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

PLANO DE CONTINUIDADE DE NEGÓCIOS

TECNOLOGIA DA INFORMAÇÃO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
22/04/2021	1	Elaboração do Plano de Continuidade de Negócios (PCN).
19/12/2023	2	Revisão de responsabilidades da equipe de tratamento e resposta a incidentes cibernéticos, indicador de desempenho e inserção de previsão orçamentária para a execução do plano de continuidade de negócios.

1. INTRODUÇÃO

O Plano de Continuidade de Negócios (PCN) objetiva prover o IFTO de um conjunto de planos de ações que suportem o gerenciamento de situações de contingência provocada por incidentes causadores de interrupção no andamento normal de suas atividades, garantindo as condições mínimas necessárias para a continuidade e normalização dos serviços de TI. Ele atua como resposta aos resultados das análises de impacto de negócios e riscos em caso de falhas e indisponibilidade dos serviços de TI. Este documento abrange as estratégias necessárias à continuidade dos serviços de TI envolvendo contingência, continuidade e recuperação.

Este documento apresenta medidas de contingência e proteção para o reestabelecimento de serviços de TI em caso de incidentes graves ou desastres. Ele visa reduzir o risco e minimizar o impacto de interrupções nos 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.

Dentro do contexto apresentado, este documento tem como objetivo estabelecer as características do plano de gestão de contingência e continuidade de serviços de TI desenvolvido pelo Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO). Ele está estruturado em uma breve introdução à temática, gestão de contingência e continuidade de serviços de TI, análise de cenário, análise de impacto no negócio, análise de riscos, papéis e responsabilidades, recursos necessários, estratégias de continuidade de serviços de TI, ações de contingência/recuperação, conscientização e treinamento, comunicação, monitoramento e controle, testes, ativação e encerramento, autoridade responsável, contatos técnicos, revisão e atualização, cronograma de execução e referências utilizadas para a elaboração do documento.

1.1. Escopo

O escopo deste documento envolve a definição e manutenção de um conjunto de planos de ações que contém estratégias de proteção necessárias à contingência e continuidade dos serviços de TI.

1.2. Objetivo

O objetivo geral deste documento é propor um conjunto de planos que possibilitem a disponibilidade dos serviços essenciais envolvendo TI durante as mais diversas

situações de falhas e interrupções.

1.3. **Abrangência**

Este documento abrange 4 (quatro) planos complementares. São eles: plano de administração de crises, continuidade operacional, recuperação de desastres e testes e verificação. Estes planos devem permitir a recuperação, contingência e continuidade dos serviços de TI durante a ocorrência de incidentes.

1.4. **Benefícios esperados**

Com a implementação deste conjunto de planos espera-se obter os seguintes benefícios:

a) capacidade de identificação proativa dos impactos de uma interrupção operacional;

b) capacidade de resposta eficiente às interrupções, o que minimiza o impacto à organização;

c) capacidade de gerenciar os riscos que não podem ser segurados;

d) infraestrutura mais resiliente e segura;

e) redução do impacto nos negócios;

f) restauração de serviços, sistemas e soluções de TI de forma mais rápida;

g) redução no volume de incidentes que impactam o negócio;

h) antecipação aos problemas;

i) minimização de interrupções dos serviços e sistemas; e

j) capacidade de demonstrar uma resposta possível por meio de um processo de testes.

1.5. **Vigência**

Este documento tem vigência de 5 (cinco) anos após a data de sua publicação. O documento deverá ser revisto anualmente e poderá ser atualizado de acordo com a necessidade.

2. **GESTÃO DE CONTINUIDADE DE NEGÓCIOS**

A gestão de continuidade de negócios (GCN) é responsável por gerenciar a capacidade da organização em continuar a prestar serviços predeterminados e acordados para suportar os requisitos mínimos do negócio, após uma interrupção. Esta abordagem 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.

A GCN previne a perda de segurança para o cliente e usuário, e produz planos integrados de recuperação para TI. Esta estratégia de gestão compreende atividades, tais como:

a) avaliar o custo/benefício de se ter uma gestão de contingência e 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 GCN ao gerenciamento de mudanças, garantindo que alterações no ambiente de produção, sejam devidamente avaliadas, e se necessário, refletir no plano de gestão de contingência e continuidade dos serviços de TI.

Diante do exposto, a gestão de continuidade de negócios no IFTO deve garantir que a infraestrutura técnica e de serviços de TI não seja interrompida em um período longo. Para a execução deste processo 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) identificar serviços primordiais para o negócio para provimento de medidas de prevenção adicionais;

c) calcular o tempo de restauração dos serviços de TI;

d) definir qual abordagem será realizada para a restauração dos serviços de TI;

e) definir e executar ações para prevenir e reduzir os efeitos do impacto de um desastre;

f) criar, manter e testar um plano de recuperação para restaurar os serviços, no período definido, após um desastre.

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

2.1. **Plano de Continuidade de Negócios (PCN)**

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

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

Dentro do contexto apresentado, este documento tem como objetivo principal apresentar as estratégias utilizadas pelo IFTO para a contingência e continuidade de serviços de TI. Ele está estruturado em introdução, gestão de continuidade de negócios, análise de cenário, análise de impacto no negócio, análise de riscos, papéis e responsabilidades, recursos necessários, estratégias de continuidade de serviços de TI, ações de contingência/recuperação, conscientização e treinamento, comunicação, monitoramento e controle, testes, ativação e encerramento, autoridade responsável, contatos técnicos, revisão e atualização, cronograma de execução e referências.

3. **ANÁLISE DE CENÁRIO**

Para que o PCN obtenha êxito em sua execução deve-se realizar a análise contínua do cenário atual em que o IFTO. Esta análise considera as perspectivas: organização, processo, pessoas, comunicação e tecnologia.

