



CENTRO UNIVERSITÁRIO FUNVIC



Credenciado pela portaria nº. 1.270, de 04/07/2019, D.O.U. nº 128, seção 1, pág. 59, de 05/07/2019

MANTENEDORA

FUNVIC – FUNDAÇÃO UNIVERSITÁRIA VIDA CRISTÃ

MANTIDO

UNIFUNVIC

CENTRO UNIVERSITÁRIO FUNVIC



**PLANO DE CONTINGÊNCIA
DO
UNIFUNVIC**

PINDAMONHANGABA/SP

2024



CENTRO UNIVERSITÁRIO FUNVIC – UNIFUNVIC

**PLANO DE CONTINGÊNCIA
DO
UNIFUNVIC**

1. OBJETIVO

O objetivo deste plano de contingência é assegurar a continuidade dos serviços essenciais de TI, mitigando os impactos de eventuais falhas nos sistemas que suportam as atividades administrativas e acadêmicas da Fundação Universitária Vida Cristã (Centro Universitário FUNVIC - UniFUNVIC). Com isso, busca-se garantir a implementação de medidas de proteção ágeis e eficazes em situações de emergência, assegurando que os processos críticos de TI, relacionados a sistemas como portais acadêmicos, plataformas de ensino a distância (EAD) e serviços administrativos, continuem operando com o mínimo de interrupção. Este plano visa também organizar procedimentos de comunicação, alocação de recursos e mobilização das equipes para que qualquer incidente ou contingência seja tratado de maneira coordenada, com ações voltadas tanto para a correção quanto para a eliminação do problema.

2. APLICAÇÃO

Este plano de contingência aplica-se a todos os serviços de tecnologia da informação que envolvem a gestão, operação e suporte da infraestrutura de TI da UniFUNVIC, abrangendo sistemas acadêmicos, redes internas, Data Center, equipamentos de informática e demais ativos de TI da instituição. Abrange tanto as operações regulares quanto as ações preventivas e corretivas em casos de emergências que afetem diretamente o desempenho dos serviços de TI.



3. ESCLARECIMENTOS / DEFINIÇÕES

- **Acionamento:** É o processo de comunicação formal com as equipes envolvidas no gerenciamento de incidentes, de acordo com as normas estabelecidas. O acionamento segue uma ordem de prioridades, garantindo que as equipes sejam mobilizadas adequadamente para agir com rapidez e precisão em resposta à emergência.

- **Administrador do Plano de Contingência:** Pessoa designada pela instituição para gerenciar a atualização, a revisão e a manutenção contínua do plano de contingência. Esta função inclui garantir que os dados e procedimentos estejam sempre atualizados e que todos os envolvidos estejam cientes de suas responsabilidades e papéis em uma situação de crise.

- **Áreas Sensíveis:** São as áreas que sofrem maiores impactos negativos em casos de emergências. Isso inclui laboratórios de informática, salas administrativas, o Data Center e outros locais que contenham equipamentos críticos de TI. Nessas áreas, qualquer interrupção pode comprometer diretamente as operações acadêmicas e administrativas.

- **Áreas Vulneráveis:** Referem-se aos locais que podem ser afetados por um evento de falha, mas cujos impactos são limitados ou indiretos. Essas áreas podem ser atingidas pelos efeitos secundários de uma falha, como a queda de sistemas internos ou interrupções de rede.

- **Contingência:** Situação de risco potencial, geralmente inerente às atividades e ao uso de equipamentos de TI. A contingência representa a possibilidade de uma situação adversa ocorrer, que, caso se concretize, pode evoluir para uma emergência real.

- **Data Center:** Centro de Processamento de Dados (CPD), onde estão concentrados os servidores e equipamentos de rede da instituição. O Data Center é projetado para garantir a segurança física e operacional dos sistemas e dados essenciais da organização.



- **Incidente:** Evento inesperado que causa uma interrupção ou degradação severa nos serviços de TI. Incidentes podem variar em gravidade e impacto, mas todos devem ser tratados imediatamente para prevenir maiores danos.
- **Hipótese Acidental:** Qualquer situação anômala que foge do controle normal das operações, como falhas técnicas ou falhas humanas, que podem resultar em danos aos sistemas e equipamentos de TI.
- **Intervenção:** Conjunto de ações executadas durante uma emergência, seguindo planos predefinidos para minimizar os danos e restaurar os sistemas de TI o mais rápido possível.
- **Situação de Emergência:** Estado crítico gerado por um incidente ou falha grave que pode prejudicar os sistemas de TI, resultando em perda de funcionalidade, interrupção do serviço e impactos no trabalho de docentes, discentes e corpo técnico-administrativo.

