Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria

PLANO DE GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

1. INTRODUÇÃO

Segundo *Information Technology Infrastructure Library* (ITIL®) a disponibilidade de Tecnologia da Informação (TI) é um aspecto crítico da garantia do serviço, cujo propósito é permitir que os processos organizacionais realizados pela empresa possam ser executados de forma rápida, eficiente e sem impactos. Este aspecto refere-se a oferta de infraestrutura adequada e confiável de TI para atender e garantir o desempenho das operações e atividades essenciais para qualquer organização (OGC, 2007).

Neste contexto, desastres podem acontecer de diversas formas e a qualquer momento. Portanto é importante que a instituição esteja preparada para sanar as consequência e problemas relacionados aos incidentes e crises.

Uma das formas de preparação para a ocorrência de sinistros envolvendo Tecnologia da Informação é a realização da gestão de continuidade de serviços de TI. Esta atividade envolve a investigação, diagnóstico, planejamento, implementação, monitoramento e controle de procedimentos visando a recuperação de serviços essenciais na ocorrência uma interrupção grave na prestação dos serviços de TI.

A cada interrupção de um serviço de TI, existe uma série de consequências, tais como: falta de atendimento ao usuário, perda de dados, descumprimentos de prazos, entre outros pontos que podem prejudicar o Instituto Federal de Educação do Tocantins (IFTO). Uma gestão de continuidade de serviços de TI eficiente auxilia a organização a planejar, implementar e melhorar suas ações de contingência e recuperação.

Para o COBIT (ISACA, 2012), framework de governança de TI, o gerenciamento de continuidade é responsável por assegurar o mínimo de impacto no negócio de um evento que possa interromper (parcial ou totalmente) um ou mais serviços. Dentro deste panorama, para que a gestão de continuidade de serviços de TI seja efetiva, deve ser criar e manter um plano de gestão de continuidade atualizado, através de constante análise de risco em conjunto com o gerenciamento da disponibilidade e segurança.

Um plano de gestão de continuidade de serviços de TI é um documento formado por um conjunto de estratégias preventivas aliadas a planos de ação que visam a manutenção dos serviços considerados essenciais para a instituição durante uma eventual crise. Este documento contém diretrizes e premissas básicas a serem cumpridas durante eventos de crise, incluindo a parada dos principais serviços essenciais para o IFTO.

Este documento documento detalhada as ameaças que podem causar incidentes, bem como os recursos necessários para a continuidade dos serviços de TI. Ao buscar a gestão de continuidade de serviços essenciais, a área de TI do IFTO cria planos de ação complementares para administração de crise, continuidade operacional e recuperação de desastres que garantem a instituição a disponibilidade de seus sistemas e recursos de TI.

O plano de continuidade de serviços de TI será administrado, avaliado e acionado no âmbito da Diretoria de Tecnologia da Informação, tendo sua manutenção, organização e melhoria revistas e atualizadas anualmente. Este documento visa reduzir o risco e minimizar o impacto de interrupções dos serviços de TI procurando assegurar processos e procedimentos para que os sistemas e serviços operem em nível de contingência, durante a ocorrência de incidentes, até que a situação se normalize.

1.1. Escopo

Este documento define um conjunto de estratégias de proteção (contingência, continuidade e recuperação) necessárias à continuidade do serviços essenciais disponibilizados pela área de TI.

1.2. **Objetivo**

O objetivo geral do plano de gestão de continuidade dos serviços de TI é traçar estratégias e planos de ação complementares que possibilitam o funcionamento e a disponibilidade dos serviços essenciais envolvendo TI no IFTO durante as mais diversas situações de falha.

1.3. **Abrangência**

O plano de gestão de continuidade de serviços de tecnologia da informação do IFTO abrange 4 (quatro) planos de ação complementares. São eles: plano de administração de crises, continuidade operacional, recuperação de desastres e testes e verificação. Estes planos de ação devem permitir a recuperação, contingência e continuidade dos serviços de TI durante a ocorrência de incidentes.

1.4. **Vigência**

O plano de gestão de continuidade de serviços de TI do IFTO tem vigência de 5 (cinco) anos após a data de sua publicação. O documento será revisto anualmente e poderá ser atualizado de acordo com a necessidade.

2. **GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO**

A gestão de continuidade de serviços de TI (GCSTI) é responsável por gerenciar a capacidade da organização em continuar a fornecer níveis de serviços de TI predeterminados e acordados para suportar os requisitos mínimos do negócio, após uma interrupção. Este processo inclui assegurar a sobrevivência do negócio reduzindo o impacto do desastre ou falha grave, reduz a vulnerabilidade e o risco para o negócio por meio de uma análise de riscos eficaz e um gerenciamento de riscos, previne a perda de segurança para o cliente e usuário, e produz planos integrados de recuperação para TI. A GCSTI compreende atividades, tais como:

a) Avaliar o custo/benefício de se ter uma gestão de continuidade de negócios;

b) Avaliar o estrago que isto pode causar na imagem da instituição diante de seus clientes;

c) Avaliar riscos (quais eventos podem prejudicar a entrega dos serviços de TI);

d) Identificar serviços mais críticos e fundamentais para a operação do negócio;

e) Planejar a implementação;

f) Desenvolver planos de recuperação;

g) Definir e realizar testes;

h) Definir e realizar auditorias;

i) Promover o alinhamento da GCSTI ao gerenciamento de mudanças, garantindo que alterações no ambiente de produção, sejam devidamente avaliadas, e se necessário, refletir no plano de gerenciamento de continuidade dos serviços de TI.

Diante do exposto, a gestão de continuidade de serviços de TI deve garantir que a infraestrutura técnica e de serviços de TI não seja interrompida em um período longo. Para a execução do processo de gestão de continuidade de serviços de TI do IFTO em caso de incidentes ou desastres será necessário realizar as seguintes atividades:

a) Após um desastre, fazer a avaliação do risco e impacto da perda dos serviços de TI;

b) Fazer a definição de tempo de restauração dos serviços;

Identificar serviços primordiais para o negócio para provimento de medidas de prevenção adicionais;

c) Fazer a definição de qual abordagem será tomada para a restauração dos serviços;

d) Tomar medidas para prevenir e reduzir os efeitos do impacto de um desastre;

e) Criar, manter e testar um plano de recuperação que seja bem detalhado para restaurar os serviços, no período definido, após um desastre.

As próximas seções detalham o artefato PGCSTI, construído a partir da execução do processo de gestão de continuidade de serviços de TI. Também apresenta práticas recomendadas para a melhoria contínua da gestão de continuidade de serviços de TI.

2.1. Processo de gestão de continuidade de serviços de Tecnologia da Informação

O processo de continuidade de serviços de TI tem por finalidade suportar o processo de gerenciamento da continuidade do negócio com a garantia de que a infraestrutura técnica e de serviços de TI sejam recuperados dentro do prazo especificado e acordado com a área de negócio. Para exemplificar, os serviços a serem garantidos por este processo tem-se: sistemas, aplicações, redes de computadores, telecomunicações, banco de dados, sistemas de informação, suporte e central de serviços.

A figura 1 apresenta o processo de gestão de continuidade de serviços de TI do IFTO com seus 5 (cinco) estágios. São eles: iniciação, requerimentos e estratégias, implantação, operação e invocação.

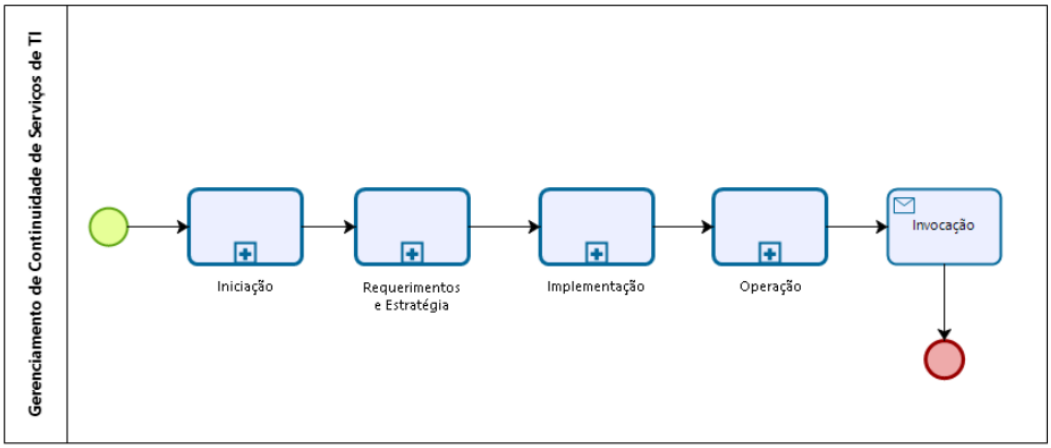


Figura 1 - Processo de Gerenciamento de Continuidade de Serviços de TI

As fases do processo de gerenciamento de continuidade de serviços de TI, apresentadas na figura 1 estão detalhadas na tabela 1 com os respectivos responsáveis pela execução. Este processo é baseado no ITIL (OGC, 2007).

Tabela 1 - Processo de Gerenciamento de Continuidade de Serviços de TI

Estágio	Atividades	Responsável
Iniciação	- Definir normas. - Especificar escopo. - Alocar recursos. - Definir Estrutura Organizacional.	Alta Gestão
Requerimentos e Estratégia	- Analisar impacto. - Analisar riscos. - Definir a estratégia de continuidade de serviço de TI.	Diretoria de Tecnologia da Informação
Implementação	- Desenvolver o Plano de Continuidade de Serviço de TI. - Desenvolver planos complementares (administração de crise, continuidade operacional, incidentes, recuperação de desastres e testes e validação). - Planejar a organização. - Testar o Plano de Continuidade de Serviço de TI.	Equipe de TI
Operação	- Educar, conscientizar e treinar. - Revisar o Plano de Continuidade de Serviço de TI. - Gerenciar mudanças no Plano de Continuidade de Serviço de TI.	Equipe de TI

Invocação	- Critérios de identificação de desastres. - Convocar Equipe de Gerenciamento de Crises.	Diretoria de Tecnologia da Informação

Fonte: Diretoria de Tecnologia da Informação (IFTO).

O processo de gestão de continuidade de serviços de TI apresentado na tabela 1 representa e descreve todas as atividades necessárias para elaborar, manter e ativar o plano de gestão de continuidade de serviços de TI. Este processo documenta as estratégias de recuperação de desastre e continuidade dos serviços de TI que devem ser adotadas pela área de TI do IFTO.

3. ANÁLISE DE CENÁRIO

Para que o plano de gestão de continuidade de serviços de TI obtenha êxito em sua execução deve ser realizada análise contínua do cenário atual em que se encontra a área de Tecnologia da Informação do IFTO. Esta análise considera as perspectivas organização, processo, pessoas, comunicação e tecnologia.

3.1. Cenário atual

Atualmente o parque tecnológico do IFTO tem apenas um site principal, localizado no prédio da Reitoria. Os sistemas e aplicativos essenciais estão armazenados neste site. Além desse prédio está em processo de análise de viabilidade técnica a contratação de serviço de infraestrutura em nuvem para disponibilização dos serviços críticos e essenciais para o IFTO. Até o presente momento o IFTO dispõe dos seguintes ativos em seu inventário tecnológico:

a) 1 Sala de Datacenter;

b) 2 links de comunicação de dados;

c) 2 servidores de grande porte;

d) 1 storage de grande porte;

e) 6 sistemas de informação;

f) 150 impressoras (outsoucing de impressão);

g) 2.000 computadores;

h) 2.500 usuários;

i) 1 grupo gerador;

j) 2 *nobreaks* de grande porte.

Com base no inventário tecnológico existente atualmente no IFTO, a Diretoria de Tecnologia da Informação fez a análise do cenário utilizando a ferramenta "Matriz SWOT". A tabela 2 apresenta o resultado obtido.

Tabela 2 - Matriz SWOT

AMBIENTE INTERNO	
FORÇAS (Pontos Fortes)	**FRAQUEZAS (Pontos Fracos)**
1. Bom nível de formação acadêmica e profissional de sua força de trabalho, aliada a experiência diversificada da equipe. 2. Apoio da alta gestão. 3. Infraestrutura tecnológica.	1. Deficiência na infraestrutura de cabeamento estruturado. 2. Estabilização da energia elétrica. 6. Processos não documentados. 7. Nível inicial de maturidade em governança de TI. 11. Indefinição de orçamento anual exclusivo para TI. 12. Falta de plano de capacitação continuada em continuidade de negócios. 13. Falta de equipamento para espelhamento de dados. 14. Falta de equipamento para redundância de dados.

	15. Inexistência de infraestrutura em nuvem para contingência.
AMBIENTE EXTERNO	
OPORTUNIDADES	**AMEAÇAS**
1. Parceria com a RNP (Capacitações/Serviços). 2. Captação de recursos externos. 3. Possibilidade de cooperação com outros órgãos públicos para uso e aperfeiçoamento de soluções de TI e compartilhamento de dados e sistemas. 4. Crescimento da quantidade demandada por cursos EAD propiciando investimentos em equipamentos, infraestrutura e qualificação dos servidores da área de TI. 5. Atualização tecnológica. 6. Emendas parlamentares.	1. Surgimento de demandas não programadas (intempestivas). 2. Alto número de modificações na legislação. 3. Instabilidade econômica e política. 4. Indefinição de recursos para investimento em TI. 5. Inexistência de orçamento anual exclusivo para TI. 6. Nível inicial de maturidade em governança e gestão de TI.

