendimentos, palestras, pregões eletrônicos, videoconferências, dentre outros.

2.10 PAPÉIS E RESPONSABILIDADES

EQUIPE DE INFRAESTRUTURA:

- Responsável pelas instalações físicas que abrigam sistemas de TI e pela garantia que as instalações alternativas serão mantidas adequadamente. Avalia os danos e supervisiona os reparos para o local principal no caso de a localização primária sofra da destruição ou danos.
- O líder desta equipe administrará e manterá o Plano de Recuperação de Desastre.
- Avaliar os danos específicos de qualquer infra-estrutura de rede e para fornecer dados e conectividade de rede de voz, incluindo WAN, LAN e quaisquer conexões de telefonia internamente dentro do Humap-UFMS ou de infraestrutura externa junto aos prestadores de serviço.
- Fornecer a infraestrutura de servidor físico e virtuais necessária para que o Humap

execute suas operações e processos essenciais durante um desastre.

- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes do SGPTI conforme necessário.
- Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.
- Responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário.
- O líder desta equipe administrará e manterá o Plano de Administração de Crise.

EQUIPE DE HARDWARE E OPERAÇÕES:

- Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar todos os funcionários do Humap-UFMS na solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas.
- Deverá atender aos usuários em caso necessário para realizar os testes de conectividade e de desempenho dos Desktops.
- Deverá verificar que as impressões estão saindo corretamente.

SUBCOMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SGSIC):

- Prover mecanismos de segurança no ambiente principal e alternativo. Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.
- Deverá ser comunicado ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SEDE) qualquer incidente.

EQUIPE DE TRATAMENTO DE INCIDENTES EM REDE DE COMPUTADORES (ETIR/HUMAP):

- Avaliar o plano periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.
- Facilitar e coordenar as atividades de tratamento e resposta a incidentes de
- Segurança da Informação e Comunicações (SIC);
- Promover a recuperação de sistemas;
- Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;
- Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

- Receber, filtrar, classificar e responder às solicitações e alertas e realizar análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
- Avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação;
- Reportar ao Subcomitê Gestor de Segurança da Informação e Comunicações (SGSIC/SGPTI/SUPRIN/Humap-UFMS) os incidentes de segurança;
- Emitir alertas sobre vulnerabilidades e outras notificações relacionadas à SIC no âmbito do Humap-UFMS;
- Avaliar o uso de ferramentas de Segurança da Informação e Comunicação - SIC;
- Analisar ataques e intrusões na rede do Humap-UFMS
- Inclui autoridades em nível institucional e tomadores de decisão do SGPTI.

EQUIPE DE SISTEMAS E AGHU

- Responsável pelo desenvolvimento, tratamento, modificação e manutenção dos sistemas do Humap-UFMS;
- Auxiliar no levantamento de requisitos de sistemas;
- Reportar à equipe do SGPTI e aos usuários de forma geral sobre atualizações de versão, modificações ou melhorias nos sistemas;
- Manter contato direto com a EBSERH SEDE sobre a implementação de sistemas, implantações, sugestões de melhoria e manutenção;
- Manter o contato com a rede de Hospitais Universitários da rede EBSERH para trazer soluções que viabilizem a melhoria no fluxo de trabalho e processos dentro do Humap-UFMS;
- Tratar e sugerir melhorias de performance em conjunto com a equipe de EQUIPE DE TRATAMENTO DE INCIDENTES EM REDE DE COMPUTADORES.

Nome	Líder	Integrantes
ETIR	Christian Ferraz Pinto Pacheco	Geyson Pereira Santana Jean Carlo Heemann
EQUIPE DE INFRAESTRUTURA	Christian Ferraz Pinto Pacheco	Geyson Pereira Santana
EQUIPE DE HARDWARE E OPERAÇÕES	Geyson Pereira Santana	Alan Massaharo Aguni Milton Marques Luis Carlos Campaner Rodrigo Valentin Coradini
SGSIC	Geyson Pereira Santana	Christian Ferraz Pinto Pacheco Edeilson Silva Cruz Luis Carlos Campaner
EQUIPE DE SISTEMAS E AGHU	Edeilson Silva Cruz	Christian Ferraz Pinto Pacheco Jean Carlo Heemann

2.11 INVOCAÇÃO DO PLANO

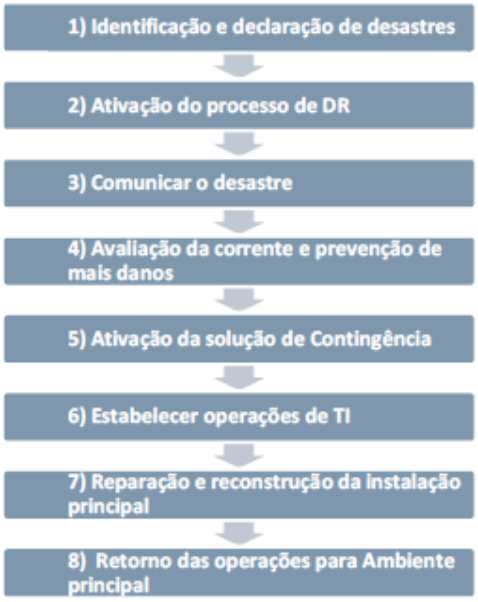
O PCTIC será acionado quando da ocorrência de algum dos cenários de desastres [2.76], a insurgência ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada.

O plano também poderá ser invocado em casos de testes ou por determinação do SUBCOMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES em conjunto com a alta governança do Humap-UFMS.

Os integrantes da EQUIPE DE INFRAESTRUTURA serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente caso seja possível.

2.12 MACROPROCESSOS DO PCTIC

O PCTIC tem seus macroprocessos definidos nas atividades a seguir e se desmembra em planos específicos para cada área de atuação quando da ocorrência de um desastre.



Os subplanos do PCTIC consistem em:

Plano de Continuidade Operacional (PCO):

- Garantir a continuidade dos serviços essenciais de TI críticos na ocorrência de desastres, enquanto recupera-se o ambiente principal.

