SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
SECRETARIA ESPECIAL DE TECNOLOGIA E INFORMAÇÃO - SETI

PLANO DE CONTINGÊNCIA

DO DATA CENTER

(SISTEMA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO)

Vigência: 2023-2024

SUMÁRIO

INTRODUÇÃO 5

1 APLICABILIDADE 5

2 DEFINIÇÕES DOS TERMOS 5

3 DESCRIÇÃO DO AMBIENTE 6

3.1 Sistema de Incêndio: 6

3.2 Sistema UPS: 7

3.3 Sistema de Climatização 8

3.4 Sistema de Geração de Energia de Emergência (Gerador) 8

3.5 Sistema de Controle de Acesso 10

3.6 Sistema Elétrico 10

3.7 Sistema de Armazenamento 10

3.8 Sistema de Backup 11

3.9 Sistema de Processamento de dados 11

3.10 Rede SAN (Storage Area Network) 11

3.11 Infraestrutura de rede 12

4 PAPÉIS E RESPONSABILIDADES 14

5 GRUPOS EXECUTORES 15

6 ANÁLISE DE RISCOS 15

7 PRINCIPAIS RISCOS E CONTINGENCIAMENTO 16

8 ANÁLISE DO IMPACTO 18

9 COMUNICAÇÃO 19

10 CATÁLOGO DE CONTATOS INTERNOS 19

11 CATÁLOGO DE PRESTADORES DE SERVIÇOS 20

12 REFERÊNCIAS 21

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
27/05/2021	1.0	Versão inicial do Plano
24/05/2023	1.1	Revisão do Plano

TERMOS E ABREVIAÇÕES

ATI – Atendimento de Tecnologia da Informação

CGD – Comitê de Governança Digital

DC – Data Center

DIAPL - Departamento de Infraestrutura de Aplicações

DIOTI – Divisão de Operações de Tecnologia da Informação

DITI – Diretoria de Infraestrutura de Tecnologia da Informação

DRT - Departamento de Redes de Telecomunicações

DS – Diretoria de Sistemas de Informação

EDA - Equipment Distribution Area

MDA – Main Distribution Area

PDTIC – Plano Diretor de Tecnologia da Informação e Comunicação

POSIC - Política de Segurança da Informação

SAN - Storage Area Network (Rede Privativa de Armazenamento)

SEO - Secretaria Especial de Obras

SET - Serviço Especial de Transportes

SETI – Secretaria Especial de Tecnologia da Informação

SGDC – Setor de Gestão do Data Center

TI - Tecnologia da Informação

TIC - Tecnologia da Informação e Comunicação

UFFS – Universidade Federal da Fronteira Sul

UPS - Uninterruptible Power Supply (Fonte de Alimentação Ininterrupta)

INTRODUÇÃO

O Data Center é um ambiente de missão crítica que foi projetado para permanecer em funcionamento ininterruptamente. A UFFS estruturou seu Data Center de acordo com a amplitude de demandas e baseado no crescimento, segurança e disponibilidade dos recursos alocados em que os diversos sistemas e cursos institucionais necessitam para proporcionar ensino, pesquisa e extensão de qualidade. Neste contexto, foram adquiridos equipamentos com diferentes níveis de complexidade, desde itens comuns com ampla disponibilidade no mercado até itens de comercialização e assistência técnica restritos a empresas específicas. Por se tratar de um ambiente essencial para o funcionamento da instituição, é necessário garantir a disponibilidade de tal forma que o ambiente seja mapeado e controlado da melhor maneira possível. O Data Center da UFFS é composto pelas seguintes áreas:

- Equipment Distribution Area - EDA, de aproximadamente 46,9 m2, revestida por paredes em alvenaria e drywall, teto composto por fibras vegetais antichamas e porta corta-fogo com barra anti-pânico e fechadura eletromagnética;

- Main Distribution Area - MDA de aproximadamente 37,14 m2, revestida por paredes em alvenaria e drywall, teto composto por fibras vegetais antichamas e porta corta-fogo com barra anti-pânico e fechadura eletromagnética;

- Entrade Romm - ER (sala de entrada das operadoras) de aproximadamente 65 m2, revestida por paredes em alvenaria e drywall, teto composto por fibras vegetais antichamas e porta corta-fogo com barra anti-pânico e fechadura eletromagnética;

- **Sala de UPS** (“no-break”) e antessala técnica, de aproximadamente 38,29m2, revestida por paredes em alvenaria e drywall, teto composto por placas minerais anti-chamas e porta corta fogo com barra anti-pânico e fechadura eletromagnética;

O principal objetivo deste Plano de Contingência é estabelecer os procedimentos adequados ao gerenciamento de situações de contingência, cenários de incidentes, desastres ou falhas nos ativos de TIC do Data Center que causem impacto nas rotinas operacionais da instituição. Para isso, estabelecemos escopos estratégicos com procedimentos, ações e medidas rápidas para os processos críticos nos ativos de TIC do Data Center.

1 APLICABILIDADE

Este plano aplica-se a todos os ativos de TIC alocados no Data Center, localizado no Campus de Chapecó da Universidade Federal da Fronteira Sul, Rod. SC 484 KM 02, Bairro Fronteira Sul, Subsolo do Bloco da Biblioteca, Data Center, Sala 013, Chapecó-SC, CEP: 89815-899.

2 DEFINIÇÕES DOS TERMOS

Analista de monitoração: equipe responsável pelo monitoramento e gestão dos eventos de TI (NOC).

Área Vulnerável: área atingida pela extensão dos efeitos provocados por um evento de falha.

Áreas Sensíveis: áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas, encontram-se as salas do UPS, EDA, MDA e ER.

Contingência: situação de risco com potencial de ocorrer, inerente às atividades, serviços e equipamentos, e que ocorrendo se transformará em uma situação de emergência.

