

RESOLUÇÃO nº1/2020 (PROAD)

“Dispõe sobre o Plano de Contingência do Setor de Tecnologia da Informação e Plano de Atualização e Manutenção de Equipamentos do Centro Universitário Campo Real. ”

O Centro Universitário Campo Real, mantido pela UB Campo Real Educacional S/A, por intermédio de seu Pró-Reitor de Administração e Planejamento,

RESOLVE:

Art. 1º. Aprovar o Plano de Contingência e Plano de Atualização e Manutenção de Equipamentos do Setor de Tecnologia da Informação.

Art. 2º. Revogam-se as disposições em contrário.

Guarapuava, 20 de janeiro de 2020.

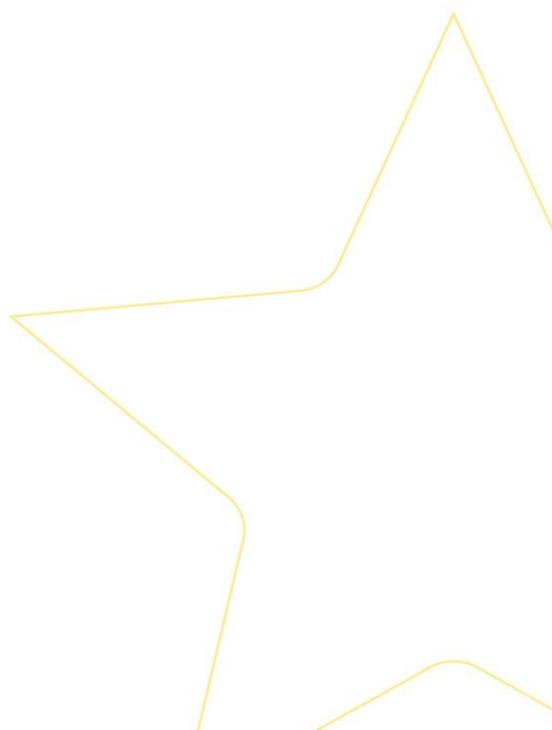
Professor Adailton Marcelo Lehrer
Pró-Reitor de Administração e Planejamento





Sumário

1. Objetivo	4
2. Contingência	5
2.1. Falta de Energia Elétrica	5
2.2. Falha de Equipamentos Eletrônicos	6
2.3. Erro Humano	6
2.4. Desastres Naturais	7
2.5. Crime Cibernético	7
2.6. Vírus	7
3. Importância dos Dados	8
4. Backup	8
5. Diretrizes	8
7. Contato de Emergência	9



1. OBJETIVO

Este documento tem por objetivo orientar o gestor de TI em casos de desastres naturais e ou por falha de equipamentos.

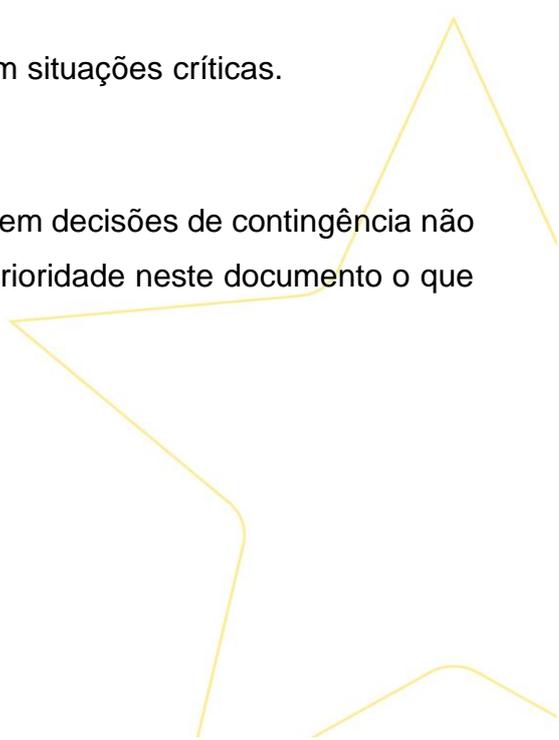
É sempre bom ter um “plano B” para situações críticas e desastrosas que aparecem de repente, mais que merecem uma atenção e dedicação total. Hoje podemos afirmar que uma empresa sem um departamento de TI estruturado não é nada, mais além disso deve-se saber o que fazer quando algo de ruim acontecer.

O plano de contingência visa, ajudar em casos em que não se tem mais o que fazer mais precisa-se tomar atitudes rápidas para que o tempo de parada seja o menor possível.