Plano de Administração de Crise (PAC):

- Definir atividade das equipes envolvidas e orquestrar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos até a superação da crise.

Plano de Recuperação de Desastre (PRD):

- O Planejar e agir para que, uma vez controlada a contingência e passada a crise, a TI do TJBA retome seus níveis originais de operação no ambiente principal.

2.13 ESTRATÉGIAS DE CONTINUIDADE

A estratégia de continuidade para o cenário atual da TI e serviços essenciais está estabelecida da seguinte forma:

TIPO: Site Backup Local

DESCRIÇÃO:

- Cópias de backup dos sistemas essenciais do Container armazenados em local alternativo: Sala Segura;
- Há um hardware específico configurado no local;
- Dispõe de conexão redundante de fibra óptica;
- *Downtime* médio-alto*.

AÇÕES DE CONTINGÊNCIA/RECUPERAÇÃO:

Mapear dados e ativos que possivelmente podem ser perdidos para que se possa, reestabelecer toda a estrutura afetada o mais rápido possível e, após o ambiente principal estar operacional, prover a recuperação dos dados em backups.

OBSERVAÇÕES:

As ações de contingência e recuperação são detalhadas nos subplanos a seguir.

3. PLANO DE CONTINUIDADE OPERACIONAL (PCO)

Este subplano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais. O SGPTI é responsável por implementar, manter e melhorar o PCO e toda a documentação inerente.

3.1 OBJETIVO E ESCOPO

É escopo deste plano garantir ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas das ações de contingência definidas na estratégia.

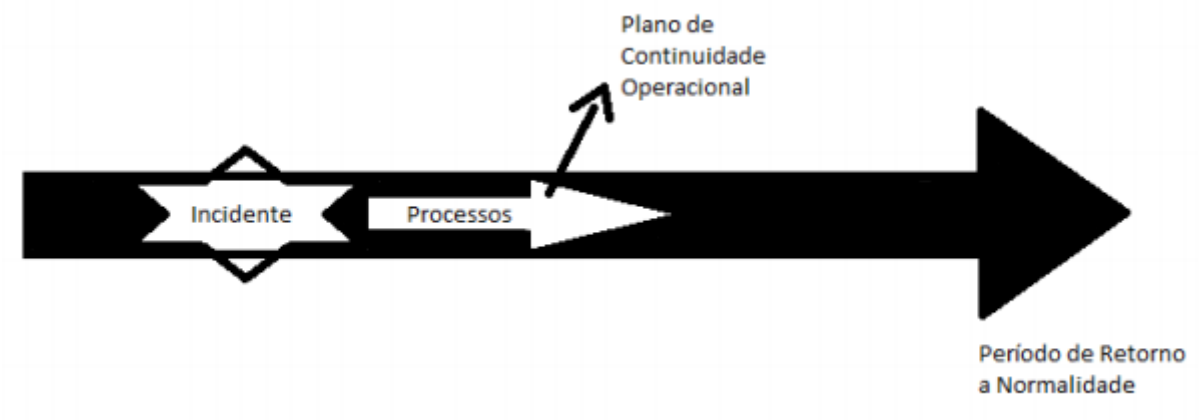


Figura 7 - Tempo PCO

São objetivos PCO:

A. Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações de TI, mesmo após a ocorrência de um desastre, dos sistemas essenciais;
B. Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre;
C. Estabelecer uma equipe para cada plano PCO, PRD e PAC;
D. Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

3.2 ATORES ENVOLVIDOS

- CHEFIA DO SGPTI;
- EQUIPE DE TRATAMENTO DE INCIDENTES EM REDE DE COMPUTADORES (ETIR/HUMAP);
- EQUIPE DE SISTEMAS E AGHU.

3.3 LISTA DE ATIVIDADES

- Avaliar situação de desastre;
- Identificar ativos afetados;
- Estimar impacto de perda de dados;
- Mapear ativos a serem recuperados;
- Levantar dados de backup para restauração;
- Implantar procedimentos de recuperação;
- Testar procedimentos realizados;
- Repassar eventuais informações para demais colaboradores.

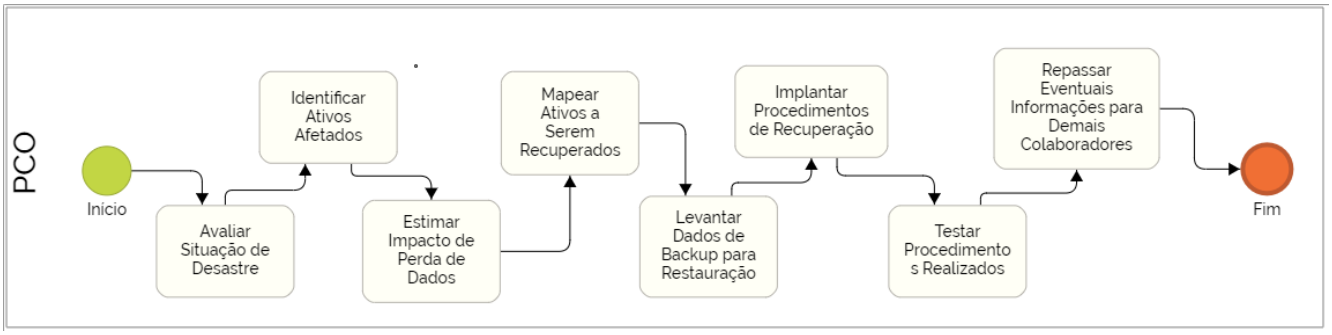


Figura 8 - Processo de Retomada de Negócio

3.4 RECURSOS NECESSÁRIOS

Durante um incidente, os recursos humanos e materiais necessários para continuidade operacional devem ser relacionados de forma a refletir a necessidade de acordo com a gravidade do evento.

