



**RESOLUÇÃO Nº 03, DE 26 DE AGOSTO DE 2022,
DO COMITÊ DE GOVERNANÇA DIGITAL**

Dispõe sobre o Sistema Gestor de Continuidade de Negócios de TIC do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, no uso das atribuições que lhe foram conferidas pelo Art. 6º, inciso IV e Art. 9º, deste comitê.

RESOLVE:

Art. 1º Aprovar a revisão do Sistema Gestor de Continuidade de Negócios do IFSC.

Art. 2º Esta Resolução entra em vigor na data de 01 de novembro de 2022.

Jesué Graciliano da Silva
Presidente do Comitê de Governança Digital

Súmula da reunião do CGD disponível em:
<https://sigrh.ifsc.edu.br/sigrh/downloadArquivo?idArquivo=2825847&key=1f546b9deb9b38d3c5a9bf9f59bbdb43>

Sistema Gestor de Continuidade de Negócios de Tecnologia da Informação e Comunicação



**INSTITUTO
FEDERAL**
Santa Catarina



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA

**Sistema Gestor de Continuidade de Negócios de Tecnologia da
Informação e Comunicação**
SGCN - TIC

COMITÊ DE GOVERNANÇA DIGITAL

Presidência

Jesué Graciliano da Silva

Pró-reitor de Desenvolvimento Institucional

Secretário-Executivo

Benoni de Oliveira Pires – Diretor de TIC

Membros do Comitê de Governança Digital

Titulares

Aloísio da Silva Júnior – Pró-reitor de Administração

Jesué Graciliano da Silva – Pró-reitor de Desenvolvimento Institucional

Adriano Larentes da Silva – Pró-reitor de Ensino

Valter Vander da Silveira – Pró-reitor de Extensão e Relações Externas

Flavia Maia Moreira – Pró-reitora de Pesquisa, Pós-Graduação e Inovação

Tiago Semprebom – Colégio de Dirigentes (São José)

Daniel Fernando Carossi – Colégio de Dirigentes (São Lourenço do Oeste)

Evaristo Marcos de Quadros Júnior – Encarregado do Tratamento dos Dados Pessoais

Suplentes

Eliana Cristina Bar – Colégio de Dirigentes (Palhoça)

José Roberto Machado – Colégio de Dirigentes (Jaraguá do Sul)

Sumário

HISTÓRICO DE VERSÕES	7
TERMOS E ABREVIACIONES	8
APRESENTAÇÃO	10
INTRODUÇÃO	10
DOCUMENTO	10
METODOLOGIA DE TRABALHO	10
DOCUMENTOS DE REFERÊNCIA	11
VIGÊNCIA	11
ABRANGÊNCIA	11
REVISÕES	11
APROVAÇÃO E PUBLICAÇÃO	11
INVOCAÇÃO DO PLANO	11
VALIDAÇÃO DO PLANO	11
SETORES ENVOLVIDOS NOS PLANOS	11
CONCEITOS E DEFINIÇÕES	12
OBJETIVO	14
PROCEDIMENTOS	16
IMPACTO NO NEGÓCIO	17
PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)	19
OBJETIVO	20
ESCOPO	20
PAPÉIS E RESPONSABILIDADES	20
AUTORIDADES RESPONSÁVEIS	21
ATIVIDADES E PAPÉIS PRINCIPAIS	21
CONDIÇÕES PARA A ATIVAÇÃO DO PLANO	21
DETALHES DE CONTATO	22
LISTA DE TAREFAS E AÇÕES	22
COMUNICAÇÃO À MÍDIA	23
LOCALIZAÇÃO PARA O GERENCIAMENTO DE INCIDENTES	23
ENCERRAMENTO DO PLANO DE GERENCIAMENTO DE CRISES	23
PLANO DE CONTINGÊNCIA (PC)	24
OBJETIVO	25
ESCOPO	25

LISTA DE ATIVIDADES	26
PAPÉIS, RESPONSABILIDADES E AUTORIDADES	27
DETALHES DE CONTATO	27
CAMPUS E ÁREAS AFETADAS	27
NOTIFICAÇÕES E COMUNICADOS	27
SOLUÇÕES FÍSICAS E LÓGICAS	28
INFRAESTRUTURA E ACESSOS FÍSICOS	28
SOLUÇÕES PARA CONTINGÊNCIAS PREVISTAS	29
ENCERRAMENTO DO PLANO DE CONTINGÊNCIA	29
PLANO DE CONTINUIDADE OPERACIONAL (PCO)	30
OBJETIVO	31
ESCOPO	31
PAPÉIS E RESPONSABILIDADES	31
LISTA DE ATIVIDADES	32
RECURSOS NECESSÁRIOS	32
ENCERRAMENTO DO PLANO DE CONTINUIDADE OPERACIONAL	33
PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)	34
OBJETIVO	35
ESCOPO	35
PAPÉIS E RESPONSABILIDADES	35
RESTAURAÇÃO EM CASO DE DESASTRES	36
AUTORIDADE RESPONSÁVEL	37
LISTA DE TAREFAS	37
RECURSOS NECESSÁRIOS	37
ENCERRAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES	38
REFERÊNCIAS	39
APÊNDICES	41
APÊNDICE I	41
APÊNDICE II	42
APÊNDICE III	43

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
14/12/2018	Versão 1.3	Sistema de Gestão de Continuidade de Negócios - Geral
14/12/2018	Versão 1.3	Plano de Contingência - PC
14/12/2018	Versão 1.3	Plano de Continuidade Operacional - PCO
14/12/2018	Versão 1.3	Plano de Recuperação de Desastres - PRD
14/12/2018	Versão 1.3	Plano de Administração de Crises - PAC
26/08/2022	Versão 2.0	Revisão 2022 do Comitê de Governança Digital.

TERMOS E ABREVIações

- ABNT** - Associação Brasileira de Normas Técnicas
- AIN** - Análise de Impacto de Negócio
- BIA** - *Business Impact Analysis* (Análise de Impacto de Negócios)
- CAFe** - Comunidade Acadêmica Federada
- CIR** - Coordenadoria de Infraestrutura de Redes
- CISSP** - Comissões Internas de Saúde do Servidor Público
- CGTI** - Coordenadoria de Governança de Tecnologia da Informação
- CODIR** - Colégio de Dirigentes
- CONSUP** - Conselho Superior
- CGD** - Comitê de Governança Digital
- COE** - Coordenação de Engenharia
- CSIRT** - Equipe de Tratamento e REspostas a Incidentes Cibernéticos
- CTIC** - Coordenação de Tecnologia da Informação e Comunicação dos Câmpus do IFSC
- DIRCOM** - Diretoria de Comunicação Institucional
- DNS** - *Domain Name System*
- DOE** - Departamento de Obras e Engenharia
- DSI** - Departamento de Sistemas de Informação
- DTIC** - Diretoria de Tecnologia da Informação e Comunicação
- EGD** - Estratégia Governança Digital
- FORTIC** - Fórum de Tecnologia da Informação e Comunicação do IFSC
- GCN** - Gestão de Continuidade de Negócios
- GTIS** - Grupo de Tratamento de Incidentes de Segurança
- IFSC** - Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina
- NBR** - Norma Brasileira
- PAC** - Plano de Administração de Crises
- PC** - Plano de Contingência
- PCN** - Plano de Continuidade de Negócios
- PCO** - Plano de Continuidade Operacional
- PDCA** - *Plan, Do, Check, Act* (Planejar, Fazer, Checar, Agir)
- PDI** - Plano de Desenvolvimento Institucional
- PDTIC** - Plano Diretor de Tecnologia da Informação e Comunicação
- PETIC** - Planejamento Estratégico de Tecnologia da Informação e Comunicação
- PN** - Processo de Negócio
- POP-SC** - Ponto de Presença de Santa Catarina
- POSIC** - Política de Segurança da Informação
- PRD** - Plano de Recuperação de Desastres
- REMEP** - Rede Metropolitana
- RNP** - Rede Nacional de Pesquisa
- SETIC** - Secretaria de Tecnologia da Informação e Comunicação
- SGCN** - Sistema Gestor de Continuidade de Negócios
- SISP** - Sistema de Administração de Recursos de Tecnologia da Informação

TCU - Tribunal de Contas da União

TI - Tecnologia da Informação

TIC - Tecnologia da Informação e Comunicação

UFSC - Universidade Federal de Santa Catarina

UN - Unidade de Negócio

Câmpus

FLN Câmpus Florianópolis

REI Reitoria

SJE Câmpus São José

Reitoria

PROAD Pró-Reitoria de Administração

PRODIN Pró-Reitoria de Desenvolvimento Institucional

PROEN Pró-Reitoria de Ensino

PROEX Pró-Reitoria de Extensão e Relações Externas

PROPPI Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação

APRESENTAÇÃO

INTRODUÇÃO

O Sistema Gestor de Continuidade de Negócios (SGCN) inclui estruturas organizacionais, políticas, atividades de planejamento, responsabilidades, procedimentos, processos e recursos.

O Sistema Gestor de Continuidade de Negócios (SGCN) fornece estratégias para garantir que serviços essenciais sejam identificados, para garantir sua preservação após a ocorrência de um desastre e até o retorno da situação normal de funcionamento da instituição. Este plano de continuidade será de nível mais macro, dividido em 4 (quatro) planos menores (Plano de Contingência, Plano de Continuidade Operacional, Plano de Recuperação de Desastres e Plano de Administração de Crises), os quais proverão basicamente: objetivo, escopo, papéis, responsabilidades e autoridades, condições de ativação do plano, procedimentos que devem ser adotados, comunicação em caso de ocorrência de desastres e encerramento do plano.

Para cada um dos planos menores deverá ser feito Planos de Ações, e estes deverão ser elaborados assim que dar-se os ocorridos, com base na sua temporalidade e impacto. Estes devem formar um banco de ações, para que para cada acontecimento seja possível verificar o que foi feito em outros momentos similares.

Os Planos de Ações serão incluídos como Apêndices Externos ao SGCN e é de responsabilidade das áreas detentoras da ação realizada para resolução do evento.

DOCUMENTO

O Sistema Gestor de Continuidade de Negócio de TIC do Instituto Federal de Santa Catarina é um instrumento que tem por objetivo a redução da interrupção das atividades do negócio e proteção dos processos críticos contra defeitos, falhas ou desastres, garantindo a retomada em tempo hábil, caso necessário.