4. RESPONSABILIDADE

- **Equipe de TI:** A equipe de tecnologia da informação é responsável por fornecer suporte técnico para docentes, discentes e colaboradores, garantindo o pleno funcionamento dos sistemas e equipamentos de TI. Suas funções incluem monitorar e administrar o ambiente físico de TI, identificar problemas e escalonar a solução para níveis superiores quando necessário, garantindo uma rápida resposta e resolução.
- **Gestão de TI:** A gestão superior de TI é responsável pela coordenação estratégica dos recursos de tecnologia, incluindo a implantação, o gerenciamento e a manutenção de dispositivos, sistemas acadêmicos e corporativos da Unifunvic. A gestão também supervisiona a execução do plano de contingência, garantindo que todos os procedimentos estejam alinhados às necessidades da instituição.

5. NÍVEIS DE INCIDENTES

Os incidentes são classificados em diferentes níveis, conforme a gravidade e o impacto que causam nas operações da instituição:



- **Nível I:** Pequenas falhas que podem ser resolvidas pela equipe de TI sem impactar o funcionamento geral da organização. Exemplo: problemas com equipamentos periféricos, como teclados e mouses.
- **Nível II:** Falhas que impedem o uso de determinados equipamentos ou sistemas, interrompendo o trabalho de um ou mais colaboradores. Exemplo: computadores que não ligam ou estão com problemas de desempenho.
- **Nível III:** Incidentes que afetam a operação de sistemas ou equipamentos essenciais, impactando toda a organização. Exemplo: falhas de rede interna ou interrupções de internet, prejudicando o acesso a sistemas corporativos e acadêmicos.
- **Nível IV:** Situações que afetam diretamente o uso de sistemas por professores e alunos, comprometendo a entrega de serviços educacionais e acadêmicos. Exemplo: a indisponibilidade do portal do aluno ou sistemas acadêmicos.
- **Nível V:** Emergências críticas que paralisam totalmente as operações da instituição, como ataques cibernéticos que comprometem os servidores principais e dados. Exemplo: violação de segurança por meio de vírus ou ataque hacker.

6. PRINCIPAIS RISCOS

Os principais riscos que podem afetar os serviços de TI e desencadear a ativação do plano de contingência incluem:

- **Interrupção de energia elétrica:** Ocorrência externa que cause interrupção, no fornecimento de energia.
- **Falhas na climatização do Data Center:** Superaquecimento dos servidores e outros equipamentos devido a falha nos sistemas de refrigeração.
- **Indisponibilidade de rede/circuitos:** Problemas como rompimento de cabos, seja por obras internas, acidentes ou desastres.
- **Falha humana:** Erros cometidos no manuseio de equipamentos de TI que comprometam seu funcionamento.
- **Ataques internos:** Danos causados por usuários insatisfeitos aos ativos de TI, como servidores e computadores.



- **Falha de hardware:** Equipamentos que apresentem defeitos e que necessitem de substituição ou reparos.
- **Ataques cibernéticos:** Ameaças virtuais, como invasões e vírus, que comprometam a integridade dos sistemas da Unifunvic.

7. PRINCIPAIS PROBLEMAS, INCIDENTES E AÇÕES DE CONTINGÊNCIA

- **Computadores em laboratórios:** Problemas relatados pelos professores ao setor de TI via e-mail são atendidos conforme agendamento. Em caso de impacto direto nas aulas, um técnico será enviado ao local para uma verificação inicial e solução rápida.



PLANO DE MANUTENÇÃO PREVENTIVA DOS LABORATORIOS DE INFORMÁTICA Departamento de Infraestrutura de TI