Objetivos:

- I – Diminuir o impacto causado pelo tempo de parada;
- II – Agilizar o processo de contingência quando necessário;
- III – Padronizar normas a serem tomadas dentro do departamento em casos de contingência;
- IV – Facilitar as tomadas de decisões em situações críticas.

Definir as prioridades a serem tomadas em decisões de contingência não é fácil, por isso vamos elencar em ordem de prioridade neste documento o que deve ser priorizado nesses casos.



2. CONTINGÊNCIA

É um acaso, uma eventualidade de algo, ou acontecimento que tem como fundamento a incerteza de que pode ou não vir acontecer.

Tendo isto em vista, podemos afirmar a importância de se ter um plano de contingência atualizado e preciso.

Podemos identificar uma contingência, quando não se sabe e/ou não se tem mais o que fazer, nesses casos procuramos o plano de contingência para nos orientar e guiar os próximos passos a serem tomados.

Possíveis contingências que podem acontecer.

2.1. Falta de energia elétrica

Os equipamentos principais do NTI do Bloco I e do CT estão ligados a um nobreak de 3300VA com um consumo atual de 680Watts proporcionando uma autonomia de 1 hora caso haja falta de energia.

Já os equipamentos do NTI do Bloco do CT estão ligados a um nobreak de 3300VA com um consumo atual de 105Watts proporcionando uma autonomia de 5 horas caso haja falta de energia.

Os equipamentos do CAU do Bloco do CT estão ligados a um nobreak de 3300VA com um consumo atual de 60Watts proporcionando uma autonomia de 5 horas caso haja falta de energia.

Os outros setores da Instituição estão em projeto orçamentário para expansão dos sistemas de segurança de energia.

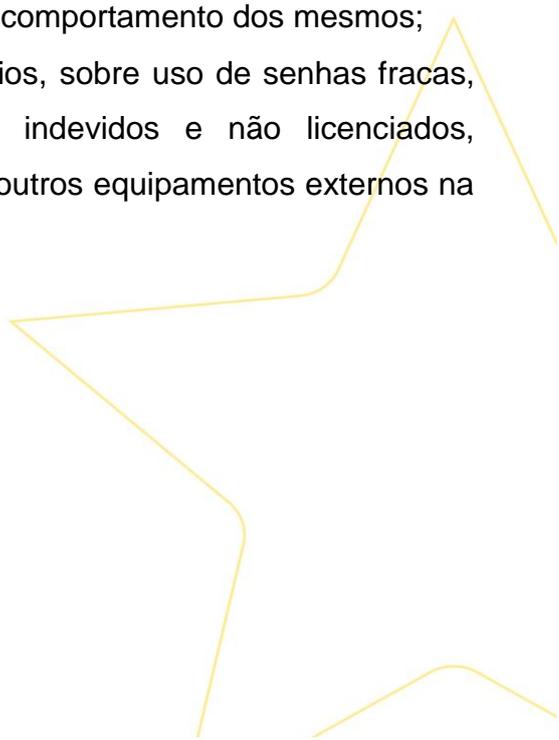
2.2. Falha de Equipamentos Eletrônicos

Eventualmente os equipamentos eletrônicos podem vir apresentar problemas, e para evitar, faz-se necessário uma manutenção preventiva nos mesmo a fim de evitar tais problemas. Laboratórios são formatados e verificados as licenças semestralmente no período de férias dos acadêmicos, também é realizada a limpeza física, troca de periféricos e demais componentes que forem necessários.

2.3. Erro humano

Algumas contingências são causadas por negligências dos gestores do departamento, não realizando manutenções preventivas em equipamentos sensíveis e que podem acarretar em contingências.

Ações realizadas, para evitar contingencias, no sentido da prevenção, como:

- Política de segurança documentada, regular o acesso de dados e softwares utilizados;
 - Controle de acesso, liberando permissões dos sistemas caso a caso e monitorar o comportamento dos mesmos;
 - Conscientização de usuários, sobre uso de senhas fracas, downloads de softwares indevidos e não licenciados, conexão de pendrives ou outros equipamentos externos na máquina.
- 

2.4. Desastres Naturais

Não estamos livres de desastres naturais como chuvas fortes, enxurradas, enchentes, quedas de estruturas e etc. Muitas vezes não temos como evitar estes acontecimentos.

Por conta disto, cópias de segurança dos principais sistemas são efetuadas diariamente na nuvem.