O SGCN é formado por procedimentos e documentos, no intuito de orientar o IFSC a responder, recuperar, retomar e restaurar um nível pré-definido de operação após um desastre ou incidente que interrompa as atividades críticas do IFSC.

METODOLOGIA DE TRABALHO

O processo de elaboração do SGCN baseou-se em normas e pesquisas de outras instituições, e de capacitação fornecida pela Escola Superior de Redes (ESR) dentro das melhores práticas para a construção de um Sistema de Gestão de Continuidade de Negócios.

As atividades foram desenvolvidas pela Coordenadoria de Governança de TIC, de forma colaborativa, com reuniões presenciais para alinhamento do plano com as políticas institucionais. Estas atividades tiveram início em Março de 2018 e conclusão em Outubro de 2018, com apreciação do extinto Comitê Gestor de Tecnologia da Informação e Comunicação, hoje Comitê de Governança Digital.

Este documento foi aprovado pelo extinto Comitê Gestor de Segurança da Informação e Comunicação em 14 de Dezembro de 2018, hoje Comitê de Governança Digital.

Na revisão de 2022, foram realizadas reuniões entre Março de 2022 e Abril de 2022, com apreciação e aprovação posterior do Comitê de Governança Digital do IFSC.

A revisão foi aprovada pelo Comitê de Governança Digital em 28 de agosto de 2022.

DOCUMENTOS DE REFERÊNCIA

1. Política de Segurança da Informação e Comunicação do IFSC;
2. Sistema de Governança de TIC do IFSC;
3. Plano de Gestão de Riscos do IFSC;
4. Política de Backup do IFSC;
5. Plano de Backup do IFSC;
6. Guia de Governança de TIC do SIS.

VIGÊNCIA

O SGCN-TIC terá vigência de 4 (quatro) anos a partir de sua última atualização.

ABRANGÊNCIA

O SGCN-TIC tem abrangência em todo o IFSC.

REVISÕES

A revisão dos Planos é realizada nas seguintes situações:

1. A cada 2 (dois) anos;
2. Nos momentos em que a CGD julgar necessário; ou
3. Em função dos resultados dos testes realizados; ou
4. Após ocorrência de algum evento ou mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

APROVAÇÃO E PUBLICAÇÃO

O SGCN-TIC foi submetido para avaliação nos seguintes fóruns e colegiados:

1. CGD (Apreciação e aprovação)

O SGCN-TIC deverá ser publicado no Portal do IFSC no seguinte endereço:
<<http://www.ifsc.edu.br/tecnologia-da-informacao>>.

INVOCAÇÃO DO PLANO

O presente plano será acionado quando a ocorrência de algum desastre, na ocorrência de um risco não conhecido, ou caso uma vulnerabilidade tenha grande probabilidade de ser explorada.

Também poderá ser acionado o plano quando ocorrer a necessidade de testes ou por determinação do CGD.

VALIDAÇÃO DO PLANO

O Sistema Gestor de Continuidade de Negócios de TIC será validado em reuniões do CGD (Comitê de Governança Digital), em reuniões específicas para esse fim.

SETORES ENVOLVIDOS NOS PLANOS

Abaixo são listados os setores que deverão estar envolvidos na Contingência de TIC:

Alta Gestão:

Reitor(a);

Pró-reitores(as);

Diretor(a)-executivo(a).

Setores e seus titulares:

Diretor de TIC

Chefe do Departamento de Sistemas (DSI);

Coordenador(a) de Infraestrutura e Redes (CIR);

Coordenador(a) de Governança de TIC (CGovTI);

Departamento de Obras e Engenharia do IFSC (DOE);

Coordenadoria de Engenharia (COE).

Representantes delegados:

Comitê de Governança de TIC (CGD);

Comitê Técnico de Tecnologia da Informação e Comunicação (CTTIC)

Comitê Técnico de Segurança da Informação (CTSI)

Comitê Permanente de Gestão de Crises.

Equipe de Tratamento e Resposta a Incidentes Cibernéticos (CSIRT)

CONCEITOS E DEFINIÇÕES

Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços.

Atividades Críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

Análise de Impacto nos Negócios (AIN) ou Business Impact Analysis (BIA): visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da APF, bem como as técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

Ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

Desastre: Evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.

Data center: Todo espaço nos quais ficam os Ativos de Informação, bem como suas estruturas auxiliares como No-Break, Banco de Baterias e Gerador de Energia Elétrica.

Estratégia de Continuidade de Negócios: abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior.

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

Sistema de Gestão da Continuidade de Negócios (SGCN): conjunto de elementos de gestão do IFSC que estabelece, implementa, opera, monitora, analisa criticamente, mantém e aprimora a continuidade de negócios.

Incidente: evento que tenha causado algum dano, colocado em risco, algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

Plano de Continuidade de Negócios: A continuidade de negócios é a capacidade que uma organização tem de continuar a entrega de produtos ou serviços em níveis aceitáveis pré-definidos após um incidente de interrupção.

Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

Plano de Recuperação de Negócios: documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas à normalidade.

Programa de Gestão da Continuidade de Negócios: processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio análises críticas, testes, treinamentos e manutenção.

Tempo Objetivo de Recuperação: é o tempo predefinido no qual uma atividade deverá estar disponível após uma interrupção ou incidente.

Ações preparatórias são realizadas apenas uma vez, e servem para preparar o terreno para uma eventual utilização do Plano. São exemplos: preparar um ambiente de trabalho alternativo por meio de acordo de cooperação, elaborar manuais de sistemas, mapear processos de trabalho etc.

Ações rotineiras são aquelas que devem ser realizadas com periodicidade determinada, servindo para manter atualizado o Plano, bem como informações vitais a ele. São exemplos: Manter cópia atualizada dos documentos de GCN em local de fácil acesso, atualizar a lista de contatos etc.

OBJETIVO

O SGCN deverá estabelecer cenários de situações inesperadas ou incidentes (quer sejam operacionais, desastres ou crises), além de formas de gerenciar os impactos imediatos de um incidente de interrupção, dando a devida atenção para:

1. Bem-estar dos públicos internos e externos conforme a Política de Comunicação do IFSC;
2. Alternativas estratégicas, táticas e operacionais para responder à interrupção;
3. Prevenção de novas perdas ou indisponibilidade de atividades prioritárias;
4. Detalhes sobre como e em que circunstâncias o IFSC irá se comunicar com as partes interessadas e seus familiares ou contatos de emergência.

O SGCN fornece normas e padrões para que o IFSC consiga recuperar, retomar e dar continuidade aos seus processos de negócios mais cruciais, evitando que eles sofram danos maiores. Ao passo que pequenas organizações podem incluir seus planos em apenas um documento, o SGCN do IFSC é dividido em quatro (4) planos menores:

1. **Plano de Administração de Crises:** Define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência;
2. **Plano de Contingência:** Define as necessidades e ações mais imediatas. Deve ser utilizado somente quando todas as prevenções tiverem falhado;
3. **Plano de Recuperação de Desastres:** Determina o planejamento para que, uma vez controlada a contingência e passada a crise, sejam retomados os níveis originais de operação;
4. **Plano de Continuidade Operacional:** Seu objetivo é restabelecer o funcionamento dos principais ativos que suportam as operações da instituição, reduzindo o tempo de queda e os impactos provocados por um eventual incidente.

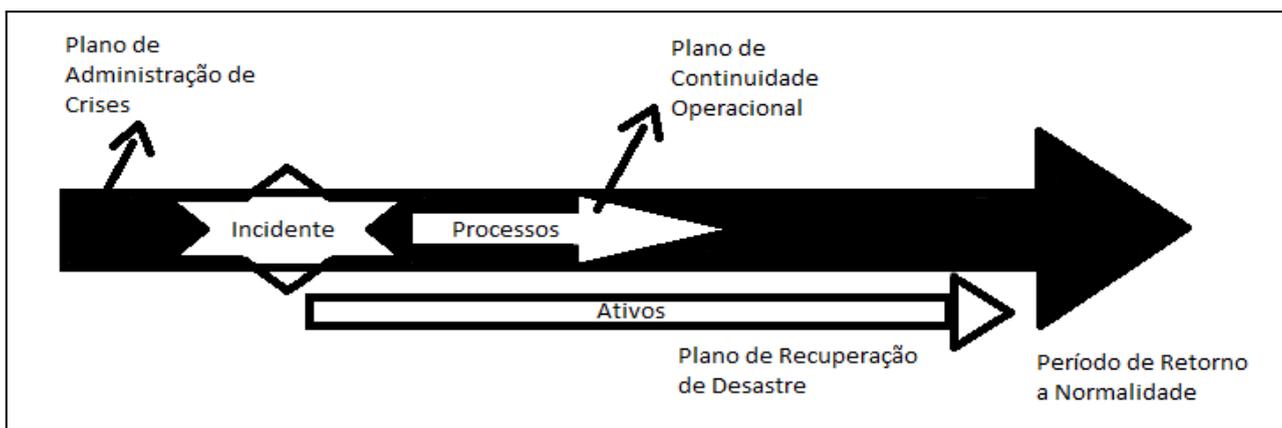


Imagem 1 - Ordem Cronológica dos Planos

Os planos aqui definidos seguirão o Modelo “Plan-Do-Check-Act” (PDCA) para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente a eficácia do Sistema Gestor de Continuidade de Negócios (SGCN) de TIC do IFSC.

Modelo PDCA: O modelo PDCA ajudará na melhoria contínua do Sistema de Gestão de Continuidade de Negócios.