Data Center: todo o espaço nos quais ficam os ativos de TIC, bem como suas estruturas auxiliares como UPS, Banco de Baterias e Gerador de Energia Elétrica.

Equipe de Especialistas: equipes de suporte de 3º nível de atendimento.

Evento: para fins deste plano, são os itens apresentados no dashboard de incidente do Zabbix, noc-monitor ou sistemas de eventos dos próprios sistemas e serviços.

Incidente: qualquer evento que representa incertezas a um serviço do negócio.

Intervenção: é a atividade de atuar durante a emergência, seguindo ações planejadas, visando minimizar possíveis impactos negativos ou imprevistos sobre os equipamentos e sistemas de TIC.

Noc-monitor: ferramenta desenvolvida internamente para monitoramento dos sistemas: Incêndio, Gerador, UPS, Climatização e serviço de internet, acessível através de rede interna em noc-monitor.uffs.edu.br.

Serviço de negócio: serviço na visão de negócios, produto final oferecido pela UFFS, exemplo: Webmail, Sistema SIG, Sistema SEI, conectividade, DNS, VPN, Repositório, etc.

Situação de Emergência: situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos ou ao desempenho das atividades institucionais.

Zabbix: ferramenta utilizada para monitoramento dos ativos da UFFS nele cadastrados, acessível em noc.uffs.edu.br.

3 DESCRIÇÃO DO AMBIENTE

3.1 Sistema de Incêndio:

O sistema é encarregado de antecipar e prevenir um princípio de incêndio. É composto pelos seguintes equipamentos:

- 1 (uma) Central Kidde-Fenwal-6000;
- 2 (dois) sistemas de detecção de Alta Sensibilidade - HSSD Air Intelligence ASD-320,
- 37 bases e detectores de fumaça,
- Sistema de Extinção de Incêndio por Agente Limpo FM-200 - 4 (quatro) cilindros.

3.1.1 Manutenção do Sistema de Incêndio

A manutenção preventiva e corretiva do sistema de Incêndio está submetida a um contrato operado pela empresa VIRTUAL INFRAESTRUTURA E ENERGIA LTDA (contrato 30/2021, Processo Administrativo nº 23205.004157/2020-65 – decorrente do Pregão nº 43/2020, vigência de 07/07/2023 a 06/07/2024).

3.2 Sistema UPS:

O Sistema de fonte de energia ininterrupta (UPS) fornece energia de emergência para o Data Center, além de corrigir falhas comuns da rede elétrica como: picos de tensão, micro interrupções, oscilações de frequência, ruído na rede, queda e/ou oscilação de tensão de entrada, etc. É composto por:

- **2 APM 300** – UPS Modulares de 300KVA cada com banco de baterias. Inicialmente os equipamentos foram entregues na potência de 120KVA, configurados para operar com redundância de módulos, sendo 90KVA de potência disponível e 30 KVA de redundância em cada um dos UPS. Sistema redundante sendo a linha X a principal e a linha Y secundária; caso ocorra algum problema na linha X, a linha Y assume automaticamente. Todos os equipamentos críticos do Data Center estão ligados em ambas as linhas;

- **Banco de baterias** (34 para cada UPS) com autonomia estimada de 7 min a plena carga. Com a carga atual, temos uma autonomia de até 45 minutos;

Apresenta os modos de operação: On-Line, Bateria, Bypass e Bypass de manutenção;

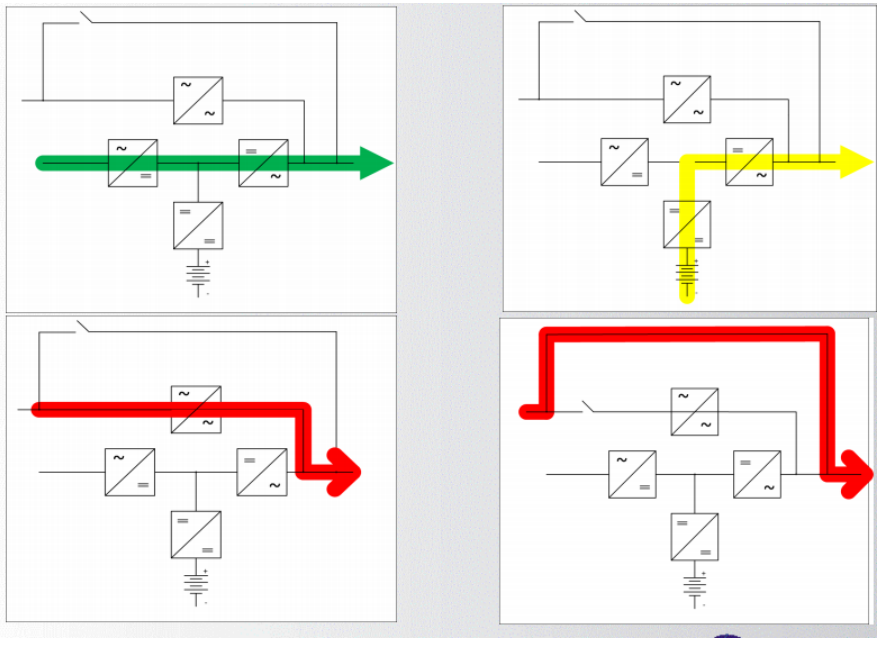

Figura 1: Modos de operação

3.2.1 Manutenção do sistema de UPS

A manutenção preventiva e corretiva deste sistema está submetida a um contrato operado pela empresa VERTIV TECNOLOGIA DO BRASIL LTDA (contrato 09/2020, Processo

Administrativo de Contratação Direta nº 23205.003394/2019-75 – decorrente da Inexigibilidade de Licitação nº 31/2019, vigência de 26/03/2023 a 25/03/2024). O Contrato abrange:

Suporte técnico especializado: canal de atendimento para sanar dúvidas técnicas a respeito do funcionamento e operação do equipamento;

Instrução operacional: demonstração sobre a correta utilização dos equipamentos, leitura de alarmes, alteração de parâmetros básicos e manobras operacionais nos equipamentos;

Manutenção Preventiva: são divididas em duas categorias:

1 – Sem parada técnica: poderá ser executada de segunda a sexta em horário comercial (das 08h00 às 18h00) conforme cronograma aprovado pela equipe responsável;

2 – Com parada técnica: poderá ser executada de segunda a sábado (exceto feriados) durante todo o dia, a qualquer horário, limitada a uma única manutenção anual.

