RESOLUÇÃO Nº2/2022 (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, 16 de Dezembro de 2022.

Professor Ayres Siqueira Silva

Pró-Reitor de Administração e Planejamento

PLANO DE CONTINGÊNCIA DO NÚCLEO DE TECNOLOGIA DA INFORMAÇÃO

Centro Universitário Campo Real

Guarapuava

SUMÁRIO

1. OBJETIVO 4
2. NÍVEIS DE INCIDENTES 4
3. PRINCIPAIS RISCOS 5
4. PROCEDIMENTOS PARA BACKUP 6
   4.1. Backup 6
   4.2. Procedimentos 6
5. CAUSAS E PROCEDIMENTOS DE CONTINGÊNCIA 6
   5.1. Problemas de conexão com a Rede de Internet 6
   5.2. Problemas de conexão com os sistemas internos 7
   5.3. Problemas com falta de energia elétrica 8
   5.4. Problemas com cabeamento da rede 8
   5.5. Problemas com equipamentos de rede 9
   5.6. Problemas com Wi-Fi 9
   5.7. Problemas com computadores em Laboratórios de Informática 10
   5.8. Problemas com computadores Administrativos 10
   5.9. Problemas com impressoras 11
   5.10. Ataques Externos e Internos 11
   5.11. Falha na climatização do Data Center 12
   5.12. Falha Humana 12
6. CONTATO DE EMERGÊNCIA 13

1. OBJETIVO

Este documento tem por objetivo orientar o gestor de Tecnologia da Informação sobre como orientar e implementar um plano de contingência, a fim de minimizar os impactos negativos causados por eventos inesperados.

Um plano de contingência, é um documento que define ações a serem tomadas para restaurar os sistemas e serviços do TI em caso de desastres ou falhas. Alguns tipos de desastres e falhas que podem ocorrer e afetar o TI são:

- Desastres naturais, como incêndios, inundações, terremotos e furacões;
- Falhas de equipamentos, como queda de energia, falha de hardware ou software;
- Ataques cibernéticos;
- Erros humanos.

2. NÍVEIS DE INCIDENTES

Nível I – Causas acidentais, que podem ser contidas pela equipe de TI e que não afetam no trabalho dos serviços e servidores. Exemplo: Problemas referentes a periféricos dos computadores, ou até mesmo os próprios computadores.

Nível II – Causas acidentais que impedem o uso de certo serviço ou sistema. Exemplo: Problemas com máquinas virtuais e serviços MySQL.

Nível III – Causas acidentais que impede o uso de todos os sistemas da Instituição. Exemplo: Falha na conexão com a internet e comunicação com os servidores ou queda total de energia elétrica.

3. PRINCIPAIS RISCOS

A tabela abaixa elenca os principais riscos que podem ocorrer na Instituição no dia a dia, o nível do risco e aponta quais parâmetros para reportar as possíveis causas da ocorrência

Riscos	Nível do Risco	Parâmetros
Interrupção de energia	Nível III	Causada por fator externo à rede elétrica dos blocos da Instituição. Causada por fator interno que possa comprometer a rede elétrica dos blocos, como curto-circuito, picos de energia, incêndio, infiltrações.
Falha na climatização do Data Center	Nível III	Causada por falha no sistema de refrigeração dos equipamentos do Data Center, o que ocasiona no superaquecimento desses ativos.
Falha na rede	Nível III	Causada por falhas dos equipamentos que fazem a distribuição como Switches ou Firewall. Causada por rompimento de cabos que façam a conectividade dos pontos de distribuição.
Falha Humana	Nível I	Causada por acidente ao manusear equipamentos
Ataques Externos	Nível II	Causado por ataque virutal que compromete a integridade dos dispositivos e serviços.

4. PROCEDIMENTOS PARA BACKUP

4.1. 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.

O sistema acadêmico e o Ambiente Virtual de Aprendizagem ficam disponível 24x7, sendo 24 horas por dia e 7 dias por semana ininterruptos.

4.2. Procedimentos

Para restauração de um Backup, o mesmo deve ser solicitado ao setor de TI e o mesmo será feito de acordo com o procedimento específico para aquela situação.