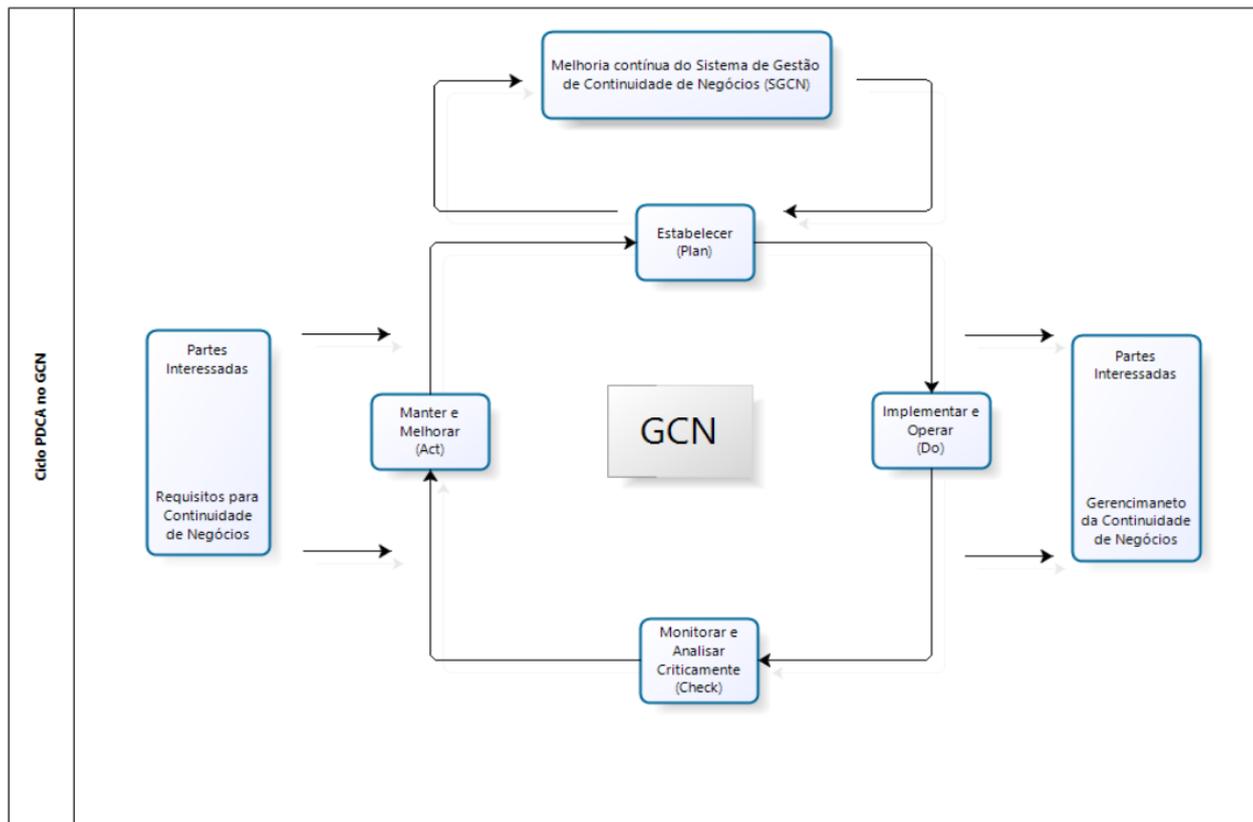


Imagem 2 - Ciclo PDCA no Gestão de Continuidade de Negócios

Plan (estabelecer) - Seguir uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimento pertinentes para a melhoria da continuidade de negócios, de forma a ter resultados alinhados com os objetivos.

Do (Implementar e operar) - Implementar e operar a política de continuidade de negócios, controles, processos e procedimentos.

Check (Monitorar e analisar criticamente) - Monitorar e analisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a direção para análise crítica, e definir e autorizar ações de melhorias e correções.

Act (Manter e Melhorar) - Manter e melhorar o SGCN tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica da direção e reavaliando o escopo do SGCN e as políticas e objetivos de continuidade de negócios.

Há um ciclo básico de atividades a ser seguido, recomendado pela NBR 15999, para a realização de um bom SGCN e que segue o modelo PDCA:

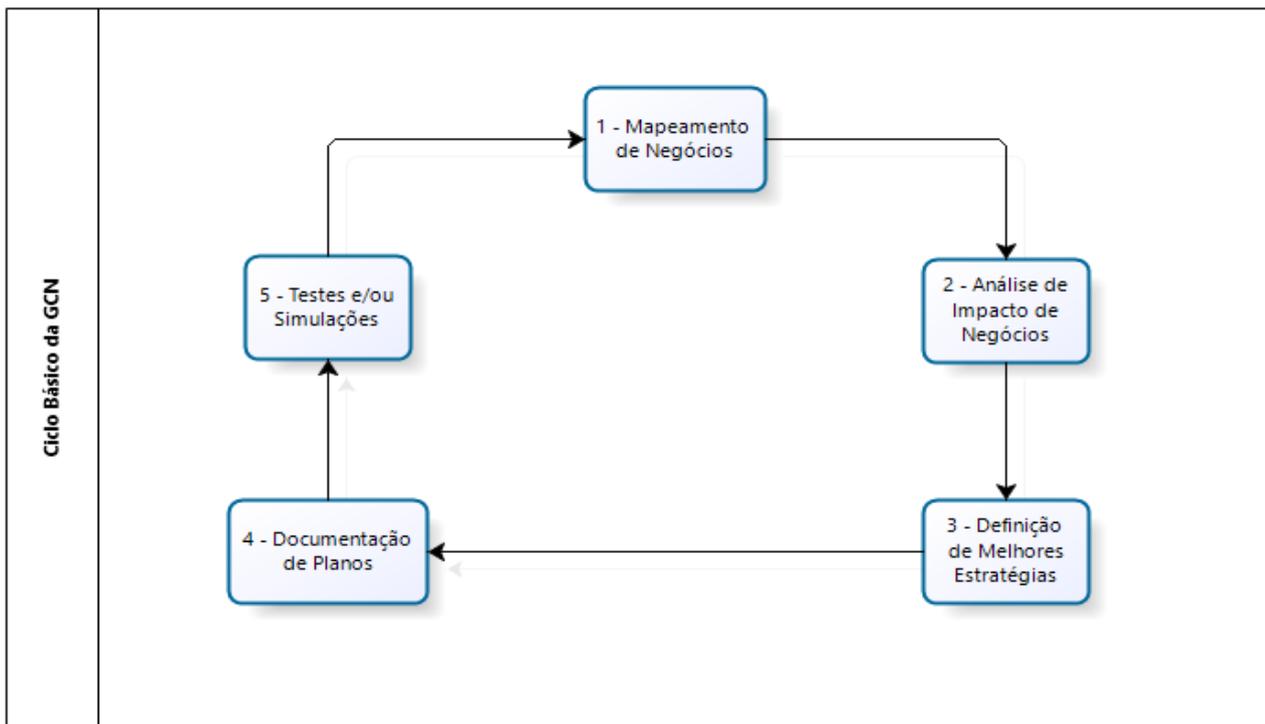


Imagem 3 - Ciclo Básico do GCN

PROCEDIMENTOS

1. Identificar processos de negócio de TIC
 - a. Identificar todos os processos de negócio de TIC, definindo atividades críticas e ranqueando-as.
2. Definir, implementar e manter um processo formal e documentado para a Análise de Impacto nos Negócios, incluindo:
 - a. identificação das atividades que suportam os serviços críticos de TI do IFSC;
 - b. avaliação dos impactos de não realização das atividades críticas ao longo do tempo;
 - c. fixação dos prazos de forma priorizada para a retomada das atividades, em um nível mínimo de execução tolerável, levando em consideração o tempo em que os impactos da interrupção tornem-se inaceitáveis;
 - d. identificação de interdependências e recursos que suportam as atividades, incluindo fornecedores, terceiros e demais partes interessadas relevantes.
3. Determinar estratégias de continuidade de negócios adequada para proteger, estabilizar, continuar, retomar e recuperar as atividades prioritárias, bem como suas interdependências e recursos de apoio;
 - a. Plano de Administração de Crises.
4. Estabelecer níveis adequados de autoridade e competência, no intuito de assegurar a comunicação efetiva às partes interessadas, bem como assegurar a continuidade das atividades críticas;
 - a. Plano de Continuidade Operacional.
5. Viabilizar a continuidade e a recuperação das atividades críticas, em caso de interrupção;

- a. Plano de Recuperação de Desastres;
 - b. Plano de Contingência.
6. Realizar treinamentos e avaliações do SGCN periodicamente para garantir a manutenção e o bom funcionamento dos planos de continuidade.
- a. Realizar testes para garantir a eficiência da continuidade de negócios;
 - b. Promover a conscientização dos servidores;
 - c. Identificar oportunidades para melhorar a continuidade de negócios.

IMPACTO NO NEGÓCIO

O BIA (Business Impact Analysis - Análise de Impacto de Negócios) identifica Unidades e Processos essenciais para a sobrevivência de uma instituição e dessa forma, quais precisam voltar em completo funcionamento após um desastre. Também identifica os recursos necessários para retornar às operações de negócios.

A análise de impacto no negócio existe para definir parâmetros sobre o **prazo requerido na recuperação dos serviços** (Indisponibilidade Máxima Aceitável/Objetivo para o Tempo de Recuperação - *Maximum Acceptable Outage/Recovery Time Objective*), e o **momento requerido para suas cópias de segurança** (Objetivo para Ponto de Recuperação/Perda Máxima de Dados - *Recovery Point Objective/Maximum Data Loss*). Parâmetros estes que serão calculados após elaboração de questionários e tabulação de levantamento de riscos.

Os questionários são elaborados para obter informações para elaboração do(s):

1. Sistemas/processos críticos de negócio sob responsabilidade da TIC;
2. Grau de criticidade dos sistemas/processos críticos;
3. Tempo máximo de paralisação;
4. Tempo objetivado de paralisação;
5. Ponto objetivado de paralisação;
6. Impactos a serem considerados.

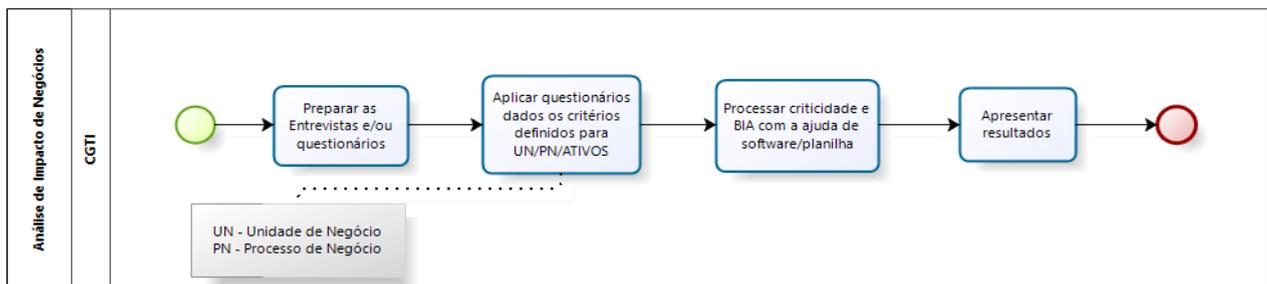


Imagem 4 - Análise de Impacto de Negócio - BIA

Preparar entrevistas e/ou questionários

Entrevista para detalhamento do Processo de Negócio (PN): este documento visa melhorar o processamento de negócios, considerados críticos diante das ameaças/impactos, de acordo com critérios preestabelecidos, visando orientar a análise de impacto.