A manutenção preventiva deve ser realizada da seguinte maneira:

TRIMESTRAL: uma das manutenções deverá ser realizada com desligamento total das máquinas (conforme cronograma aprovado pela equipe responsável). As manutenções restantes serão executadas sem parada técnica.

- Manutenção Corretiva: são serviços ilimitados, prestados sempre que necessários, 24x7x365, enquanto o contrato estiver em vigor;

- Plantão técnico 24x7x365: canal de atendimento disponível para solicitar atendimentos emergenciais. Durante a vigência do contrato, 24 horas por dia sem limite de atendimentos;

- CONTACT CENTER da VERTIV TECNOLOGIA DO BRASIL LTDA:

Telefone: 0800-208-8000

SAC.CRC@vertivco.com

- Tempo de resposta para atendimento corretivo: A partir do chamado, a chegada até o site é de até 8 horas.

3.3 Sistema de Climatização

O sistema independente de climatização de precisão é responsável por garantir a segurança na precisão da climatização do Data Center. É composto por:

- Na sala do Data Center (EDA/MDA): sistema composto por 02 (duas) máquinas de climatização de precisão, marca EMERSON, modelo Liebert PEX 2050, de 43.2 kW de calor sensível, com resfriamento, desumidificação e filtragem do ar em circuito fechado, composto por 2 (duas) unidades evaporadoras e 2 (duas) unidades condensadoras remotas para sala de UPS;

- Na Sala de UPS: sistema composto por 02 (duas) máquinas de climatização de precisão, marca EMERSON, modelo Liebert PEX 1035, de 29.4 kW de calor sensível, com resfriamento, desumidificação e filtragem do ar em circuito fechado, composto por 2 (duas) unidades evaporadoras e 2 (duas) unidades condensadoras remotas para sala de UPS;

3.3.1 Manutenção do Sistema de Climatização

A manutenção preventiva e corretiva deste sistema está submetida a um contrato operado pela empresa VERTIV TECNOLOGIA DO BRASIL LTDA, (contrato 09/2020, Processo Administrativo de Contratação Direta nº 23205.003394/2019-75 – decorrente da Inexigibilidade de Licitação nº 31/2019, vigência de 26/03/2023 a 25/03/2024), vide item 3.2.1 Manutenção.

3.4 Sistema de Geração de Energia de Emergência (Gerador)

Este sistema fornece energia elétrica em regime de emergência e/ou temporária, quando da ocorrência de alguma falha ou oscilação de energia no abastecimento. É composto por:

- Grupo Moto Gerador STEMAC – GMG
    - Potência de 460/434 kVA
    - Trifásico
    - Fator de potência 0,8 na tensão 380 /220 Vca em 60 Hz
    - USCA nideki DSE7320
    - Modulo SNMP 892
    - QTA
    - Sistema Motriz Scania Diesel 6 cilindros
        - Possui regulador eletrônico de velocidade (1800 RPM)
        - Capacidade do tanque de combustível de 200lts
        - Reserva local de combustível: 100 litros
        - Autonomia aproximada de 6 a 8 horas, a plena carga.
        - Autonomia do tanque com a carga atual: em torno de 10 horas.
    - Sistema de Gerador alternado WEG
    - Tratamento acústico da sala para 65dB

3.4.1 Manutenção do Sistema de Geração de Energia de Emergência

Atualmente atendido pelo CONTRATO 36/2022; GRUPO 1; PROCESSO LICITATÓRIO 23205.022663/2022-06; PREGÃO ELETRÔNICO 44/2022; contratada Chico Geradores.

3.4.1.1 Ações de rotina

Responsáveis: DIOTI, SGDC

- Realizar auto teste **semanalmente**;

- Verificar níveis de combustível **semanalmente**, abastecer e solicitar reposição do combustível reserva;

- Auxiliar na manutenção e limpeza dos equipamentos adjacentes da infraestrutura local do Gerador.

3.5 Sistema de Controle de Acesso

O sistema de controle de acesso é composto por 05 (cinco) leitoras com tecnologia de reconhecimento biométrico das digitais (marca Control ID, modelo CX 700). O acesso é liberado apenas para pessoal devidamente cadastrado no sistema de controle.

Responsável pelo controle e gerenciamento: SGDC.

3.6 Sistema Elétrico

Toda a rede elétrica do Data Center garante uma distribuição redundante desde a subestação até a tomada elétrica do Servidor.

- 9 quadros elétricos;

- 2 circuitos elétricos monofásicos 220v/ 32ª, sendo 2 circuitos provenientes do QDX e 2 do QDY;

- Nomenclatura E1-QDX-UPS-X, E1-QDY-UPS-Y;

- Condutores do tipo anti-chama, livre de gases tóxicos e alógenos.