Fonte: Diretoria de Tecnologia da Informação

A partir da análise de cenário apresentada na tabela 2 e dados do levantamento de governança publicado pelo TCU é possível observar que o IFTO encontra-se atualmente no nível de maturidade inicial de seus processos de governança e gestão de TI. Com isso, a instituição enfrenta um grande desafio relacionado à continuidade dos serviços de TI.

Atualmente a infraestrutura tecnológica da instituição está em processo de atualização de equipamentos e softwares. Para que seja possível executar o PGCSTI além de investir em recursos tecnológicos é necessário manter atualizados seus sistemas de informação e o catálogo de serviços essenciais de TI como também a realização de capacitações técnicas.

3.1.1. Serviços Essenciais de TI

Para o desenvolvimento do PGCSTI são considerados como serviços essenciais de TI, aqueles críticos e que se interrompidos podem causar impacto considerável para o IFTO. Neste sentido, a área de TI do IFTO considerada como serviços essenciais a serem resguardados por este PGCSTI os seguintes serviços de TI:

a) DNS;

b) ForPDI;

c) Internet;

d) Moodle;

e) Portal Institucional;

f) Revista Eletrônica;

g) SEI: Sistema Eletrônico de Informações;

h) SIGA_EPCT: Sistema de Informações Gerenciais Acadêmica;

i) SI: Sistema Integrado;

j) Sistema de Submissão de Artigos Científicos;

k) Sistema do Processo Seletivo;

l) Sophia: Sistema de Bibliotecas;

m) SUAP: Sistema Unificado de Administração Pública.

4. ANÁLISE DE IMPACTO NO NEGÓCIO

A análise de impacto no negócio identifica os processos essenciais para o IFTO e dessa forma apresenta quais serviços de TI precisam voltar em funcionamento completo o

mais rápido possível, após a ocorrência de um incidente ou desastre. Dentro deste contexto, a análise de impacto no negócio realizada pela equipe de TI identifica os recursos necessários para retomar as operações de negócios em caso de ocorrência de incidentes ou desastres.

Esta análise leva em consideração os processos organizacionais considerados mais críticos para o IFTO. A tabela 3 apresenta os processos organizacionais que serão tratados no PGCSTI.

Tabela 3 - Processos Organizacionais críticos para o IFTO

Sistema	Área	Processo Organizacional	Criticidade
Sistema Unificado de Administração Pública (SUAP)	Gestão	- Gestão de Frotas. - Gestão de Patrimônio. - Gestão de Pessoas. - Central de Serviços.	Alta
	Pesquisa	- Gestão de Projetos de Pesquisa.	Alta
	Extensão	- Gestão de Projetos de Extensão.	Alta
SEI	Gestão	- Gestão de Processos. - Gestão de Documentos.	Alta
SIGA_EDU	Ensino	- Gestão de Estudantes. - Gestão de Cursos. - Gestão de Planos de Ensino. - Gestão de Matrículas. - Gestão de Estágios. - Diário de Classe. - Emissão de Documentos.	Alta
Processo Seletivo	Ensino	- Seleção de Estudantes	Alta
SOPHIA	Gestão	- Gestão de Bibliotecas.	Alta
Sistemas Internos	Gestão	- Gestão de Concursos. - Gestão de Eventos. - Gestão de Creche.	Alta
Moodle	Ensino	- Gestão de turmas EAD.	Alta
ForPDI	Gestão	- Gestão de Riscos.	Alta
	Gestão	- Gestão do Plano de Desenvolvimento Institucional.	Alta
Revista Eletrônica (Sítio Novo)	Pesquisa	- Gestão de submissão de artigos científicos.	Alta
Internet	Gestão	-	Alta
DNS	Gestão	-	Alta

Fonte: Diretoria de Tecnologia da Informação (IFTO)

Os serviços essenciais de TI que suportam e apoiam os processos organizacionais críticos do IFTO apresentados na tabela 3 poderão ser alterados e atualizados de acordo com o contexto interno e externo do IFTO. Para a construção do PGCSTI foi realizada a análise de impacto dos serviços de TI existentes no cenário do ano de 2021.

4.1. Avaliação de impacto dos serviços de TI

A partir da definição das atividades críticas que compõem os processos organizacionais que dependem do uso de Tecnologia da Informação foi definida a a criticidade e o impacto de uma interrupção ou desastre na prestação de serviços disponibilizados pela área de TI do IFTO. Inicialmente foram definidos como críticos os serviços apresentados na tabela 4. Esta tabela apresenta os tempos de recuperação e o tempo do backup que serão considerados nas estratégias de continuidade a serem executadas pelo planos de ação.

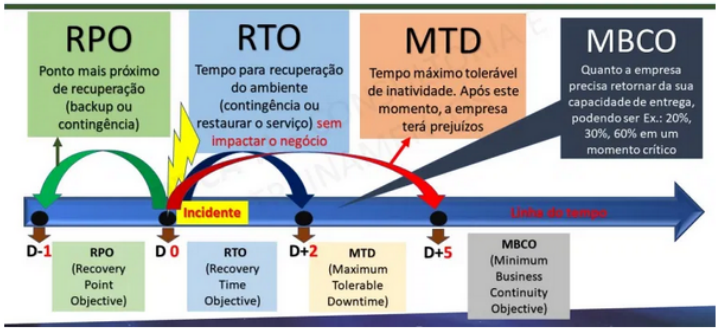
Tabela 4 - Serviços de TI

Recurso/ Serviço	Criticidade	RPO (Backup)	RTO (Restabelecer)	MTD (Tolerância)	Impacto			
					Financeiro	Legal	Imagem	Operacional
Internet	alta	-	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
DNS		24 horas		8 horas	Indefinido	Indefinido	Indefinido	

	alta		8 horas					Alto
ForPDI	média	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Médio
ForPDI	média	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Médio
E-mail	alta	-	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Moodle	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Portal	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Processo Seletivo	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Revista Eletrônica	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
SEI	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
SIGA	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
SI	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
SOPHIA	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
SUAP	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Submissão de Artigos Científicos	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto

Fonte: Diretoria de Tecnologia da Informação (IFTO)

Conforme demostrado na tabela 4 para a análise de impacto foram definidos tempos de tolerância a interrupções e pontos de recuperação das informações. O IFTO precisa retornar da sua capacidade de entrega dos serviços de TI em no mínimo 50% em um momento crítico. A figura 2 detalha as siglas apresentadas na tabela 4.



RPO (Recovery Point Objective)

Ponto Objetivado de Recuperação -> Ponto mais próximo de recuperação (backup ou contingência)

RTO (Recovery Time Objective)

Tempo Objetivado de Recuperação -> Tempo para recuperação do ambiente (contingência ou restaurar o serviço) sem impactar o negócio

MTD (Maximum Tolerable Downtime)

Máximo de Tempo Tolerável de Indisponibilidade -> Tempo máximo tolerável de inatividade. Após este momento, a empresa terá prejuízos

MBCO (Minimum Business Continuity Objective)

Objetivo Mínimo de Continuidade de Negócio -> Quanto a empresa precisa retornar da sua capacidade de entrega, podendo ser, 20%, 30% ou 60% em um momento crítico

Figura 2 - Conceitos sobre tempo de recuperação (PDCATI, 2020).

Os conceitos apresentados na figura 2 são fundamentais para a análise de impacto no negócio. A tabela 5 apresenta a prioridade de recuperação dos serviços de TI considerados essenciais para a área de TI do IFTO. Este resultado foi obtido por meio de análise de criticidade e dependência entre os serviços de TI. Esta priorização leva em consideração a importância de cada serviço para os processos de negócio do IFTO.

Tabela 5 - Priorização de serviços de TI e suas interdependências

Prioridade	Serviços/ Sistema	Criticidade	Interdependência
1	Internet	Alta	Link
2	VPN	Alta	Firewall
3	DNS	Alta	Internet
4	SEI	Alta	Internet DNS SUAP
5	Portal Institucional	Alta	Internet DNS
6	SUAP	Média	Internet DNS
7	SIGA_EDU	Alta	Internet DNS SUAP
8	Moodle	Alta	Internet DNS SIGA_EDU
9	Processo Seletivo	Alta	Internet DNS
10	Sistemas Integrados	Alta	Internet DNS SIGA_EDU SUAP
11	ForPDI	Alta	Internet DNS
12	Sophia	Alta	Internet DNS SIGA_EDU SUAP VPN
13	E-mail Institucional	Alta	Internet DNS
14	Revista Eletrônica	Alta	Internet DNS

Fonte: Diretoria de Tecnologia da Informação (IFTO).

A prioridade apresentada na tabela 5 leva em consideração o cenário do ano de 2021. Esta análise poderá ser alterada de acordo com o contexto o qual o IFTO se encontra.

5. ANÁLISE DE RISCOS

Riscos e ameaças afetam os serviços essenciais de TI e devem ser identificados, avaliados, tratados, monitorados, controlados e documentados, de forma a mitigar o impacto de sua ocorrência na continuidade de serviços de TI. A análise de riscos apresentada na tabela 6 detalha o risco, causa, consequência, probabilidade, impacto e controle a serem observados para garantir a continuidade de serviços de TI.

Tabela 6 - Análise de Riscos

Risco	Causa	Consequência	Probabilidade	Impacto	Controle
Incêndio.	-Ações humanas -Curto-circuitos -Queimadas	-Indisponibilidade de recursos, serviços e sistemas informatizados.	média	médio	-Sistemas de Profissionais de combate a incêndio para Data Center -Extintores. -Programas de capacitação contra incêndios.
Interrupção de	- Fator externo	-Indisponibilidade	média	alto	-Sistema de

energia elétrica.	com duração superior a 8 horas. - Falha Humana. - Fator externo (curto-circuitos, - incêndio e infiltrações. - Impossibilidade de acionar o grupo gerador	de recursos, serviços e sistemas informatizados. - Dano físico nos equipamentos.			Proteção de Energia.
Desastres Naturais.	-Vendavais. -Chuvas. -Tempestades atmosféricas. - Alagamentos. -Raios.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	média	médio	-Infraestrutura de serviços redundante em nuvem computacional terceirizada.
Ataques cibernéticos (ransomware, phishing, DNS cache poisoning, malware entre outros).	-Falha humana relacionada a configuração das regras de segurança dos Sistemas de detecção de intrusos HIDS/NIDS. -Desatualização de sistemas operacionais e softwares. -Vulnerabilidades ou erros de configuração em equipamentos, serviços e sistemas operacionais. - Falta de capacitações periódicas.	-Roubo de informações armazenadas em computadores, servidores ou outros dispositivos com a intenção de comprometer a privacidade ou obter/divulgar informações confidenciais. -Vazamento de informações críticas como senhas de sites com autenticação, como redes sociais, painéis administrativos, e-mails, etc. -Comprometimento da imagem institucional. Perda de dados. -Indisponibilidade de serviços, recursos e sistemas informatizados.	média	alto	-Atualizações periódicas do Sistema de Gestão de Segurança da Informação. - Plano de Capacitações periódicas.
Interrupção da comunicação com o provedor de internet.	-Quedas de link devido rompimento de fibra óptica decorrente de execução de obras públicas, desastres ou acidentes. -Queda de link em razão o mal funcionamento de componentes eletrônicos. -Configuração incorreta de roteador ou firewall.	- Parada na comunicação de dados entre servidores e serviços e sites externos ao IFTO. - Indisponibilidade de sistemas informatizados do IFTO.	média	médio	-Contratação de Link Backup.
Falha na restauração de backups.	- Erros de comunicação na rede. - Quedas ou oscilações de energia.	- Dados corrompidos. - Perda de dados. - Indisponibilidade de Backup. - Indisponibilidade de sistemas informatizados.	média	médio	- Monitoramento contínuo de estratégias de criação e restauração de backups.
Falha na climatização da sala de equipamentos.	- Variação de temperaturas na sala de	- Superaquecimentos dos ativos.	média	médio	-Sistema redundante de