Matriz de Cálculo do Custo de Parada de Processamento de Negócio: identificar valores que a instituição pode vir a perder no caso de uma paralisação de um Processo de Negócios ou indisponibilidade de ativos.

Matriz do Cálculo do Custo de Recuperação de Processo de Negócio: identificar valores que a instituição deve dispensar para a aquisição de novos ativos para a recuperação de um Processo de Negócio.

Aplicar questionários dados os critérios definidos

Trata-se da aplicação efetiva dos questionários.

Processar criticidade e BIA

Alimentação dos dados em sistema/planilha para o processamento e consequente obtenção dos resultados. Primeiramente se faz a análise da criticidade e após, avaliação de todos os impactos (financeiro, legal, operacional, administrativo, de recursos humanos, imagem).

Apresentar resultados

Estruturação das informações, e para cada realidade e necessidade da instituição. Apresentação na forma de discutir e corrigir o que for necessário.

Considera-se que comunicação é a parte mais importante do Plano de Continuidade de Negócios, pois uma apresentação pode não refletir adequadamente as questões relevantes para a alta administração.

Particularização do BIA

Esta etapa mensura o custo de uma paralisação dos negócios e ativos. Deve informar o valor que se perde com a ocorrência de um incidente.

A critério de exemplificar a estrutura deste documento, apresenta-se uma tabela referência:

Ameaças	Impacto	Valor	Importância	Procedimento
Defeito de Hardware	Direto	Alto	1	Utilizar redundância ou comprar novo equipamento
Ataques à Sistemas	Direto	Alto	2	Mapeamento e fechamento da falha
Desatualização de Softwares	Indireto	Médio	3	Atualização
Falha estrutural	Indireto	Baixo	4	Buscar área responsável

Tabela 1 - Mensuração de Custo de Negócio



PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

OBJETIVO

O PAC busca definir ações e responsabilidades das equipes envolvidas com o acionamento da contingência, antes, durante e após a ocorrência do desastre. Ele consiste em administrar todos os outros planos de Continuidade.

Representa a garantia mais eficaz em termos de administração em situações adversas. O PAC relaciona o funcionamento das equipes (recursos humanos) antes, durante e depois da ocorrência do evento. Através deste programa são definidos os planos de ação para o retorno à normalidade num determinado período.

No PAC também é definido o ciclo de capacitações e treinamentos do pessoal envolvido, divulgações, programação de testes e gerenciamento de resultados.



Imagem 5 - Tempo do PAC

ESCOPO

A abrangência deste plano é focada nas equipes (recursos humanos) e leva em conta os fatores históricos. Também considera os fatos que estão ocorrendo e por fim as ações futuras, que são delimitadas somente após a ocorrência de um evento.

PAPÉIS E RESPONSABILIDADES

Diretoria de Tecnologia da Informação e Comunicação (DTIC) - Diretoria responsável por orquestrar ações de suas coordenações durante eventuais disrupções e suas consequências.

Coordenadoria de Infraestrutura e Redes (CIR) - Responsável pelas ações de manutenção dos serviços de redes e infraestrutura do data center do IFSC, bem como configuração e instalação de sistemas em geral. Deve ser acionada sempre que houverem disrupções nos serviços de internet, intranet e aplicações fora do ar.

Departamento de Sistemas (DSI) - Atua na parte de parametrização e programação de sistemas, bem como na manutenção de aplicações institucionais. Deve ser acionada no caso de bugs ou defeitos que impossibilitam o uso mínimo das ferramentas de software hospedadas no IFSC.

Coordenação de Governança de TI (CGTI) - Trabalha como setor de regulação e regulamentação, atuando na parte de planejamento e projetos de TI sempre que solicitada. Atende demandas de órgãos de controle, como auditorias externas e internas, referentes a planos ou políticas que dizem respeito a organização da TI.

Coordenadoria de TIC dos Câmpus (CTICs) - Equipe responsável pelas ações de manutenção dos serviços de voz/dados e computadores dos câmpus, bem como

configuração e instalação de sistemas que eventualmente estão sob responsabilidade do Câmpus.

Departamento de Obras e Engenharia do IFSC (DOE) - Departamento responsável por viabilizar a gestão de equipes no que tange a manutenção da infraestrutura da Reitoria.

Coordenadoria de Engenharia (COE) - Equipe que é responsável por assegurar e garantir o cumprimento de serviços como Energia Elétrica e climatização do data center.

Diretoria de Comunicação (DIRCOM) - Equipe responsável por garantir o fluxo de informações aos diversos públicos, bem como assessorar possíveis comunicados aos públicos do IFSC.

AUTORIDADES RESPONSÁVEIS

As autoridades designadas neste plano seguirão a seguinte linha decisória:

1. Reitor(a)
2. Pró-Reitor(a) de Desenvolvimento Institucional (PRODIN)
3. Diretor(a) de TIC
4. Coordenadoria de Governança de TI (CGovTI)

ATIVIDADES E PAPÉIS PRINCIPAIS

Caberá ao mais alto Gestor de TI em exercício, atuar como elo de ligação entre o corpo técnico e as áreas interessadas ou afetadas pela não Continuidade de Negócios. Além disso, poderá ter representação pontual no Comitê Permanente de Gestão de Crises, sempre que a crise for relacionada à Tecnologia da Informação e Comunicação.

CONDIÇÕES PARA A ATIVAÇÃO DO PLANO

Na ocorrência de um desastre, as respectivas áreas deverão informar os respectivos órgãos:

1. A Pró-reitoria de Administração - PROAD deve comunicar às autoridades competentes, quando em caso de catástrofe, principalmente se envolver risco às pessoas.

Autoridade	Telefone	Data/Hora Registro
Corpo de Bombeiros	193	
SAMU	192	
Polícia Militar	190	
Defesa Civil	199	
Polícia Federal	(48) 3281-6500	

Tabela 2 - Autoridades

2. A Coordenadoria de Engenharia - COE deverá comunicar seus principais prestadores de serviços, entre eles:

Fornecedor	Contato	Data/Hora Registro
Celesc	196	
Casan	195	
Empresa Gerador	(48) 3258-5000	
Empresa No-Break	(47) 9682-2189 0800-771-5555	
Empresa Climatização	(48) 99127-3215 (48) 3258-8786	

Tabela 3 - Prestadores de Serviço de Energia Elétrica e Infraestrutura

3. A Diretoria de TIC - DTIC deve comunicar aos seus principais prestadores de serviços., entre eles:

Fornecedor	Contato	Data/Hora Registro
POP-SC NoC UFSC	(48) 3721-3000	

Tabela 4 - Prestadores de Serviço de Telecomunicações e Data Center

4. A Diretoria de Comunicação - DIRCOM deve comunicar todas as demais unidades e repassar as informações necessárias para os órgãos conforme preconiza a Política de Comunicação do IFSC.

DETALHES DE CONTATO

Conforme preconiza o TCU (Tribunal de Contas da União)¹, no SGCN devem ser listados somente os respectivos cargos e não seus ocupantes. Por sua vez, estes contatos estão listados em um documento à parte, que deve constar como anexo desmembrado da publicação deste documento.

LISTA DE TAREFAS E AÇÕES

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

1. Coordenador de TIC da área afetada pela crise deve avaliar a extensão do que foi avariado;
2. Diretor de TIC deve ser informado para buscar soluções para a gestão da crise;
3. Pró-Reitor(a) de Desenvolvimento Institucional (PRODIN) deve ser informado e consultado;
4. DIRCOM deve ser informada sobre a abrangência e desdobramentos possíveis da crise;
5. Deve-se instituir o Comitê Permanente de Gestão de Crises de acordo com o especificado no Manual de Crises do IFSC, que leva em conta os Câmpus afetados e setores necessários.
6. Montar um centro de Gerenciamento de Incidentes em local disponível e seguro.

¹ <https://portal.tcu.gov.br/comunidades/gestao-de-continuidade-de-negocios/home/>

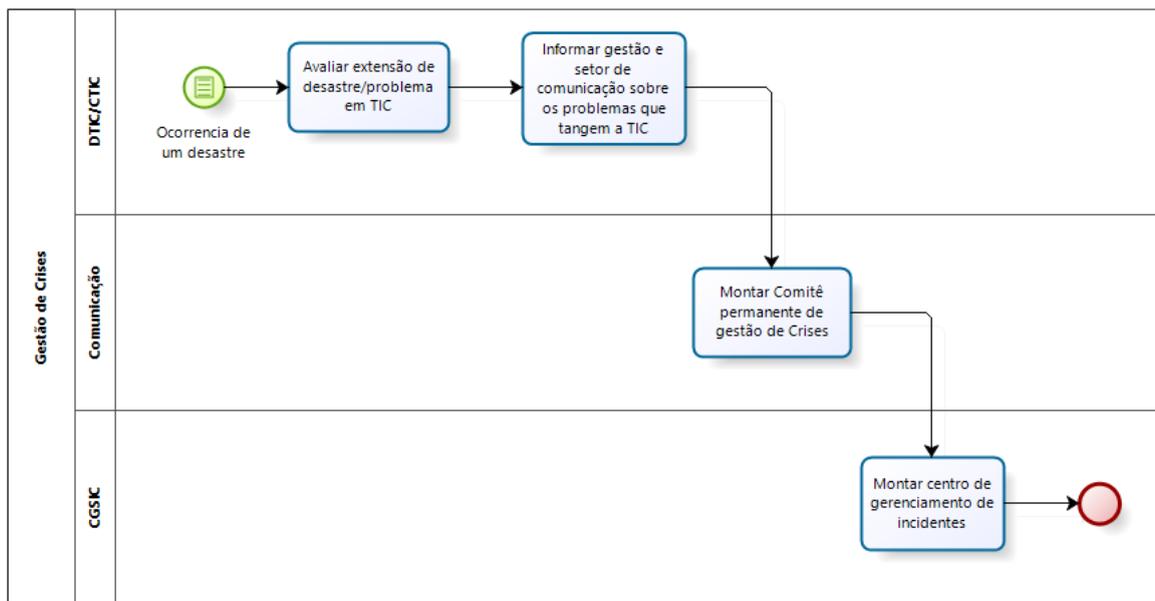


Imagem 6 - Processo Gestão de Crises

COMUNICAÇÃO À MÍDIA

De acordo com Manual de Comunicação do IFSC, deve-se:

“Na ocorrência de uma crise, a Diretoria de Comunicação do IFSC deve ser imediatamente informada dos seus motivos e participar ativamente do processo de gestão a ser implementado para solucioná-la. Sobretudo, deve ser consultada antes que sejam tomadas decisões que impliquem ações específicas de comunicação, como o contato com os públicos estratégicos.”

