GRAN FACULDADE

PLANO DE CONTINGÊNCIA DA BASE E RECURSOS TECNOLÓGICOS

CURITIBA/PR
2023

SUMÁRIO

PLANO DE CONTINGÊNCIA DA BASE E RECURSOS TECNOLÓGICOS

1. POLÍTICAS DE INFORMATIZAÇÃO

Em consonância com sua Proposta Pedagógica Institucional, a IES garante o uso de seus laboratórios como uma das formas de possibilitar a interação entre teoria e prática. Para tal, permite a utilização dos laboratórios de informática, laboratório de hardware e de redes, em horário integral e mantém permanentemente à disposição um técnico para dar suporte aos usuários e garantir o perfeito funcionamento dos equipamentos.

Para acompanhar esse processo, impõe-se às instituições educacionais a disponibilização aos seus alunos de recursos sempre atualizados de informática, que serão importantes auxiliares para o ensino-aprendizagem. A informatização igualmente é de extrema importância para a organização, o acompanhamento e o controle dos serviços administrativos e acadêmicos de uma instituição de ensino.

Para a efetivação da proposta desta IES, o papel dos recursos informáticos ganha em relevância, pois deverão ser dominados pelos alunos também como instrumental pedagógico, como uma ferramenta de trabalho, da qual o profissional professor não pode prescindir.

Com essa visão, a Instituição disponibiliza um Laboratório de Informática para os alunos e implanta gradativamente sistemas informatizados que deem suporte aos serviços administrativos e acadêmicos. A seguir são listadas as ações tomadas para a implantação e funcionamento de nossa política de informatização:

- Criação de uma cultura de informática, disponibilizando constante apoio e orientação aos usuários;
- Manter uma política de uso de laboratórios, de forma a atender com eficácia tanto às atividades curriculares, como às outras demandas da comunidade acadêmica;
- Formular sistemas informatizados de acompanhamento e controle acadêmico discente e docente;
- Implantação de sistema informatizado na Biblioteca e na Secretaria Financeira;
- Interligar em rede todas as áreas da Instituição, agilizando a troca de informações;
- Capacitar docentes e técnico-administrativos para uso dos sistemas;
- Modernizar constantemente o parque computacional, por meio de novas aquisições ou de "upgrade" constante do hardware;
- Manter o acervo de softwares atualizado.

2. OBJETIVO DO PLANO DE CONTINGÊNCIA

Este plano objetiva estabelecer procedimentos de comunicação e mobilização para controle e tratamentos de incidentes, uma vez que as falhas nos serviços de TI (Tecnologia da Informação) impactam diretamente na continuidade da prestação de serviços da educação, almeja-se com este plano prover medidas de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes graves ou desastres. O plano de contingência atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos.

3. APLICAÇÃO

Este documento aplica-se a todos os serviços e infraestruturas de Tecnologia da Informação executados no âmbito do GRAN CENTRO UNIVERSITÁRIO. Este documento deverá ser empregado no preenchimento dos planos de ações cabíveis à cada ocorrência.

4. RESPONSABILIDADES E FLUXO DE INFORMAÇÃO

Cabe ao Gestor de T.I. identificar e analisar os impactos nos processos e perdas potenciais para garantir a continuidade dos serviços priorizando processos críticos por meio do estabelecimento de procedimentos, divisão de responsabilidades e alocação de recursos.

4.1 Colaboradores da Instituição
Responsáveis por informar o Setor de TI da Instituição via o Portal de Chamados detectem algum tipo de emergência ou hipótese acidental que ocorram em alguma das áreas sensíveis da Instituição. Caso ocorra a impossibilidade de realizar a comunicação via Portal de Chamados no momento da identificação do problema a solicitação deverá ser realizada via e-mail caso de indisponibilidade dos anteriores deve ser acionado via ramal telefônico, devendo ser registrado no portal posteriormente para regularização, a fim de análise e controle.

4.2 Equipe do Setor de Tecnologia da Informação da Instituição
Devem mitigar os impactos que por ventura venham a ocorrer decorrentes de emergências ou situações de emergência que afetem os sistemas, equipamentos ou infraestrutura de TI da Instituição. A equipe também deve elaborar uma documentação após a conclusão da ocorrência descrevendo os desafios superados via Portal de Chamados soluções e os aprendizados obtidos na resolução dos problemas.

