Resolução nº 2/2023 – Pró-Reitoria de Administração e Planejamento

Aprova Plano de Contingência do Departamento de Tecnologia da Informação do Centro Universitário Campo Real – Laranjeiras do Sul.

O Pró-Reitor de Administração e Planejamento do Centro Universitário Campo Real, no uso de suas atribuições legais

RESOLVE:

Art 1º Aprovar o Plano de Contingência do Departamento de Tecnologia da Informação do Centro Universitário Campo Real – Laranjeiras do Sul.

Art 2º Revogam-se as disposições em contrário

Centro Universitário Campo Real, 6 de fevereiro de 2023.

Professor Ayres Siqueira Silva Pró-Reitor de Administração e Planejamento

SUMÁRIO

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 estão ligados a um nobreak de 1200VA com um consumo atual de 140Watts proporcionando uma autonomia de 40 minutos 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 mesmos 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 contingências.

Ações realizadas, para evitar contingências, 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 etc. Muitas vezes não temos como evitar estes acontecimentos.

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

2.5. 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. 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 reincidente verificar para dar uma solução definitiva para o mesmo se possível.

4. CONTATO DE EMERGÊNCIA

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

Andrei Alves Albuquerque dos Santos - Encarregado de TI
(42) 9 9903-2774

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