Atualmente, além da operação do Container principal do Humap-UFMS, com gerador à diesel que possui autonomia de até 4h sem energia elétrica externa, também foram realizadas ações para garantir a manutenção dos sistemas em caso de falhas de hardware ou software de

forma externa ao espaço físico (Sala Segura/Site Backup Local), no qual se encontram os equipamentos de processamento e armazenamento de dados:

- Aquisição de dois servidores de 128Gb de memória para alocação na Sala Segura que já conta com No-Breaks e Gerador próprio para o caso de falhas elétricas. A aquisição visa garantir que em caso de falha nos servidores do Container, os dados possam ser migrados e restaurados nos servidores na Sala Segura;
- Aquisição de software de virtualização Vmware para permitir o *"moving"* e restauração das máquinas virtuais em caso de falha;
- Processo de aquisição de software backup para auxiliar em uma rápida restauração de dados em caso de falha crítica nos servidores principais;
- Em caso de parada parcial no Container, como falha dos climatizadores de ar, ou gerador de energia, já existe solução de contorno fornecida pela empresa Gemelo, atual contratada responsável pela manutenção do Container.
- No caso de parada total do Container, deverão ser avaliadas as possibilidades de execução dos serviços na Sala Segura, de forma a permitir a manutenção dos serviços de TI em parcial funcionamento dos sistemas críticos.

3.5 ENCERRAMENTO DO PCO

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter deverá ser emitido um parecer ao comitê relatando as atividades realizadas neste PCO.

A equipe responsável pelo retorno deve emitir um parecer, relatando as atividades realizadas, para então fornecer os dados necessários para um comunicado de retorno das atividades à instituição, estando a mesma representada pela sua Governança.

4. PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

Este plano especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos, inerente ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

4.1 OBJETIVO E ESCOPO

O objetivo deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de uma catástrofe. Já a abrangência (Escopo), é focada nas equipes (Recursos Humanos) e leva em conta os fatores históricos. Também considera os fatos que estão ocorrendo e por fim as ações futuras, que são delimitadas somente após a ocorrência de um evento.

São objetivos específicos do PAC:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.
- Orientar os colaboradores do SGPTI, usuários e colaboradores de forma geral, incluindo terceirizados, com informações e procedimentos de conduta.
- Informar a Governança em tempo e com esclarecimentos condizentes com o ocorrido.

Figura 9 - Tempo do PAC

4.2 ATORES ENVOLVIDOS

- CHEFIA DO SGPTI;
- EQUIPE DE INFRAESTRUTURA;

- EQUIPE DE HARDWARE E OPERAÇÕES;
- SUBCOMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SGSIC);
- EQUIPE DE TRATAMENTO DE INCIDENTES EM REDE DE COMPUTADORES (ETIR/HUMAP);
- EQUIPE DE SISTEMAS E AGHU.

4.3 AUTORIDADES RESPONSÁVEIS

As autoridades designadas neste plano serão envolvidas, não afastando a possibilidades de que outras autoridades na linha decisória hierárquica inferior possam ser envolvidas em caso de necessidade:

- Superintendente;
- Gerente de Atenção à Saúde;
- Gerente Administrativo;
- Gerente de Ensino e Pesquisa;
- Chefe do SGPTI.

4.4 ATIVIDADES E PAPÉIS PRINCIPAIS

Caberá ao mais alto Gestor de TIC em exercício, atuar como elo de ligação entre o corpo técnico e as áreas interessadas ou afetadas pela não continuidade dos negócios. Além disso, poderá ter representação pontual no Comitê Gestor de Tecnologia da Informação e das Comunicações, sempre que a crise for relacionada a Tecnologia da informação e Comunicação.

4.5 LISTA DE TAREFAS E AÇÕES

A gestão de crises na área de TIC deverá ser executada conforme o tipo da crise, seguindo uma linha geral de procedimentos listados:

- Equipes de Infraestrutura e Sistemas e AGHU devem avaliar a extensão do que foi afetado;
- Chefe do SGPTI deve ser informado para buscar soluções para a gestão da crise;
- Superintendente e/ou Gerentes devem ser informados e consultados;
- CGSIC monta um centro de gerenciamento de crises;

- Chefia do SGPTI mantém a comunicação entre equipe interna e Governança;
- Após recovery, Chefia do SGPTI informa à Governança;
- Registro de informações para melhor Gestão de Crises futuras.