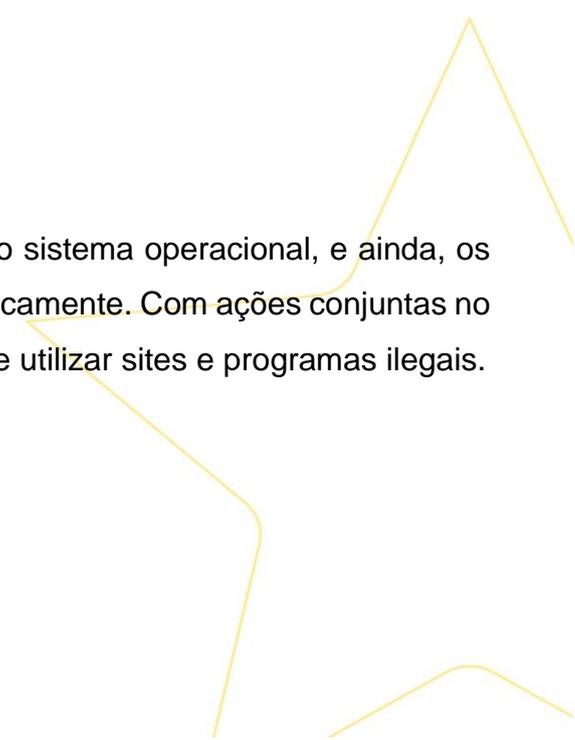
2.5. Crime Cibernético

Tecnologias e recursos de trabalho se expandem diariamente, e por isso as incidências de segurança se apresentam diariamente. Seja por ações de usuários ou softwares mal-intencionados (MalWare), sites maliciosos entre outros.

E para uma pequena prevenção contra instalações indevidas e mau uso dos equipamentos, na rede administrativa nós temos domínio configurado e políticas de segurança configuradas através de GPO fornecidas por sistema operacional Windows Server e na rede acadêmica, os equipamentos são verificados periodicamente a procura de instalações indevidas.

2.6. Vírus

Usa-se o antivírus oferecido através do sistema operacional, e ainda, os equipamentos são preparados do zero periodicamente. Com ações conjuntas no sentido de orientar usuários dos perigos de se utilizar sites e programas ilegais.



3. IMPORTÂNCIA DOS DADOS

Podemos elencar os principais, para que possam ser tratados com prioridades. Sendo eles de maior prioridade para menor:

1. Banco de dados - Sistema de gestão de pessoas, contabilidade, sistema antigo de gestão acadêmica, CPJ (sistema para o escritório de práticas jurídicas), sistema da biblioteca e mais os sistemas internos como: clinica, agenda telefônica, revista, repositório, cadastro eventos;
2. Documentos relacionados aos departamentos.

4. BACKUP

Os mesmos são realizados 2 vezes ao dia, são subscritos da semana anterior ficando sempre disponível 14 backups, sendo realizados de segunda a segunda no período da manhã e da noite. Os documentos dos setores estão em nuvem.

5. DIRETRIZES

As diretrizes definidas que podem ser aplicadas pelo departamento.

- **Identificação da Contingência**

Antes de se tomar qualquer decisão deve-se identificar o motivo da paralisação de um serviço, software, hardware ou de algum departamento específico.

- **Verificar o impacto e a urgência.**

Quanto mais alto o impacto mais urgente será realizado a contingência.

- **Ações**

- Substituição de peças ou partes caso haja necessidade;
- Reinstalação ou atualização de sistemas;
- Reestabelecimento dos serviços parados;

- **Histórico de contingência**

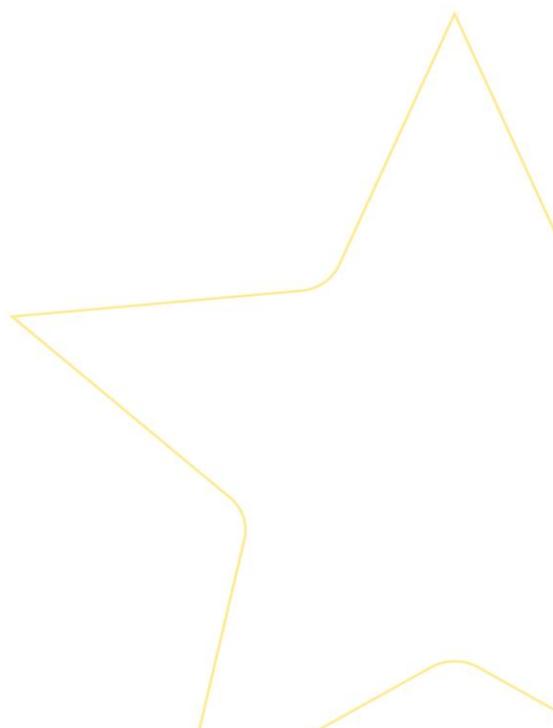
Verificar se o problema está se repetindo pelo mesmo motivo ou se é por outro, caso seja recorrente verificar para dar uma solução definitiva para o mesmo se possível.