	Equipamentos (Datacenter). - Defeitos em componentes eletrônicos dos aparelhos de ar condicionado.	- Danos pontuais aos equipamentos, podendo causar defeitos ao longo de tempo de vida do equipamento. -Queima de componentes. eletrônicos -Indisponibilidade recursos, serviços e sistemas informatizados.			climatização de salas.
Defasagem tecnológica.	-Evolução tecnológica muito rápida não compatível com processos públicos como licitações.	-Falhas na disponibilização de recursos, serviços e sistemas informatizados redundantes.	média	médio	-Plano Anual de Capacitações.
Ataques internos.	-Ausência de sistema de monitoramento de vulnerabilidades. -Ausência de mecanismos de proteção contra invasão. -Ausência de sistema de detecção de intrusão. -Ausência de norma sobre controle de acesso à rede. -Ausência de - Política de Segurança da Informação. -Dano ao Datacenter.	-Roubo ou perda de informações. Indisponibilidade recursos, serviços e sistemas informatizados.	alta	alto	- Gerenciamento de eventos e redundância de equipamentos de Firewall. - Equipe de tratamento de análise de risco e tratamento de incidente.
Indisponibilidade de pessoas chave para a segurança da informação.	-Ausência de capacitações na área de segurança da informação.	-Indisponibilidade de serviços, recursos e sistemas informatizados. -Perda de dados. -Roubo de informações.	alta	alto	-Plano Anual de Capacitações.
Falhas no acesso aos dados armazenados no banco de dados.	-Inexistência de conectividade de rede. -Falhas ou erros na configuração do serviço. - Comprometimento do sistema operacional. -Ataques internos e externos.	-Indisponibilidade de recursos, serviços e sistemas informatizados. -Perda de dados. -Roubo de informações.	alta	alto	-Estratégias de Restauração de Dados.
Falhas de conexão com a rede lógica de dados.	-Erros de configuração de ativos de rede. -Quedas ou oscilações de energia. -Queima ou falhas de componentes eletrônicos dos ativos de rede. -Falta de conhecimento	-Indisponibilidade de recursos, serviços e sistemas informatizados.	alta	alto	-Link redundante de Dados. -Configuração de alta disponibilidade com balanceamento de carga e *failover*.

	sobre cabeamento estruturado. -Ausência de capacitações em redes de comunicação de dados. -Falha humana.				
Falhas de validação de credenciais no sistema de autenticação do usuário.	-Falhas em componentes eletrônicos. -Falha humana.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	alta	alto	-Monitoramento periódico do sistema de autenticação de usuários. -Configuração de controladores de domínio adicionais.
Interrupções no acesso dos dados armazenados no *storage* de dados.	-Falhas na comunicação de dados. -Oscilações de energia elétrica. -Procedimento incorreto de acesso ao *storage*. -Procedimento incorreto de configuração do *storage*. - Falhas nos componentes eletrônicos (placa-mãe, controladora etc).	-Indisponibilidade de recursos, serviços e sistemas informatizados.	alta	alto	-Aquisição de *storage* redundante. -Definição de estratégias de criação e restauração de dados.
Falha Humana.	- Falta de conhecimento técnico. - Falta de capacitações continuadas.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	média	alto	-Curso de capacitação periódica.
Falha de Hardware.	-Queima de componentes eletrônicos.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	média	médio	-Aquisição de *hardware* redundante.
Indisponibilidade de Informação.	- Falha humana. - Erros de sistema. - Falhas em dispositivos de armazenamento. - Falhas na comunicação de dados.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	média	médio	-Estratégias automatizadas de criação e restauração de dados na infraestrutura em nuvem computacional.

Fonte: Diretoria de Tecnologia da Informação (IFTO).

Os riscos apresentados na tabela 6 poderão ser alterados e atualizados de acordo com o contexto interno e externo do IFTO. No período da revisão deste plano de gestão de continuidade de serviços de TI, os riscos e controles deverão ser atualizados de forma a refletir o atual cenário das instituições públicas brasileiras.

6. PAPÉIS E RESPONSABILIDADES

Para garantir a eficiência na execução do plano de gestão de continuidade de serviços de TI são definidos papéis e responsabilidades. Estas definições são fundamentais para a eficiência da continuidade de serviços de TI. São eles:

a) **Alta Gestão:** responsável pela decisão final sobre o escopo, política e diretrizes sobre a gestão de continuidade de serviços de TI. São responsabilidades deste papel no âmbito do PGCSTI:

I - Nomear o Comitê Gestor de Segurança da Informação.

II - Aprovar as diretrizes estratégicas que norteiam a elaboração do plano de gestão de continuidade de serviços de TI.

III - Garantir os recursos necessários para estabelecer, implementar, operar e manter o plano de gestão de continuidade de serviços de TI.

IV - Aprovar a estratégia de continuidade dos serviços de TI.

b) **Comitê Gestor de Tecnologia da Informação:** responsável pela avaliação e aprovação do PCSTI. Este comitê tem como responsabilidades no âmbito do PCSTI:

I - Avaliar e validar os planos de ação elaborados pelas áreas da DTI e definir os testes a serem realizados. Quando necessário, retornar avaliação a DTI, indicando os ajustes a serem realizados.

II - Avaliar a relação custo/benefício das estratégias de continuidade propostas e dos planos de ação que compõem o Sistema de Gestão da Continuidade de TI e decidir sobre sua implementação.

III - Aprovar e supervisionar o plano de gestão de continuidade de serviços de TI e seus planos de ação complementares, zelando por sua qualidade e efetividade.

c) **Comitê gestor de segurança da informação:** responsável por propor diretrizes estratégicas de segurança da informação para o PGCSTI.

I - Propor diretrizes estratégias de segurança da informação para o Plano de Continuidade de Serviços de TI.

II - Analisar e manifestar-se sobre a documentação de Continuidade de Serviços de TI, apoiando a alta gestão na avaliação do processo de continuidade de serviços de TI.

III - Avaliar o Plano de Tratamento de Riscos relacionados à continuidade de serviços de TI;

IV - Supervisionar a elaboração, implementação, testes e atualização dos planos de ação;

V - Propor melhorias na implantação de novos controles relativos ao Plano de Continuidade de Serviços de TI.

d) **Diretoria de Tecnologia da Informação:** responsável por documentar as estratégias de contingência e recuperação adotadas pela área de TI do IFTO dentro do PGCSTI.

I - Desenvolver a cultura de Gestão de Continuidade de Serviços de TI.

II - Deliberar as estratégias, as respostas aos incidentes de impactos críticos (elevados).

III - Definir estratégias para a comunicação às alçadas superiores da organização e às áreas afetadas, além de outros públicos estratégicos ou partes interessadas, durante todo o período de crise.

IV - Encaminhar os planos de ação às instâncias superiores, para avaliação e aprovação.

V - Supervisionar a elaboração, implementação, testes e atualização dos planos de ação que compõem o Plano de Continuidade de Serviços de TI.

VI - Zelar para que a estratégia de continuidade de TI do IFTO e para que os respectivos orçamentos sejam efetivamente cumpridos, bem como manter o comitê periodicamente informado do cumprimento das estratégias e dos orçamentos.

VII - Aprovar calendário anual de testes.

VIII - Comunicar, periodicamente, aos responsáveis pelos setores sobre o andamento da gestão de continuidade de TI e das necessidades de aprimoramentos identificadas.

IX - Comunicar à sociedade as ações de continuidade de Serviços de TI desenvolvidas pelo IFTO.

X - Orquestrar ações de suas coordenações durante eventuais disrrupções e suas consequências.

XI - Atuar como elo de ligação entre o corpo técnico e as áreas interessadas ou afetadas pela não Continuidade dos Serviços de TI.

XII - Propor acordos de nível de serviços que garantam o alinhamento das prestações de serviços de terceiros com as estratégias de continuidade de negócios das suas áreas.

XIII - Estabelecer níveis adequados de autoridade e competência, no intuito de assegurar a comunicação efetiva às partes interessadas, bem como assegurar a continuidade das atividades críticas.

XIV - Viabilizar a continuidade e a recuperação das atividades críticas, em caso de interrupção.

XV - Acompanhar e revisar o resultado dos testes realizados e recomendar aos responsáveis das áreas/processos, alguma reavaliação, além de comparar os resultados das análises em relação ao exercício anterior, avaliando se houve evolução na qualidade dos resultados para mitigar e reduzir os níveis de exposição de riscos.

e) **Equipe de crises:** representada pela equipe de TI formada por técnicos e analistas de TI, Esta equipe é responsável pela implantação e operação do PGCSTI.

I - Realizar, periodicamente, a análise de impacto nos negócios.

II - Identificar e documentar riscos que possam comprometer a continuidade das atividades críticas.

III - Identificar, documentar e avaliar os possíveis impactos à continuidade das atividades críticas, caso riscos se concretizem.

IV - Propor estratégias de continuidade de negócios adequada para proteger, estabilizar, continuar, retomar e recuperar as atividades prioritárias, bem como suas interdependências e recursos de apoio.

V - Documentar e publicar o processo de Continuidade de Serviços de TI.

VI - Elaborar os planos de ação previstos no Plano de Continuidade de Serviços de TI.

VII - Acompanhar o processo de implementação da estratégia de continuidade de TI, em função dos riscos operacionais envolvidos.

VIII - Realizar os testes e exercícios dos planos de ação de continuidade de TI.

IX - Aprimorar os planos a partir dos resultados dos testes e exercícios.

X - Administrar a contingência quando da interrupção de atividades, com base nos planos desenvolvidos.

XI - Propor os recursos necessários para a implantação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes e dos exercícios dos planos de ação.

XII - Fornecer, tempestivamente, todas as informações solicitadas à área ou responsável interno de gestão de continuidade de negócios.

XIII - Implementar os procedimentos adequados para minimizar os riscos de descontinuidade de acordo com a estratégia aprovada.

XIV - Realizar treinamentos e avaliações do plano de gestão de continuidade de serviços de TI periodicamente para garantir a manutenção e o bom funcionamento dos planos de continuidade.

f) **Equipe de redes e segurança da informação:** responsável pela configuração e manutenção da infraestrutura do PGCSTI.

I - Fornecer a infraestrutura de servidores físicos e virtuais necessários para que a TI execute suas operações e processos essenciais durante um desastre ou crise.

II - Prover mecanismos de segurança no ambiente principal e alternativo.

III - Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.

IV - 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.

V - Avaliar os danos específicos de qualquer infraestrutura de rede e para fornecer dados e conectividade de rede, incluindo WAN, LAN ou de infraestrutura externa junto aos prestadores de serviço.

g) **Equipe de Sistemas de Informação**: responsável pelo desenvolvimento, configuração e manutenção dos sistemas de informação que compõem os serviços essenciais descritos no PCSTI. São responsabilidades deste papel no âmbito do PCSTI:

I - Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre ou crise.

h) **Equipe de infraestrutura predial:** responsável pela manutenção e atualização da infraestrutura predial necessária para a execução do PGCSTI. São responsabilidades deste papel no âmbito do PGCSTI:

I - Garantir a climatização das salas de equipamentos de TI.

II - Garantir o funcionamento adequado do grupo gerador.

III - Garantir a estabilização da energia elétrica.

7. RECURSOS NECESSÁRIOS

Para que o plano de gestão de continuidade serviços de TI possa ser executado de forma eficiente são necessários diversos recursos. Para facilitar a compreensão os recursos foram categorizados em pessoas, sistemas de comunicação, infraestrutura tecnológica, redundância, energia, backups e locais de recuperação.

7.1. Pessoas

O IFTO deve disponibilizar recursos humanos capacitados minimamente em configuração de recursos, serviços, sistemas e segurança da informação. O profissional de TI alocado para a execução do PCSTI deve ter minimamente os seguintes conhecimentos:

a) Sistemas de proteção da informação;

b) Gerência de serviços, sistemas e redes;

c) Instalação, configuração e manutenção de sistemas operacionais;

d) Segurança da Informação envolvendo infraestrutura de redes, sistemas operacionais e aplicações web.

7.2. Sistemas de comunicação de dados

O sistema de comunicação de dados deve permitir que a instituição se comunique com as outras unidades e instituições públicas e privadas. Neste sentido, a Reitoria do IFTO deverá manter ativos dois links de saída para Internet.

a) Rede Nacional de Pesquisa (RNP): link de no mínimo 1 Gbps (link principal).

b) Prestadora de Serviços: link de no mínimo 100 Mbps (link backup).

Para a comunicação entre as unidades e a Reitoria do IFTO deverá ser configurada uma Rede Virtual Privada (VPN) de forma a permitir a troca de informações através de um canal de comunicação criptografado interno. Este canal de comunicação deverá ser utilizado apenas para serviços e recursos de TI disponibilizado entre as unidades.

7.3. Infraestrutura tecnológica

A infraestrutura tecnológica do IFTO deve possibilitar a restauração dos serviços de TI no menor tempo possível. Para isso, cada unidade deverá ter minimamente:

a) Sistema de incêndio nas salas de equipamentos;

b) *Nobreaks* de grande porte com baterias acopladas na sala de equipamento para estabilização de ativos de TI;

c) Servidores;

d) Sistema redudante de climatização de ambiente;

e) 1 link de comunicação de dados principal;

f) 1 link de comunicação de dados redundante;

g) Software para virtualização de servidores;

h) Software para automação de backups;

i) Software para gerencia de redes de computadores.

Além da infraestrutura tecnológica o IFTO deverá manter o seu sistema de gestão de segurança da informação atualizado de acordo com as normas vigentes. O IFTO deverá adotar minimamente as seguintes recomendações:

a) Os dados sensíveis de estudantes, servidores, terceirizados e informações institucionais devem ser armazenados em Datacenter cumprindo as normas sobre segurança da informação.

b) A prevenção contra ataques e vazamentos de informações deve ser respaldada por meio de:

I - Política de Segurança da Informação;

II - Normas complementares sobre segurança da informação;

III - LGBD;

IV - Firewall de Borda.