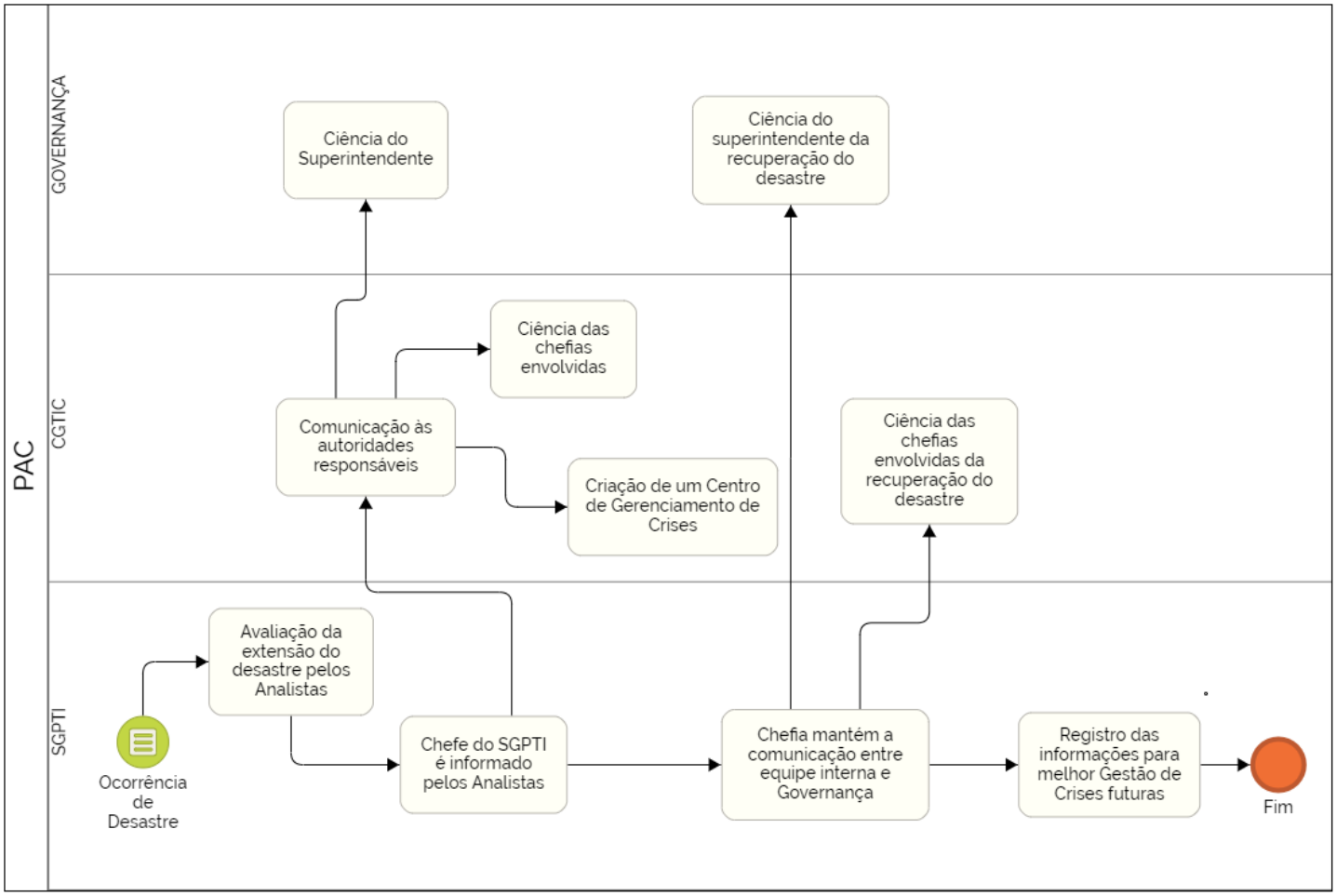


Figura 10 - Processo de Administração de Crises

4.6 ENCERRAMENTO DO PLANO DE ADMINISTRAÇÃO DE CRISES

O plano será encerrado assim que o funcionamento de sistemas essenciais do Container estiver normalizado. A equipe responsável pelo retorno deve emitir um parecer relatando as atividades realizadas para o chefe do SGPTI, que por sua vez deve informar do retorno das atividades à instituição.

4.7 ENCERRAMENTO DO PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter a Chefia do SGPTI entrará em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

Compor relatório com relação das atividades necessárias após a ocorrência dos desastres como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

5. PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para reestabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

5.1 OBJETIVO E ESCOPO

Este documento determina o plano para que, uma vez controlada a contingência e passada a crise, a organização retorne aos seus níveis normais de operação.

Além de avaliar possíveis vulnerabilidades dos componentes que suportam os processos de negócios críticos ao se deparar com eventos. Cabe executar um mapeamento e planejamento de sua recuperação ou restauração, sempre considerando as necessidades do Humap-UFMS. No PRD devem ser detalhados os planos de ações relativos a sites alternativos, visando à continuidade dos negócios da organização.

O escopo deste documento se restringe a última etapa da recuperação de desastres. Visa garantir o retorno a normalidade das operações e não mais sua recorrência no caso de riscos

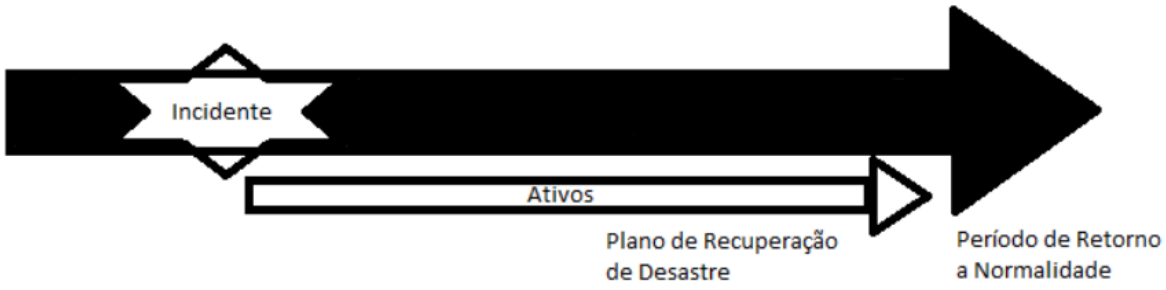


Figura 11 - Tempo PRD

controláveis.

5.2 ATORES ENVOLVIDOS

- EQUIPE DE INFRAESTRUTURA;
- SUBCOMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SGSIC);
- EQUIPE DE TRATAMENTO DE INCIDENTES EM REDE DE COMPUTADORES (ETIR/HUMAP);
- EQUIPE DE SISTEMAS E AGHU.

5.3 ATIVIDADES ENVOLVIDAS

Algumas atividades são essenciais durante o processo de recuperação de um desastre, sendo elas listadas nos tópicos abaixo.

5.3.1 Identificar ativos danificados

As equipes de INSTALAÇÃO/BACKUP/SERVIDORES/REDE deverão identificar e listar todos os ativos danificados da ocorrência do desastre. As informações de cada ativo encontram-se no MAPA GERENCIADOR DE CONFIGURAÇÕES/GLPI.

5.3.2 Identificar acessos interrompidos

A EQUIPE DE REDE E COMUNICAÇÕES deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, rede WAN ou com o provedor de serviços.

5.3.3 Listar Serviços Descontinuados

A equipe do PRD deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento da Chefia do SGPTI. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, *firewall*, *storage*, *routers* e switches, bem como respectivas configurações de *firewall*, DNS, rotas, *vlans* etc.