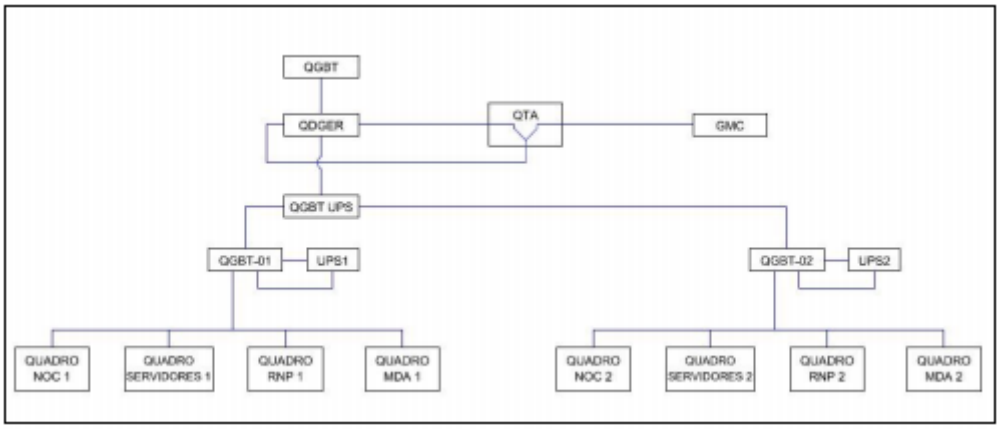

Figura 2: Quadros de distribuição

3.6.1 Manutenção do Sistema Elétrico

A manutenção preventiva e corretiva deste sistema é de responsabilidade da Secretaria Especial de Obras.

3.7 Sistema de Armazenamento

O sistema de armazenamento é formado por:

- 2 (dois) Storages EMC VNX 5200 (Storage C e Storage D): cada Storage tem capacidade total líquida de 72,35TB, totalizando 144,70TB de armazenamento.

3.7.1 Manutenção do Sistema de Armazenamento

A manutenção preventiva e corretiva dos storages EMC VNX 5200 desse sistema está submetida a um contrato operado pela empresa DAT SOLUÇÕES EM TECNOLOGIA EIRELI, (contrato 33/2021, Processo Administrativo nº 23205.0014069/2020-71 – decorrente do Pregão nº 47/2020, vigência de 18/08/2022 a 17/08/2023).

3.8 Sistema de Backup

O sistema de backup exerce a função de garantir que a instituição esteja preparada para reagir nos casos em que os dados sejam afetados por qualquer tipo de incidente. Além da redundância utilizada no armazenamento de dados, um dos sistemas utilizados para a proteção da informação nesse ambiente é o de backup de informações.

Para isso, a instituição utiliza o equipamento EMC Data Domain DD2500 que atende em relação a capacidade, eficiência, rapidez em salvaguardar e restaurar dados, automatização, centralização, possibilidade de desduplicação e economia de custos.

O equipamento tem capacidade de armazenamento de 126TB de área bruta, 89,75TB de área líquida, sendo que desse total até a data de 13 de junho de 2023 tem consumido em torno de 65TB de dados líquidos não duplicados. Esse volume é representado por rotinas diárias, onde são salvaguardados ambientes de dados em Produção como: bases de dados, repositórios de arquivos, sistemas acadêmicos, administrativos, entre outros.

Ainda, são realizadas cópias em Fitas Magnéticas, em períodos mais esparsos, de dados essenciais como: bases de dados, repositórios de arquivos e sistemas. Por segurança, as fitas são armazenadas em um cofre em local fisicamente distinto do Data Center.

3.8.1 Manutenção do Sistema de Backup

A manutenção preventiva e corretiva do dispositivo “EMC Data Domain DD2500” deste sistema está submetida a um contrato operado pela empresa DAT SOLUCOES EM TECNOLOGIA EIRELI, (contrato 02/2021, Processo Administrativo nº 23205.004143/2020-41 – decorrente do Pregão nº 33/2020, vigência de 11/01/2023 a 10/01/2024).

3.9 Sistema de Processamento de Dados

O sistema de processamento de dados é composto basicamente por:

- 2 Chassis HP BLc7000 interligados;

- 16 Lâminas HP ProLiant BL460c Gen9;

- 7 Lâminas HP ProLiant BL460c G6;

Esse sistema está organizado em Cluster de modo que proporcione redundância em casos de falha de um dos hosts.

3.9.1 Manutenção do Sistema de Processamento de Dados

A manutenção corretiva dos dispositivos alocados para o ambiente de produção é feita pela própria equipe de TI da instituição Considera-se a existência de equipamentos redundantes e uma infraestrutura que absorve eventuais falhas, e que conforme a demanda, haverá tempo hábil para aquisição de peças de reposição.

3.10 Rede SAN (Storage Area Network)

Rede dedicada e de alta velocidade que interconecta e disponibiliza os dispositivos de armazenamento de dados ao pool de servidores.

3.11 Infraestrutura de rede

A infraestrutura de redes do Data Center é composta por equipamentos do tipo: Switch Core, Firewall, Roteadores, Controladora WLAN e Links de Internet.

3.11.1 Núcleo de Rede

O Data Center da UFFS é o ponto central da rede da UFFS, onde estão localizados todos os sistemas e serviços hospedados em nossa rede, além do tráfego proveniente do Campus Chapecó, que se conecta aos switches de distribuição.

3.11.1.2 Switch Core Campus Chapecó

No Campus Chapecó, utilizamos um switch Cisco modelo Nexus 5548UP como equipamento de núcleo da rede. No entanto, o suporte e a garantia deste equipamento fornecidos pelo fabricante expiraram em junho de 2020. Porém, temos um equipamento sobressalente com 48 portas de fibras, proveniente de uma doação da Receita Federal, que pode ser utilizado como substituto em caso de falha.

As configurações são regularmente copiadas e armazenadas no Cisco Prime Infrastructure (prime.uffs.edu.br) por meio de uma rotina de backup. Dessa forma, caso ocorra algum problema com o equipamento em operação, é possível reverter as configurações para outro equipamento, realizar a realocação no rack e nos cabos, e retomar as operações com um tempo de inatividade de meio período após a identificação da falha e a impossibilidade de recuperação.