7.4. **Redundância de Dados**

O IFTO está em processo de análise de viabilidade técnica para a contratação de infraestrutura redundante de TI por meio de nuvem computacional privada. Dentro desta realidade a instituição deve contratar nos próximos anos uma empresa especializada em computação em nuvem de forma a possibilitar a alta disponibilidade e redundância de seus serviços de TI. Esta nuvem computacional deverá ter minimamente a seguinte infraestrutura redundante.

a) 2 Servidores de grande porte que possibilitem a criação de 10 máquinas virtuais com no mínimo 8 GB de RAM, 100 GB de disco contendo 2 processadores com 8 cores.

b) 1 Storage para armazenamento de dados com no mínimo 5 TB de espaço.

c) 1 Serviço de backup de dados contendo no mínimo 5 TB de espaço para armazenamento.

7.5. **Energia**

Atualmente, o IFTO tem instalado no prédio da Reitoria um grupo gerador que garante o fornecimento de energia estabilizada por até 2 (duas) horas após a interrupção de energia da concessionária. Além disso, conta com dois nobreaks de 6 KVA (APC) acoplados a um banco contendo 4 baterias que garantem autonomia de no mínimo 2 (duas) horas.

Para que o PGCSTI possa ser considerado eficiente faz-se necessário que os equipamentos de estabilização de energia estejam em pleno funcionamento a partir da realização de manutenções periódicas no grupo gerador e nobreaks.

7.6. **Backups**

O IFTO estabelece de forma automatizada estratégias de backups locais e em nuvem para garantir a segurança dos dados institucionais. Estas rotinas definem o tipo de backup a ser realizado (full, incremental e diferencial), periodicidade dos dados armazenados (hora, dia, mês e ano) e forma como estes serão armazenados.

Além das estratégias de backup já implantadas, devem ser estabelecidas brevemente novas rotinas automatizadas para a recuperação mensal de dados dos principais serviços de TI em infraestrutura em nuvem. Esta configuração permitirá que os serviços de TI sejam retomados o mais breve possível.

Para que os backup tenham condições de serem utilizado dentro do contexto do PGCSTI tem-se a necessidade de se ter infraestrutura para armazenamento de dados de no mínimo 5 TB.

7.7. Locais de Recuperação

Para a recuperação de seus recursos, serviços e sistemas informatizados o IFTO deverá utilizar infraestrutura em nuvem computacional a ser contratada brevemente. Esta estratégia está sendo estudada, analisando-se os riscos, investimentos e capacidade técnica para sua implantação.

8. ESTRATÉGIAS DE CONTINUIDADE DE SERVIÇOS DE TI

A área de TI do IFTO deverá adotar estratégias de continuidade de serviços de TI que possibilitem a recuperação total ou parcial. Estas ações deverão considerar as seguintes opções:

a) **Cold:** o IFTO deverá dispor de backups de dados dos principais serviços de TI. No caso de necessidade de reparação total, o serviço deverá ser reinstalado em outro servidor, seja ele do próprio do IFTO, locado ou cedido externamente. Este processo poderá demorar até uma semana para ser completado. No caso de reparação parcial, o processo de restauração pode levar até dois dias, dependendo do volume e tipo de dado a ser restaurado.

b) **Warm:** o IFTO deverá dispor dispor de backup dos dados e *snapshot* dos servidores envolvidos no serviço de TI. No caso de necessidade de reparação total, o serviço poderá ser reinstalado em outro servidor, seja ele do próprio IFTO, locado ou cedido externamente. Este processo poderá demorar até 72 horas para ser completado, pois no momento da falha deverá ser definido/contratado um servidor para suprir a demanda, além de realizada a restauração do snapshot e restauração dos dados do backup.

c) **Hot:** o IFTO deverá dispor de equipamento/espaço reservado próprio, locado ou cedido, onde serão feitas atualizações constantes do serviço e dados relacionados. No caso de necessidade de reparação total, poderá ser feita a restauração apenas das diferenças em relação ao último backup (se houver). Este processo poderá levar até 8 horas. No caso de necessidade de reparação parcial, o tempo para restauração previsto é de 4 horas.

d) **Mirrored:** o IFTO deverá dispor de equipamento idêntico ao em operação, que recebe atualizações de sistemas e dados em tempo real, de forma que, se o serviço é interrompido no IFTO, basta realizar o redirecionamento do mesmo para o espelhamento, que passará a operar em modo de produção. Após correção do problema, o espelhamento deverá ser restaurado, de forma que ambos voltam a estar compatíveis. Este processo não possui tempo de restauração, pois o espelhamento assume imediatamente as funções do serviço interrompido. É, entretanto, a alternativa mais custosa e de maior grau de manutenção. Este processo poderá levar 8 horas.

Além das estratégias mencionadas o IFTO deverá observar as seguintes boas práticas:

e) Distância mínima entre sites principal e backup de no mínimo de 15 km.

f) Configuração de site backup sem balanceamento de carga evitando assim ataques cibernéticos.

g) Plano de realização de testes de serviços de TI periódicos.

h) Atualização periódica do parque tecnológico.

i) Replicação de aspectos de segurança lógica e física no site backup.

j) Cronograma anual para avaliação periódica de serviços de TI que são essenciais para o IFTO.

As priorizações dos serviços mais críticos a serem contemplados no PGCSTI deverão ser realizadas com base no catálogo atual de serviços de TI, de forma que as estratégias de prevenção e recuperação possam ser adequadamente implantadas dentro dos principais serviços disponibilizados pela área de TI.

9. AÇÕES DE CONTINGÊNCIA/RECUPERAÇÃO

O IFTO deverá realizar ações para a contingência/recuperação de seus serviços de TI. De forma a facilitar a implementação destas ações de contingência/recuperação, a área de TI deverá minimamente realizar as seguintes atividades:

9.1. Mapeamento de serviços essenciais de TI

O mapeamento atualizado dos serviços considerados essenciais para o negócio é fundamental para a criação de estratégias de backup e contingência de dados. A Diretoria de Tecnologia da Informação deverá manter atualizado o catálogo de serviços de TI, bem como os acordos de níveis de serviço acordados com as áreas de negócio. Este mapeamento de serviços, que são essenciais para a execução dos processos organizacionais, deverá ser realizado pelo menos uma vez ao ano.

9.2. Estratégias de backup e recuperação de dados local e em nuvem computacional

O IFTO deverá manter cópias de todas as informações fundamentais relacionadas à prestação de serviços educacionais no site principal e site backup em um ambiente seguro, podendo ser “nuvem” ou outra unidade do IFTO. Toda informação eletrônica classificada como importante e crítica deverá ser backupeada diariamente e salva em meio eletrônico no ambiente de contingência. No mercado existem diversas soluções de backup. O IFTO deverá considerar as seguintes estratégias de backup e recuperação de dados:

a) **Solução de contorno manual:** solução de contorno temporária que requer intervenção manual, geralmente utilizada para minimizar o impacto no negócio, até que se tenha uma solução definitiva. É uma solução que utiliza um tempo alto para recuperação de dados.

b) **Backup ou contingência:** garante que os dados vitais do negócio estejam armazenados em outro local físico diferente do original. Atualmente os backups de alguns sistemas são realizados localmente e em nuvem.

c) **Acordo recíproco:** acordo entre duas empresas para compartilhar recursos similares durante uma emergência.

d) **Recuperação gradual:** também conhecida como *cold standby* (prontidão a frio). Inclui a provisão de recursos e componentes de TI para reposição e uso em caso de indisponibilidade dos recursos e componentes em operação. Esta opção não é recomendada para serviços que devam ser restaurados rapidamente. Se a necessidade de restauração for rápida ou imediata, é sugerido que seja utilizada outra opção de restauração de serviços com prazo de restauração menor. Esta opção é utilizada para *firewalls* e rede sem fio.

e) **Recuperação intermediária:** também conhecida como *warm standby* (prontidão a morno). Inclui a provisão dos recursos e componentes sobressalentes já planejados para tal, ou recursos e componentes fornecidos por provedores de serviços externos. Solução em estudo de viabilidade técnica.

f) **Recuperação rápida:** também conhecida como *hot standby* (prontidão a quente). Inclui a recuperação de recursos de maneira rápida como uma evolução da recuperação intermediária. Pode ser realizada através de recursos e componentes sobressalentes prontos para assumirem o serviço em caso de falha. Este procedimento pode demandar alguma configuração ou intervenção automática ou manual para assumir o serviço. Solução em estudo de viabilidade técnica.

g) **Recuperação imediata:** conhecida como “espelhamento”. Provê a recuperação imediata dos serviços através da duplicação de recursos e componentes de TI. Os serviços geralmente são configurados através de espelhamento (todos os espelhos são iguais e contém as mesmas características e dados) e atualizados através de balanceamento de carga (a utilização dos serviços é dividida entre os recursos dinamicamente ou por regra de uso). Os clientes não devem perceber a indisponibilidade. Ela somente é perceptível para TI. A recuperação imediata é utilizada para os serviços críticos do negócio, por serem de alto custo pela duplicação dos recursos e componentes de TI. Solução ideal para o IFTO. Entretanto possui alto custo operacional. Em razão do custo está em estudo de viabilidade técnica.

9.3. Infraestrutura de servidores e dados redundantes

O IFTO deverá manter infraestrutura de servidores e dados redundantes por meio de contratação de infraestrutura em nuvem computacional. Esta estratégia além de disponibilizar serviços críticos de TI deverá armazenar o backup dos dados considerados críticos para a instituição. A infraestrutura de servidores e dados redundantes deverá ser espelhada de forma a refletir a situação atual do IFTO em relação aos serviços de TI.

10. CONSCIENTIZAÇÃO E TREINAMENTO

O desenvolvimento da cultura de continuidade de serviços de TI no IFTO deverá ser suportado por programas de conscientização e treinamento. A conscientização, além de envolver todos os estudantes, servidores, terceirizados, fornecedores e outras partes interessadas, deverá ser contínua e feita através de informativos, apresentações, palestras, inclusão de informações no portal institucional além de ser tópico presente em reuniões administrativas.

Já o treinamento, por sua vez, deverá envolver uma quantidade menor de pessoas (equipe e servidores ligados à GCSTI). Esta atividade deverá abordar tópicos como a gestão do plano de continuidade de serviços de TI, execução da análise de impacto nos negócios e avaliação de riscos, desenvolvimento, implantação e testes e comunicação.

O programa de treinamento deverá contemplar os riscos, ameaças, controles, responsabilidades, premissas e as estratégias de continuidade de serviços de TI, incluindo as alterações recentes. As atividades contempladas neste programa deverão obedecer às seguintes diretrizes:

a) A área de TI deverá ser responsável por definir e conduzir o plano de treinamento sobre continuidade de serviços de TI;

b) O plano de treinamento deverá contemplar todas as áreas de TI envolvidas na disponibilização e manutenção dos Serviços de TI;

c) Os treinamentos deverão assegurar que coordenadores, servidores e prestadores de serviço sejam conscientizados dos riscos e ameaças que poderão gerar interrupção dos processos organizacionais, das consequências e da importância do estabelecimento de estratégias e dos planos de continuidade para os serviços de TI.

11. COMUNICAÇÃO

A comunicação é essencial para que o PGCSTI seja conhecido por todos os envolvidos na continuidade de serviços essenciais de TI. Para a realização da comunicação devem ser adotadas as seguintes práticas:

a) Sempre que houver evento que gere a indisponibilidade, mesmo que parcial, de serviço, deverão ser consolidadas as informações recebidas dos responsáveis pelos setores envolvidos e registrar em relatório específico, com remessa aos respectivos setores:

b) descrição do incidente;

c) causa da paralisação;

d) os aprimoramentos implementados ou a serem implementados, com os respectivos prazos, que objetivam minimizar novas ocorrências do gênero.

As dúvidas técnicas pertinentes deverão ser relacionadas antes de qualquer publicação. No caso de detalhamento técnico do problema à imprensa falada ou televisiva, a Diretoria de Tecnologia da Informação deverá ser assessora pela Diretoria de Comunicação do IFTO.

Qualquer servidor ao constatar alguma anormalidade que paralise quaisquer processos críticos do IFTO deve comunicar o fato ao seu superior imediato, e este por sua vez deve apresentar o fato ao responsável pela continuidade dos serviços de TI. Atualmente o IFTO possui os seguintes canais de comunicação para relato de incidentes envolvendo serviços de TI:

a) Portal institucional: portal.ifto.edu.br;

b) Central de Serviços: suap.ifto.edu.br;

c) E-mail institucional: dti@ifto.edu.br.

A Equipe de TI deve registrar toda e qualquer incidência que implique na ativação dos procedimentos de contingência descritos neste documento. O registro das reuniões deve ficar armazenado no setor de TI, contendo no mínimo as seguintes informações:

a) Descrição do incidente;

b) Data e hora (quando aplicável) do início da ocorrência;

c) Descrição das medidas adotadas;

d) Data e hora (quando aplicável) do restabelecimento das condições normais de trabalho;

e) Informações adicionais (eventualidades, estragos e afins).