5. CAUSAS E PROCEDIMENTOS DE CONTINGÊNCIA

5.1. Problemas de conexão com a Rede de Internet

O setor de TI será alertado via Zabbix (Sistema de monitoramento), ao qual será emitido um alerta descrevendo qual dispositivo e porta não está respondendo.

Zabbix Monitor Switch Core

Identificar a causa do problema:

- Primeiro deve-se identificar se o problema é em apenas um equipamento;
- Verificar se o dispositivo conectado a ele está conseguindo se comunicar com o serviço de DHCP (protocolo de configuração dinâmica de host);
- Verificar se o Switch Core está operante;
- Em seguida verificar se o Firewall está operante;
- Verificar se a porta de UPLink do dispositivo está operante.

Caso seja detetado um problema externo relacionado ao link de internet, o setor de TI é responsável por abrir um chamado diretamente com a operadora, visando reestabelecer a conexão do serviço.

Informar a previsão de tempo de retomada dos serviços.

5.2. Problemas de conexão com os sistemas internos

Identificar a causa do problema:

- Verificar se o Servidor ao qual possui a máquina virtual responsável pelo serviço, está operante;
- Caso esteja operante, deve-se verificar se a máquina virtual que possui o serviço está em execução;
- Verificar se as interfaces de rede do servidor estão funcionando corretamente;
- Verificar a comunicação com o servidor da mantenedora;
- Se for necessário, acionar os Backups para recuperação dos dados;

Informar a previsão de tempo de retomada dos serviços.

5.3. Problemas com falta de energia elétrica

Caso seja identificada uma falta de energia na Instituição, o setor de TI deve informar a PROAD Pró Reitoria de Administração e Planejamento para que as devidas providências sejam tomadas.

- Os principais equipamentos do setor de TI de ambos os blocos da Instituição estão ligados a um nobreak de 3300VA com um consumo atual de 680Watts, o que proporciona uma autonomia de 60 minutos;
- Os equipamentos do setor de atendimento estão ligados a um nobreak de 3300VA com um consumo atual de 70Watts, o que proporciona uma autonomia de 280 minutos;

Demais setores da Instituição estão em projeto orçamentário para expensão dos sistemas de segurança e energia elétrica.

5.4. Problemas com cabeamento da rede

O setor de TI será alertado via Zabbix (Sistema de monitoramento), ao qual será emitido um alerta descrevendo qual dispositivo e porta não está respondendo.

- Detectar o problema fazendo testes no cabeamento utilizando Zumbador (equipamento ao qual é conectado em cada ponta do cabo, e caso o cabo esteja em funcionamento será emitido um som pelo equipamento);
- Caso o equipamento não emita nenhum som, deve-se refazer as conexões;

Caso o cabo não volte a operar, o setor de TI é responsável por agendar a troca do cabo o quanto antes.

5.5. Problemas com equipamentos de rede

O setor de TI será alertado via Zabbix (Sistema de monitoramento), ao qual será emitido um alerta descrevendo qual dispositivo e porta não está respondendo.

- Primeiro deve-se fazer o processo de reinicialização do equipamento;
- Em seguida verificar o cabeamento ao qual o dispositivo está ligado, e refazendo as conexões caso necessário;
- Caso o equipamento continue apresentando a mesma falha, deve-se acionar a garantia, caso ainda possua.
- Se possível fazer a manutenção do equipamento;

Se não foi possível acionar a garantia e nem realizar a manutenção, será necessário efetuar a troca do equipamento o quanto antes.

5.6. Problemas com Wi-Fi

O setor de TI poderá visualizar se algum AP ou Access Point (Equipamento Wi-Fi) está inoperante através do Controlador Unifi (Sistema que faz o gerenciamento das AP)