3.1. **Cenário atual**

Atualmente o parque tecnológico do IFTO tem um site principal, localizado no prédio da Reitoria e outro site secundário em nuvem computacional. Os serviços, sistemas e aplicativos essenciais estão armazenados no site principal. Atualmente os principais sistemas de informação estão sendo migrados para a nuvem computacional. Até o presente momento o IFTO dispõe dos seguintes ativos em seu inventário tecnológico:

a) 1 sala de Datacenter;

b) 1 nuvem computacional;

c) 2 *links* de comunicação de dados;

d) 2 servidores de grande porte;

e) 1 *storage* de grande porte;

f) 6 sistemas de informação;

g) 150 impressoras (*outsoucing de impressão*);

h) 2.000 computadores;

i) 1 grupo gerador; e

j) 2 *nobreaks* de grande porte.

Com base no inventário tecnológico a análise do cenário foi elaborada com o auxílio da ferramenta de gestão "Matriz SWOT". A tabela 1 apresenta o resultado obtido.

Tabela 1 - 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. Instabilização no fornecimento de energia elétrica para a infraestrutura tecnológica. 3. Indefinição de orçamento anual exclusivo para TI. 4. Falta de plano de capacitação continuada em continuidade de negócios.
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.

Fonte: Diretoria de Tecnologia da Informação

Atualmente a infraestrutura tecnológica da instituição está em processo de atualização de *hardware, software e* sistemas operacionais. Para que seja possível executar o PCN além de investir em recursos tecnológicos é necessário manter atualizado o catálogo de serviços de TI, como também a realização de capacitações técnicas.

A partir da análise de cenário apresentada na tabela 1 e dados do levantamento de governança publicado pelo TCU é possível observar que o IFTO encontra-se atualmente no nível de maturidade intermediário de seus processos de governança e gestão

de TI. Com isso, a instituição enfrenta um grande desafio relacionado à continuidade dos serviços de TI.

3.1.1. **Serviços essenciais de TI**

Para o desenvolvimento do PCN 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 considerada como serviços essenciais a serem resguardados por este PCN os seguintes serviços de TI:

a) e-mail institucional;

b) impressão e digitalização de documentos;

c) internet;

d) moodle;

e) portal institucional;

f) rede cabeada;

g) rede Wi-Fi;

h) SEI: Sistema Eletrônico de Informações;

i) SIGA_EPCT: Sistema de Informações Gerenciais Acadêmica;

j) SI: Sistemas Integrados;

k) sistema de submissão de artigos científicos;

l) sistema do processo seletivo;

m) Sophia: Sistema de Bibliotecas;

n) SUAP: Sistema Unificado de Administração Pública; e

o) telefonia fixa.

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 identificou os recursos necessários para retomar as operações de negócios em caso de ocorrência de incidentes ou desastres.

Esta análise levou em consideração os processos organizacionais considerados mais críticos para o IFTO no momento de elaboração deste documento. A tabela 2 apresenta os sistemas/serviços e os processos organizacionais que serão tratados no PCN.

Tabela 2 - Sistemas, serviços e processos organizacionais críticos para o IFTO

Sistema/Serviço	Área	Processo Organizacional	Criticidade
E-mail	- DTI	- Todos	Alta
Impressão e digitalização de documentos	- PROAD	- Todos	Alta
Internet	- DTI	- Todos	Alta
Moodle	- PROEN - PROEX	- Ensino - Extensão	Alta
Portal Institucional	Diretoria de Comunicação	- Comunicação	Alta
Rede Cabeada	Todas	- Todos	Alta
Rede Wi-Fi	Todas	- Todos	Alta

Sistema de submissão de artigos científicos	- PROPI	- Pesquisa	Alta
Sistema do processo seletivo	- PROAE	- Seletivo	Alta
Sistema Unificado de Administração Pública (SUAP)	Administração	- Almoxarifado. - Boletins de Serviços. - Compras. - Contratos. - Frota. - Materiais. - Patrimônio. - Reservas de Salas. - Telefones.	Alta
	Central de Serviços	- Abrir chamado. - Base de Conhecimentos. - Cadastros. - Chamados. - Dashboard. - Meus Chamados. - Relatórios.	Alta
	Comunicação Social	- Enquetes. - Eventos. - Relatórios.	Alta
	Des. Institucional	- Gestão. - Planejamento. - Planejamento Estratégico. - Planejamento Institucional.	Alta
	Documentos e Processos	- Documentos Eletrônicos. - Processos Eletrônicos. - Processos Físicos.	Alta
	Ensino	- Alunos e Professores. - Cadastros Gerais. - Cursos, Matrizes e Componentes. - Estatísticas. - ETEP. - Processos Seletivos. - Relatórios. - Atas Eletrônicas.	Alta
	Extensão	- Estágios e Afins. - Projetos. - Demandas Externas.	Alta
	Gestão de Pessoas	- Servidores. - Setores. - Campi. - Administração de Pessoal. - Desenvolvimento de Pessoal. - Atenção a Saúde do Servidor. - Licença Capacitação. - Programa de Gestão. - SIAPE. - Relatórios. - Cadastros.	Alta
	Pesquisa	- Editais. - Projetos. - Declarações. - Editora. - Laboratórios.	Alta
	Segurança Institucional	- Solicitações de Entrada.	Alta
	Tecnologia da Informação	- Acessibilidade. - Desenvolvimento. - Segurança. - Serviços. - Usuários.	Alta
SEI	Gestão	- Gestão de Processos. - Gestão de Documentos.	Alta
SIGA_EPCT	Ensino	- Gestão de Estudantes. - Gestão de Cursos. - Gestão de Planos de Ensino. - Gestão de Matrículas. - Gestão de Estágios.	Alta

		- Diário de Classe. - Emissão de Documentos.	
SOPHIA	Gestão	- Gestão de Bibliotecas.	Alta
Sistemas Internos	Gestão	- Gestão de Concursos. - Gestão de Eventos. - Gestão de Creche. - Gestão de Restaurante.	Alta
Telefonia fixa	DTI	- Todos	Alta

Fonte: Diretoria de Tecnologia da Informação

Os sistemas, serviços, recursos e processos organizacionais no IFTO estão em constante evolução. Com isso, a tabela 2 está periodicamente sendo revisando visando a promoção de eventuais ajustes necessários.