4.3 Departamentos de Gestão
A depender do impacto e urgência dos incidentes a gestão, representada por setores como: Direção Geral, Direção Administrativa e Financeira, entre outros tem papel estratégico de tomada de decisão, principalmente em casos que envolva aquisições/compras de emergência.

4.4 Prestadores de Serviços Terceirizados e Fornecedores
Se necessário, fabricantes e prestadores de serviços terceirizados serão acionados quando houver contrato de suporte e garantia vigentes, como nos casos do outsourcing de impressão e nos ativos de rede com garantia estendida ou vitalícia.

5. COMUNICAÇÃO

5.1. Quem deve comunicar
Qualquer colaborador que detecte qualquer tipo de problema que diga respeito a sistemas, equipamentos e/ou infraestrutura de TI.

5.2. A quem comunicar
A comunicação deve ser feita para o Setor de TI da Instituição.

5.3. Como comunicar
Os problemas detectados devem ser informados através do Portal de Chamados, e-mail (na indisponibilidade do primeiro ou Telefone na indisponibilidade dos anteriores.

6. PRIORIDADES

A definição da prioridade no atendimento precisa ser técnica e pragmática, sendo assim a opção é seguir as boas práticas. Portanto a PRIORIDADE é definida pela relação **URGÊNCIA X IMPACTO.**

O número de usuários afetados (Alunos, Professores, etc.) define o impacto do incidente. Já a urgência pode levar em conta a característica da atividade e o quanto ela impacta, por exemplo, as atividades que não podem ser interrompidas: aulas, palestras, web conferências.

7. NÍVEIS DE INCIDENTES

Nível I – Hipótese acidental que pode ser controlada pela equipe de TI da Instituição e que não afeta o andamento do trabalho do servidor. Ex.: Problemas com equipamentos periféricos de computadores.

Nível II – Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo colaborador. Ex.: Problema com o funcionamento do Computador (não liga, travado, etc.) ou ainda sistemas off-line impedindo o uso do mesmo.

Nível III – Hipótese acidental que impede o uso de sistemas ou equipamentos de todo o prédio, impedindo assim o desenvolvimento do trabalho de todos os colaboradores da Instituição. Ex.: Falha na conexão com a internet ou queda de energia elétrica no prédio ou ainda problema técnico em algum servidor de rede que controla a conexão interna da Instituição.

8. PRINCIPAIS RISCOS

O Plano de Contingência foi desenvolvido para ser acionado quando da ocorrência de cenários que apresentam risco à continuidade dos serviços essenciais. O quadro abaixo define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

Evento Possíveis

01 - Interrupção de energia elétrica causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 30 minutos. Causada por fator interno que comprometa a rede elétrica do prédio com curto circuitos, incêndio e infiltrações.

02 - Falha na climatização do Data Center Superaquecimento dos ativos devido a falha no sistema de climatização.

03 - Indisponibilidade de rede/circuitos Rompimento de cabeamento decorrente de execuções obras internas, desastres ou acidentes.

04 - Falha humana Acidente ao manusear equipamento.

05 - Ataques internos (usuários insatisfeitos) Ataque aos ativos do Data Center e equipamentos de TI com origem nos laboratórios, salas de aula e de uso administrativo/ensino.

06 - Falha de hardware que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo compras.

07- Ataque cibernético, ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.

9. ESTRATÉGIAS DE CONTROLE, MONITORAMENTO E TRATAMENTO DE INCIDENTES

9.1 Problemas com computadores nos laboratórios de informática

a). Professores que estão utilizando ou que irão utilizar o referido laboratório, informam. ao Setor de TI da Instituição através do Sistema de Suporte enviando um e-mail para o endereço do núcleo.
b). O chamado de suporte chega até o setor de TI e o atendimento é agendado;
c). Após o atendimento o solicitante é informado da conclusão/resolução do problema informado;
d). Caso o problema impeça o andamento da aula, o Setor de TI vai até o local fazer uma primeira verificação do problema e tenta solucioná-lo in-loco.