DEVICE NAME	STATUS ↑	EXPERIENCE	MODEL
Corredor Piso 3 CT	CONNECTED	No clients	UAP
EPJ	CONNECTED	95%	U6-LR
Recepção Real Clin	CONNECTED	96%	UAP
Chanceler - Sala Dr Pacheco	CONNECTED	No clients	UAP
Reitoria - Sala Prof Edson	CONNECTED	98%	UAP
Sala dos Professores Bloco I	CONNECTED	97%	UAP
Corredor Labs BI	CONNECTED	95%	UAP
Corredor NTI	CONNECTED	93%	UAP-AC-LR
Salão Nobre	CONNECTED	86%	UAP-AC-Pro
Corredor Labs Restaurante	CONNECTED	86%	UAP
Auditorio	CONNECTED	95%	U6-LR
Clinica Veterinaria	CONNECTED	97%	UAP
Sala Pós	CONNECTED	No clients	UAP
Sala dos Professores CT	CONNECTED 100 FDX	94%	UAP-AC-LR
CAU - Nova Sec/Fin	CONNECTED 100 FDX	95%	UAP-AC-Pro

Unifi Controller

- Caso o Status esteja com Disconnect, é necessário verificar o cabo ao que está conectado na AP e refazer as conexões se necessário;
- Se estiver com status de “Failed Adopting” deve-se realizar o procedimento de Reset do equipamento e em seguida configura-lo novamente.

Caso o problema persista é necessário realizar a troca do equipamento.

5.7. Problemas com computadores em Laboratórios de Informática

As máquinas passam por manutenções periódicas a cada 6 meses nos intervalos dos semestres, onde são feitas imagens com atualizações do sistema operacional e softwares solicitados e aprovados. Durante este período cabos e conexões são testados e reparados se necessário.

Os professores que estão utilizando o laboratório, podem entrar em contato com o setor de TI através do número de WhatsApp ou solicitar nas recepções, para verificar o problema. Caso seja um problema que impeça a continuidade da aula, é feito um remanejamento de laboratório até que o problema seja solucionado.

5.8. Problemas com computadores Administrativos

O funcionário que estiver com problemas no equipamento, pode entrar em contato com o setor de TI através do número de ramal, número de WhatsApp ou solicitando na recepção.

- O setor de TI destina alguém para realizar o atendimento para resolução do problema;
- Caso não seja possível realizar a manutenção no momento, o equipamento é transportado até o setor de TI para realizar a manutenção e o funcionário é direcionado a outro equipamento para continuar o trabalho.

Caso não hajam equipamentos disponíveis, o setor de TI pode solicitar uma máquina de backup para uma empresa terceirizada, para que o funcionário dê continuidade aos trabalhos.

5.9. Problemas com impressoras

O funcionário que estiver com problemas com impressora, pode entrar em contato com o setor de TI através do número de ramal, número de WhatsApp ou solicitando na recepção.

- O setor de TI destina alguém para realizar o atendimento para resolução do problema;
- Se o problema for papel atolado, é feito o procedimento de desatolamento;
- Se o problema for falta de tinta de tonner, é feita a troca do mesmo, caso o setor possua em estoque;
- Se o problema for conexão de impressora com o computador, é feita a reinstalação da mesma no computador;

Se for outro problema, o setor de TI pode entrar em contato com uma empresa terceirizada para agendar uma manutenção mais especializada.

5.10. Ataques Externos e Internos

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.

5.11. Falha na climatização do Data Center

O Setor de TI possui sistemas de refrigeração nos Data Centers espalhados pelos blocos, o mesmo auxilia a manter os equipamentos em baixa temperatura. Caso um dos sistemas falhar, o Data Center acaba ficando comprometido tendo a sua temperatura aumentada e causando superaquecimento dos equipamentos.

O Setor de TI periodicamente deve realizar a verificação da integridade dos sistemas de refrigeração.

E caso algum deles comece a falhar, o Setor de TI deve imediatamente entrar em contato com a empresa terceirizada responsável para realizar a manutenção em cunho emergencial.

5.12. Falha Humana

Alguns erros são causados por negligências dos gestores do departamento, não realizando manutenções preventivas em equipamentos sensíveis e que podem acarretar em 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 monitorando o comportamento dos mesmos;
- Conscientizando os usuários, sobre o uso de senhas fracas, download de softwares indevidos e não licenciados, conexão de pendrives ou outros equipamentos externos no computador.

6. 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

Lucas Vinicius Kolody – Auxiliar de TI
(42) 9 9165-7349

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

Cartuchos Maxtoner – Empresa responsável pelas impressoras
(42) 9 8804-3703

Artec Climatização – Empresa responsável pelo sistema de refrigeração
(42) 9 9132-2804