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 criticidade e o impacto de uma interrupção ou desastre na prestação de serviços disponibilizados pela área de TI. Inicialmente foram definidos como críticos os serviços apresentados na tabela 3. Esta tabela apresenta os tempos de recuperação e o tempo do backup que serão considerados nas estratégias de continuidade a serem executadas pelo planos complementares este documento.

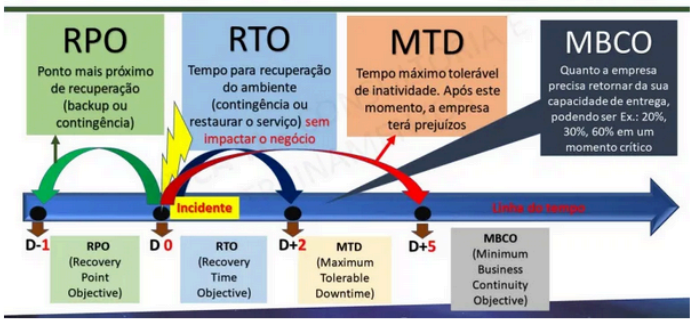
Tabela 3 - Serviços de TI

Recurso/ Serviço	Criticidade	RPO (Backup)	RTO (Restabelecer)	MTD (Tolerância)	Impacto			
					Financeiro	Legal	Imagem	Operacional
Internet	alta	-	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
E-mail	alta	-	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Impressão e digitalização de documentos	alta	-	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Moodle	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Portal Institucional	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Rede cabeada	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Rede Wi-Fi	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
SEI	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
SIGA_EPCT	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
SI	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Sistema de submissão de artigos científicos	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto
Sistema do processo seletivo	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
Telefonia fixa	alta	24 horas	8 horas	8 horas	Indefinido	Indefinido	Indefinido	Alto

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 da instituição. Conforme apresentado na tabela

3 para a análise de impacto foram definidos tempos de tolerância a interrupções e pontos de recuperação das informações. A instituição deve retornar da sua capacidade de entrega dos serviços de TI em no mínimo 50% em um momento crítico. A figura 1 detalha as siglas apresentadas na tabela 3.



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 1 - Conceitos sobre tempo de recuperação (PDCATI, 2020)

Os conceitos apresentados na figura 1 são fundamentais para a análise de impacto no negócio. A tabela 4 apresenta a prioridade de recuperação dos serviços de TI considerados essenciais para a área de TI. 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 instituto.

Tabela 4 - Priorização de serviços de TI e suas interdependências

Prioridade	Serviços/ Sistema	Criticidade	Interdependência
1	Rede Cabeada	Alta	-
2	Rede Wi-Fi	Alta	Rede Cabeada
3	Internet	Alta	Rede Cabeada
4	Moodle	Alta	Internet
5	E-mail institucional	Alta	Internet
6	Portal Institucional	Alta	Internet
7	SEI	Alta	Internet
8	SIGA_EPCT	Alta	Internet
9	SI	Média	Internet
10	Sistema de submissão de artigos científicos	Alta	Internet
11	Sistema do Processo Seletivo	Alta	Internet
12	Sophia	Alta	Internet
13	SUAP	Alta	Internet
14	Telefonia fixa	Alta	Rede Cabeada
15	Impressão e digitalização de documentos	Alta	Rede cabeada Rede Wi-Fi

Fonte: Diretoria de Tecnologia da Informação (IFTO)

A prioridade apresentada na tabela 4 leva em consideração o cenário em que este documento foi elaborado. 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 5 detalha o risco, causa, consequência, probabilidade, impacto e controle a serem observados para garantir a continuidade de serviços de TI.

Tabela 5 - Análise de riscos

Risco	Causa	Consequência	Probabilidade	Impacto	Controle	Responsável
Incêndio.	-Ações humanas. -Curto-circuitos. -Queimadas.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	média	médio	-Sistemas Profissionais de combate a incêndio para Data Center -Extintores. -Programas de capacitação contra incêndios.	Diretoria de Infraestrutura
Interrupção de energia elétrica.	-Ações humanas. -Curto-circuitos. -Queimadas. -Vendavais. - Chuvas. - Tempestades atmosféricas.	-Indisponibilidade de recursos, serviços e sistemas informatizados. - Dano físico nos equipamentos.	média	alto	-Sistema de Proteção de Energia.	Diretoria de Infraestrutura
Desastres naturais.	-Vendavais. -Chuvas. -Tempestades atmosféricas. - Alagamentos.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	média	médio	-Plano de gestão de contingência e continuidade de serviços de TI.	Diretoria de Infraestrutura
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.	Diretoria de Tecnologia da Informação
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	- Parada na comunicação de dados entre servidores e serviços e sites externos ao IFTO. - Indisponibilidade de sistemas informatizados do IFTO.	média	médio	- Plano de gestão de contingência e continuidade de serviços de TI.	Diretoria de Tecnologia da Informação

	roteador ou firewall.					
Falha na restauração de backups.	- Erros de comunicação na rede. - Quedas ou oscilações de energia. - Queima de componentes eletrônicos.	- Dados corrompidos. - Perda de dados. - Indisponibilidade de Backup. - Indisponibilidade de sistemas informatizados.	média	médio	- Monitoramento contínuo de estratégias de criação e restauração de backups.	Diretoria de Tecnologia da Informação
Falha na climatização da sala de equipamentos.	- Variação de temperaturas na sala de equipamentos. - Oscilações elétricas. - Defeitos em componentes eletrônicos dos aparelhos de ar condicionado.	- Superaquecimentos dos equipamentos. - 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.	média	médio	- Plano de gestão de contingência e continuidade de serviços de TI	Pró-Reitoria de Administração
Defasagem tecnológica.	-Evolução tecnológica em descompasso com os recursos orçamentários existentes para expansão do parque tecnológico.	-Falhas na disponibilização de recursos, serviços e sistemas informatizados redundantes.	média	médio	-Plano Anual de Contratações.	Diretoria de Tecnologia da Informação
Ataques internos.	-Falhas de sistema de monitoramento de vulnerabilidades. -Falhas nos mecanismos de proteção contra invasão. - Falhas no sistema de detecção de intrusão.	-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.	Diretoria de Tecnologia da Informação
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.	Diretoria de Tecnologia da Informação
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.	Diretoria de Tecnologia da Informação
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	-Indisponibilidade de recursos, serviços e sistemas informatizados.	alta	alto	-Link redundante de Dados. -Configuração de alta disponibilidade com balanceamento	Diretoria de Tecnologia da Informação