Aqui, a criticidade é alta, pois qualquer interrupção afetaria todos os acessos LAN e WLAN no Campus Chapecó.

3.11.1.2 Switch Core DMZ

Atualmente, utilizamos dois switches empilhados como núcleo da DMZ, totalizando 48 portas Ethernet e 16 portas de fibra. Esses equipamentos são responsáveis pela comunicação interna entre os dispositivos de processamento da rede interna do data center. É importante mencionar que os equipamentos são novos e estão cobertos pela garantia. Também temos um equipamento adicional idêntico, em "spare", disponível para troca caso seja necessário

As configurações são regularmente copiadas e armazenadas no Cisco Prime Infrastructure (prime.uffs.edu.br) por meio de uma rotina de backup. Dessa forma, caso ocorra algum problema com o equipamento em operação, é possível reverter as configurações para outro equipamento,

fazer a realocação no rack e nos cabos, e retomar as operações com um tempo de inatividade de meio período após a identificação da falha e a impossibilidade de recuperação.

Aqui, a criticidade é alta, pois todos os sistemas hospedados no data center da UFFS seriam comprometidos.

3.11.2 Firewall

O Firewall no Data Center é um "Next Generation Firewall" da marca Palo Alto, modelo 3410. Possui licenças ativas para gerenciamento de ameaças e filtragem de URLs, e conta com suporte 24 horas, válido até março de 2026, através do Contrato nº 63/2022.

O firewall está conectado aos links de internet através de roteamento estático ao PARC Chapecó e, em seguida, à RNP, onde recebe dois links. Além disso, o firewall está conectado ao switch core do campus Chapecó, onde ocorre a distribuição de toda a LAN, ao switch core DMZ, que interconecta os sistemas institucionais à rede, e ao roteador da UFFS, responsável pela publicação dos blocos de IPs da UFFS.

Todas as configurações do equipamento são gerenciadas por uma console virtual com um sistema operacional próprio, que opera dentro de uma máquina virtual no Data Center denominada srv-panorama-01. Nessa máquina virtual, estão armazenados os backups não apenas do firewall do Data Center, mas também de todos os Campi.

Em caso de falha, temos um equipamento PALOALTO já em funcionamento, com o cabo console conectado e pré-configurado minimamente para entrar em operação imediatamente caso ocorra uma falha no equipamento principal. O tempo de inatividade esperado, em caso de falha que possa afetar o equipamento principal, seria de até 2 horas após a detecção da falha. A criticidade neste local é alta, pois qualquer interrupção afetaria todos os acessos de LAN e WAN ao Data Center e ao Campus.

3.11.3 Roteadores e Links de Internet

Atualmente temos um roteador Cisco ISR 4400 Series, responsável pela publicação dos blocos de IP da UFFS na internet, que se liga diretamente ao Firewall. Os IPs são publicados na internet através do protocolo de roteamento dinâmico conhecido como BGP, fazendo vizinhança com os roteadores do POP-SC.

A criticidade neste ambiente é baixa, pois para a saída de link utilizamos os blocos proprietários da RNP.

Além deste roteador, temos hospedado em nossa sala de WLAN do roteador Huawei de propriedade da RNP, onde chegam os links de internet. Caso o Juniper apresente problemas, possuímos um Roteador Cisco, também de propriedade da RNP, na sala ao lado do DC que pode facilmente ser ativado através do remanejamento de cabos. Nesse caso, seria necessária uma intervenção da RNP/Pop-SC para possíveis configurações no roteador. Para a UFFS, o tempo de resposta em uma situação assim seria de até 1 hora, porém, não temos como responder quanto ao parceiro.

Serviço de internet: Os acessos ao Data Center são providos pelo POP-SC da RNP através da Rede Metropolitana Comunitária de Educação e Pesquisa de Chapecó, que conecta 12 pontos entre universidades, hospitais e centros de pesquisa. Essa infraestrutura faz parte do programa Pontos de Agregação da Rede Acadêmica Catarinense (PARC), resultado da

colaboração entre a RNP e a Fundação de Amparo à Pesquisa e Inovação do Estado de Santa Catarina (Fapesc). A construção do PARC foi possível graças a uma parceria por meio de permuta com a empresa ALT Telecom (Acessoline Telecomunicações LTDA).

Atualmente, a UFFS é um dos Pontos de Agregação de Tráfego (POA) do PARC - Chapecó. O acesso à rede metropolitana e, consequentemente, o acesso da UFFS, ocorre por meio de dois links que interconectam o PAR-Chapecó ao POP-SC em Florianópolis.

Os links de escoamento são fornecidos pela RCT/FAPESC e pela RNP. Ambos operam atualmente com uma capacidade de 3Gbps em formato de agregação/backup. O link da RNP é fornecido pela operadora MHNET Telecom, enquanto o link da FAPESC é fornecido pela ALGAR TELECOM. Ambos os enlaces seguem o mesmo caminho físico até os postes. Falhas relacionadas ao LINK são de responsabilidade dos provedores de acesso à Internet. Nesses casos, a UFFS aciona a RNP, que é a contratante, para que a mesma tome as medidas necessárias junto ao provedor.

3.11.4 Controladora WLAN

A controladora WiFi é responsável pela gestão da infraestrutura de acesso sem fio da UFFS. O equipamento atual possui fonte redundante, mas está fora da garantia em caso de problemas de hardware. Em caso de perda desse equipamento, toda a estrutura de WiFi ficaria inoperante. No entanto, está previsto para 2023 um processo de contratação para renovar a solução de WiFi da UFFS.