Para que a comunicação ocorra de forma satisfatória o IFTO tem como autoridade responsável pela comunicação sobre o PGCSTI sua Diretoria de Tecnologia da Informação. A tabela 7 apresenta os dados de contato.

Tabela 7 - Contato

Setor	Telefone	E-mail
Diretoria de Tecnologia da Informação	63 3229-2212	dti@ifto.edu.br

Fonte: Diretoria de Tecnologia da Informação (IFTO)

12. MONITORAMENTO E CONTROLE

O monitoramento e controle da execução deste documento deverá ser realizado através de reuniões com a equipe de TI. Estas reuniões permitirão a manutenção, organização e melhoria do PGCSTI. O monitoramento e controle deverão ser realizados nas seguintes situações:

a) A cada ano quando da análise e validação das atividades e processos críticos do IFTO;

b) No momento em que a Diretoria de Tecnologia da Informação achar conveniente;

c) Em razão dos resultados obtidos nos testes e validação dos planos de ação que compõem o Plano de Continuidade de Serviços de TI;

d) Após a ocorrência de algum evento ou mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

13. TESTES

A Diretoria de Tecnologia da Informação deverá coordenar a realização de testes de segurança para garantir que os procedimentos previstos neste PGCSTI são viáveis e eficazes. Há vários tipos de testes que poderão ser executados. Dentre eles podem ser citados:

a) **Simulação:** conduzido assim que o plano de gestão de continuidade de serviço de TI for concluído, através de simulação dos procedimentos por todas as pessoas relevantes para a execução do plano, para avaliar o entendimento e a integração das atividades do plano.

b) **Teste total:** conduzido assim que o plano de gestão de continuidade de serviço de TI for concluído. Deve ser realizado de forma periódica. Deverá envolver as áreas de negócio para acompanhar e validar os testes de restauração dos serviços.

c) **Teste parcial:** não substitui a necessidade do teste total, mas pode ser realizado como complemento do teste total, em um espaço de tempo menor e em uma escala menor com somente alguns serviços ou componentes de TI.

d) **Teste de cenário:** simula condições específicas, eventos e cenários de risco.

Os testes a serem realizados pela equipe de TI deverão minimamente abordar:

a) Testes dos equipamentos operacionais, como softwares de gestão e controles instalados e hardwares compatíveis com as exigências operacionais dos softwares e redes, a cada 12 meses;

b) Testes para aferir bom funcionamento dos servidores a cada 12 meses;

c) Testes de segurança, integridade e acessibilidade dos dados capturados e arquivados pelo sistema de *backup* do procedimento de *restore* de backups (sistema de informações) a cada 12 meses;

d) Testes para apurar a eficácia e/ou eventual necessidade de atualização dos sistemas operacionais adotados (Windows, Linux, LibreOffice, antivírus etc.), conforme a necessidade;

e) Caminho percorrido para restaurar serviços de TI, ou seja assegurar que cada integrante do processo crítico se familiarize com o PGCSTI;

f) Simular uma situação real de interrupção por queda de energia, falha de comunicação de dados etc.

Ao final os testes deverá ser emitido relatório apresentando os resultados obtidos bem como a necessidade da implementação de melhorias nos procedimentos adotados, e caso necessário a incorporação de novas tecnologias disponíveis. A Diretoria de Tecnologia da Informação deverá guardar o relatório de testes para futuras análises.

14. ATIVAÇÃO E ENCERRAMENTO

O plano de gestão de continuidade de serviços de TI deverá ser administrado, avaliado, acionado e encerrado no âmbito da Diretoria de Tecnologia da Informação. A ativação do PGCSTI deverá ocorrer quando da ocorrência de algum dos cenários de desastres, a insurgência ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada.

O PGCSTI também poderá ser invocado em casos de testes ou por determinação do Comitê Gestor de TI, Comitê Gestor de Segurança da Informação ou Diretoria de Tecnologia da Informação. A ativação dependerá do cenário de crise enfrentado pelo IFTO.

O encerramento da execução do PGCSTI poderá ocorrer após a execução dos planos de ação que garantirão a continuidade dos Serviços de TI. Após o encerramento deste plano a Diretoria de Tecnologia da Informação deverá guardar informações históricas para futuras análises.

14.1. Matriz de acionamento do PGCSTI

A Diretoria de Tecnologia da Informação é o setor responsável por manter atualizada a matriz de acionamento do PGCSTI. Esta matriz está apresentada na tabela 8.

Tabela 8 - Matriz de Acionamento do PGCSTI

Responsável pela ativação do PCSTI?	Diretoria de Tecnologia da Informação.
Ambiente a ser contingenciado?	Datacenter Reitoria.
Qual o prazo de recuperação?	72 horas.
Ambiente de Contingência?	Infraestrutura em Nuvem Computacional.
Quando acionar o PCSTI?	Na ocorrência de incidentes de interrupção com potencial

	superior a 8 horas.
Quem executa o PCSTI?	- Equipe de TI. - Equipe de Infraestrutura Predial.
Qual o tempo de recuperação do ponto de informação (RPO)?	24 horas.

Fonte: Diretoria de Tecnologia da Informação

15. AUTORIDADE RESPONSÁVEL

A Diretoria de Tecnologia da Informação será responsável por acionar todos os contatos e partes interessadas na execução do PGCSTI. A comunicação prioritariamente deverá ser por telefone, ou pessoalmente, caso não seja possível o contato.

A Diretoria de Tecnologia da Informação deverá relatar à equipe de crise, o evento que ocasionou a interrupção do serviços de TI, bem como a data e o horário. A tabela 9 apresenta os dados de contato da autoridade responsável pelo PGCSTI.

Tabela 9 - Autoridade Responsável

Autoridade	E-mail	Telefone
Diretoria de Tecnologia da Informação	dti@ifto.edu.br	63 3229-2212

Fonte: Diretoria de Tecnologia da Informação (IFTO).

16. CONTATOS TÉCNICOS

A tabela 10 apresenta a lista de contatos dos principais atores envolvidos na solução do incidente ou desastre, na eventualidade de acionamento do plano de gestão de continuidade de serviços de TI. Estes contatos referem-se às áreas envolvidas na execução dos planos de ação que complementam o PGCSTI.

Tabela 10 - Contatos

Setor	E-mail	Telefone
Diretoria de Tecnologia da Informação	dti@ifto.edu.br	63 3229-2212
Coordenação de Governança de Tecnologia da Informação	governancati@ifto.edu.br	63 3229-2212
Coordenação de Sistemas de Informação	sistemas.reitoria@ifto.edu.br	63 3229-2212
Coordenação de Redes e Segurança da Informação	redes.reitoria@ifto.edu.br	63 3229-2212
Coordenação de Suporte e Manutenção	-	63 3229-2212
Diretoria de Infraestrutura	dinfra@ifto.edu.br	63 3229-2218

Fonte: Diretoria de Tecnologia da Informação (IFTO).

17. REVISÃO E ATUALIZAÇÃO

O plano de gestão de continuidade de serviços de TI deverá ser testado, revisado, avaliado e acionado no âmbito da Diretoria de Tecnologia da Informação. A manutenção, organização e melhoria das ações a serem implementadas pelas estratégias de continuidade deverão ser realizadas pelas Coordenações de Redes e Segurança da Informação, Coordenação de Manutenção e Suporte, Coordenação de Sistemas de Informação e Coordenação de Governança de TI.

Dentro deste contexto, os planos de ação que compõem o plano de gestão de continuidade de serviços de TI deverão ser atualizados e melhorados sempre que:

a) Detectar problemas e dificuldades reveladas durante o exercício;

b) Ocorrer rotatividade do pessoal interno e externo;

c) Desenvolvimento de procedimentos relacionados com a contingência e recuperação de dados;

d) Alterações das estratégias de backup;

e) Atualizações do sistema de proteção das informações;

f) Atualização dos lugares alternativos de operações;

g) Implantação de novos serviços de TI.

18. CRONOGRAMA DE EXECUÇÃO

Para a execução deste plano de gestão de continuidade de serviços de TI foram definidas as ações e prazos conforme apresenta a tabela 11. Os prazos previstos para a execução das ações apresentadas na tabela 11 levam em consideração as contratações de infraestrutura de nuvem computacional, equipamentos de rede e capacitação de servidores a serem adquiridos nos próximos anos.

Tabela 11 - Cronograma de Execução

Ação	Prazo
Iniciação	2020-2021
Requerimentos e Estratégia	2021
Implementação	2022
Operação	2023
Invocação	2024

19. REFERÊNCIAS

ABNT. NBR ISO 22301:2020. **Segurança e resiliência: sistema de continuidade de negócios (requisitos).**

ABNT. NBR ISO 22313:2020. **Segurança e resiliência: sistemas de gestão de continuidade de negócios (orientações para o uso da ABNT NBR ISO 22301)**.

ABNT. NBR ISO 22316:2020. **Segurança e resiliência: resiliência organizacional (princípios e atributos).**

ABNT. ISO/TS 22317:2020. **Segurança da sociedade: sistemas de gestão de continuidade de negócios (Diretrizes para análise de impacto nos negócios (BIA)).**

ABNT NBR ISO 22320:2020. **Segurança e resiliência: gestão de emergências (Diretrizes para gestão de incidentes).**

ABNT NBR ISO 22322:2020. **Segurança da sociedade: gestão de emergências (Diretrizes para aviso público).**

AXELOS. **Itil Service Design**. Axelos, 2011.

BRASIL. Gabinete de Segurança Institucional. **Instrução Normativa Nº 1, de 13 de junho de 2008. Gestão de Segurança da Informação e Comunicações na Administração Pública**

Federal, direta e indireta. Brasília-DF, 2008.

BRASIL. Departamento de Segurança da Informação e Comunicações / Gabinete de Segurança Institucional da Presidência da República. **Norma Complementar Nº 06, de 11 de novembro de 2009. Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações. Brasília-DF, 2009.** Disponível em: http://dsic.planalto.gov.br/legislacao/nc_6_gcn.pdf Acesso em: 4 de Nov. 2020.

IFTO. Diretoria de Tecnologia da Informação. **Política de Segurança da Informação do IFTO.** Palmas-TO, 2020.

IFTO. Diretoria de Tecnologia da Informação. **Plano de Gestão de Riscos para área de TI do IFTO.** Palmas-TO, 2020.

IFTO. Diretoria de Tecnologia da Informação. **Norma Complementar Gestão de Continuidade de Negócios para a área de TI.** Palmas-TO, 2020.

ISACA. **COBIT 5: A Business Framework for the Governance and Management of Enterprise IT**.USA, 2012

MANOEL, Sergio da Silva. **Sistema de Gestão de Continuidade de Negócios: esteja preparado para salvar a sua vida e os seus negócios de um incidente ou desastre. Tenha um plano "B" profissional.** Brasport, 2019.

Office of Government Commerce (OGC). ***ITIL v3 Service Strategies.*** Inglaterra: TSO 2007. Vol1.

Office of Government Commerce (OGC). ***ITIL v3 Service Design.*** Inglaterra: TSO 2007. Vol2.

Office of Government Commerce (OGC). ***ITIL v3 Service Transition.*** Inglaterra: TSO 2007. Vol3.

Office of Government Commerce (OGC). ***ITIL v3 Service Operation.*** Inglaterra: TSO 2007. Vol4.

Office of Government Commerce (OGC). **ITIL v3 Service Continual Service Improvement.** Inglaterra: TSO 2007. Vol5.

PDCATI. Estrutura do Sistema de Gestão de Continuidade de Negócios. (SGCN). Disponível em: https://www.pdcati.com.br/plano-de-continuidade-de-negocios/ Acesso em: 23 jan. 2020.

ANEXO I

PLANO DE ADMINISTRAÇÃO DE CRISES - (PAC)

1. INTRODUÇÃO

O Plano de Administração de Crises (PAC) especifica ações e responsabilidades para a comunicação entre equipes envolvidas com o acionamento da contingência antes, durante e após a ocorrência de uma interrupção ou desastre. Estas 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 de uma comunicação eficaz.

1.1. Escopo

O PAC compreende o tratamento de eventos definidos como crise relacionados com a disponibilidade dos Serviços de TI. Não inclui no escopo deste documento estabelecer os procedimentos operacionais de cada área ou procedimentos para tratamento e restauração dos ativos de informação em caso de crise, dado que estes documentos são estabelecidos e mantidos dentro das áreas responsáveis pelo tratamento da crise.

1.2. Objetivos

O escopo do PAC é estabelecer a estratégia básica e elencar os procedimentos e protocolos a serem adotados pela Diretoria de Tecnologia da Informação quando em situação de crise ou ameaça de crise. O objetivo geral deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos nas ações de contingência e recuperação, antes, durante e após a ocorrência de uma catástrofe. São objetivos específicos do PAC:

a) Garantir a segurança à vida das pessoas;

b) Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.

c) Orientar os funcionários e demais colaboradores com informações e procedimentos de conduta.

d) Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido.