	eletrônicos dos ativos de rede. -Falta de conhecimento sobre cabeamento estruturado. -Ausência de capacitações em redes de comunicação de dados. -Falha humana.				de carga e *failover*.	
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.	Diretoria de Tecnologia da Informação
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.	Diretoria de Tecnologia da Informação
Falha Humana.	- Falta de conhecimento técnico. - Falta de capacitações continuadas.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	média	alto	-Curso de capacitação periódica.	Diretoria de Tecnologia da Informação
Falha de Hardware.	-Queima de componentes eletrônicos.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	média	médio	-Aquisição de *hardware* redundante.	Diretoria de Tecnologia da Informação
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.	Diretoria de Tecnologia da Informação

Fonte: Diretoria de Tecnologia da Informação

Os riscos apresentados na tabela 5 poderão ser alterados e atualizados de acordo com o contexto interno e externo do IFTO. No período da revisão deste PCN, os riscos e controles deverão ser atualizados de forma a refletir o atual cenário das instituições públicas brasileiras.

6. PAPÉIS E RESPONSABILIDADES

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função. Para garantir a eficiência na execução do plano de gestão de contingência e continuidade de serviços de TI são definidos papéis e responsabilidades.

6.1. **Comitê Gestor de Tecnologia da Informação**

Representado por Pró-Reitorias, Diretorias Sistêmicas e Direção de Geral de Campus. É responsável pela decisão final sobre o escopo, política e diretrizes sobre a gestão de contingência e continuidade de serviços de TI. Este papel tem as seguintes responsabilidades: Este papel tem as seguintes responsabilidades:

a) aprovar a estratégia de contingência e continuidade dos serviços de TI;

b) avaliar e validar os planos de ação elaborados pelas áreas de TI e definir os testes a serem realizados. Quando necessário, retornar avaliação a DTI, indicando os ajustes a serem realizados;

c) avaliar a relação custo/benefício das estratégias de e contingência e continuidade propostas e dos planos de ações que compõem o Sistema de Gestão de Contingência e Continuidade de TI e decidir sobre sua implementação;

d) aprovar as diretrizes estratégicas que norteiam a elaboração do plano de gestão de contingência e continuidade de serviços de TI;

e) aprovar e supervisionar o plano de gestão de contingência e continuidade de serviços de TI e seus planos de ações complementares, zelando por sua qualidade e efetividade; e

f) garantir os recursos necessários para estabelecer, implementar, operar e manter o plano de gestão de contingência e continuidade de serviços de TI.

6.2. **Comitê de Segurança da Informação**

Representado por vários servidores das áreas finalísticas do IFTO. Este papel tem as seguintes responsabilidades:

a) propor diretrizes estratégias de segurança da informação para o plano de contingência e continuidade de serviços de TI;

b) analisar e manifestar-se sobre a documentação de contingência e continuidade de serviços de TI, apoiando a alta gestão na avaliação do processo de continuidade de serviços de TI;

c) avaliar o plano de tratamento de riscos relacionados à contingência e continuidade de serviços de TI;

d) supervisionar a elaboração, implementação, testes e atualização dos planos de ações; e

e) propor melhorias na implantação de novos controles relativos ao Plano de Contingência e Continuidade de Serviços de TI.

6.3. **Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR**

Representada por assistentes, técnicos, e analistas e engenheiros lotados nas áreas de TI e Infraestrutura. Este papel tem as seguintes responsabilidades:

a) realizar, periodicamente, a análise de impacto nos negócios;

b) identificar e documentar riscos que possam comprometer a continuidade das atividades críticas;

c) identificar, documentar e avaliar os possíveis impactos à continuidade das atividades críticas, caso riscos se concretizem;

d) 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;

e) documentar e publicar o processo de continuidade de serviços de TI;

f) elaborar os planos de ações previstos no plano de contingência e continuidade de serviços de TI;

g) acompanhar o processo de implementação da estratégia de contingência e continuidade de TI, em função dos riscos operacionais envolvidos;

h) realizar os testes e exercícios dos planos de ações de contingência e continuidade de TI;

i) aprimorar os planos de ações a partir dos resultados dos testes e exercícios;

j) administrar a contingência quando da interrupção de atividades, com base nos planos desenvolvidos;

k) 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;

l) fornecer, tempestivamente, todas as informações solicitadas à área ou responsável interno de gestão de continuidade de negócios;

m) implementar os procedimentos adequados para minimizar os riscos de descontinuidade de acordo com a estratégia aprovada;

n) realizar treinamentos e avaliações do plano de gestão de contingência e continuidade de serviços de TI periodicamente para garantir a manutenção e o bom funcionamento dos planos de ações;

o) fornecer a infraestrutura de servidores físicos e virtuais necessários para que a TI execute suas operações e processos essenciais durante um desastre ou crise;

p) prover mecanismos de segurança no ambiente principal e alternativo;

q) resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança;

r) 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;

s) 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;

t) desenvolvimento, configuração e manutenção dos sistemas de informação; e

u) garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre ou crise.