Como medida de mitigação em caso de falha no equipamento, adotaremos a ativação do Access Point Cisco C9115AXIZ com a funcionalidade de controladora. Esse Access Point pode gerenciar até 100 outros equipamentos. Essa solução garantirá a continuidade do serviço de WiFi em caso de falha da controladora principal.

A criticidade desse serviço é moderada, pois, apesar da conectividade ainda estar disponível por meio da rede cabeada, a recuperação completa da infraestrutura de WiFi pode levar até uma semana.

3.12 Infraestrutura de telefonia

A infraestrutura de telefonia é composta por um PABX IP em uma máquina virtual e um gateway de voz IP modelo Khomp EBS Modular com um módulo E1 e um módulo GSM localizado no ER institucional. O serviço de telefonia fixa comutada é prestado pela operadora Algar Telecom.

Em caso de falha no gateway de voz, é possível realizar a conexão com a operadora através de um tronco SIP através da rede IP caso o link WAN da operadora esteja disponível, tendo tempo de resposta médio de 3 horas. Em caso de falha no PABX IP, é possível realizar uma restauração de backup da máquina virtual, tendo tempo de resposta médio de 2 horas.

A criticidade do serviço é média, considerando outras formas de comunicação existentes do público usuário do Campus e datacenter como telefonia móvel e comunicação via aplicativos de mensageria.

4 PAPÉIS E RESPONSABILIDADES

Secretaria Especial de Tecnologia e Informação (SETI): Secretaria responsável por propor políticas, planejar, coordenar, supervisionar e orientar normativamente as atividades relativa à TIC no âmbito da UFFS, assim como o acompanhamento das diretrizes e normativas dos órgãos de controle e sua aplicação na UFFS. Deve ser informada sempre que houver disrupções em quaisquer dos serviços e sistemas institucionais.

Diretoria de Infraestrutura de Tecnologia da Informação (DITI): Diretoria responsável por orquestrar ações de seus departamentos durante eventuais disrupções e suas consequências e garantir a execução deste plano de contingência. Deve ser acionada sempre que houver disrupções em quaisquer dos serviços e sistemas institucionais.

Diretoria de Sistemas de Informação (DS): Diretoria responsável por implantar e manter funcionais os sistemas de informação de âmbito acadêmico e administrativo utilizados na UFFS, sejam eles sistemas de uso corporativo produzidos por terceiros ou sistemas desenvolvidos internamente. Deve ser acionada em caso de defeitos que impossibilitam o uso mínimo das ferramentas de software hospedadas na UFFS.

Setor de Gestão do Data Center (SGDC): Responsável por gerir e manter a infraestrutura do Data Center. Desenvolve atividades e ações de prevenção e testes corriqueiros e deve ser acionado sempre que houver disrupções nos sistemas: Incêndio, UPS, Climatização, Geração de Energia de Emergência e Controle de Acesso do Data Center. Deve contatar e abrir chamado para os fornecedores responsáveis pela manutenção preventiva e corretiva desses sistemas.

Departamento de Redes de Telecomunicações (DRT): Responsável pelas ações de gerenciar e manter os serviços de redes de telecomunicações institucionais, serviços de telefonia fixa, rede lógica e segurança de redes. Deve ser acionado sempre que houver disrupções nos serviços de internet, intranet, telefonia fixa e aplicações fora do ar ou em qualquer dos sistemas de infraestrutura de redes (Switch Core, Firewalls, Roteadores).

Departamento de Infraestrutura de Aplicações (DIAPL): Responsável pelas ações que envolvem infraestrutura de aplicações, virtualização, sistemas de processamento e armazenamento de dados, sistema de Backup e rede SAN. Deve ser acionado sempre que houver disrupções nos serviços de Sites, Portais, Sistemas Web, sistemas de Armazenamento, Backup, Processamento de dados e rede SAN.

Divisão de Operações de Tecnologia da Informação (DIOTI): Responsável pelos atendimentos de 1º e 2º Níveis do Sistema de Atendimento de Chamados de TI (ATI) e suporte aos serviços de TI institucionais, bem como a manutenção da infraestrutura do Data Center. Deve ser acionada sempre que houver disrupções em quaisquer serviços e sistemas de TI institucionais.

Serviço Especial de Transportes (SET): Setor responsável pelo Contrato de Manutenção Mecânica da Reitoria. Deve ser acionado sempre que houver problemas mecânicos no Gerador do Data Center, além de ser o responsável pela reposição de combustível.

Secretaria Especial de Obras (SEO): Equipe responsável por assegurar e garantir o cumprimento de serviços como energia elétrica que chega da subestação até o Data Center. Deve ser acionada sempre que houver problemas elétricos no gerador ou na entrada de energia do Data Center.

Equipe de Vigilância do Campus Chapecó: Responsável por informar ao SGDC e à DITI caso detectem algum tipo de emergência ou hipótese acidental que venha a ocorrer em alguma das áreas sensíveis do Data Center.

5 GRUPOS EXECUTORES

Listagem dos setores/unidades responsáveis pela execução das atividades correlatas.

Sistemas	**Grupo Executor**
Incêndio	DITI, SGDC, DIOTI
UPS	DITI, SGDC, DIOTI
Climatização	DITI, SGDC, DIOTI
Gerador	DITI, SGDC, DIOTI
Controle de Acesso	DITI, SGDC, DIOTI
Elétrico	DITI, SEO, SGDC
Armazenamento	DITI, DIAPL
Backup	DITI, DIAPL
Processamento de Dados	DITI, DIAPL
Rede SAN	DITI, DIAPL
Infraestrutura de Rede	DITI, DRT
Infraestrutura de Telefonia	DITI, DRT

6 ANÁLISE DE RISCOS

Os cenários de riscos são eventos em que podem gerar um possível impacto positivo ou não à infraestrutura da instituição, são eventos que alteram o estado seguro dos elementos do ambiente. Neste, serão avaliados os impactos para auxiliar na tomada de decisões sobre quais riscos necessitam de tratamento e a prioridade para implementação do tratamento.