5.3.4 Elaborar Cronograma de Recuperação

O líder do PRD após o mapeamento das perdas e impactos elaborará um breve cronograma

de recuperação das aplicações levando em consideração:

- A priorização dos serviços essenciais, ou de acordo com determinação de nível institucional.
- O RTO definido para cada serviço essencial.
- A força de trabalho disponível.

5.3.5 Substituição de ativos e equipamentos

Em caso de perda de ativos, deverá ser imediatamente informado ao chefe do SGPTI a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. O SGPTI irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço comunicando ao

COMITÊ DE GOVERNANÇA DE TIC se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.

A equipe de INSTALAÇÕES deve verificar quais ativos foram danificados estão cobertos por garantia e se poderá ser acionada neste caso através da lista de fornecedores.

As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC

5.3.6 Reconfiguração de ativos e equipamentos

A equipe de INFRAESTRUTURA deverá verificar que as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos informando à chefia do SGPTI.

5.3.7 Teste de ambiente

O ambiente principal do datacenter antes do *recovery* dos dados do backup deverá ser testado a fim de garantir que o processo de recuperação ocorra conforme o planejado.

5.3.8 Recuperar dados do backup

Proceder a recuperação dos dados para as aplicações, seja do *storage* ou de arquivos de

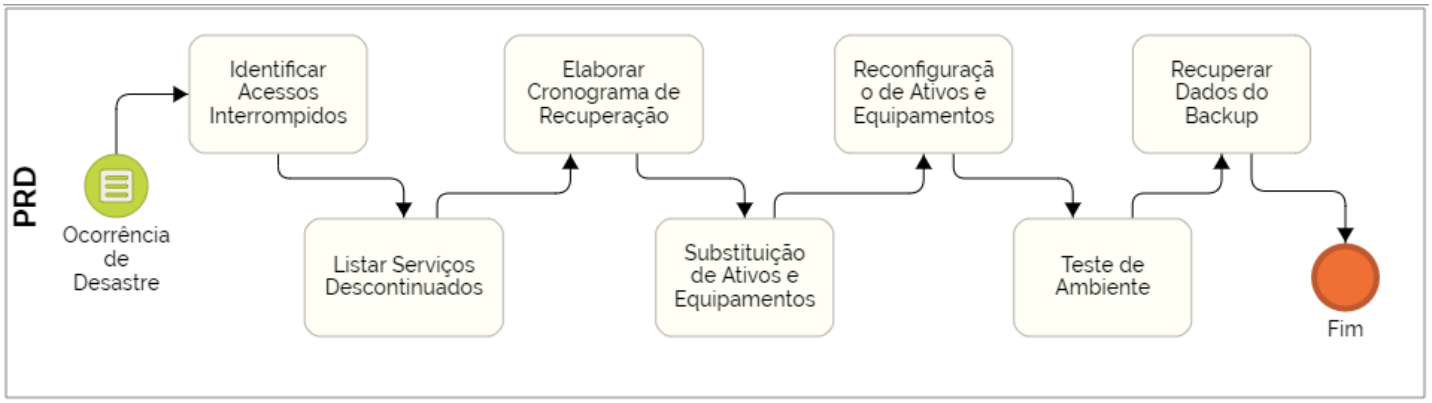


Figura 12 - Processo de Recuperação ou Restauração

backup.

5.4 ENCERRAMENTO DO PRD

Ao término do procedimento de recovery, as informações da recuperação de serviços serão consolidadas em parecer específico informando horário de reestabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

6. PLANO DE CONTINGÊNCIA EM PERÍODO DE AMEAÇA BIOLÓGICA

Em resposta à emergência nacional do surto de epidemia biológica, o Setor de Gestão de Processos e Tecnologia da Informação deve preparar a atividades administrativas para realizar conexões remotas prolongada no trabalho. Durante essas circunstâncias em rápida mudança, algumas situações extremas deverão ser adotadas.

6.1 OBJETIVO E ESCOPO

Serão mantidos os objetivos do PLANO DE ADMINISTRAÇÃO DE CRISES.

6.2 ÁREA

O PCTIC será avaliado e acionado no âmbito do Setor de Gestão de Processos e Tecnologia da Informação do Humap-UFMS tendo sua manutenção, organização e melhoria revistas e atualizadas periodicamente pelo Comitê de Governança de Tecnologia da Informação e Comunicações do Humap-UFMS.

Área de abrangência:

SUPERINTENDÊNCIA
SETOR JURÍDICO
SETOR DE GESTÃO DE PROCESSOS E TECNOLOGIA DA INFORMAÇÃO
Unidade De Apoio Corporativo
Ouvidoria
Unidade De Planejamento
Unidade De Comunicação

GERÊNCIA DE ATENÇÃO À SAÚDE
Divisão de Gestão do Cuidado
Divisão Médica
Divisão de Enfermagem
SETOR MATERNO INFANTIL
Unidade De Cabeça E Pescoço
Unidade De Especialidades Clínicas
Unidade De Cuidados Intensivos E Semi Intensivos

Unidade De Clínica Cirúrgica
Unidade De Cuidados Intensivos E Semi intensivos Pediátricos
Unidade De Urgência E Emergência
Unidade De Hematologia, Oncologia E Radioterapia
Unidade De Clínica Médica
Unidade Do Sistema Musculoesquelético
Unidade De Doenças Infecciosas E Parasitarias.
Unidade Do Sistema Urinário
Unidade De Atenção À Saúde Da Criança E Do Adolescente
Unidade Do Sistema Cardiovascular
Unidade De Atenção Psicossocial
Unidade De Enfermagem Assistencial
Divisão De Apoio Diagnóstico E Terapêutico
SETOR DE APOIO DIAGNÓSTICO E TERAPÊUTICO
Unidade Laboratório De Anatomia Patológica
Unidade De Reabilitação
Unidade De Nutrição Clínica
Unidade Laboratório De Análises Clínicas
Unidade De Diagnóstico Por Imagem E Métodos Gráficos
Unidade De Cirurgia/RPA/CMF
SETOR DE FARMACIA HOSPITALAR
Unidade De Abastecimento.
Unidade De Farmácia Clinica E Dispensação.
SETOR DE VIGILANCIA EM SAUDE
SETOR DE REGULAÇÃO E AVALIAÇÃO EM SAÚDE
Unidade De Regulação Assistencial
Unidade De Processamento De Informação Assistencial
Unidade De Monitoramento E Avaliação