6.4. **Diretoria de Tecnologia da Informação**

Representado pelo responsável pela área de TI no IFTO. Este papel tem as

seguintes responsabilidades:

a) desenvolver a cultura de gestão de contingência e continuidade de serviços de TI;

b) deliberar as estratégias, as respostas aos incidentes de impactos críticos (elevados);

c) 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;

d) encaminhar os planos de ações às instâncias superiores, para avaliação e aprovação;

e) supervisionar a elaboração, implementação, testes e atualização dos planos de ações que compõem o plano de contingência e continuidade de serviços de TI;

f) zelar para que a estratégia de contingência e continuidade de TI e para que os respectivos orçamentos sejam efetivamente cumpridos, bem como manter o comitê periodicamente informado do cumprimento das estratégias e dos orçamentos;

g) aprovar calendário anual de testes;

h) comunicar, periodicamente, aos responsáveis pelos setores sobre o andamento da gestão de contingência e continuidade de TI e das necessidades de aprimoramentos identificadas;

i) comunicar à sociedade as ações de contingência e continuidade de serviços de TI desenvolvidas pelo IFTO;

j) orquestrar ações de suas coordenações durante eventuais disrrupções e suas consequências;

k) atuar como elo de ligação entre o corpo técnico e as áreas interessadas ou afetadas pela não continuidade dos serviços de TI;

l) propor acordos de nível de serviços que garantam o alinhamento das prestações de serviços de terceiros com as estratégias de contingência e continuidade de negócios das suas áreas;

m) estabelecer níveis adequados de autoridade e competência, no intuito de assegurar a comunicação efetiva às partes interessadas, bem como assegurar a contingência e continuidade das atividades críticas;

n) viabilizar a contingência e continuidade e a recuperação das atividades críticas, em caso de interrupção; e

o) 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.

7. **RECURSOS NECESSÁRIOS**

Para que o PCN 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 PCN deve ter minimamente os seguintes conhecimentos:

a) sistemas de proteção da informação;

b) gerência de serviços, sistemas e redes de computadores;

c) instalação, configuração e manutenção de sistemas operacionais;

d) segurança da Informação envolvendo infraestrutura de redes, sistemas operacionais e aplicações web;

e) virtualização; e

f) docker.

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); e

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

Para a comunicação entre as unidades e 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 seguro. 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 proteção contra 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 de rede;

d) sistema redundante 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; e

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. A instituição deverá adotar minimamente as seguintes recomendações:

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

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

- Política de segurança da informação;

- Normas complementares sobre segurança da informação;

- Lei geral de proteção de dados; e

- Firewall de borda.

7.4. **Redundância de dados**

O IFTO contratou infraestrutura redundante de TI por meio de nuvem computacional privada. Esta nuvem computacional atualmente possui 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; e

c) 1 link de comunicação de dados através de VPN.

7.5. **Energia**

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. Também conta com dois *nobreaks* de 6 KVA acoplados a um banco contendo 4 baterias.

7.6. **Backups**

O IFTO estabeleceu 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.

7.7. **Locais de recuperação**

Para a recuperação de seus recursos, serviços e sistemas informatizados o IFTO deverá utilizar infraestrutura em nuvem computacional. Esta estratégia está sendo implantada gradativamente, analisando-se os riscos, investimentos e capacidade técnica da equipe responsável pelo projeto.

8. **ESTRATÉGIAS DE CONTINGÊNCIA E CONTINUIDADE**

A área de TI deve adotar estratégias de contingência e continuidade de serviços de TI para os próximos anos, possibilitando a recuperação total ou parcial. Estas ações devem considerar as seguintes opções:

a) ***cold*****:** a instituição deve 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. 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*****:** a instituição deve dispor de *backup* dos dados e *snapshot* dos servidores envolvidos no serviço de TI em local alternativo. No caso de necessidade de reparação total, o serviço poderá ser reinstalado em outro servidor. 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:*** a instituição deve 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:*** a instituição deve 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 deve 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 cara e de maior grau de manutenção.

Além das estratégias mencionadas deve-se observar as seguintes recomendações:

- distância mínima entre sites principal e backup de no mínimo de 15 km;

- configuração de site *backup* sem balanceamento de carga evitando assim ataques cibernéticos;

- execução periódica de plano de testes de serviços de TI;

- atualização periódica do parque tecnológico;

- replicação de configuração de segurança lógica e física no site *backup*; e

- cronograma anual para avaliação periódica de serviços de TI.

As priorizações dos serviços mais críticos a serem contemplados no PCN devem 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 deve realizar ações para a contingência/recuperação de seus serviços de TI. De forma a facilitar a implementação destas ações, deve-se minimamente realizar as atividades apresentadas nas próximas seções.

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 deve manter atualizado o catálogo de serviços de TI, bem como os acordos de níveis de serviço acordados com as áreas de negócio.

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

O IFTO deve 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 deve ser copiada diariamente e salva em meio eletrônico no ambiente de contingência. A instituição deve 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.

9.3. **Infraestrutura de servidores e dados redundantes**

O IFTO deve 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 deve armazenar o *backup* dos dados considerados críticos para a instituição. A infraestrutura de servidores e dados redundantes deve ser espelhada de forma a refletir a situação atual do instituto em relação aos serviços de TI.

10. CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO

O desenvolvimento da cultura de contingência e continuidade de serviços de TI no IFTO deve ser suportado por programas de conscientização e treinamento. A conscientização, além de envolver todos os estudantes, servidores, terceirizados, fornecedores e outras partes interessadas, deve 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, deve envolver uma quantidade menor de pessoas (equipe e servidores ligados à GCN). Esta atividade deve abordar tópicos como a gestão do PCN, execução da análise de impacto nos negócios e avaliação de riscos, desenvolvimento, implantação e testes e comunicação.