Sendo assim, cabe a Diretoria de Comunicação do IFSC estabelecer critérios de postura junto ao público externo. Porém, para eventuais comunicados escritos à imprensa por parte do setor de Comunicação, as dúvidas técnicas pertinentes deverão ser relacionadas antes de qualquer publicação, sem exceção. No caso de detalhamento técnico do problema à imprensa falada ou televisiva, o Porta-Voz do IFSC deve ser assessorado por uma pessoa do corpo Técnico de TI, designado pelo mais alto Gestor de TI em exercício.

LOCALIZAÇÃO PARA O GERENCIAMENTO DE INCIDENTES

Deverá ser eleito um local pela autoridade máxima presente, preferencialmente pertencente aos imóveis da União, que ofereça as condições mínimas de trabalho necessárias para que o Comitê Permanente de Gestão de Crises possa se reunir, com todos os membros necessários de acordo com o especificado no Manual de Crises do IFSC.

Em caso da impossibilidade de reunião presencial por qualquer motivo, deve-se buscar meios tecnológicos para comunicação remota entre os membros do Comitê.

ENCERRAMENTO DO PLANO DE GERENCIAMENTO DE CRISES

O plano será encerrado assim que o funcionamento de sistemas essenciais do data center estiverem validados.

A equipe responsável pelo retorno deve emitir um parecer relatando as atividades realizadas para a DTIC (o qual será usado para gerar os Planos de Ações) que por sua vez deve informar do retorno das atividades à instituição.



PLANO DE CONTINGÊNCIA (PC)

OBJETIVO

Este documento busca estabelecer um plano para recuperação após desastres, com objetivo de assegurar o restabelecimento das atividades do IFSC. Seu propósito é listar um conjunto de procedimentos definidos formalmente para permitir que serviços de processamento e armazenamento de dados continuem a operar, mesmo que com um certo grau de degradação, caso ocorra algum evento que não possibilita seu funcionamento normal.

ESCOPO

O Plano de Contingência de TIC está baseado em três vértices

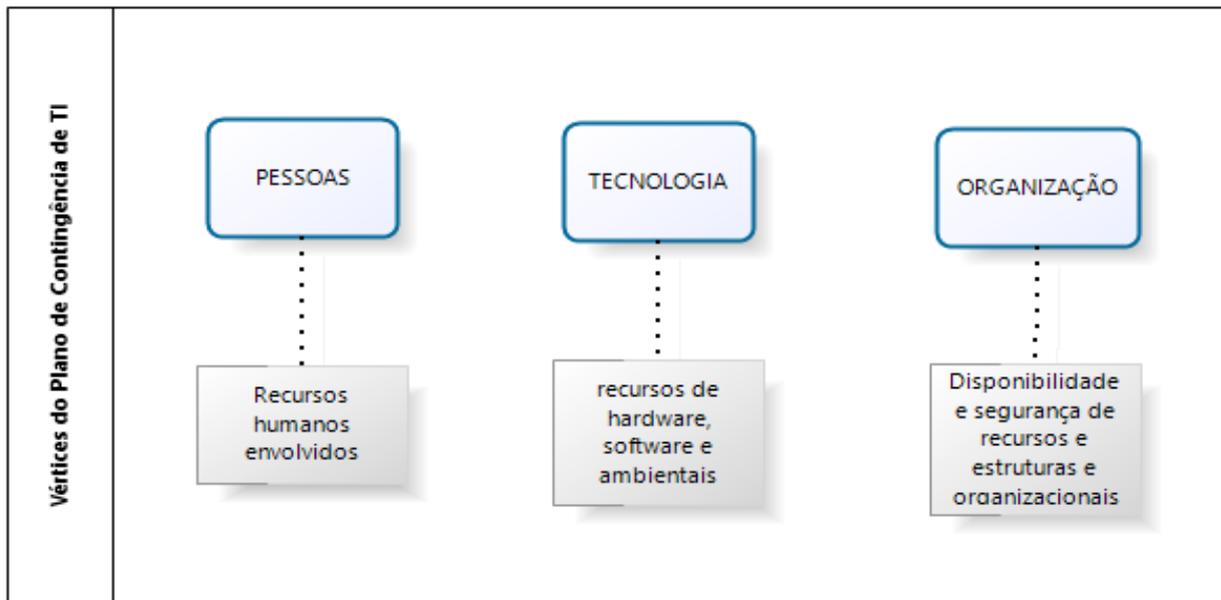


Imagem 7 - Vértices do Plano de Contingência

- Pessoas - que trata dos recursos humanos envolvidos nas atividades em Contingência.
- Organização - que trata especificamente sobre a disponibilidade e segurança de recursos estruturais e organizacionais para suportar as atividades necessárias em Contingência.
- Tecnologia - que contempla os recursos de hardware, software e ambientais apoiados em tecnologias de TI e complementares para atender em contingência.

Este plano de envolve basicamente quatro grupos, a saber:

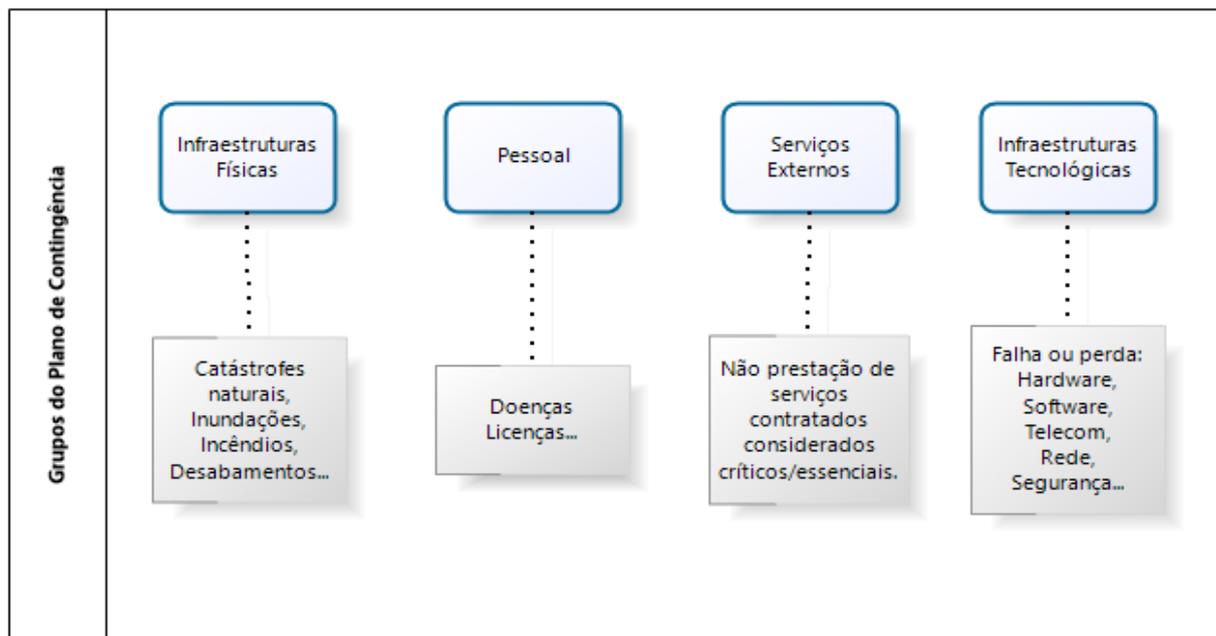


Imagem 8 - Grupos do Plano de Contingência

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

LISTA DE ATIVIDADES

São recomendadas algumas etapas a serem seguidas para um Plano de Contingência de TI:

- Diagnóstico – consiste na identificação dos pontos fracos que poderiam ser foco de problemas para o setor de TI da empresa.
- Análise de riscos – A partir das vulnerabilidades, deve-se considerar as possíveis ameaças e os fatores que possam levar à concretização desses riscos, como o ataque de vírus e a ausência de um antivírus corporativo.
- Definição de prioridades – Identificar os processos vitais da empresa e apontar quais os sistemas que precisam ser recuperados primeiro ou preferencialmente em casos de problemas.
- Determinação de estratégias – Esse é o caminho para se definir como cada sistema deve ser recuperado (usando softwares ou aplicações), quando e quem são os responsáveis por isso.

- Redação e divulgação do documento – o plano de contingência precisa ser detalhadamente redigido e divulgado para que os envolvidos conheçam seus papéis no processo de gerenciamento de crises, bem como as estratégias a serem seguidas em cada caso.

PAPÉIS, RESPONSABILIDADES E AUTORIDADES

Conforme a Resolução Nº 10 de 03 de Dezembro de 2021, a Equipe de Tratamento e Respostas a Incidentes Cibernéticos é instituída em conformidade com normas e procedimentos específicos.

Caberá ao CSIRT a designação dos responsáveis para gerenciar as fases da continuidade e recuperação de negócios, que ocorram após uma interrupção de serviços ou que afetem a normalidade operacional do IFSC.

DETALHES DE CONTATO

De acordo com o TCU (Tribunal de Contas da União)², no SGCN devem ser listados somente os respectivos cargos e não seus ocupantes. Por sua vez, estes contatos deverão ser listados em um documento à parte, que deve ser mantido atualizado e armazenado em diversos meios para que esteja acessível sempre que necessário.

O documento “Contatos de Responsáveis pelo SGCN” é um anexo deste Plano.