9.2 Problemas com computadores administrativos
a). O colaborador que está utilizando o equipamento, informa ao Setor de TI da Instituição através do Sistema de Suporte via Portal Web, enviando um e-mail para o endereço do núcleo. Caso não seja possível acessar o e-mail, o chamado pode ser aberto através do ramal telefônico do Setor de TI;
b). O chamado de suporte chega até o setor de TI e o atendimento é agendado;
c). Após o atendimento o solicitante é informado da conclusão/resolução do problema informado;
d). Caso o problema impeça o andamento do trabalho do colaborador, o Setor de TI vai até o local fazer uma primeira verificação do problema e tenta solucioná-lo in-loco. Caso não seja possível a resolução do problema, é disponibilizado um computador provisório para o colaborador poder continuar desenvolvendo suas atividades.

9.3 Problemas de conexão com a rede interna
a). Identificar em qual andar do Campus está ocorrendo o problema;
b). Analisar a conexão do servidor central até o bloco afetado;
c) Identificar a causa do problema;
d) Caso o problema de conexão seja em todo o campus, verificar se os servidores de endereços DHCP e de autenticação estão funcionando adequadamente.

9.4 Problemas de conexão com a internet
a) Identificar em qual andar do prédio está ocorrendo o problema;
b) Analisar a conexão do servidor central até o andar afetado
c) Identificar a causa do problema;
d) Caso o problema de conexão seja em todo o prédio, verificar se há conexão até o Roteador e até o Modem da Operadora. Caso haja conexão interna até os referidos equipamentos, deverá ser aberto um chamado de suporte com a Operadora e alterar a conexão para a rede alternativa.

9.5 Problemas com acesso aos sistemas internos da Instituição
a) Identificar qual o sistema está apresentando problema de acesso;
b) Verificar se a VM onde o mesmo está instalado está em execução;
c) Caso esteja em execução, verificar a conexão de rede da VM;
d) Caso não esteja em execução, iniciá-la no servidor (Monitor de Máquina Virtual) e testar seu acesso novamente;
e) Por fim, identificar e resolver o problema informando a solução aos demais servidores.

9.6 Problemas com acesso à internet pelos alunos em equipamentos particulares
a) Verificar se a rede acadêmica está online e funcionando em caso negativo reiniciar serviços ou voltar backup;
b) Verificar se o roteador/access point ao qual o aluno está se conectando está funcional;
c) Se o problema for no equipamento do aluno orientá-lo a procurar uma assistência técnica;
d) É aberto um chamado técnico para estatística e feedback futuro.

9.7 Problemas com acesso à internet pelos colaboradores em equipamentos particulares
a) Verificar configurações definidas de forma manual no equipamento;
b) Verificar se a rede administrativa está online e funcionando em caso negativo reiniciar serviços ou voltar backup;
c) Verificar se o roteador/access point ao qual o colaborador está se conectando está funcional;

d) Se o problema for no equipamento do colaborador orientá-lo a procurar uma assistência técnica.

9.8 Problemas com acesso a algum site específico

a) O colaborador que está utilizando o equipamento, informa ao Setor de TI da Instituição através do Sistema de Suporte e informando o site que está com problemas ao abrir;
b) O chamado de suporte chega até o setor de TI e o atendimento é agendado;
c) O Setor verifica o site e o motivo do problema de acesso procedendo com a liberação no firewall caso não entre em conflito com outras regras ou normativas;
d) Após a resolução o solicitante é informado da conclusão/resolução do problema informado.

9.9 Problemas com UPS/no-break

a) Verificado problema ou anormalidade informado pelo próprio no-break, com o multímetro testa-se a entrada de energia no equipamento pela porta trifásica (entrada da fornecedora) bem como pela porta do banco de baterias;
b) Intervenção imediata para problemas adicionais deve-se contatar de imediato o Departamento de Administração e planejar medidas corretivas junto a empresa técnica especializada externa;
c) Verificar a possibilidade de desligar equipamentos e/ou serviços não essenciais enquanto o funcionamento do no-break não é normalizado;
d) Em caso de desligamento total proceder com o passo "B" e, em paralelo ligar o servidor que possui o firewall e a internet em fonte de energia alternativa para que pelo menos o DHCP e a internet continuem disponíveis no prédio;
e) É aberto um chamado técnico para estatística e feedback futuro.