1.3. Abrangência

O PAC abrange procedimentos e protocolos a serem executados, quando em situação de crise ou ameaça de crise. Este plano de ação envolve fatos que estão ocorrendo e por fim as ações futuras, que são delimitadas somente após a ocorrência de um evento.

2. ADMINISTRAÇÃO DE CRISE DE TI

Crise é o momento em que ocorre qualquer incidente que comprometa a operação normal da empresa. É uma situação caracterizada pela ocorrência de um evento ou série de eventos que culminam no rompimento significativo das operações normais, podendo gerar consequências graves à imagem do IFTO. Neste contexto, a administração de crises de TI no IFTO é estruturada em três níveis de atuação: Estratégico, Tático e Operacional.

e) **Nível Estratégico:** formado pelo Comitê Gestor de TI. Neste nível são deliberadas as decisões estratégicas do negócio, as respostas aos incidentes de impactos críticos, a comunicação às alçadas superiores da organização e todas as partes interessadas durante a crise.

f) **Nível Tático:** formado pelos líderes das equipes da Diretoria de Tecnologia da Informação, que atuam inicialmente na avaliação e resolução do incidente, que dependendo do tipo, podem convocar outras pessoas para identificação e tratamento do incidente. Neste nível decide-se pela ativação ou não do plano de gestão de continuidade de serviços de TI.

g) **Nível Operacional:** formado pelos analistas e técnicos de TI. Estes atores entram em ação quando é iniciado o plano de continuidade de serviços de TI e reportam o status da resolução do incidente para o nível tático.

O PAC utiliza o processo de gerenciamento de crises apresentado na figura 1. Este processo é composto por 4 (quatro) atividades.

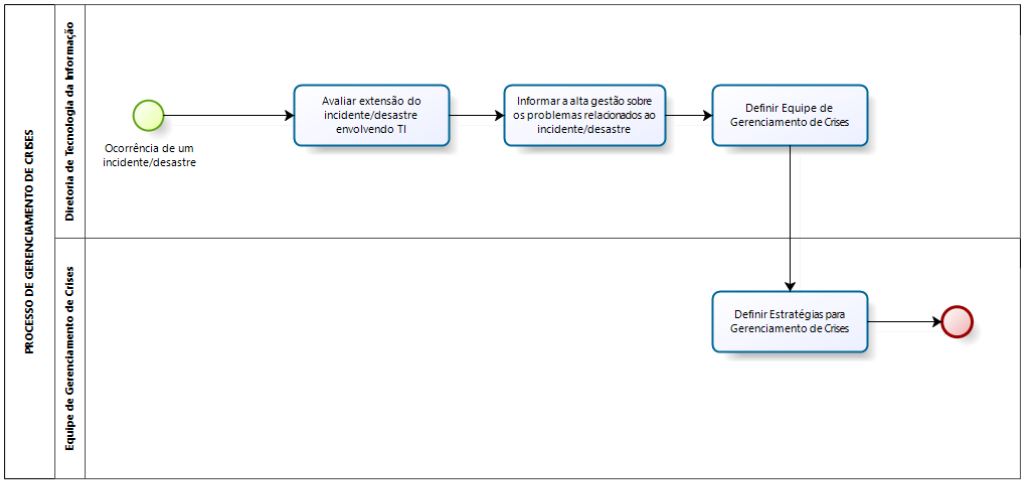


Figura 1 - Processo de gerenciamento de crises

A figura 1 apresenta as 4 (quatro) atividades que compõem o processo de gerenciamento de crises. São elas: avaliar a extensão do incidente/desastre envolvendo TI; informar a alta gestão sobre os problemas relacionados ao incidente/desastre; definir equipe de gerenciamento de crises; e definir estratégias para gerenciamento de crise.

2.1. Avaliar a extensão do incidente/desastre envolvendo a TI

A Diretoria de Tecnologia da Informação juntamente com sua equipe de TI deverão avaliar a extensão do incidente/desastre envolvendo a área de TI de forma a elaborar um PAC. Este documento deverá conter estratégias de contingência e recuperação de serviços de TI, bem como os procedimentos de comunicação da crise.

2.2. Informar a alta gestão sobre os problemas relacionados ao incidente/desastre

A Diretoria de Tecnologia da Informação deverá comunicar a alta gestão os problemas relacionados ao incidente/desastre. Este setor deverá emitir relatório contendo estratégias de contingência e recuperação do desastre.

2.3. Definir equipe de gerenciamento de crises

Para a resolução da crise a Diretoria de Tecnologia da Informação deverá escolher os servidores capacitados para resolução da crise. Esta equipe de gestão de crise deverá ser formada por técnicos e analistas de TI. Estes profissionais ficarão responsáveis pelas ações de recuperação imediata da infraestrutura tecnológica dos serviços de TI.

2.4. Definir estratégias para gerenciamento de crises

A Diretoria de Tecnologia da Informação conjuntamente com a equipe de TI deverão definir as estratégias de gerenciamento de crise. Estas estratégias deverão contemplar ações envolvendo procedimentos antes, durante e após a crise.

3. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades para a execução do Plano de Administração de Crises são:

a) Comitê Gestor de TI: responsável por atuar como elo de ligação entre a área de TI e as áreas interessadas ou afetadas pela não continuidade de serviços de TI.

b) Diretoria de Tecnologia da Informação: responsável por orquestrar ações de suas coordenações durante eventuais disrrupções e suas consequências.

c) Equipe de Tecnologia da Informação: responsável por realizar as ações previstas no PAC. Esta equipe é formada por analistas e técnicos de TI lotados na Diretoria de Tecnologia da Informação e servidores da Diretoria de Comunicação.

4. ATIVAÇÃO E ENCERRAMENTO DO PAC

A ativação e encerramento do PAC deverá ser feita pela Diretoria de Tecnologia da Informação. Este plano de ação deverá ser acionado nas seguintes situações:

a) Roubos, furtos, sabotagem, sequestros, vandalismo e crimes de qualquer natureza;

b) Queda de energia elétrica;

c) Perda, roubo ou vazamento de informações computacionais;

d) Incêndios, explosões, queda de edifícios ou sinistros de qualquer natureza;

e) Boicotes, greves;

f) Boatos, intrigas ou acusações desonestas e/ou antiéticos de concorrentes;

g) Crises de mídia eletrônica e/ou impressas;

h) Extravio de documentos eletrônicos;

i) Paralisações de setores em razão de indisponibilidade de serviços de TI;

j) Desastres naturais;

k) Doenças do tipo contágio/contaminação ou química;

l) Vazamento de documentos internos;

m) Falha de equipamentos eletrônicos de qualquer natureza.

n) Colapso em rede de computadores.

o) Outros imprevistos que afetem a continuidade dos negócios.

O PAC deverá ser encerrado assim que os procedimentos de administração de crises forem realizados/validados por todas as equipes. A equipe de gestão de crise deverá fornecer relatório com as informações de horário de restabelecimento dos serviços, especificando equipamentos que foram realocados, procedimentos de recuperação, fornecedores que tiveram de ser acionados, entre outras informações relevantes.

5. AUTORIDADE RESPONSÁVEL PELO PAC

A Diretoria de Tecnologia da Informação é a autoridade responsável por acionar e encerrar o PAC conjuntamente com suas coordenações de áreas de TI. A tabela 1 apresenta os dados de contato da autoridade responsável.

Tabela 1 - Autoridade Responsável

Autoridade	E-mail	Telefone
Diretoria de Tecnologia da Informação	dti@ifto.edu.br	63 3229-2212

Fonte: Diretoria de Tecnologia da Informação (IFTO).

6. ATIVIDADES, TAREFAS E AÇÕES DO PAC

Na ocorrência de uma crise, a equipe de gestão de crise deverá informar às autoridades responsáveis os motivos relacionados à crise e participar ativamente do processo de gestão a ser implementado para solucioná-la. O PAC é composto por várias atividades, são elas:

a) Atividades a serem realizadas antes da crise

As atividades a serem realizadas antes da ocorrência da crise estão detalhadas na tabela 2. Conforme pode ser verificado nesta tabela, cada atividade possui tarefas e um responsável por sua execução.

Tabela 2 - Atividades e tarefas para preparação para administração de crises

Atividade	Tarefa	Responsável
1. Avaliar e aprovar ações a serem tomadas para solução da crise.	1. Analisar as estratégias de administração de crise. 2. Aprovar as estratégias de administração de crises.	Comitê Gestor de TI.
2. Definir um local para a administração de crises.	1. Escolher o local para a administração de crises e possíveis entrevistas.	Diretoria de Tecnologia da Informação.
3. Definir papéis e responsabilidades.	1. Definir o Porta-Voz para a crise (escolher o membro com melhor habilidade para comunicar sobre crises envolvendo a área de TI). 2. Definir os servidores responsáveis pelo gerenciamento da crise, suas funções e atribuições.	
4. Planejar a comunicação sobre crises.	1. Definir os meios de comunicação para informar sobre os desdobramentos da crise.	
5. Identificar a crise e seus riscos.	1. Mapear e avaliar processos identificando os pontos que podem desencadear uma crise. 2. Identificar potenciais crises com seus riscos, probabilidade e impacto (matriz de riscos).	Equipe de Tecnologia da Informação
6. Analisar o impacto da crise.	1. Avaliar o impacto segundo os critérios de imagem, reputação, conformidade. 2. Avaliação das crises mais prováveis.	
7. Monitorar cenários pré-crise.	1. Identificar cenários possíveis de crises. 2. Definir projeção de cenários favoráveis ao desencadeamento de uma crise e do cenário da situação de crise, propriamente dita. 3. Avaliar ações para controle dos cenários.	
8. Planejar tratamento de crises (Plano de Ação).	1.Desenvolver um plano de contingência especificando seus possíveis desdobramentos, as ações padrão a serem adotadas e as áreas a serem acionadas em cada situação. 2.Definir procedimentos necessários para administração de crises. 3.Preparar documentos com informações necessárias em casos de crise.	

Fonte: Diretoria de Tecnologia da Informação (IFTO)

Conforme apresenta a tabela 2, na ocorrência de um desastre será necessário entrar em contato com diversas áreas, principalmente as afetadas para informá-las de seu efeito na continuidade dos serviços e tempo de recuperação. A Diretoria de Tecnologia da Informação será responsável por contatar estas unidades e repassar as informações pertinentes a cada grupo, setor ou segmento.

b) Atividades a serem realizadas durante a crise

Durante uma crise envolvendo a indisponibilidade de serviços de TI, a Diretoria de Tecnologia da Informação deve entrar em contato com as áreas afetadas para informá-las sobre o efeito na continuidade dos serviços de TI e tempo de recuperação. A tabela 3 apresenta as principais atividades a serem realizadas.

Tabela 3 - Atividades para realização durante a crise

Atividade	Responsável
1. Encaminhar comunicado aos membros do Comitê Gestor de Segurança da Informação sobre o incidente ocorrido. 2. Informar as áreas afetas sobre a crise ocorrida. 3. Redigir um release sobre o assunto, esclarecendo as condições da ocorrência e reforçando os aspectos favoráveis das medidas adotadas, bem como a idoneidade da instituição.	Diretoria de Tecnologia da Informação
4. Identificar o problema que ocasionou a crise.	Equipe de Tecnologia da Informação
5. Coletar o máximo de informações e provas possíveis.	
6. Identificar o problema. 7. Registrar o motivo por que ocorreu. 8. Registrar quando ocorreu o problema. 9. Registrar as consequências em curto e médio prazos. 10. Registrar quem são os responsáveis pelo ocorrido. 11. Registrar se houve outras ocorrências. 12. Registrar quem está envolvido na apuração da ocorrência. 13. Registrar as medidas que já foram tomadas.	

Fonte: Diretoria de Tecnologia da Informação (IFTO)

c) Atividades a serem realizadas após a crise

Após reunião com o Comitê de Segurança da Informação, o Porta-Voz da crise deverá elaborar um breve relatório de crise para informar as partes envolvidas e afetadas de modo a manter todos bem informados e passar a todos a perspectiva dos esforços necessários para o restabelecimento dos serviços inativos. A Equipe de TI deverá atualizar todas as informações sobre a crise. A tabela 4 apresenta as atividades a serem realizadas após a crise.

Tabela 4 - Atividades após a crise

Atividades	Responsável
1. Relatório de crise.	Diretoria de Tecnologia da Informação
2. Atualizar o manual de gestão de crises.	Equipe de Tecnologia da Informação
3. Atualizar o plano de administração de crises.	
4. Registro a solução para a crise no inventário de crises.	