CAMPUS E ÁREAS AFETADAS

Em caso de evento ocorrido no data center da Reitoria do IFSC, todos os sistemas serão afetados. Os serviços hospedados na Reitoria ficarão inoperantes, exceto aqueles atualmente operados de forma independente pelos Câmpus ou executados por terceiros:

- Acesso a internet de todos os Câmpus, incluindo os interligados pela REMEP (Rede Metropolitana) são mantidos pelo POP-SC (Ponto de Presença) da RNP (Rede Nacional de Pesquisa) que fica localizado na UFSC (Universidade Federal de Santa Catarina);
- Replicação de serviços de DNS (Domain Name Service) através de um servidor secundário disponibilizado pelo POP-SC provido pela RNP, permitindo a delegação de sub-domínios (ex.: Serviços e sites independentes hospedados nos Câmpus ou Terceiros continuam a operar);
- Serviço de e-mail provido por terceiros (como Google e Microsoft), nos quais as credenciais são armazenadas pelo provedor através de *hashs* sincronizadas.
- Todos os demais serviços providos por terceiros (como RNP CAFe), que não necessitem de autenticação na infraestrutura do IFSC através de rede federada CAFe (cafe.rnp.br).

NOTIFICAÇÕES E COMUNICADOS

Atualmente o IFSC possui canais de comunicação internos e externos à infraestrutura de TIC.

Hospedagem Interna:

- Portal institucional: www.ifsc.edu.br

² <https://portal.tcu.gov.br/comunidades/gestao-de-continuidade-de-negocios/home/>

- Sistema de solicitação de suporte e FAQ: chamados.ifsc.edu.br
- E-mail e Listas de e-mails para servidores: gmail.com e listas.ifsc.edu.br
- Sistema integrado com opção para comunicados e notícias: sig.ifsc.edu.br

Hospedagem Externa:

- Redes sociais abertas para todos os públicos:
 - Twitter: <https://twitter.com/ifsc>
 - Facebook: <https://www.facebook.com/ifsantacatarina>
 - Instagram: <https://www.instagram.com/ifsc/>
- Canal de vídeos no Youtube IFSC TV: <https://www.youtube.com/user/ifsccomunicacao>
- Serviço de mailing hospedado externamente, com listas da Imprensa para envio de notas.

A utilização dos canais externos, bem como o conteúdo de seus comunicados, serão orquestrados pela Diretoria de Comunicação (DIRCOM), seguindo regimento próprio.

Cabe a DTIC informar através dos canais disponíveis, as possíveis manutenções que possam vir a causar indisponibilidade dos serviços de TIC durante períodos pré-determinados.

SOLUÇÕES FÍSICAS E LÓGICAS

Se encontram disponíveis as seguintes alternativas:

- Link redundante de Fibra Óptica para o data center do IFSC³, operado pela RNP⁴ no qual ambos os cabos de fibra óptica saem por caminhos distintos;
- No-break e banco de baterias redundante, operando em paralelo diretamente nas conexões de energia dos equipamentos que possuem fontes redundantes (exceto Firewall). Em 2021, a autonomia medida foi de 40 minutos na carga atual;
- Grupo moto-gerador operando testes semanais automatizados, com contrato vigente para reabastecimento de diesel, manutenção de suas peças mecânicas e eventual troca do equipamento com horas de reposição pré-definidas em contrato;
- Cópias em discos de Storage com dados copiados localmente e em nuvem através de armazenamento em serviços de terceiros;
- Novo contrato de serviços em nuvem através de Broker licitado através de Pregão Nacional, podendo atuar como serviço de contingência, mas sem processos ainda definidos.

INFRAESTRUTURA E ACESSOS FÍSICOS

Atualmente o IFSC possui seu backup armazenado remotamente em um serviço de armazenamento tercerizado e está contratado como serviço em nuvem, que poderia ser utilizado como contingência para caso de incidente no site principal.

O acesso ao data center da Reitoria do IFSC se dá atualmente por uma porta principal do prédio ou através de uma porta secundária. Além disso há uma saída de emergência, porém se

³ Disponível em: <https://www.pop-sc.rnp.br/publico/monitoramento.php?map=REMEP-BB-PUBLICO.html>

⁴ Link do monitoramento disponível em: <https://www.pop-sc.rnp.br/publico/monitoramento.php?map=REMEP-CLIENTES.html>

localiza no andar térreo após um lance de escadas, e para acessá-la se faz necessário a abertura de 3 portas.

O controle de acesso ao ambiente do data center se dá mediante uso de fechadura digital, da qual a equipe da CIR tem acesso através de cópias da TAG, senha ou biometria. A Sala da DTIC é acessível por uso de fechadura digital, com acesso através de cópias da TAG, senha ou biometria. Além disso, o ambiente é monitorado por uma câmera de segurança, em seu ambiente interno e no corredor.

SOLUÇÕES PARA CONTINGÊNCIAS PREVISTAS

Em caso de desastres e catástrofes naturais ou não, estão disponíveis os seguintes artefatos:

- Incêndio: Alarme através de detector de fumaça interno ao data center, além de extintor de incêndio com Gás Carbônico CO₂ (específico para equipamentos elétricos), localizado na coluna esquerda depois da entrada da Sala principal, antes da porta do data center;
- Energia elétrica: Há dois sistemas No-Break locados através de contrato, com banco de baterias independentes providos por empresa terceirizada, até que o gerador entre em funcionamento. A fiscalização do contrato está sob responsabilidade da Coordenadoria de Infraestrutura e Redes do IFSC;
- Condicionadores de ar: Existem dois aparelhos de ar condicionado com tecnologia inverter, e uma central de automação para monitoramento e revezamento do seu funcionamento. Entretanto, na sala de baterias onde agora se encontram os No-Breaks, somente havia um aparelho de ar condicionado, estando previsto a instalação de outro aparelho, mas ainda não atendido pela central de monitoramento. Ambos os equipamentos são gerenciados pela equipe de Engenharia da Reitoria do IFSC através de contrato de manutenção específico.
- Serviço de internet: Os acessos são providos pela RNP, que também disponibiliza um link redundante para a Reitoria do IFSC. Atualmente ambos os enlaces possuem o mesmo caminho interno dentro da Reitoria, mas saem em postes distintos.

ENCERRAMENTO DO PLANO DE CONTINGÊNCIA

O plano será encerrado assim que todos os serviços estiverem estáveis e o funcionamento de sistemas essenciais (conforme anexo) operando normalmente.

A equipe responsável pelo retorno deve emitir um parecer relatando as atividades realizadas para a DTIC (o qual será usado para gerar os Planos de Ações) que por sua vez deverá fornecer um comunicado de retorno das atividades à toda a instituição.



PLANO DE CONTINUIDADE OPERACIONAL (PCO)

OBJETIVO

Este documento tem como objetivo restabelecer o funcionamento dos principais ativos que suportam a operação de TI do IFSC, reduzindo o tempo de queda e os impactos provocados por eventual incidente.

Este plano é composto por um conjunto de procedimentos previamente definidos, destinados a manter a continuidade dos processos de negócios e serviços vitais de uma organização, considerando-se a ausência de componentes que os suportem, devido à ocorrência de eventos previamente identificados e definidos. Através do PCO, os gestores dos processos de negócios saberão como agir na falta ou falha de algum componente que o suporte, garantindo a continuidade do processo de negócio reduzindo o impacto no negócio da Organização.

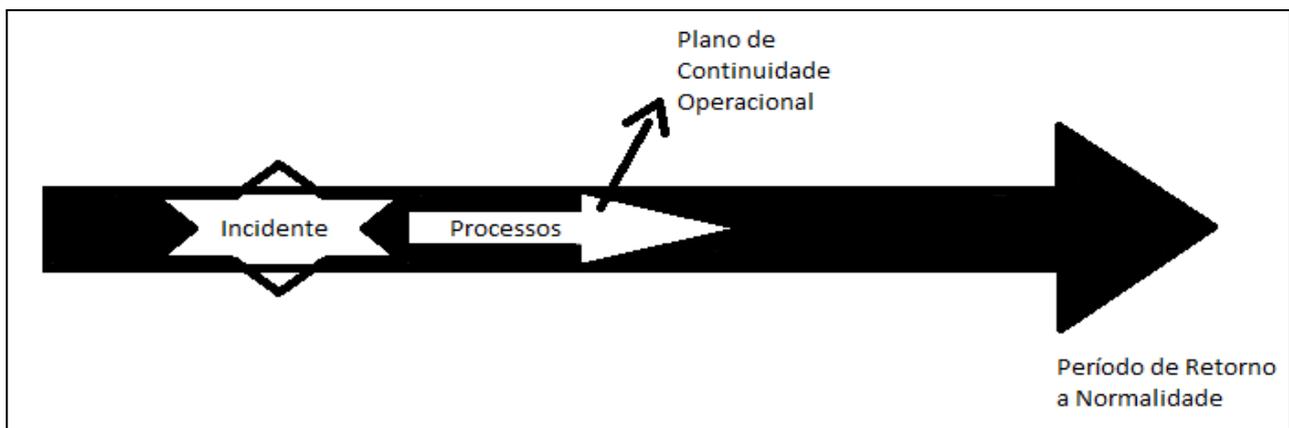


Imagem 8 - Tempo PCO

ESCOPO

Este plano se aplica a Reitoria do IFSC, prédio no qual se encontra atualmente o data center principal, que provê serviços para todos os Câmpus.

PAPÉIS E RESPONSABILIDADES

As principais responsabilidades dos setores e seus papéis são listados abaixo:

Diretor de Tecnologia da Informação e Comunicação (DTIC) - Diretor responsável por delegar às equipes e planejar ações para diminuir os impactos dos incidentes.

Coordenadoria de Infraestrutura e Redes (CIR) - Responsável pelas ações de manutenção dos serviços de redes e infraestrutura do data center do IFSC, bem como configuração e instalação de sistemas em geral. Deve ser acionada sempre que houverem interrupções nos serviços de internet, intranet e aplicações fora do ar.

Departamento de Sistemas (DSI) - Atua na parte de parametrização e programação de sistemas, bem como na manutenção de aplicações institucionais. Deve ser acionada no caso de bugs ou defeitos que impossibilitam o uso mínimo das ferramentas de software hospedadas no IFSC.

Coordenação de Governança de TI (CGovTI) - Trabalha como setor de regulação e regulamentação, atuando na parte de planejamento e projetos de TI sempre que necessário. Atende demandas de órgãos de controle, como auditorias externas e internas, referentes a planos ou políticas que dizem respeito à organização da TIC.

Diretor de Obras e Engenharia do IFSC (DOE) - Diretor responsável por garantir o menor impacto possível na manutenção dos serviços para operação da TI do IFSC em caso de incidentes.

Coordenadoria de Engenharia (COE) - Equipe ativa que é responsável por assegurar e garantir o cumprimento de serviços como energia elétrica e climatização do data center.