Nível ALTO: Representa um incidente que está causando ou irá causar uma degradação do ambiente operacional do ambiente físico seguro do DATA CENTER. Apesar da degradação, continuam em operação os serviços essenciais para a manutenção dos sistemas e da atividade jurisdicional da UFFS. Ex.: Queda de energia elétrica e o gerador não foi reabastecido;

Nível MÉDIO: Representa um incidente que possa tornar inoperante qualquer serviço de Tecnologia da Informação essencial à manutenção dos sistemas e da atividade jurisdicional da UFFS. Ex.: Problema na conectividade do Storage, indisponibilidade da rede, gerador indisponível numa eventual queda de energia elétrica;

Nível BAIXO: Representam falhas mínimas que não afetam o desempenho, serviço ou operação dos sistemas e da atividade jurisdicional da UFFS, ou então, a função afetada só é usada eventualmente ou temporariamente. Hipótese que pode ser controlada e mitigada pela equipe da DITI. Ex.: Reservatório de combustível não reabastecido.

7 PRINCIPAIS RISCOS E CONTINGENCIAMENTO

Este plano tem como objetivo ser acionado quando algum risco afetar diretamente o funcionamento dos serviços críticos, impactando na continuidade das atividades institucionais. A tabela abaixo mostra os principais riscos que podem impactar na continuidade dos serviços críticos:

Risco	**Descrição**	**Contingenciamento**
Interrupção de energia elétrica	Causada por fator externo ou interno à rede elétrica de chegada da subestação com duração da interrupção superior a 5 horas.	Gerador com tanque interno com capacidade/autonomia de 6 a 8 horas a plena carga, contando com 100 litros de reserva, totalizando em torno de 9 a 12 horas de autonomia a plena Carga. **1) A partir de 2 horas:** - Acionar a SEO e equipe responsável pela manutenção elétrica da subestação; - Verificar níveis de combustível através do sistema noc-monitor; - Verificar níveis de combustível de reserva; - Verificar situação dos demais sistemas. **2) A partir de 5 horas:** - Abastecer gerador; - Acionar o Serviço Especial de Transportes para providenciar o abastecimento de combustível para repor o estoque; - Acionar o DITI/ DIOTI/ SGDC para providenciar o abastecimento de combustível para repor o estoque; **3) Impossibilidade de reposição de combustível:** - Comunicar a toda equipe da DITI; - Efetuar o desligamento de todos os equipamentos sensíveis para não causar perdas;

Problema com equipamentos (hardwares dos sistemas)	Causado por equipamentos no final de seu ciclo de vida ou degradados que por algum motivo necessite de reparos físicos (troca de peças).	Monitoramento via Zabbix, noc-monitor e mensageria (whatsapp e telegram). Contrato com os fabricantes dos equipamentos, contrato de manutenção preventiva e corretiva com garantia e troca de peças (se necessário). Política de substituição de equipamentos no final do ciclo de vida.
Indisponibilidade de rede/circuitos	Causados principalmente por rompimento de cabos de rede e fibra óptica ou por problemas em equipamentos de redes como: roteadores, firewalls, Switches.	Monitoramento via Zabbix. Equipamentos em garantia e/ou para a troca imediata/reposição temporária. Redundância nos enlaces de internet.
Acesso ao Data Center	Acesso de pessoas não autorizadas ao ambiente interno do Data Center.	A sala do Data Center possui controle de acesso biométrico e câmera de vigilância com monitoramento 24x7x365.
Ataques externos	Ataques cibernéticos que podem causar danos ou roubo de informações dos serviços disponíveis externamente.	Equipamentos para a troca imediata e/ou reposição temporária, retorno imediato de backups caso ocorram danos aos dados armazenados.
Ataques Internos	Usuários legítimos da rede tentando acessar serviços ou equipamentos para deixá-los indisponíveis.	Monitoramento e controle de acesso aos serviços e sistemas.
Falha humana acidental	Falta de atenção dos usuários	Capacitação e política de controle de acesso aos serviços e sistemas.
Falha humana por imperícia	Falta de capacidade técnica ou conhecimento suficiente para dar suporte em algum serviço ou sistema.	Capacitação, treinamento e política de controle de acesso aos serviços e sistemas.
Risco Pessoal	Causado pela perda de capital humano.	Plano de capacitação e apoio à educação continuada.

8 ANÁLISE DO IMPACTO

A tabela a seguir mostra o mapeamento das relações de cada um dos Sistemas do Data Center com as principais Áreas/Serviços afetados.

Sistemas x Áreas afetadas	**Sistemas (Aplicações) (infraestrutura de rede local)**	**Sistemas (Aplicações) (acesso externo)**	**Acesso Externo (VPN)**	**Telefonia**	**Internet nos Campi**	**Webmail dos Alunos (Nuvem)**
Incêndio	**X**	**X**	**X**	**X**	**A**	**X**
UPS	**A**	**A**	**A**	**A**	**A**	**A**
Climatização	**A**	**A**	**A**	**A**	**A**	**A**
Gerador	**B**	**B**	**B**	**B**	**A**	**B**
Controle de acesso ao Data Center	**A**	**A**	**A**	**A**	**A**	**A**
Sistema elétrico do Data Center	**A**	**A**	**A**	**A**	**A**	**A**
Companhia de fornecimento de energia	**X**	**X**	**X**	**X**	**A**	**X**
Armazenamento de dados	**A**	**A**	**A**	**A**	**A**	**A**
Backup	**B**	**B**	**B**	**B**	**A**	**A**
Processamento de Dados	**A**	**A**	**A**	**A**	**A**	**A**
Rede SAN	**A**	**A**	**A**	**A**	**A**	**A**
Switch Core	**B**	**B**	**B**	**B**	**A**	**B**
Enlace Internet	**A**	**A**	**A**	**A**	**A**	**A**
Firewall	**B**	**B**	**B**	**B**	**A**	**B**

Catálogo de códigos:

X - Serviço fica inoperante;

A - Alternativa disponível para o serviço (Redundância < 1 minuto)

B - Alternativa disponível para o serviço (Reparo técnico > 4 horas)

9 COMUNICAÇÃO

Quem deve comunicar: Analista de monitoramento ou qualquer servidor que detecte algum incidente que possa gerar risco aos sistemas e serviços.