Fonte: Diretoria de Tecnologia da Informação (IFTO)

d) Enfrentamento de crises

A Diretoria de Tecnologia da Informação deverá adotar como estratégia para enfrentamento de crises, a transparência e o planejamento de suas ações de acordo com a urgência e prioridade da crise.

e) Avaliação de crises

Após a crise, a Diretoria de Tecnologia da Informação juntamente com a equipe de TI deverá realizar a análise detalhada das ações e das estratégias implementadas, o que inclui o desempenho das ações realizadas para a solução da crise. Este setor deverá mensurar o impacto da crise na imagem do IFTO e a percepção dos públicos e da opinião pública. Além disso, deverá avaliar a necessidade de ações complementares de comunicação para reverter um possível cenário desfavorável.

f) Monitoramento de crises

A Diretoria de Tecnologia da Informação deverá monitorar a crise e acompanhar a sua repercussão nos meios de comunicação, buscando agir com proatividade e agilidade, atendendo às demandas da sociedade, sobretudo prestando esclarecimentos, quando necessário, e permitindo a veiculação da posição oficial do setor de TI do IFTO.

Uma vez validado o funcionamento do retorno dos sistemas essenciais de TI e estabilidade do Datacenter, a Diretoria de Tecnologia da Informação deverá entrar em contato com as partes interessadas no restabelecimento do serviço de TI, provendo as informações de retorno das operações e as informações de status dos serviços de TI.

7. COMUNICAÇÃO

A comunicação do PAC será feita pela Diretoria de Tecnologia da Informação e será realizada por meio de e-mails, SEI e do Portal Institucional, quando for o caso. Este setor deverá emitir relatório apresentando como a crise foi solucionada.

8. RECURSOS NECESSÁRIOS

Para a administração de crises deverá ser utilizado como ferramenta eletrônica de monitoramento e controle o e-mail institucional de forma a documentar todas as ações realizadas. Além deste recurso poderão ser utilizados o sistema de informação SEI e o Portal Institucional.

9. LOCAL PARA ADMINISTRAÇÃO DE CRISES

A administração da crise deverá ser realizada através de ferramenta eletrônica de comunicação disponibilizada pelo IFTO. A administração de crise deverá ser gerenciada a partir de salas de conferência, utilizando ferramentas como por exemplo: conferenciaweb, hangout, meet, e google drive.

ANEXO II

PLANO DE CONTINUIDADE OPERACIONAL - (PCO)

1.INTRODUÇÃO

O Plano de Continuidade Operacional (PCO) descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais disponibilizados pela área de TI do IFTO. Este plano é responsável por manter as funções mínimas da instituição durante os impactos causados pela eventual crise, como por exemplo a descontinuidade da conexão com a Internet. Ele é implementado, mantido, melhorado e documentado pela Diretoria de Tecnologia da Informação.

1.1. Escopo

É escopo do PCO 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. Não faz parte do escopo definir os procedimentos técnicos a serem executados para garantir a continuidade dos serviços de TI.

1.2. Objetivos

O objetivo principal do PCO é garantir a continuidade dos serviços essenciais de TI críticos na ocorrência de um desastre, enquanto recupera-se o ambiente principal. O PCO é fortemente orientado aos processos (sistemas) e serviços. Os objetivos específicos do PCO são:

a) Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações de TI, dos sistemas essenciais;

b) Estabelecer atividades, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre;

c) Definir os formulários, *checklists* e relatórios a serem entregues pelas equipes envolvidas na executar a contingência.

1.3. Abrangência

O PCO abrange ações para a continuidade operacional dos serviços de TI. Este documento aborda estratégias a serem realizadas pela equipe de TI e Diretoria de Tecnologia da Informação.

2. CONTINUIDADE OPERACIONAL

A continuidade operacional refere-se à capacidade que uma empresa tem de manter seus equipamentos e sistemas funcionando normalmente mesmo diante de um evento crítico, como um desastre. A figura 1 apresenta as atividades que compõem o processo de gerenciamento de continuidade operacional.

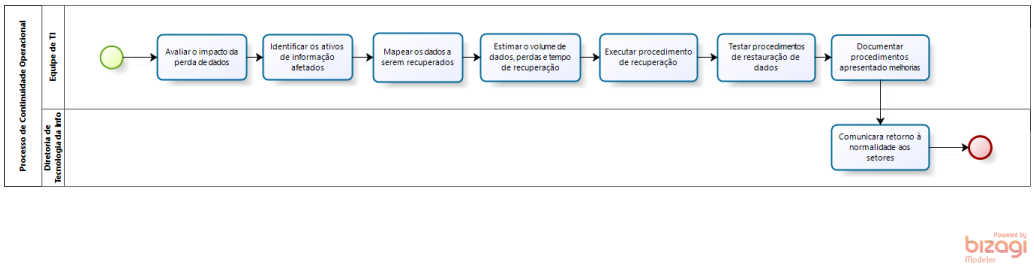


Figura 1 - Processo de Continuidade Operacional.

Conforme demonstra a figura 1 o processo de continuidade operacional é composto por 7 (sete) atividades. São elas: avaliar o impacto da perda de dados; identificar os ativos de informação afetados; mapear os dados a serem recuperados; estimar o volume de dados, perdas e tempo de recuperação; executar procedimento de recuperação; testar procedimentos de restauração de dados; documentar procedimentos apresentando melhorias e comunicar o retorno à normalidade aos setores.

2.1. Avaliar o impacto da perda de dados

A equipe de TI juntamente com a Diretoria de Tecnologia da Informação deverão identificar a ocorrência do incidente ou crise e verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorridos. Após a avaliação deverá ser registrado o impacto por meio de um relatório de perda de dados.

2.2. Identificar ativos de informação afetados

A equipe de TI deverá identificar e listar todos os ativos danificados da ocorrência do desastre. Esta equipe deverá emitir um relatório dos ativos afetados.

2.3. Mapear os dados a serem recuperados

A equipe de TI deverá mapear quais serviços foram descontinuados e as informações de perda de ativo e de conexão com intuito de levar ao conhecimento da Diretoria de Tecnologia da Informação. 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 proxy, dns, rotas, vlans etc.

2.4. Estimar o volume de dados, perdas e tempo de recuperação

A equipe de TI deverá estimar o volume de dados a serem recuperados e o prazo para recuperação das informações. Após o mapeamento das perdas e impactos deverá elaborar um breve cronograma de recuperação das aplicações levando em consideração o tempo de recuperação de cada sistema crítico.

2.5. Executar procedimento de recuperação

A equipe de TI deverá executar os procedimentos de recuperação necessários para a continuidade operacional dos serviços de TI. Esta equipe deverá seguir um *checklist* aprovado por todos os membros dos setores envolvidos. Este documento deverá estar acessível a todos os envolvidos neste procedimento.

2.6. Testar procedimentos de restauração de dados

A Diretoria de Tecnologia da Informação conjuntamente com a equipe de TI deverá simular diversos tipos de eventos. Estes eventos poderão ser simples, como uma queda de energia ou mesmo complexos como um incêndio, para descobrir se as ações de contingência são eficientes. Testes deverão ser realizados para identificar falhas e corrigi-las antes de uma ocorrência real. Por meio de simulações a equipe terá condições de conhecer a estratégia de continuidade e o que fazer em cada situação.

2.7. Documentar procedimentos apresentando melhorias

O PCO deverá ser documentado e formalmente divulgado. Essa divulgação deverá ser feita pelo e-mail corporativo, comunicados ou reuniões. É importante que todos os envolvidos conheçam os procedimentos detalhados e quem é o responsável por cada ação evitando estresse, correria e desespero.

3. PAPÉIS E RESPONSABILIDADES DO PCO

Os papéis e responsabilidades para a execução do PCO são:

h) **Diretoria de Tecnologia da Informação:** responsável por delegar ações de contingência a serem realizadas pelas equipes envolvidas e planejar ações para diminuir os impactos dos incidentes. Este setor é responsável por identificar a ocorrência de um incidente ou crise e delegar para a Equipe de TI a responsabilidade de restabelecer a normalidade dos serviços de TI.

i) **Equipe de TI:** responsável pelas ações de manutenção dos serviços de TI, bem como a configuração e instalação de sistemas e restabelecimento dos Serviços de TI à normalidade.

Esta equipe deverá ser acionada sempre que houverem disrrupções nos serviços de internet e sistemas informatizados. A equipe é formada por servidores lotados nas áreas de sistemas de informações e redes e segurança da informação. Esta equipe deverá verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido e divulgar informações para as demais equipes envolvidas.

j) **Equipe de Infraestrutura Operacional:** responsável por manter a estabilização de energia e a climatização da sala de equipamentos de TI. Esta equipe deverá ser formada por servidores lotados na Diretoria de Infraestrutura.

4. ATIVAÇÃO E ENCERRAMENTO DO PCO

A ativação do PCO será iniciada pela Diretoria de Tecnologia da Informação que convocará reunião de emergência com os líderes responsáveis pelo plano de recuperação de desastres e plano de administração de crise com o intuito de:

a) Coordenar prazos e orquestrar as ações de contingência;

b) Informar as equipes quais serão as ações de contingência com a priorização dos serviços essenciais.

O encerramento do PCO deverá ocorrer após a normalização dos sistemas informatizados em seu ambiente principal. Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter, a Diretoria de Tecnologia da Informação deverá emitir um parecer relatando as atividades realizadas neste plano.

5. AUTORIDADE RESPONSÁVEL PELO PCO

Conforme apresenta a tabela 1, a Diretoria de Tecnologia da Informação é a autoridade responsável por implementar, manter e melhorar o PCO. Este setor deverá documentar todas as atividades referentes à execução deste plano de forma que possibilite a melhoria contínua dos Serviços de TI.

Tabela 1 - Autoridade Responsável

Autoridade	E-mail	Telefone
Diretoria de Tecnologia da Informação	dti@ifto.edu.br	63 3229-2212

Fonte: Diretoria de Tecnologia da Informação (IFTO).

6. ATIVIDADES, TAREFAS E AÇÕES DO PCO

Uma vez restabelecidos os Serviços de TI, a Diretoria de Tecnologia da Informação deverá emitir um parecer relatando as atividades realizadas neste PCO. Este setor também deverá informar às partes interessadas a normalização dos recursos, serviços e sistemas informatizados do IFTO. Para garantir a normalidade dos serviços de TI, a área de TI deverá realizar as atividades apresentadas na tabela 2:

Tabela 2 - Atividades de retorno à normalidade

Atividade	Responsável
Manter funcionando os sistemas de estabilização de energia (Grupo Gerador).	- Equipe de Infraestrutura Predial.
Manter funcionando os equipamentos de climatização da sala de equipamentos.	
Garantir a integridade dos ativos de rede para reconexão.	- Equipe de TI.
Testar os equipamentos de processamento e armazenamento de dados.	
Restaurar os serviços de acordo com uma sequência pré-definida de continuidade e restauração.	

Verificar a integridade dos dados e restaurar os backups caso necessário.	
Garantir o retorno dos sistemas de acordo com as demandas pontuais.	
Garantir a integridade dos dados, que podem estar corrompidos ou defasados.	
Garantir que as funcionalidades básicas de acesso estão funcionando novamente.	
Comunicar às partes interessadas o retorno da normalidade.	- Diretoria de Tecnologia da Informação.

Fonte: Diretoria de Tecnologia da Informação (IFTO)

Para a realização das atividades e tarefas definidas no PCO a Diretoria de Tecnologia da Informação juntamente com os setores envolvidos deverá elaborar checklist para cada ação de contingência. Estes documentos deverão ser compartilhados com todos os servidores envolvidos na execução do PCO.

ANEXO III

PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

1. INTRODUÇÃO

O Plano de Recuperação de Desastres (PRD) 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. Este plano é responsável por planejar e agir para que uma vez controlada a contingência e passada a crise, a área de TI retome seus níveis originais de operação no ambiente principal.

1.1. Escopo

O escopo do PRD é garantir o retorno das operações do ambiente principal depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas dos ativos, conexões e configurações deste ambiente.

1.2 Objetivos

O PRD visa restaurar e recuperar o ativo no menor tempo possível e restabelecer o ambiente e as condições originais de operação. Este plano tem como objetivos específicos:

a) Avaliar danos aos ativos e conexões do datacenter e prover meios para sua recuperação.

b) Estabelecer procedimentos de comunicação e mobilização adequados ao gerenciamento de situações de contingência, cenários de incidentes, desastres ou falhas que causem impacto nas rotinas operacionais relacionadas a Tecnologia da Informação;

c) Aplicar ações necessárias para correção e/ou eliminação do problema de forma a garantir o nível adequado de funcionamento dos recursos, serviços e sistemas informatizados do IFTO;

d) Possibilitar a avaliação dos danos aos ativos, serviços essenciais e conexões do datacenter;

e) Prover meios para a recuperação de danos aos ativos;

f) Evitar desdobramentos de outros incidentes na instalação principal;

g) Restabelecer o serviço/sistema essencial no datacenter principal dentro do prazo tolerável.

1.3. Abrangência

Este documento aplica-se a todos os recursos, serviços e sistemas informatizados considerados críticos para o IFTO e restringe a última etapa da recuperação de desastres, garantindo o retorno à normalidade das operações e não mais sua recorrência no caso de riscos controláveis.

2. RECUPERAÇÃO DE DESASTRES

Este plano de ação aborda atividades a serem realizadas após a contingência e passada a crise, permitindo a TI ter condições de retomar seus níveis originais de operação no ambiente principal. Este documento baseia-se no processo de recuperação de desastres definido pela área de TI, conforme apresenta a figura 1.