LISTA DE ATIVIDADES

As etapas aqui realizadas são denominadas “Procedimentos de Retomada”:

1. Estimar impacto de perda de dados;
2. Identificar ativos afetados;
3. Mapear ativos a serem recuperados;
4. Estimar volume de dados a serem recuperados, tempo de recuperação e possíveis perdas operacionais;
5. Implantar procedimentos de recuperação;
6. Testar procedimentos realizados;
7. Repassar procedimentos aos servidores e verificar melhorias.

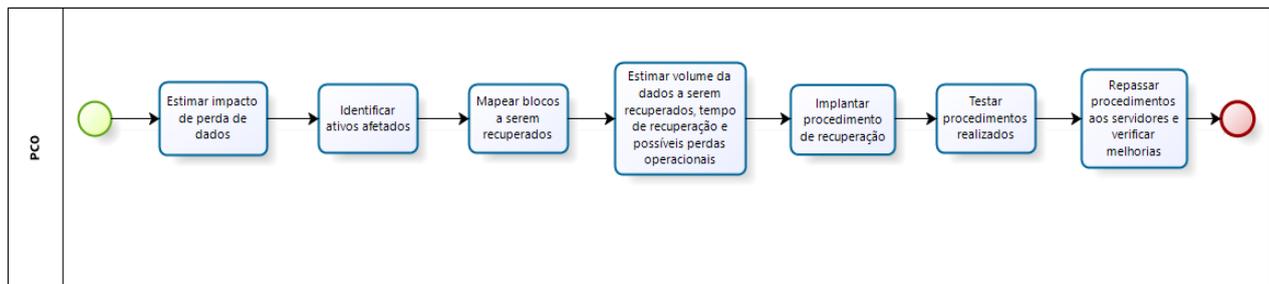


Imagem 9 - Processo de Retomada de Negócio

RECURSOS NECESSÁRIOS

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

Atualmente, além da operação do data center principal do IFSC *in loco*, também foram realizadas ações para garantir as operações de forma externa ao espaço físico (sala), no qual se encontram os equipamentos de processamento e armazenamento de dados:

1. Instalação de 8 tomadas na Sala 32B, ligadas aos 2 sistemas de No-break com Gerador. A medida visa garantir que, os computadores dos servidores responsáveis pela manutenção das operações, continuem ligados durante eventuais quedas de energia;
2. Possibilidade de uso de Notebooks presentes nos setores da Reitoria para eventuais utilizações durante quedas de energia. No caso de queda dos enlaces de internet, poderão ser utilizados os aparelhos telefônicos institucionais conectados a internet através da rede celular da operadora com contrato vigente;
3. No caso de impossibilidade no acesso ao prédio da Reitoria (onde se encontra o data center), deverão ser utilizadas temporariamente as estruturas das Unidades do IFSC.

4. Em caso de parada parcial do Data Center, como falha dos climatizadores de ar ou gerador de energia, devem ser avaliadas possibilidades de contratos emergenciais para suprir as necessidades, através de locações ou manutenções corretivas de curto prazo;

Demais atividades não previstas poderão passar pelo Comitê Permanente de Gestão de Crises.

ENCERRAMENTO DO PLANO DE CONTINUIDADE OPERACIONAL

O plano será encerrado assim que o funcionamento de sistemas essenciais estiverem instituídos e o data center estável.

A equipe responsável pelo retorno deve emitir um parecer por e-mail, relatando as atividades realizadas junto a DTIC (o qual será usado para gerar os Planos de Ações), para então fornecer os dados necessários para um comunicado de retorno das atividades à instituição. Caso o relatório tenha relação com Segurança da Informação, também deverá ser enviado para CSIRT.



PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

OBJETIVO

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

Além de avaliar possíveis vulnerabilidades dos componentes que suportam os processos de negócios críticos ao se deparar com eventos. Cabe executar um mapeamento e planejamento de sua recuperação ou restauração, sempre considerando as necessidades do IFSC.

No PRD devem ser detalhados os planos de ações relativos a sites alternativos, visando à continuidade dos negócios da Organização.

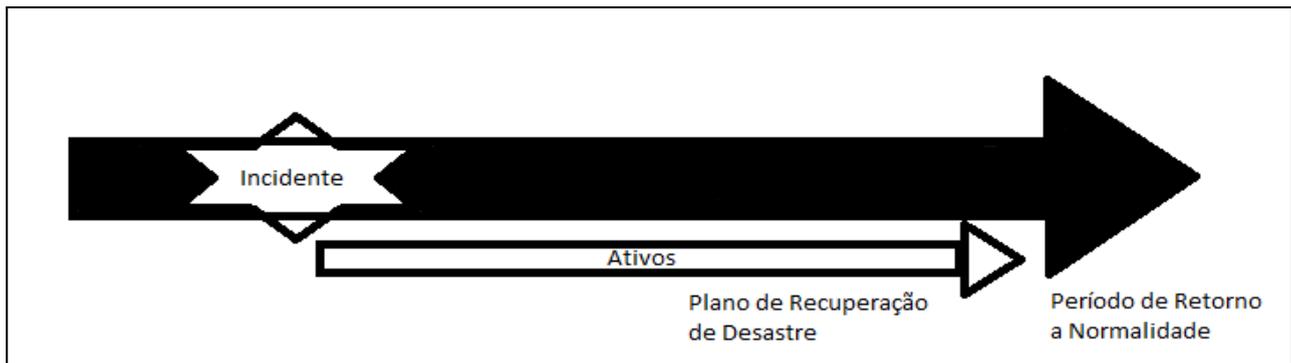


Imagem 10 - Tempo PRD

ESCOPO

Este documento se restringe à última etapa da recuperação de desastres. Visa garantir o retorno à normalidade das operações e não mais sua recorrência no caso de riscos controláveis.

PAPÉIS E RESPONSABILIDADES

Ao passo que durante as demais etapas a alta gestão deveria estar mais presente, nesta etapa as equipes técnicas deverão operacionalizar as ações e repassar para a alta gestão seu andamento.

Entre as equipes necessárias para restauração dos sistemas e serviços, são necessárias ações encadeadas, sendo cada equipe abaixo listada de acordo com sua precedência:

1. Coordenadoria de Engenharia - COE deve exercer o papel de prestador de serviço do negócio:
 - a. Responsável por garantir segurança do retorno às instalações do IFSC;
 - b. Deve verificar os níveis mínimos aceitáveis de fornecimento de serviços e contratos;
 - c. Restabelecer para níveis aceitáveis o fornecimento de energia elétrica, através de geradores e não somente sistema de no-break (pois este tem ação temporária, limitada pela carga prévia no banco de baterias).
2. Coordenadoria de Infraestrutura e Redes - CIR (Operação e manutenção):
 - a. Restabelecimento dos ativos de rede que interligam o acesso a internet e aos Câmpus;
 - b. Religamento de todos os equipamentos de armazenamento e processamento de dados;

- c. Garantia de que os sistemas operacionais e demais serviços necessários para execução dos sistemas estão funcionando perfeitamente.
3. Departamento de Sistemas - DSI (Testes e ajustes):
 - a. Verificação de parâmetros de auto inicialização dos sistemas após quedas, para que ocorra de forma automatizada;
 - b. Garantia do restabelecimento de todos os sistemas, seguindo uma lista de precedência previamente elencada como essencial pelo Comitê de Crises, até completá-la em sua integralidade.
 4. Coordenadorias de TIC dos Campus - CTICs (Suporte local):
 - a. Restabelecimento dos serviços de rede e voz que dão acesso a internet no câmpus;
 - b. Restabelecimento dos sistemas e serviços de TI hospedados na infraestrutura do Câmpus;
 - c. Reportar sobre suas causas a DTIC e ao POP-SC após possíveis quedas e falhas.

RESTAURAÇÃO EM CASO DE DESASTRES

Os processos aqui realizados são denominados “Procedimentos de Recuperação ou Restauração”. As seguintes macro etapas devem ser necessárias para normalizar os serviços de forma ampla:

1. Identificar ativos danificados: CIR deve listar ativos danificados com a ocorrência de um desastre.
2. Listar serviços interrompidos: CIR deve identificar interrupções de conexões e acessos gerados, informando abrangência.
3. Elaborar passos de recuperação: DTIC deve manter seu Catálogo de Serviços atualizado e informar componentes necessários para a plena operação de todos os ativos físicos (servidores, banco de dados, storages, switches), assim como suas configurações através de diagramas e documentação. Com isso a DTIC deve elaborar um cronograma de recuperação de aplicações, levando em conta os prazos de entrega dos fornecedores.
4. Executar ciclos de recuperação: Substituir ativos perdidos, reconfigurar ativos que podem ser reparados ou reconfigurados.
5. Testar procedimentos de recuperação: DTIC deve testar os ativos de forma a garantir que o processo de recuperação esteja conforme o planejado. Este teste deve garantir os mesmos níveis anteriores ao desastre.
6. Desenvolver relatório do que foi realizado: desenvolver relatório com todos os problemas encontrados e como foi resolvido.

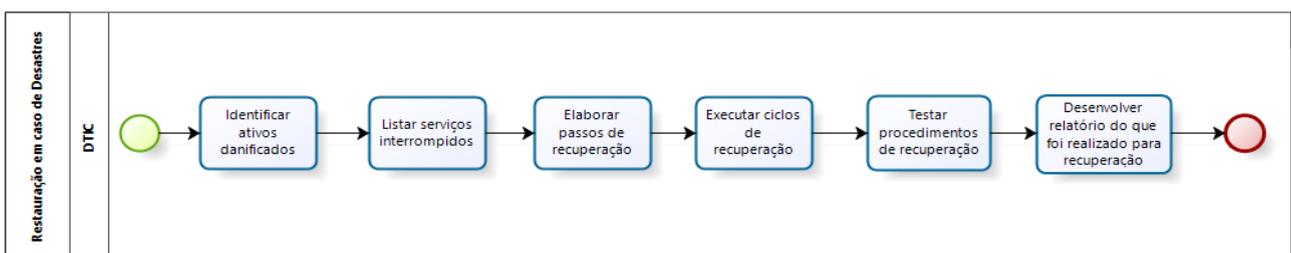


Imagem 11 - Processo de Recuperação ou Restauração

No caso de possível perda de dados ao restaurar os serviços, deverão ser avaliadas opções de ponto de restauração do último *backup* disponível. Neste caso a restauração dependerá da disponibilidade de *backup*, sendo que cabe à Coordenadoria de Redes e Infraestrutura (CIR) avaliar a forma disponível que seja mais confiável e rápida de acordo com a Política de *Backup* e o Plano de *Backup* do IFSC.