6. CONTATO DE EMERGÊNCIA

Em caso de emergência a Instituição poderá entrar em contato com os responsáveis através dos números:

Briana do Prado Lopes - Encarregada de TI
(42) 9 9903-5423

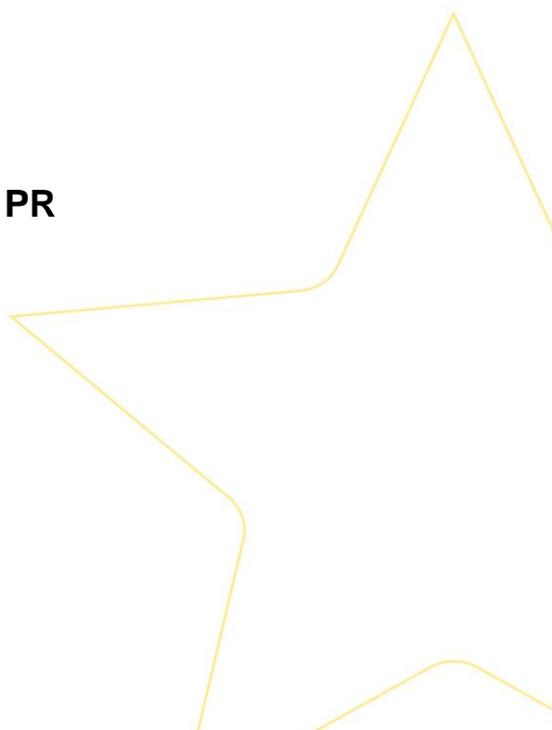
Marcelo Ribeiro Salmon - Consultor de TI
(42) 9 8803-4707



**PLANO DE ATUALIZAÇÃO E MANUTENÇÃO DOS
EQUIPAMENTOS**

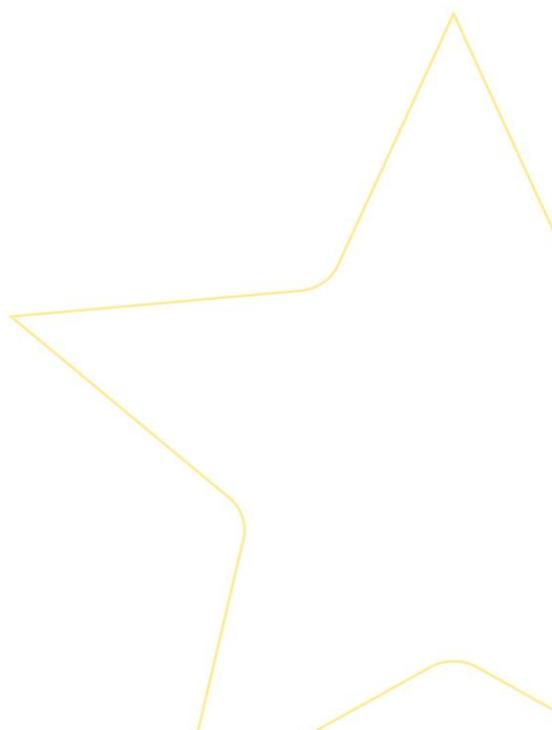
Centro Universitário Campo Real

Guarapuava - PR



SUMÁRIO

1. Introdução	4
2. Objetivos	4
3. Atualização Tecnológica	5
3.1 Plano de Melhorias de Acesso à Internet	5
3.2 Plano de Melhorias do Sistema de Manutenção de Energia	5
3.3 Conectividade dos Setores NTI CT e CAU	6
4. Expansão de Hardware e Software	6
5. Manutenção Preventiva e Corretiva	6



1. INTRODUÇÃO

O Centro Universitário Campo Real, dispõe atualmente de infraestrutura de Tecnologia da Informação com uma rede que contém 284 computadores só para os acadêmicos.

A Campo Real conta com uma estrutura própria de acesso à Internet, para uso acadêmico, que opera com velocidade máxima de 500MB por banda larga, disponível através de computadores ligados a rede cabeada com pontos de transmissão de rede sem fio, nos corredores e dentro de algumas salas de aula.

Este recurso está disponível internamente aos alunos, tanto para as atividades de aula como para as atividades extra aula, oferecendo possibilidades de pesquisa e desenvolvimento de trabalhos.