A quem comunicar: Seguir o Item 4 - Papéis e Responsabilidades.

Como comunicar: O item 4 - Papéis e Responsabilidades possui a lista dos responsáveis por cada sistema e também deverá ser feito o registro do incidente no sistema ATI (https://ati.uffs.edu.br) e encaminhar para o Grupo Executor - Item 6.

10 CATÁLOGO DE CONTATOS INTERNOS

FUNÇÃO	NOME	CONTATO
Diretor de Infraestrutura de TI (DITI)	Jefferson Caramori	49 2049-2612/ 49 98435-7099 dir.diti@uffs.edu.br
Diretor de Sistemas de Informação (DS)	Ariel Escobar	49 2049-2621 dir.ds@uffs.edu.br
Secretário de TI (SETI)	Ronaldo Antonio Breda	49 2049-2655 seti@uffs.edu.br
Chefe de Infraestrutura de Aplicações (DIAPL)	Geovano Lago Quatrin	49 2049-2611 diti.diapl@uffs.edu.br
Chefe de Redes e Telecomunicações (DRT)	Neimar Marcos Assmann	49 2049-2630 diti.drt@uffs.edu.br
Chefe da Divisão de Operações de Tecnologia da Informação (DIOTI)	Rafael Arcari	49 2049-2610 diti.dioti@uffs.edu.br
Chefe do Setor de Gestão do Data Center (SGDC)	Ezequiel Roque dos Santos	49 2049-2609 data.center@uffs.edu.br
Serviço Especial de Transportes (SET)	Gelson Guzzon	49 2049-3122 transportes.reitoria@uffs.edu.br
Secretaria Especial de Obras (SEO)	Fabio Correa Gasparetto	49 2049-3119 seobras@uffs.edu.br

Monitoramento - Vigilantes	Sala de Vigilância Prédio Data Center	49 2049-6490

11 CATÁLOGO DE PRESTADORES DE SERVIÇOS

O Grupo Executor deve comunicar aos seus principais prestadores de serviços, entre eles:

Empresa	**Responsável**	**Contato**
VERTIV (UPS e Climatização)	Gilmar Silva	(11) 3618-5441 (12) 991895105 gilmar.silva@vertiv.com
DAT TECNOLOGIA (Sistema de Backup e Storage)	Danillo Serra Leonel Serra	(61) 3043-8111 (61)99120-8145 danillo.serra@dattec.com.br (61)3043-8111 (61)99301-9216 leonel.serra@dattec.com.br www.dattec.com.br
VIRTUAL TI (Central de Incêndio)	Supervisão técnica Ruy Miamoto Gerência Técnica Weslei Cunha Engenharia Carlos L. Dorow Diretoria Comercial Leandro Nalin	(47) 3422-5858 (47) 99219-6300 (47) 3422-5858 (47) 99222-9819 (47) 99142-8391 (47) 98890-3796 (47) 3422-5858 (47) 99923-0200 0800 740 4530
TELTEC Solutions (Firewall e Switch DMZ)		0800-719-9903 (048)3031-3470

12 REFERÊNCIAS

BRAUNM, Charles, **Projeto de disponibilidade de Data Center para suportar serviços críticos em uma indústria de artefatos de borracha no interior do Rio Grande do Sul**:

Estudo de caso. Trabalho de Conclusção do Curso de Especialização em Datacenter: Projetos, Operações e Serviços, UNISUL.

DAT tecnologia. Disponível em: <https://www.dattec.com.br/>. Acesso em: 12 de jul. de 2021.

FREITAS, Thiago. **Business Contingency Plans**. 2013. 50 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamentos Acadêmicos de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Plano de Contingência, Continuidade de Negócios e Recuperação de Desastres, da INFRA ASSET. Disponível em: <http://www.infraasset.com>. Acesso em 08 de jul. de 2021.

PLANO de contingência da Universidade de Brasília. Centro de Informática. Disponível em: <https://unb.br/images/Noticias/2020/Documentos/2020-PlanoContingenciaCovid19_v6.pdf>. Acesso em: 30 de ago. de 2021.

PLANO de contingência e continuidade dos serviços de tecnologia da informação. Coordenadoria de Tecnologia da Informação, IFSP - Campus Ipatinga. Disponível em: <https://itp.ifsp.edu.br/files/CTI/Plano_de_Contingencia_IFSP_Campus_Itapetininga.pdf>. Acesso em: 23 de jun. de 2021.

PLANO de continuidade de TI. SETIM (Secretaria de Tecnologia da Informação e Modernização). TJBA. Disponível em: <http://www5.tjba.jus.br/setim/images/pdf/Plano-de-continuidade.pdf>. Acesso em: 16 de jun. de 2021.

SISTEMA de Gestão de Continuidade de Negócios de Tecnologia da Informação e Comunicação. SGCN - TIC, IFS. Disponível em: <https://www.ifsc.edu.br/documents/526028/877206/Sistema+de+Gest%C3%A3o+de+Continuidade+de+Neg%C3%B3cios+de+TI+do+IFSC.pdf/f8680616-60be-9a03-3f9d-28159ebe5ab6>. Acesso em: 27 de jul. de 2021.