Caso possível, deverá ser provido estimativas de prazos para restabelecimento dos serviços, tendo em vista o cálculo que depende do volume de dados gerados. Demais etapas que envolvam operacionalização de restauração e testes, deverão estar explicitadas na Normativa do Plano de *Backup* do IFSC.

AUTORIDADE RESPONSÁVEL

Considera-se aqui, que a Instituição deva delegar os setores e/ou comissões pertinentes às autoridades responsáveis por cada público ou ativo.

Considerando que nesta etapa os fatores de risco já foram extintos, cabe a Comissão Interna de Saúde do Servidor Público (CISSP) buscar reduzir os riscos para os servidores que atuam próximos ao data center do IFSC.

Para os ativos, como equipamentos de rede ou de manutenção do data center, são elencadas a seguir as áreas competentes e suas tarefas.

LISTA DE TAREFAS

A. Coordenadoria de Engenharia:

- a. Manter os sistemas de energia ininterrupta como No-Breaks e Gerador funcionando;
- b. Garantir o restabelecimento de energia elétrica através de contingência (gerador) ou concessionária se disponível;
- c. Restabelecer os equipamentos de climatização do data center e suas automações.

B. Coordenadoria de Infraestrutura e Redes:

- a. Garantir a integridade dos ativos de rede para reconexão;
- b. Testar os equipamentos de processamento e armazenamento de dados;
- c. Restaurar os serviços de acordo com uma sequência pré-definida em anexo;
- d. Verificar a integridade dos dados e restaurar os backups caso necessário.

C. Departamento de Sistemas:

- a. Suportar o retorno dos sistemas de acordo com as demandas pontuais;
- b. Garantir a integridade dos dados, que podem estar corrompidos ou defasados;
- c. Garantir que as funcionalidades básicas de acesso estão funcionando novamente.

RECURSOS NECESSÁRIOS

As equipes envolvidas nos processos de restauração e recuperação deverão elencar à Pró-Reitoria de Administração possíveis recursos avariados que devam ser substituídos. No caso de desastres que necessitem a compra de novos equipamentos, estes deverão ser especificados pelas equipes técnicas responsáveis, nas seguintes áreas:

- A. Coordenadoria de Engenharia: Equipamentos de energia e climatização;
- B. Coordenadoria de Infraestrutura e Redes: Ativos de rede, processamento ou armazenamento;
- C. Departamento de Sistemas: Softwares e suas licenças.

Cabe à DTIC do IFSC, avaliar possibilidades como alocação de recursos computacionais em regime emergencial, de acordo com a legislação de contratos vigente, com a devida anuência dos gestores envolvidos nestes processos.

ENCERRAMENTO DO PLANO DE RECUPERAÇÃO DE DESASTRES

O plano será encerrado assim que os procedimentos de recuperação forem realizados por todas as equipes. Cada equipe responsável pelo retorno 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.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO/IEC Guia 73:2009: Gestão de riscos – Vocabulário. Rio de Janeiro: ABNT, 2009a.

_____. ABNT NBR 15999-1:2007 – Gestão de Continuidade de Negócios – Código de Prática. Rio de Janeiro: ABNT, 2007.

_____. ABNT NBR 15999-2: Gestão de continuidade de negócios – Parte 2: Requisitos. Rio de Janeiro: ABNT, 2008a.

_____. ABNT NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

_____. NBR ISO 31000:2009 – Gestão de Riscos – Princípios e Diretrizes. Rio de Janeiro: ABNT, 2009b.

_____. ABNT NBR ISO/IEC 27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2008b

_____. ABNT NBR ISO/IEC 22301: 2013 Segurança da Sociedade — Sistema de Gestão de Continuidade de Negócios — Requisitos. Rio de Janeiro: ABNT, 2013.

_____. ABNT NBR ISO/IEC 22313: 2015 Segurança da Sociedade — Sistema de Gestão de Continuidade de Negócios — Orientações. Rio de Janeiro: ABNT, 2015.

_____. ABNT NBR ISO/IEC 31010:2012. Gestão de riscos — Técnicas para o processo de avaliação de riscos. ABNT - Associação Brasileira de Normas Técnicas, 2012.

_____. ABNT NBR ISO/IEC 38500:2015. Governança de tecnologia da informação para a organização. ABNT - Associação Brasileira de Normas Técnicas, 2015.

_____. ABNT NBR ISO/IEC 15999-1:2007. Gestão de Continuidade de Negócios. Parte 1: Código de Prática. ABNT - Associação Brasileira de Normas Técnicas, 2007.

_____. ABNT NBR ISO/IEC 17799:2005. Tecnologia da Informação - Técnicas de Segurança - Código de Práticas para a Gestão de Segurança da Informação. ABNT - Associação Brasileira de Normas Técnicas, 2005.

BRASIL. Portaria SETIC/MP nº 19, de 29 de maio de 2017. Dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISF. Ministério do Planejamento, Desenvolvimento e Gestão.

BRASIL. Decreto nº 8.638, de 15 de janeiro de 2016. Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, 2016.

BRASIL. Estratégia de Governança Digital da Administração Pública Federal 2016-19. Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI/MP), 2016.

COBIT 5. Control Objectives for Information and Related Technologies. Modelo Corporativo para Governança e Gestão de Tecnologia da Informação de Organizações. Information System Audit and Control - Icasa, 2012.

DSIC/GSIPR. Departamento de Segurança da Informação e Comunicações / Gabinete de Segurança Institucional da Presidência da República. Norma Complementar nº06, de 11 de novembro de

2009. Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações. Brasília, 2009.

GSIPR. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008. Diretrizes para Gestão de Segurança da Informação e Comunicações para os órgãos e entidades da Administração Pública Federal, direta e indireta. Brasília, 2008a

TCU, TRIBUNAL DE CONTAS DA UNIÃO. Acórdão TCU 1603/2008 – Plenário. Levantamento de auditoria. Situação da governança de Tecnologia da Informação - TI na Administração Pública Federal. Ausência de planejamento estratégico institucional. Deficiência na estrutura de pessoal. Tratamento inadequado à confidencialidade, integridade e disponibilidade das informações. Brasil, 2008c.

TJBA, Tribunal de Justiça da Bahia. PLANO DE CONTINUIDADE DE TI. Conservação, ininterrupção dos sistemas essenciais de TI do Tribunal de Justiça do Estado da Bahia. Disponível em: <http://www5.tjba.jus.br/setim/images/pdf/Plano_Continuidade_TIC_SETIM.pdf>.

APÊNDICES

APÊNDICE I

Lista de Serviços em Ordem de Precedência e Interdependência:

1. Firewall
2. Sistema Virtualizador
3. DHCP
4. DNS e Replicação de Zonas em Site Remoto
5. Sistema de Autenticação Centralizada
6. Portal do IFSC
7. Serviço de Listas de e-mails (Listas)
8. Sistema ERP
9. Moodle
10. Sistema de Bibliotecas e Banco de Dados
11. Sistema de Ingresso
12. Serviço de Formulários Online
13. Servidores de Hospedagem de Páginas
14. Sistema de Chamados

Obs.: Esta lista deve ser atualizada sempre que necessário para refletir as necessidades do IFSC.

APÊNDICE II

Nesta tabela deverão ser registradas as situações e incidentes já ocorridos.

O quê?	Quando?	Como?	Porquê?
Dias sem internet da REMEP - POP/SC	2016 - Março	Falha na distribuição de energia do POP	Falha elétrica geral na SETIC da UFSC
Bomba de Diesel do gerador	2016 - Junho	Falta de energia com defeito no gerador	Empresa contratada falhou na manutenção
Falha nas Baterias	2016 - Dezembro	Perderam validade	Troca não efetuada
Ar condicionado falhou	2017 - Novembro	Falta de energia causou defeito no ar	Falha em uma fase da energia danificou o ar
No-Break e módulos queimando	2017 - Agosto	Componentes de potência explodiram	Falta de manutenção e fora da garantia
Falta de energia com falha da Celesc	2017 - Dezembro	Gerador com pouco Diesel em domingo	Celesc não arrumou o defeito da rede
Dreno do ar condicionado entupido	2018 - Janeiro	Falta de limpeza dos drenos	Falta de manutenção preventiva
Novo ar condicionado desligou no feriado	2018 - Junho	Datacenter chegou a 45º após feriado	Automação pode ter falhado
Automação do Ar Condicionado antiga	2018 - Agosto	Sistema automatizado falhou	Mudança da tecnologia do inverter
Falha na bomba do gerador	2018 - Novembro	Biodiesel entupiu a bomba de óleo	Falta de manutenção preventiva
Nova automação do Ar falhou ao ligar	2018 - Dezembro	Troca da automação causou a nova falha	Programação errada em um dos aparelhos
Novas tomadas no data center para redundância	2019 - Junho	Manutenção nas tomadas do data center	Erro na troca de tomadas redundantes
Pandemia	2020 - Março	Obrigou afastamento de todos os servidores	Doença contagiosa com distanciamento social
Gerador ficou em modo manual	2021 - Janeiro	Esqueceu-se de voltar o modo automático	Na troca do No-Break foi modificada a chave
Furto dos fios do gerador	2022 - Março	Corte dos cabos do gerador	Contactora danificada gerou desligamento total

APÊNDICE III

Lista de Contatos de cada Gestor dos Setores citados neste plano.

Evento ou problema	Setor ou Cargo	Celular Institucional
Ensino ou Alunos	Pró-Reitoria de Ensino	48 999 400 151
Ensino ou Alunos	Diretoria de Ensino	48 999 400 019
Águas ou estrutural	Diretoria de Administração	47 988 567 422
Gestão de Crises	Diretoria Executiva	(48) 3877 9004
Datacenter	Diretoria de TIC	48 999 400 121
Comitê de Crises	Diretoria de Comunicação	48 999 400 065
Gestão	Chefia de Gabinete	48 999 400 013
Datacenter ou Redes	Coordenadoria de Redes e Infra	48 999 400 118
Manutenção Predial	Coordenadoria de Engenharia	48 996 023 770
Anúncios e Comunicação	DIRCOM - Jornalismo e Comunicação	48 999 480 457
Chefia DTIC	Pró-Reitoria de Des. Institucional	48 999 400 159

Obs.: Esta lista deve ser atualizada sempre que necessário e não deve ser divulgada publicamente.