Para manter este parque tecnológico, a Instituição conta com um Setor de Tecnologia da Informação, composto pelo corpo técnico especializado, Encarregada de TI, Consultor de TI e estagiários . Estes são responsáveis pela manutenção preventiva e corretiva dessa infraestrutura.

2. OBJETIVOS

A política de aquisição, atualização e manutenção de equipamentos de Tecnologia da Informação visa garantir aos cursos de graduação e extensão da Campo Real a infraestrutura de tecnologia adequada para seu melhor funcionamento.

3. ATUALIZAÇÃO TECNOLÓGICA

Anualmente são revistas todas as necessidades de atualização tecnológica dos equipamentos e softwares. Estas revisões são baseadas no orçamento corporativo para os investimentos. As revisões acontecem nos

meses de Dezembro, Janeiro e Julho, acompanhando o início dos períodos letivos semestrais.

O Plano Gestor da Tecnologia da Informação tem como objetivo fornecer diretrizes para a organização, alinhando tecnologia e planejamento e alocando de maneira estruturada os recursos orçamentários de infraestrutura tecnológica.

Este plano abrange os seguintes componentes de Tecnologia da Informação:

- Softwares Acadêmicos
- Hardware
- Infraestrutura
- Sistemas Operacionais

3.1 Plano de Melhorias de Acesso à Internet

Hoje a Campo Real conta com um link de 500MB de internet banda larga distribuída em toda a rede acadêmica e administrativa através de rede cabeada e rede wi-fi. Para proporcionar melhorias na rede, a Campo Real contará com um sistema de check in interno dos alunos para uso da rede wi-fi, onde o aluno irá logar com o e-mail institucional e uma senha previamente cadastrada pelo Setor de TI, possibilitando uma expansão gradativa na melhoria de conexão.

3.2 Plano de Melhorias do Sistema de Manutenção de Energia

Pretende-se ampliar os sistemas de nobreaks aos setores mais sensíveis da Instituição.

3.3 Conectividade dos Setores NTI CT e CAU

Colocado na previsão orçamentária a atualização da conectividade entre os setores NTI do Bloco do CT e CAU que hoje é feita por par metálico e futuramente por fibra optica.

4. EXPANSÃO DE HARDWARE E SOFTWARE

A expansão da infraestrutura de tecnologia está prevista no PDI (Plano de Desenvolvimento Institucional) no período de 2018-2022, do Centro Universitário Campo Real.

Após aprovação pela direção, a necessidade de expansão deve ser encaminhada ao Setor de Tecnologia da Informação que, por sua vez, definirá as configurações de hardwares e softwares necessárias, bem como o projeto de implantação, e encaminhará para o Setor de Compras.

A Campo Real vem periodicamente substituindo os equipamentos da marca Ubiquiti por equipamentos da marca Aruba. Como já foi feito em outros espaços da Instituição.

5. MANUTENÇÃO PREVENTIVA E CORRETIVA

O Setor de Tecnologia da Informação possui uma equipe de técnicos e monitores de laboratórios de informática. Essa equipe é responsável por manter a infraestrutura em condições perfeitas de uso, oferecendo serviços de suporte, manutenção preventiva e manutenção corretiva.

O Setor de Tecnologia da Informação planeja e executa um cronograma de manutenção preventiva anualmente em todos os equipamentos de Tecnologia da Informação da Instituição.

As manutenções corretivas são realizadas através das ocorrências identificadas na manutenção preventiva. E também podem ser solicitadas pelos usuários diretamente ao Setor de Tecnologia da Informação, através do e-mail nti@camporeal.edu.br ou do WhatsApp 42 9 8873-5977.

O suporte e manutenção dos equipamentos obedecem ao seguinte programa de manutenção:

- **Manutenção Permanente:** Consiste na verificação diária do funcionamento normal de todos os computadores, antes do início de utilização do Laboratório de Informática;
- **Manutenção Preventiva:** Realizada semanalmente no

Laboratório de Informática, onde é realizada a verificação das conexões e estado geral dos equipamentos;

- **Manutenção Corretiva (interna):** Consiste na solução dos problemas detectados na manutenção permanente e preventiva;
- **Manutenção Corretiva (externa):** Realizada por empresa de suporte externa. Consiste na solução dos problemas detectados na manutenção permanente e preventiva, não solucionados pela manutenção corretiva interna. Realiza manutenção e/ou troca de componentes. As manutenções externas são realizadas por empresas contratadas pelo Setor de Tecnologia da Informação do Grupo Educacional.