GERÊNCIA DE ENSINO E PESQUISA

Unidade de Web Saúde
SETOR DE GESTÃO DA PESQUISA E INOVAÇÃO TECNOLÓGICA
SETOR DE GESTÃO DO ENSINO
Unidade de Gerenciamento de Atividades de Graduação e Ensino Técnico
Unidade de Gerenciamento de Atividades de Pós Graduação

GERÊNCIA ADMINISTRATIVA
Divisão Administrativa Financeira
SETOR DE ORÇAMENTO E FINANÇAS
Unidade De Programação Orçamentária E Financeira
Unidade De Pagamento Da Despesa
Unidade De Liquidação Da Despesa
SETOR DE AVALIAÇÃO E CONTROLADORIA
UNIDADE DE CONTABILIDADE FISCAL
UNIDADE DE CONTABILIDADE DE CUSTOS
SETOR DE ADMINISTRAÇÃO
Unidade De Compras
Unidade De Contratos
Unidade De Apoio Operacional
Unidade De Patrimônio
Unidade De Licitações
Divisão De Gestão De Pessoas
Divisão De Logística E Infraestrutura Hospitalar
SETOR DE ENGENHARIA CLÍNICA
SETOR DE INFRAESTRUTURA FÍSICA
SETOR DE HOTELARIA HOSPITALAR
SETOR DE SUPRIMENTOS
Unidade De Produtos Para Saúde
Unidade De Almoxarifado

6.3 EXECUÇÃO DO PLANO

Os portões do SGPTI manter-se-ão trancados e os contatos deverão ser, preferencialmente, por sistema de chamados ou pelo telefone (67)3345-3350.

Em caso de urgência o telefone (67) 3345-3123 (chefia SGPTI) estará ativo por 24h.

Será ativada a conexão VPN 1196 e 1197 no firewall do Humap-UFMS para que os colaboradores do Humap possam realizar o teletrabalho.

Empregados e terceirizados que sejam do grupo de colaboradores vulneráveis previstas no Artigo 6º da Instrução Normativa 02, de 26 de março de 2020 deverão realizar suas atividades remotas através de suas residências com exceção da Chefia do SGPTI.

Fica a critério do Superintendente autorizar o Teletrabalho aos demais colaboradores, devendo obrigatoriamente a presença no local de trabalho de pelo menos 2 técnicos em regime de escala de revezamento a ser definido pela chefia do SGPTI.

As reuniões presencias estão restritas àquelas as quais os assuntos sejam estritamente necessários. Devendo ser utilizadas alternativas de teleconferência ou videoconferência quando possível através dos aplicativos do office 365 (Skype for *Bussiness* ou Microsoft Teams).

Estarão suspensas as participações de servidores em treinamentos presenciais, congressos e eventos, a trabalho, pelo período que durarem as ameaças.

Fica temporariamente suspenso o acesso de colaboradores do SGPTI aos diversos Setores/Unidades do Humap-UFMS. Novas instalações de cabeamento e computadores não serão realizadas.

Os colaboradores do SGPTI realizarão atendimentos por meio de softwares remotos e apenas realizarão atendimentos locais em caso de extrema urgência determinados pelo Superintendente e/ou chefe do SGPTI e com devidos equipamentos de proteção individual como luvas, óculos e máscaras.

Em caso de indisponibilidade de algum serviço, o colaborador responsável tentará sanar o problema remotamente e caso não obtenha êxito, deverá retornar ao Humap-UFMS em até 2h.

Caso haja problemas em alguma impressora, será redirecionada para outra mais próxima, caso não houver, será enviada uma de backup. O chefe do SGPTI, será responsável em prover os tonners e fotocondutores para não haver interrupção na impressão.

Toda troca de ativos e equipamentos deverão ser relatados para não haver descontrole dos equipamentos.

6.4 ENCERRAMENTO DO PLANO

Ao término da ameaça biológica, os colaboradores deverão retornar aos seus locais de trabalho.

As VPNs 1196 e 1197 serão desativadas.

A equipe de INFRAESTRUTURA deverá realizar todos os testes de serviços e conectividade e prover a manutenção de todos ativos substituídos.

A equipe de HARDWARE E OPERAÇÕES deverá manutenir todos equipamentos substituídos e aqueles que não forem possíveis, deverão ser informados ao chefe do SGPTI.

7. RESULTADOS ESPERADOS

Visa atender a necessidade de continuidade do negócio. Por haver uma diversidade de processos de negócios existentes no Humap, foram divididos em subplanos, de acordo com os aspectos estratégicos do negócio do Humap.

Espera manter os serviços de TIC disponíveis em 99% ao ano, isto é, com indisponibilidades toleráveis conforme o quadro abaixo:

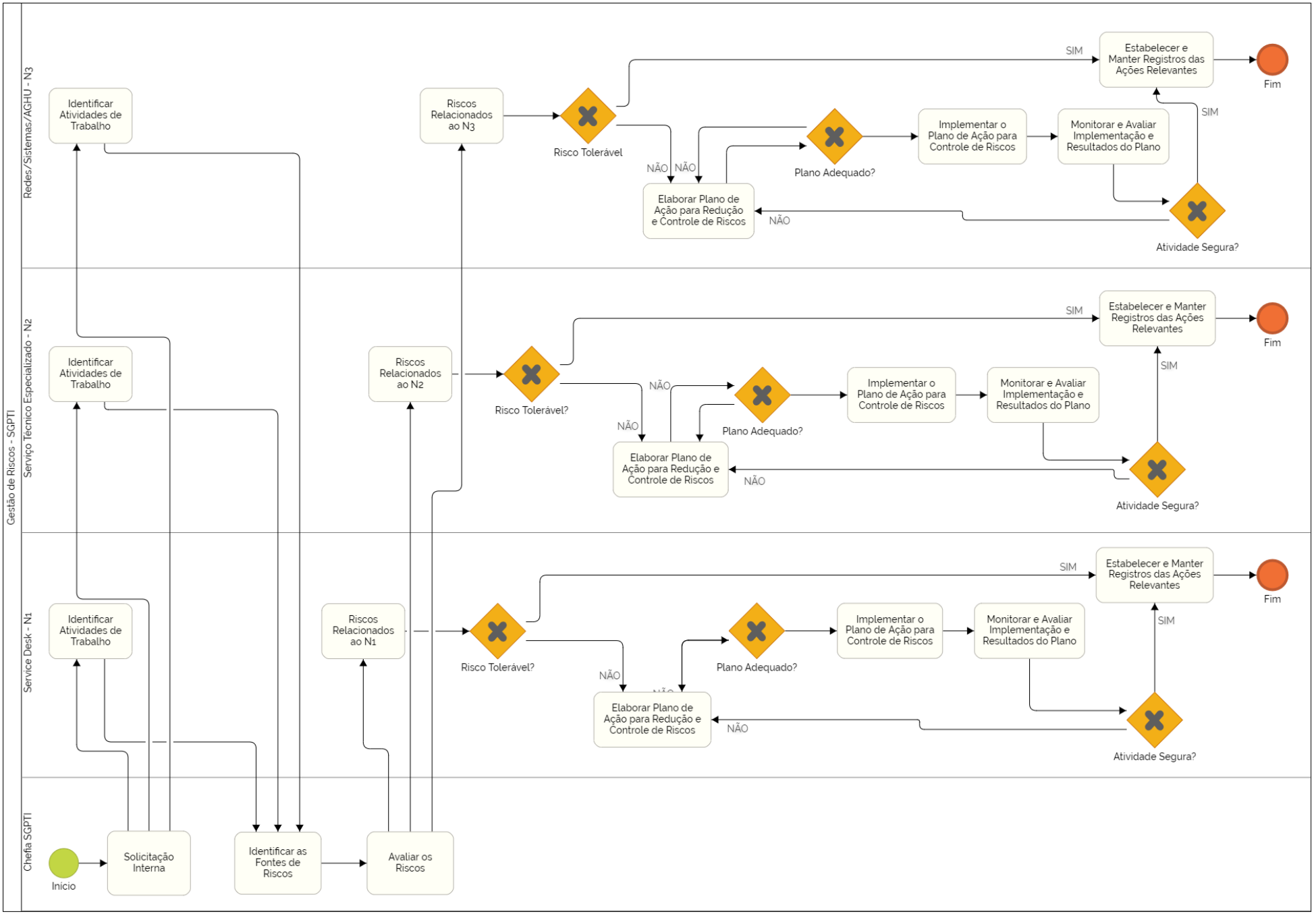
Disponibilidade (%)	***Downtime*/ano**	***Downtime*/mês**
99%	3 dias 15h36min	0 dias 7h12min

8. HISTÓRICO DE REVISÃO

VERSÃO	DATA	DESCRIÇÃO DA ALTERAÇÃO
1	13/05/2020	

Elaboração/Revisão **Nome:** Christian Pacheco **Função:** Chefe SGPTI **Nome:** Geyson Santana **Função:** Analista Telecom	Data: 12/05/2020
Análise **Nome:** Edeilson Silva Crz **Função:** Analista de TI - processo	Data: 17/03/2021
Validação **Nome:** Comissão Permanente de Gestão de Documentos **Função:** Portaria n°26 de 22 de janeiro de 2021	Data:
Aprovação (Nome, Função, Assinatura) **Nome:** Colegiado Executivo **Função:** **Assinatura:**	Data:

ANEXO I


Gestão de Riscos - SGPTI
Redes/Sistemas/AGHU - N3
Serviço Técnico Especializado - N2
Service Desk - N1
Chefia SGPTI
Início
Solicitação Interna
Identificar Atividades de Trabalho
Identificar as Fontes de Riscos
Avaliar os Riscos
Riscos Relacionados ao N3
Riscos Relacionados ao N2
Riscos Relacionados ao N1
Risco Tolerável?
Plano Adequado?
Implementar o Plano de Ação para Controle de Riscos
Monitorar e Avaliar Implementação e Resultados do Plano
Elaborar Plano de Ação para Redução e Controle de Riscos
Atividade Segura?
Estabelecer e Manter Registros das Ações Relevantes
SIM
NÃO
Fim

ANEXO II

Gestão de Risco - Escopo, Contexto e Critérios (SGPTI)			
Escopo		**Contexto**	**Critérios de Risco**
Nível Operacional	Infraestrutura de Redes	Interno	**Tangíveis:** erros de configuração, falta de componentes de reposição; **Intangíveis:** falha elétrica, falha de hardware; **Fatores positivos:** não há; **Fatores negativos:** indisponibilidade de serviços, responsabilização do setor, incapacidade de solução rápida.
	Sistemas	Interno e Externo	**Tangíveis:** erros de configuração, versão com erros, tecnologia obsoleta; **Intangíveis:** falta de código fonte, falha irrecuperável sem backup; **Fatores positivos:** não há; **Fatores negativos:** indisponibilidade de sistemas, responsabilização do setor, incapacidade de solução rápida.
	AGHU	Interno e Externo	**Tangíveis:** erros de configuração, falta de componentes de reposição; **Intangíveis:** falha elétrica, falha de hardware, erros de versão da sede; **Fatores positivos:** administração central na EBSERH SEDE; **Fatores negativos:** indisponibilidade de serviços, responsabilização do setor, incapacidade de solução rápida, dependência de resolução pela EBSERH SEDE.
	Segurança da Informação	Interno e Externo	**Tangíveis:** vazamento de dados internamente, acesso a dados sensíveis sem permissão; **Intangíveis:** vazamento de dados fora do Humap-UFMS; **Fatores positivos:** capacidade de melhoria dos processos internos relacionados à segurança de dados; **Fatores negativos:** má reputação do Humap-UFMS na mídia, judicialização de processos.
	Serviço Técnico ao Usuário	Interno e Externo	**Tangíveis:** erros de configuração, falta de componentes de reposição; **Intangíveis:** falha elétrica, falha de hardware, perda de dados de usuários; **Fatores positivos:** não há; **Fatores negativos:** responsabilização do setor, impacto no trabalho do usuário, perda de dados impactando no setor.