9.10 Problemas com equipamentos de rede

a) Identificar qual equipamento está apresentando problema;
b) Caso possível realizar a manutenção do mesmo;
c) Caso não tenha como consertar, realizar a troca do equipamento de forma que haja o menor transtorno possível no desempenho das atividades dos demais colaboradores da Instituição.
d) Verificar o estoque do ativo substituído e providenciar aquisição de equipamento de reposição.

9.11 Problemas físicos com cabeamento da rede interna e externa

a) Identificar qual o problema e onde está ocorrendo;
b) Verificar as ligações (Switches) do cabeamento que está com defeito e testá-lo, bem como os conectores RJ45;
c) Se necessário refazer a crimpagem dos conectores RJ45 imediatamente;
d) Caso haja necessidade, efetuar a troca do cabo ou cabos que estão apresentando falhas.

9.12 Problemas físicos com cabeamento da rede de fibra óptica externa e interna

a) Identificar qual o problema e onde está ocorrendo;
b) Verificar as ligações (Switches e Conversores) do cabeamento que está com defeito e testá-lo, bem como seus conectores;
c) Acionar empresa terceirizada para consertos e fusões de fibra;
d) Caso haja necessidade, efetuar a troca do cabo ou cabos que estão apresentando falhas.

9.13 Problemas com falta de energia elétrica

a) Caso seja identificada queda ou falta total de energia elétrica no prédio informamos o Departamento de Administração e Planejamento (DAP) para as devidas providências;
b) Se a falta de energia for de curta duração os sistemas e servidores de rede continuam em funcionamento, pois estão ligados em um nobreak;
c) Caso a falta de energia dure mais de 1 hora aproximadamente, os sistemas são desligados, bem como os equipamentos e serão religados assim que a energia for restabelecida.

9.14 Incidentes de Segurança e Ataques Cibernéticos

a) Caso sejam detectadas anomalias de tráfego de rede pela central de tratamentos de ameaça, o tráfego deve ser monitorado, se necessário, origem e destino podem ser colocados em quarentena ou banidos da rede.
b) Salvar relatórios e logs de acesso para investigação futura.

9.15 Outros Problemas
Para qualquer outro tipo de problema que envolva a TI, como configurações de e-mail, impressoras, problemas de acesso que envolvam login e senha e etc.
Os passos a serem seguidos são os seguintes:
a) Informar o problema ao Setor de TI da Instituição através do Sistema de Suporte;
b) O chamado de suporte chega até o setor de TI e o atendimento é agendado;
c) Após o atendimento o solicitante é informado da conclusão/resolução do problema reclamado;

10. CONTROLES PREVENTIVOS E ESTRATÉGIA DE RECUPERAÇÃO

a) O Setor de TI deverá manter cópias backup de VMs com serviços importantes para uma possível restauração mesmo com alguma perda de informação para situações onde a VM em execução entre em um estado crítico de não inicialização ou bug geral;
b) Sempre que possível um computador e/ou notebook estarão à disposição para substituir outro equipamento em uso que apresentou problema;
c) A Direção de Ensino possui projetores reservas que poderão ser usados fora da Instituição ou em sala de aula no caso de problemas com os projetores fixos;
d) Os servidores poderão ter mais de uma impressora cadastrada para realizar impressões institucionais bastando solicitar o cadastro;
e) Servidor de arquivos efetua backups regulares possibilitando a recuperação de arquivos quando da detecção de algum problema.
f) A aquisição de equipamentos deve prever inclusão de garantia estendida, sendo ideal pelo menos 3 anos, renovando-a quando possível

11. MANUTENÇÃO PREVENTIVA

a) Anualmente o no-break e seu banco de baterias deverá receber manutenção preventiva realizada por empresa técnica especializada;
b) Se possível, anualmente os projetores deverão receber manutenção preventiva especializada;
c) Semestralmente o sistema de climatização do CPD deverá receber manutenção preventiva.

CURITIBA, 2023

GRAN CENTRO UNIVERSITÁRIO