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

a) a área de TI deve ser responsável conjuntamente com o Comitê Gestor de TI por definir e conduzir o plano de treinamento sobre contingência continuidade de negócios;

b) o plano de treinamento deve contemplar as áreas de TI e infraestrutura envolvidas na disponibilização e manutenção dos serviços de TI; e

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

11. COMUNICAÇÃO

A comunicação é essencial para que o PCN seja conhecido por todos os envolvidos na contingência e continuidade de serviços essenciais de TI. Para a realização da comunicação deve-se adotar as seguintes práticas:

a) sempre que houver evento que gere a indisponibilidade, mesmo que parcial, de serviço, devem 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 devem ser relacionadas antes de qualquer publicação. No caso de detalhamento técnico do problema à imprensa falada ou televisiva, a Diretoria de Tecnologia da Informação deve ser assessorada pela Diretoria de Comunicação.

Qualquer servidor ao constatar alguma anormalidade que paralise quaisquer processos críticos deve comunicar o fato. 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: suap.ifto.edu.br; e

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

A ETIR deve registrar toda e qualquer incidência que implique na ativação dos procedimentos de contingência descritos neste documento. Para que a comunicação ocorra de forma satisfatória o IFTO tem como autoridade responsável pela comunicação sobre o PCN a Diretoria de Tecnologia da Informação. A tabela 6 apresenta os dados de contato do setor.

Tabela 6 - 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 ETIR, Comitê de Segurança da Informação e Comitê Gestor de TI. Estas reuniões permitirão a manutenção, organização e melhoria do PCN. 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; e

c) em razão dos resultados obtidos nos testes e validação dos planos de ações que compõem o PCN.

13. TESTES

A Diretoria de Tecnologia da Informação deve coordenar a realização de testes de segurança para garantir que os procedimentos previstos neste PCN 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 contingência e 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 contingência e 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 ETIR deverão minimamente abordar:

a) testes dos equipamentos operacionais, como *softwares* 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 PCN;

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

Ao final os testes deve 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 deve guardar o relatório de testes para futuras análises.

14. **ATIVAÇÃO E ENCERRAMENTO**

O PCN deve ser administrado, avaliado, acionado e encerrado no âmbito da Diretoria de Tecnologia da Informação. A ativação do PCN deve 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 PCN também pode ser invocado em casos de testes ou por determinação do Comitê Gestor de TI, Comitê 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 PCN pode ocorrer após a execução dos planos de ações que garantirão a contingência e a continuidade dos serviços de TI. Após o encerramento deste plano a Diretoria de Tecnologia da Informação deve guardar informações históricas para futuras análises.

14.1. **Matriz de acionamento do PCN**

A Diretoria de Tecnologia da Informação é o setor responsável por manter atualizada a matriz de acionamento do PCN no que se refere aos serviços de Tecnologia da Informação. Esta matriz está apresentada na tabela 7.

Tabela 7 - Matriz de Acionamento do PCN

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 24 horas.
Quem executa o PCN?	- ETIR.
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 PCN. A comunicação deve ser por telefone, ou pessoalmente, caso não seja possível o contato.

A Diretoria de Tecnologia da Informação deve relatar à ETIR, o evento que ocasionou a interrupção do serviços de TI, bem como a data e o horário. A tabela 8 apresenta os dados de contato da autoridade responsável pelo PCN.

Tabela 8 - Autoridade responsável

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

Fonte: Diretoria de Tecnologia da Informação

16. **CONTATOS TÉCNICOS**

A tabela 9 apresenta a lista de contatos dos principais atores envolvidos na solução do incidente ou desastre, na eventualidade de acionamento do PCN. Estes contatos referem-se às áreas envolvidas na execução dos planos de ações que complementam o PCN.

Tabela 9 - 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

17. **REVISÃO E ATUALIZAÇÃO**

O PCN deve 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 contingência e continuidade devem 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 PCN devem 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; e

g) implantação de novos serviços de TI.

18. **CRONOGRAMA DE EXECUÇÃO**

Para a execução deste PCN foram definidas as ações e prazos conforme apresenta a tabela 10. Os prazos previstos para a execução das ações apresentadas nesta tabela levam em consideração as contratações de infraestrutura de nuvem computacional, equipamentos de rede e capacitação de servidores a serem adquiridos nos próximos anos.

Tabela 10 - Cronograma de execução

Ação	Prazo
Planejar	2020
Desenvolver	2021

Checar	2022
Agir	2023-2024
Revisar	2024

Fonte: Diretoria de Tecnologia da Informação

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 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 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 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 é estruturada em três níveis de atuação: estratégico, tático e operacional.

a) 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;

b) 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 PCN;

c) Nível operacional: formado pelos analistas e técnicos de TI. Estes atores entram em ação quando é iniciado o plano de contingência e 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.

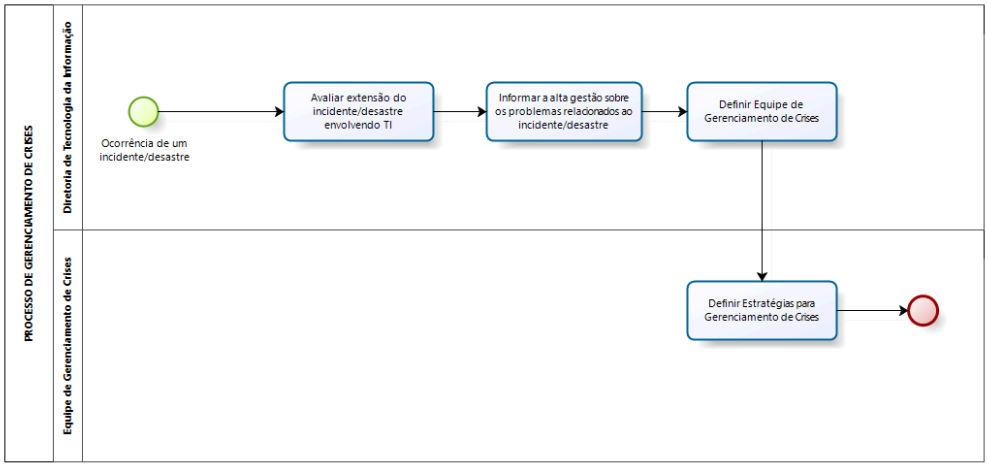


Figura 1 - Processo de gerenciamento de crises

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 deve 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 deve comunicar a alta gestão os problemas relacionados ao incidente/desastre. Este setor deve 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 deve escolher os servidores capacitados para resolução da crise. Esta equipe de gestão de crise deve 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 deve definir as estratégias de gerenciamento de crise. Estas estratégias devem 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) Diretoria de Tecnologia da Informação: responsável por orquestrar ações de suas coordenações durante eventuais disrrupções e suas consequências;

b) Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR: responsável por realizar as ações previstas no PAC. Esta equipe é formada por analistas e técnicos de TI lotados nas áreas de TI e Infraestrutura.