Nível de Projeto	Circuito Fechado de TV	Interno e Externo	**Tangíveis:** necessidade de instalação de novas câmeras após conclusão do projeto, inviabilidade pelo alto preço; **Intangíveis:** atraso na entrega pela empresa contratada; **Fatores positivos:** aumento da segurança do ambiente de trabalho, inibição de furtos e condutas duvidosas; **Fatores negativos:** áreas descobertas, responsabilização do setor.
	Telefonia	Interno e Externo	**Tangíveis:** atraso na entrega do serviço, descumprimento de cláusulas contratuais; **Intangíveis:** falha elétrica, falha de hardware, indisponibilidade por falha externa; **Fatores positivos:** não há; **Fatores negativos:** indisponibilidade do serviço de telefonia, responsabilização do setor, incapacidade de solução rápida.
	Impressoras/Etiquetas	Interno e Externo	**Tangíveis:** erros de configuração, falta de componentes de reposição, erros de programação; **Intangíveis:** falha elétrica, falha de hardware; **Fatores positivos:** gerenciamento do contrato pela EBSERH SEDE; **Fatores negativos:** indisponibilidade de impressão, responsabilização do setor, incapacidade de solução rápida.
Nível de Atividades	Mudança de Servidores	Interno	**Tangíveis:** erros de configuração, não instalação de componentes necessários; **Intangíveis:** falha elétrica durante migração, falha de hardware, falha de software; **Fatores positivos:** maior estabilidade após migração; **Fatores negativos:** indisponibilidade de serviços, responsabilização do setor, incapacidade de solução rápida, ambiente novo e desconhecido.

	Alteração em Ativos de Rede	Interno	**Tangíveis:** erros de configuração; **Intangíveis:** falha elétrica, falha de hardware; **Fatores positivos:** melhoria na performance da rede; **Fatores negativos:** indisponibilidade de serviços, responsabilização do setor, incapacidade de solução rápida.
	Atualização de Sistema Operacional de Servidor	Interno	**Tangíveis:** erros na micração, problemas de incompatibilidade de versão; **Intangíveis:** falha elétrica durante atualização, falha de hardware; **Fatores positivos:** Melhoria de performance, maior segurança dos dados; **Fatores negativos:** indisponibilidade de serviços, responsabilização do setor, incapacidade de solução rápida.
	Permissão de Acesso a Pastas e Sistemas	Externo	**Tangíveis:** permissão indevida a usuário; **Intangíveis:** mudança de chefia e alteração de permissão não informada ao SGPTI; **Fatores positivos:** não há; **Fatores negativos:** acessos indevidos após troca de chefia, responsabilização do setor.
	Atualização do AGHU	Interno e Externo	**Tangíveis:** erros críticos de verão; **Intangíveis:** falha elétrica local durante atualização, falha de hardware; **Fatores positivos:** melhorias no sistema; **Fatores negativos:** indisponibilidade de serviços, responsabilização do setor, incapacidade de solução rápida por depender da EBSERH SEDE.
	Reinstalação do Sistema Operacional de Estação	Externo	**Tangíveis:** erros de configuração, perca de arquivos críticos de usuários; **Fatores positivos:** melhoria da performance do computador; **Fatores negativos:** indisponibilidade de uso local, responsabilização do setor.

ANEXO III

NR	EVENTO DE DESASTRE	POSSÍVEIS CAUSAS	IMPACTO	PROBABILIDADE	NÍVEL DE RISCO
1	**Interrupção de energia elétrica**	Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 12 horas. Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuito, incêndio e infiltrações. Impossibilidade de acionar o Grupo Moto-gerador no momento de uma queda de energia.	Muito Relevante	Baixa	Elevado
2	**Falha Climatização do Container Data Center**	Superaquecimento dos ativos devido a falha no dimensionamento de carga no Container	Catastrófico	Baixa	Elevado
3	**Indisponibilidade de rede/circuitos**	Rompimento de fibra ótica decorrente de execução obras públicas, desastres ou acidentes.	Relevante	Baixa	Médio
4	**Falha humana**	Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível.	Relevante	Muito Baixa	Médio
5	**Ataques internos (funcionários insatisfeitos)**	Ataque aos ativos do DataCenter.	Pouco Relevante	Muito Baixa	Baixo

6	**Incêndio**	Incêndio ou princípio de incêndio que pode afetar uma área ou várias áreas do Humap-UFMS e causar danos aos equipamentos.	Catastrófico	Médio	Extremo
7	**Desastres Naturais**	Chuvas torrenciais, raios, ventania ou qualquer eventual dano ocorrido por fatores naturais.	Muito Relevante	Baixa	Elevado
8	**Falha de hardware**	Falha que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo licitatório	Relevante	Média	Elevado
9	**Falha de software**	Falha em alguma atualização, crash de banco de dados, super alocação de memória, aumento descontrolado de logs provocando falta de espaço em disco etc	Pouco Relevante	Baixa	Médio
10	**Ataque cibernético**.	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais	Muito Relevante	Média	Elevado
11	**Acesso Não Autorizado**	Acesso de pessoas não autorizadas aos sistemas por não terem esse acesso ou não fazerem mais parte da instituição	Relevante	Baixa	Médio