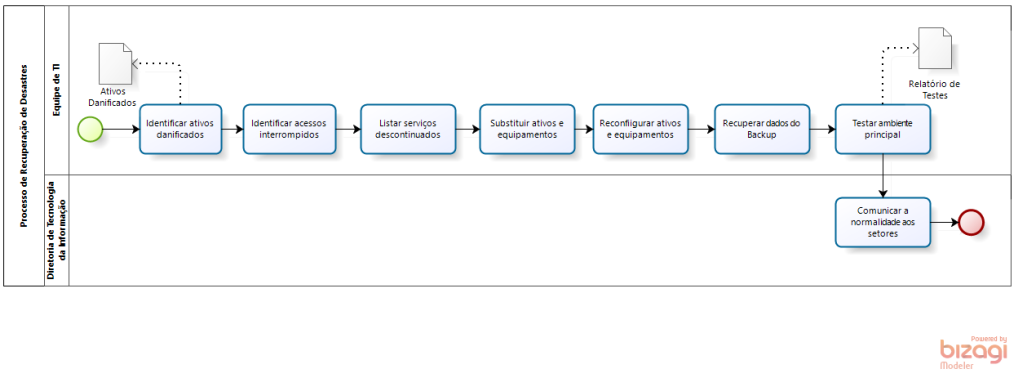


Figura 1 - Processo de Recuperação de desastres

A figura 1 apresenta as 8 (oito) atividades que compõem o processo de recuperação de desastres. São elas: identificar ativos danificados; identificar acessos interrompidos; listar serviços descontinuados; substituir ativos e equipamentos; reconfigurar ativos e equipamentos; recuperar dados do backup; testar o ambiente principal e comunicar a normalidade aos setores.

2.1. identificar ativos danificados

A equipe de TI deverá identificar e lista todos os ativos danificados na ocorrência do desastre. Para isso deverá construir um relatório de ativos danificados. Este relatório deverá ser compartilhado com todos os servidores envolvidos na recuperação de desastres.

2.2. Identificar acessos interrompidos

A equipe de TI 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. Estas informações deverão ser registradas em um relatório de acessos interrompidos.

2.3. Listar serviços descontinuados

A Equipe de TI deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento da Alta Gestão. 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 proxy, dns, rotas, vlans etc.

2.4. Substituir ativos e equipamentos

A equipe de TI é responsável por apresentar a quantidade de ativos e equipamentos que deverão ser substituídos e a necessidade de novas aquisições. Esta equipe deverá informar se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição, devendo observar se há garantia e se a mesma poderá ser acionada.

A equipe de TI deverá verificar se as configurações dos ativos substituídos estão em pleno funcionamento. As informações pertinentes à alteração do tempo de recuperação dos serviços de TI deverão ser passadas para a Diretoria de Informática comunicar aos setores afetados.

2.5. Recuperar dados do backup

A Equipe de TI deverá mensurar o tempo necessário para a recuperação dos dados do backup. Após a estimativa de tempo de recuperação deverá iniciar os procedimentos de recuperação de dados. Para otimizar a recuperação de dados recomenda-se que mantém a documentação atualizada sobre as estratégias de backup utilizadas.

2.6. Testar o ambiente principal

O ambiente principal do datacenter deverá ser constantemente testado a fim de garantir que o processo de recuperação ocorra conforme o planejado. Os testes garantem os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre. Os testes deverão incluir a validação das configurações ativas no ambiente principal. Para a realização de testes recomenda-se que sejam definidos e atualizados constantemente checklists. Na medida do possível os testes deverão ser automatizados.

3. PAPÉIS E RESPONSABILIDADES

A fim de não sobrepor atividades e duplicar estruturas organizacionais, caberá à Diretoria de Tecnologia da Informação, a designação dos responsáveis para gerenciar as fases da continuidade de recuperação de serviços de TI. A equipe responsável por realizar o PRD deverá ter minimamente:

a) Equipe de infraestrutura predial: responsável por garantir segurança do retorno às instalações do IFTO que deverá verificar os níveis mínimos aceitáveis de fornecimento de serviços. Esta equipe deverá restabelecer para níveis aceitáveis o fornecimento de energia elétrica, através de geradores e não somente sistema de *nobreak* (pois este tem ação temporária, limitada pela carga prévia no banco de baterias);

b) Equipe de TI: responsável por operacionalizar ações de recuperação de desastres.

c) Diretoria de Tecnologia da Informação: repassar para a alta gestão o andamento das ações de recuperação de desastres.

4. ATIVAMENTO E ENCERRAMENTO DO PRD

A ativação do PRD será feita pela Diretoria de Tecnologia da Informação. Este plano de ação deverá ser encerrado assim que os procedimentos de recuperação forem realizados pela equipe de TI.

Esta equipe deve fornecer relatório com as informações de procedimentos de recuperação, fornecedores que tiveram de ser acionados, entre outras informações relevantes para a Diretoria de Informática tenha condições de informar às partes interessados o andamento das ações de recuperação realizadas.

O PRD deverá ser encerrado pela Diretoria de Tecnologia da Informação, assim que os procedimentos de administração de crises forem realizados por todas as equipes. Ao término do procedimento de recuperação, as informações deverão ser consolidadas em parecer específico informando horário de restabelecimento de cada serviço, especificando equipamentos que foram realocados, procedimentos de recuperação, entre outras informações relevantes.

5. AUTORIDADE RESPONSÁVEL PELO PRD

A Diretoria de Tecnologia da Informação é a autoridade responsável por implementar, manter e melhorar o PRD e deverá manter atualizada toda documentação inerente a desastre visando a melhoria contínua.

Tabela 1 - Autoridade Responsável.

Autoridade	E-mail	Telefone
Diretoria de Tecnologia da Informação	dti@ifto.edu.br	63 3229-2212

Fonte: Diretoria de Tecnologia da Informação (IFTO).

6. ATIVIDADES, TAREFAS E AÇÕES DO PRD

A tabela 2 apresenta as atividades, tarefas, ações e responsáveis pela execução do PRD. A equipe de TI deverá criar documentos modelos para o monitoramento e controle das atividades definidas na tabela 2.

Tabela 2 - Atividades para recuperação de desastres.

Atividade	Tarefa	Responsável
Elaborar cronograma de recuperação de Serviços de TI.	1. Identificar os serviços a serem recuperados.	Equipe de TI
Identificar todos os ativos danificados.	1.Identificar e listar todos os ativos danificados da ocorrência do incidente ou desastre.	Equipe de TI
Identificar acessos interrompidos.	1.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.	Equipe de TI
Listar serviços descontinuados.	1.Mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão.	Equipe de TI
Substituir ativos e equipamentos danificados.	1. Substituir ativos perdidos.	Equipe de TI
Reconfigurar ativos e equipamentos.	1. Reconfigurar ativos que podem ser reparados ou reconfigurados.	Equipe de TI
Recuperar de dados do Backup.	1. Verificar a integridade dos dados e restaurar os backups. 2. Restaurar os serviços de acordo com uma sequência pré-definida. 3.Restabelecer recursos, serviços e sistemas informatizados dentro do prazo tolerável.	Equipe de TI
Testar funcionamento dos ativos e equipamentos.	1.Validar as configurações dos ativos reparados ou substituídos. 2. Verificar os parâmetros de auto inicialização dos sistemas após quedas, para que ocorra de forma automatizada. 3. Testar os equipamentos de processamento e armazenamento de	Equipe de TI

	dados.	
Apresentar relatório de recuperação.	1.Desenvolver relatório com todos os problemas encontrados e como foi resolvido. 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 proxy, dns, rotas, vlans etc.	Diretoria de Tecnologia da Informação
Manter funcionando os sistemas de proteção de energia e climatização.	1.Manter os sistemas de energia ininterrupta como Nobreaks e Gerador funcionando. 2. Garantir o restabelecimento de energia elétrica através de contingência (gerador) ou concessionária se disponível. 3. Restabelecer os equipamentos de climatização do data center e suas automações.	Equipe de Engenharia (Diretoria de Infraestrutura)

Fonte: Diretoria de Tecnologia da Informação (IFTO)

7. PROCEDIMENTOS DE RECUPERAÇÃO

Conforme descrito na ABNT ISO 22313 (2020), os procedimentos de continuidade de serviços de TI deverão ser documentados de forma a prover uma avaliação detalhada da situação do incidente de interrupção e de seu impacto e a determinação das atividades necessárias para a correta recuperação. A equipe de TI deverá documentar e tornar disponíveis para todos os envolvidos os seguintes procedimentos:

a) Restauração de backups;

b) Instalação e configuração de ativos de rede;

c) Instalação e configuração de servidores de rede;

d) Instalação e configuração de serviços de TI;

e) Testes e validação de serviços de TI e sistemas informatizados.

8. RECURSOS NECESSÁRIOS PARA PRD

Para a execução do PRD será necessário a contratação de infraestrutura tecnológica em nuvem computacional. Este contrato deverá prever todos os recursos necessários para manter minimamente os principais serviços de TI do IFTO.

9. COMUNICAÇÃO

A Diretoria de Tecnologia da Informação por meio dos canais disponíveis deverá informar a ocorrência de desastres envolvendo serviços de TI. Atualmente o IFTO possui os seguintes canais para notificação e comunicação sobre desastres envolvendo a área de TI:

a) Portal Institucional: portal.ifto.edu.br

b) E-mail: dti@ifto.edu.br

ANEXO IV

PLANO DE TESTES E VALIDAÇÃO - (PTV)

1. INTRODUÇÃO

Os testes devem ser realizados em situações o mais próximo possível da realidade para efetivamente garantir que, em caso de crise ou eventos de falha, o plano de gestão de continuidade de serviços de TI possa atender satisfatoriamente aos seus propósitos. Os testes deverão ser planejados e executados com periodicidade mínima anual a partir da data de sua publicação.

O plano de gestão de continuidade de serviços de TI deverá ser testado e validado em reunião entre os líderes de cada plano de ação, a cada ano ou com a insurgência de novos fatores de risco, mudança na análise de impacto, ou com a inclusão de um novo serviço no plano de gestão de continuidade de serviços de TI.

1.1. Escopo

Apresentar o plano de ação para realização de testes do plano de gestão de continuidade de serviços de TI.

1.2. Objetivos

O PTV tem por objetivo principal assegurar a eficiência e a efetividade do plano de gestão de continuidade de serviços de TI.

1.3. Abrangência

Os testes abrangem todos os serviços de TI considerados como essenciais no plano de gestão de continuidade de serviços de TI.

2. TESTES

Os testes deverão ser formalmente registrados observando as necessidades de aprimoramento que, quando identificadas, deverão ser alvo de plano de ação por parte do responsável pelas ações de correções e (ou) adequações que visem a acrescentar melhorias na sua utilização. A área de TI poderá realizar os seguintes tipos de testes:

a) Simulação do teste: conduzido assim que o plano de gestão de continuidade de serviço de TI for concluído, através de simulação dos procedimentos por todas as pessoas relevantes para a execução das ações contindas no plano de ação de forma a avaliar o entendimento e a integração das atividades.

b) Teste total: conduzido assim que o plano de gestão de continuidade de serviço de TI for concluído. Deverá ser realizado de forma periódica. Deverá envolver as áreas de negócio para acompanhar e validar os testes de restauração dos serviços.

c) Teste parcial: não substitui a necessidade do teste total, mas poderá ser realizado como complemento do teste total, em um espaço de tempo menor e em uma escala menor com somente alguns serviços ou componentes de TI.

d) Teste de cenário: deverá simular condições específicas, eventos e cenários de risco.

3. PAPÉIS E RESPONSABILIDADES

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da Diretoria de Tecnologia da Informação que definirá a equipe de testes que trabalhará conjuntamente com a equipe de TI. Os testes deverão ser revistos de acordo com:

a) Mudanças nos processos do IFTO;

b) Mudanças na tecnologia utilizada para disponibilização dos recursos, serviços e sistemas de informação;

c) Mudança na equipe de continuidade de negócios;

d) Eventos antecipados que possam resultar em uma possível interrupção nos negócios (ex., percepção de que uma pandemia possa ser iminente).

4. RECURSOS UTILIZADOS

Para a realização dos testes e validação dos serviços de TI, a área de TI deverá configurar um ambiente de testes contendo minimamente:

a) Virtualização de servidores;

b) Link de Internet;
c) Principais serviços implantados pela área de TI.

Palmas, 08 de janeiro de 2021.

Kleyton Matos Moreira
Diretor de Tecnologia da Informação

Paula Karini Dias Ferreira Amorim
Presidente do Comitê Gestor de Tecnologia da Informação
PORTARIA Nº 242/2019/REI/IFTO, DE 28 DE FEVEREIRO DE 2019

Documento assinado eletronicamente por **Kleyton Matos Moreira**, **Diretor**, em 16/04/2021, às 09:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Paula Karini Dias Ferreira Amorim**, **Presidente**, em 16/04/2021, às 11:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1274568** e o código CRC **E8BD1520**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200
portal.ifto.edu.br — reitoria@ifto.edu.br