PERIODICIDADE	NOME DA TAREFA	DESCRIÇÃO DA TAREFA	PROCEDIMENTO
SEMANAL DIÁRIO	Verificação de Problemas Equipamentos	Verificar se foi registrado pela professor ou pelos técnicos de laboratório alguma ocorrência de problema ocorrido com equipamentos do laboratório no decorrer da aula.	Caso seja encontrado alguma ocorrência, ela se torna prioritária. Tentar resolver o problema in-loco caso contrário encaminhar para manutenção em bancada alterando para prioritário a ordem de serviço.
	Dispositivo Ligado	Verificar se o computador esta ligando normalmente, observando sempre se aparece alguma mensagem de erro, tanto do hardware quanto do software.	Caso seja encontrado algum erro ou mensagem de erro, tentar solucionar in-loco caso contrário encaminhar para manutenção em bancada abrindo uma ordem de serviço com o estado de prioridade.
	Rede de Dados Operacional	Checkando a configuração dos ips, executando comando de ping e acessando a internet para verificar a funcionalidade.	Encontrando algum erro, verificar as configurações testada para o equipamento, se o ponto de rede esta operacional, se o rack geral do laboratório esta ligado se a instituição esta com acesso a internet. Caso seja feito todo este procedimento e o erro continuar encaminhar para manutenção em bancada abrindo uma ordem de serviço com estado de prioridade.
	Periféricos Funcionais	Testar cada periférico das estações, teclado, mouse, monitor entre outros.	Caso seja encontrado algum problema realizar a substituição e encaminhar o periférico com problema para manutenção em bancada abrindo uma ordem de serviço.
	Organização do Laboratório	Verificar a organização de cabos, mesas, cadeiras e posicionamentos dos mesmos.	Caso estes itens esteja fora do padrão dos laboratórios, providenciar a organização.
	Número de Cadeiras e Mesas	Conferir o número de mesas e cadeiras dos laboratórios. Estes dados estão fixados nos painéis de acrílico nas portas dos laboratórios.	Se a quantidade não estiver de acordo com as anotações do laboratório, comunicar o coordenador direto, responsável pelos laboratórios.
	Limpeza Física	Verificar a limpeza do chão, mesas, cadeiras, lousa e as lixeiras.	No caso de encontrar problemas neste item comunicar a equipe de limpeza para providenciar a limpeza do local.
	Iluminação e Rede Elétrica	Conferir se todas as luminárias estão funcionando, juntamente com as tomadas elétricas do laboratório.	Caso encontrado problemas neste item comunicar o coordenador direto, responsável pelo laboratório para a abertura de uma ordem de serviço junto a equipe de manutenção predial.
	Ar Condicionado	Verificar o funcionamento das máquinas de ar condicionado.	Caso encontrado problemas neste item comunicar o coordenador direto, responsável pelo laboratório para a abertura de uma ordem de serviço junto a equipe de manutenção predial.
	Atualização de Antivirus	Fazer a atualização do antivírus e passar uma vareadura no computador.	Caso encontre algum vírus, fazer o procedimento padrão e confirmar a limpeza e a remoção do vírus.
	Verificação do Sistema Operacional	Entrar no sistem log do sistema operacional e conferir se teve algum erro.	Se teve erro, corrigir conforme procedimento de cada tipo de erro e sistema operacional.
	Verificação da Atualização do Sistema Operacional	Entrar no Windows Update ou equivalente ao sistema operacional para verificar se tem atualização para implementar.	Executar o procedimento de atualização conforme cada sistema operacional, se tiver algum erro fazer a atualização manual conforme procedimento padrão.
	Limpeza e desfragmentação de disco	Executar a limpeza de disco e a desfragmentação com os programas padrões do sistema operacional.	Caso encontrar algum erro que não for possível corrigir, entrar em contato com o suporte para verificar a gravidade do caso e se necessário fazer a troca do HD.
	Manutenção Preventiva	Fazer a manutenção preventiva conforme norma e procedimentos do departamento de infraestrutura de TI setor de manutenção para o hardware. Para os software fazer a formatação, configuração e a instalação conforme cronograma de aula de cada curso.	Este procedimento será acompanhado pelos técnicos do suporte e conforme orientação do coordenador direto responsável pelos laboratórios.

- **Equipamentos administrativos:** Os colaboradores reportam problemas via e-mail ou telefone ao setor de TI, que agenda o suporte. Caso o problema impeça o trabalho, será fornecido um equipamento provisório.
- **Problemas de rede:** A equipe de TI identificará o serviço afetado, investigará a causa e tomará medidas para corrigir a falha.

- **Sistemas internos:** A equipe verificará o alcance do problema (individual ou coletivo) e notificará os responsáveis para que as correções sejam feitas, em casos de falha no sistema TOTVS entramos em contato com suporte via chamado ou chat e aguardamos manutenção, neste período avisamos os usuários até que o sistema retorne.

- **Energia Elétrica:** A Na falta de energia, em segundos e automaticamente o sistema de gerador é acionado imediatamente, mantendo a funcionabilidade total do Campus Universitário do UniFUNVIC, e simultaneamente o prestador de serviço responsável pela rede elétrica do campus é avisado para entrar em contato com a operadora de energia local e regional.





8. COMUNICAÇÃO

- **Quem comunica:** Qualquer colaborador que identificar problemas relacionados a sistemas, equipamentos ou infraestrutura de TI.
- **Como comunicar:** A comunicação deve ser realizada via e-mail, telefone ou pessoalmente para o setor de TI da Unifunvic.