4. ATIVAÇÃO E ENCERRAMENTO DO PAC

A ativação e encerramento do PAC deve ser feita pela Diretoria de Tecnologia da Informação. Este plano de ação deve 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 deve ser encerrado assim que os procedimentos de administração de crises forem realizados/validados por todas as equipes. A equipe de gestão de crise deve 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

6. ATIVIDADES, TAREFAS E AÇÕES DO PAC

Na ocorrência de uma crise, a equipe de gestão de crise deve 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. - Comitê de Segurança da Informação
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).	ETIR
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

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 entrar em contato com os setores e repassar as informações pertinentes.

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.	ETIR
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

c) Atividades a serem realizadas após a crise

Após reunião com o Comitê de Segurança da Informação, o porta-voz da crise deve elaborar um breve relatório 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 deve 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.	ETIR
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

d) Enfrentamento de crises

A Diretoria de Tecnologia da Informação deve 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 deve 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 deve 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 deve 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.

Uma vez validado o funcionamento do retorno dos sistemas essenciais de TI e estabilidade do Datacenter, a Diretoria de Tecnologia da Informação deve 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

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 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 deve emitir relatório apresentando como a crise foi solucionada. A comunicação com cada parte ocorrerá da seguinte forma:

a) Comunicar às autoridades: a prioridade da equipe de comunicação será assegurar que as autoridades competentes apresentadas na tabela 5 tenham sido notificadas da catástrofe, principalmente se envolver risco às pessoas, fornecendo as seguintes informações de localização, natureza, magnitude e impacto do desastre;

Tabela 5 - Autoridades

Autoridade	Número para Contato
Polícia	190
Bombeiros	193
SAMU	192

b) Comunicação após um desastre: após reunião com líderes do plano de recuperação de desastres e plano de continuidade operacional a equipe de comunicação elaborará um breve programa de comunicação para acionar 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;

c) Comunicação com os funcionários: a equipe de comunicação deverá prover um meio de contato específico para este fim, com intuito de que os setores mantenham-se informados da ocorrência de um desastre e da inatividade dos serviços essenciais de TI;

d) Comunicar com os setores: acionar diretamente os setores afetados pelo desastre. Informar a natureza, o impacto e a abrangência da catástrofe, como também as ações de contingência em andamento;

e) Comunicar colaboradores externos, cidadãos e mídia: a equipe de comunicação deverá fornecer informações pertinentes aos colaboradores externos: fornecedores, cidadãos e outros órgãos;

f) Comunicar retorno das operações: comunicar a todas as partes acima citadas quando ocorrer o retorno das operações à normalidade.

8. RECURSOS NECESSÁRIOS

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

9. LOCAL PARA ADMINISTRAÇÃO DE CRISES

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

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. Este documento deve ser implementado, mantido, melhorado e documentado pela Diretoria de Tecnologia da Informação.

1.1. Escopo

É escopo do PCO é 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 execução da contingência.

1.3. Abrangência

O PCO abrange ações para a continuidade operacional dos serviços de TI. Este documento aborda estratégias a serem realizadas pela ETIR 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.

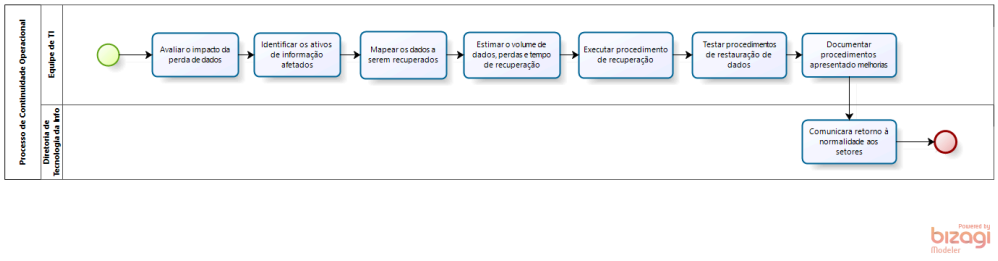


Figura 1 - Processo de continuidade operacional

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 ETIR juntamente com a Diretoria de Tecnologia da Informação devem identificar a ocorrência do incidente ou crise e verificar a dimensão do impacto, extensão e possíveis desdobramentos. Após a avaliação deve ser registrado o impacto por meio de um relatório de perda de dados.

2.2. Identificar ativos de informação afetados

A ETIR deve identificar e listar todos os ativos danificados com a ocorrência do desastre. Esta equipe deve emitir um relatório dos ativos afetados.

2.3. Mapear os dados a serem recuperados

A ETIR deve 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 deve 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 ETIR deve 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 ETIR 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 ETIR deve 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 deve ser documentado e formalmente divulgado. Essa divulgação deve 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:

a) 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;

b) ETIR: equipe 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 deve 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, redes e segurança da informação. Esta equipe deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido e divulgar informações para as demais equipes envolvidas**.**

4. ATIVAÇÃO E ENCERRAMENTO DO PCO

A ativação do PCO deve ser 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 deve 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 deve 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

6. ATIVIDADES, TAREFAS E AÇÕES DO PCO

Uma vez restabelecidos os serviços de TI, a Diretoria de Tecnologia da Informação deve emitir um parecer relatando as atividades realizadas neste PCO. Este setor também deve informar às partes interessadas a normalização dos recursos, serviços e sistemas informatizados do IFTO. Para garantir a normalidade dos serviços de TI, devem ser 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).	- Área de Infraestrutura.
Manter funcionando os equipamentos de climatização da sala de equipamentos.	
Garantir a integridade dos ativos de rede para reconexão.	- Área 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

Para a realização das atividades e tarefas definidas no PCO a Diretoria de Tecnologia da Informação juntamente com os setores envolvidos deve elaborar *checklist* para cada ação de contingência. Estes documentos devem 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 as 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.

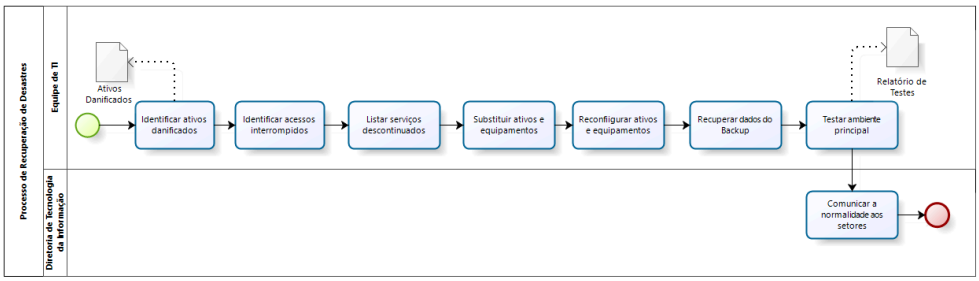


Figura 1 - Processo de recuperação de desastres

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 ETIR deve identificar e lista todos os ativos danificados na ocorrência do desastre. Este relatório deve ser compartilhado com todos os servidores envolvidos na recuperação de desastres.

2.2. Identificar acessos interrompidos

A ETIR deve 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 devem ser registradas em um relatório de acessos interrompidos.

2.3. Listar serviços descontinuados

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

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

2.5. Recuperar dados do backup

A ETIR deve mensurar o tempo necessário para a recuperação dos dados do *backup*. Após a estimativa de tempo de recuperação deve 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 deve 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 devem 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 devem ser automatizados.

3. PAPÉIS E RESPONSABILIDADES

A fim de não sobrepor atividades e duplicar estruturas organizacionais, cabe 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 deve ter minimamente:

a) Área de Infraestrutura: responsável por garantir segurança do retorno às instalações do IFTO que deve verificar os níveis mínimos aceitáveis de fornecimento de serviços. Esta equipe deve 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) Área 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 deve ser feita pela Diretoria de Tecnologia da Informação. Este plano de ação deve ser encerrado assim que os procedimentos de recuperação forem realizados pela equipe de TI.

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

O PRD deve 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 deve manter atualizada toda documentação inerente a desastre visando a melhoria contínua. A tabela 1 apresenta a autoridade responsável pelo PRD.

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

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 deve 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.	Área de TI
Identificar todos os ativos danificados.	1.Identificar e listar todos os ativos danificados da ocorrência do incidente ou desastre.	Área 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.	Área de TI
Listar serviços descontinuados.	1.Mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão.	Área de TI
Substituir ativos e equipamentos danificados.	1. Substituir ativos perdidos.	Área de TI
Reconfigurar ativos e equipamentos.	1. Reconfigurar ativos que podem ser reparados ou reconfigurados.	Área 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.	Área 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 dados.	Área de TI
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 de energia funcionando. 2. Garantir o restabelecimento de energia elétrica através de contingência (gerador) ou concessionária se disponível. 3. Restabelecer os equipamentos de climatização do Datacenter e suas automações.	Área de Infraestrutura

Fonte: Diretoria de Tecnologia da Informação

7. PROCEDIMENTOS DE RECUPERAÇÃO

Conforme descrito na ABNT ISO 22313 (2020), os procedimentos de continuidade de serviços de TI devem 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 ETIR deve 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 foi realizada a contratação nuvem computacional. Este contrato prevê os 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 deve 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 PCN possa atender satisfatoriamente aos seus propósitos. Os testes devem ser planejados e executados com periodicidade mínima anual a partir da data de sua publicação.

O PCN deve 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.

1.1. Escopo

Apresentar o plano de ação para realização de testes do PCN.

1.2. Objetivos

O plano de testes e validação tem por objetivo principal assegurar a eficiência e a efetividade do PCN.

1.3. Abrangência

Este plano abrange todos os serviços de TI considerados como essenciais no PCN.

2. TESTES

Os testes devem 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 pode realizar os seguintes tipos de testes:

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

b) Teste total: conduzido assim que o PCN for concluído. Deve ser realizado de forma periódica. Deve 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: deve 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 será da Diretoria de Tecnologia da Informação que definirá a equipe de testes que trabalhará conjuntamente com a equipe de TI. Os testes devem ser revistos de acordo com:

a) Mudanças nos processos organizacionais da instituição;

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 da restauração de recursos, sistemas de informação e serviços de TI definidos no Plano de Continuidade de Negócios, a área de TI deve configurar um ambiente de restauração de dados contendo minimamente:

a) Contratação de Nuvem Computacional;

b) Contratação de Link de Internet Redundante;

c) Contratação de Software.

ANEXO V

PREVISÃO ORÇAMENTÁRIA PARA INFRAESTRUTURA REDUNDANTE

Ação	Valor Estimado por Ano
Contratação de Nuvem Computacional.	R$ 80.814,48
Contratação de Link de Internet Redundante.	R$ 17.270,52
Contratação de Software (Colaboração e Produtividade).	R$ 204.400,00
Software de *Backups.*	R$ 210.000,00
Equipamentos de Infraestrutura de Redes.	R$ 721.933,63

TOTAL ESTIMADO DE CUSTO ANUAL	**R$ 1.234.418,63**

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 19/12/2023, às 11:09, 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 **Kleyton Matos Moreira**, **Diretor**, em 22/12/2023, às 16:22, 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 **2218376** e o código CRC **425EA50A**.