PLANO DE CONTINGÊNCIA DA TI

1 OBJETIVO

Uma vez que falhas nos serviços de TI impactam diretamente nos setores administrativos e de ensino do campus, almeja-se com este plano prover medidas de proteções rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais.

Este plano também procura estabelecer procedimentos de comunicação e mobilização para controle, em caso de contingências e emergências que possam ocorrer durante as atividades relacionadas à Tecnologia da Informação, visando aplicar as ações necessárias para correção e/ou eliminação do problema.

2 DEFINIÇÕES

Acionamento: é o processo de comunicação com as equipes envolvidas no controle da emergência, de acordo com a ordem estabelecida para que as equipes desempenhem as atividades sob sua responsabilidade, a fim de controlar a emergência.

Administrador do Plano de Contingência: Responsável pela manutenção e atualização dos dados e procedimentos necessários à plena operacionalidade do Plano de Contingência.

Área Vulnerável: Área atingida pela extensão dos efeitos provocados por um evento de falha.

Áreas Sensíveis: Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas, encontram-se os laboratórios de informática, salas administrativas, Centro de Processamento de Dados e demais locais que possuam equipamentos de informática.

Centro de Processamento de Dados: É um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores, e outros do Campus.

Contingência: Situação de risco com potencial de ocorrer, inerente às atividades, serviços e equipamentos, e que, ocorrendo, transformar-se-á em uma situação de emergência.

Hipótese Acidental: Toda ocorrência anormal, que foge ao controle de um processo, sistema ou atividade, da qual possam resultar danos aos sistemas e equipamentos de TI do Campus.

Incidente: É o evento não programado de grande proporção, capaz de causar danos graves aos sistemas e aos equipamentos de TI do Campus.

Intervenção: É a atividade de atuar durante a emergência, seguindo ações planejadas, visando minimizar os possíveis dados aos equipamentos e sistemas de TI do Campus.

Núcleo de Tecnologia da Informação – NTI: Setor responsável pelo gerenciamento e pela manutenção dos recursos de Tecnologia da Informação da Faculdade.

Situação de Emergência: Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos, ou ao desempenho do trabalho de servidores do Campus.

3 RESPONSABILIDADES

Equipe do Setor de Tecnologia da Informação: Deve mitigar os impactos que porventura venham a ocorrer, decorrentes de emergências ou situações de emergência que afetem os sistemas, equipamentos ou infraestrutura de TI do Campus.

Colaboradores do Campus: Responsáveis por informar o NTI do Campus, caso detectem algum tipo de emergência ou hipótese acidental que ocorra em alguma das áreas sensíveis do Campus.

4 NÍVEIS DE INCIDENTES

Nível 1: Hipótese acidental que pode ser controlada pela equipe de TI do Campus, e que não afeta o andamento do trabalho do setor. Por exemplo: Problemas com equipamentos periféricos de computadores.

Nível 2: Hipótese acidental que impede a utilização do equipamento ou sistema, e acaba impedindo a continuação do trabalho do setor. Por exemplo: Problema com o funcionamento do computador (não liga, fica travado, etc.), ou ainda sistemas offline, impedindo o uso do mesmo.

Nível 3: Hipótese acidental que impede o uso de sistemas ou equipamentos de todo o Campus, impedindo assim o desenvolvimento do trabalho de múltiplos setores. Por exemplo: Falha na conexão com a internet ou queda de energia elétrica no campus, ou ainda problema técnico em algum dispositivo de rede que controla a conexão interna do Campus.

5 PRINCIPAIS RISCOS

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

Indisponibilidade de circuitos: Rompimento de cabeamento decorrente de execuções de obras internas, desastres ou acidentes.

Falha de hardware: Falha nos sistemas computacionais que exija reposição de peça ou reparo.

Falha humana: Acidente ao manusear equipamentos.

Ataque físico: Ataque aos ativos do Centro de Dados e equipamentos de TI dos laboratórios, salas de aula e de uso administrativo ou acadêmico.

Ataque virtual: Ataque virtual que comprometa o desempenho, os dados configurações dos serviços essenciais.

6 INCIDENTES E AÇÕES DE CONTINGÊNCIA

6.1 Problemas com computadores nos laboratórios de informática

a) Professores que estão utilizando ou que irão utilizar o referido laboratório, informam o problema ao NTI.
b) Caso o problema impeça o andamento da aula, o NTI vai até o local fazer uma primeira verificação do problema e tenta solucioná-lo in-loco.

6.2 Problemas com computadores administrativos

a) O colaborador que está utilizando o equipamento, informa o problema ao NTI. Caso não seja possível acessar o e-mail, o contato pode ser feito por telefone (whatsapp).
b) Caso o problema impeça o andamento do trabalho do setor, o NTI vai até o local fazer uma primeira verificação do problema e tenta solucioná-lo in-loco.
c) Caso não seja possível a resolução do problema, é disponibilizado um computador provisório para o colaborador poder continuar desenvolvendo suas atividades.

6.3 Problemas de conexão com a rede interna

a) Identificar em qual bloco 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, verifica-se se os servidores de endereços DHCP e de autenticação estão funcionando adequadamente.

6.4 Problemas de conexão com a internet

a) Identificar em qual bloco do Campus está ocorrendo o problema.
b) Analisar a conexão do servidor central até o bloco afetado.
c) Identificar a causa do problema.
d) Detectado o problema externo de internet, ativar o link de internet de contingência.
e) Abrir chamado de suporte com a operadora, visando o reestabelecimento do serviço.

6.5 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 setores do Campus.

6.6 Problemas físicos com cabeamento da rede interna

a) Identificar qual o problema e onde está ocorrendo.
b) Detectado problema de cabeamento de rede, refazer a conexões e ponteiras.
c) Verificar as ligações do cabeamento que está com defeito e testá-lo, bem como os conectores RJ45.
d) Caso haja necessidade, efetuar a troca do cabo ou cabos que estão apresentando falhas.

6.7 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, etc., informar o problema ao NTI.

7 COMUNICAÇÃO

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

A quem comunicar: A comunicação deve ser feita para o NTI do Campus.

Como comunicar: Os problemas detectados devem ser informados ora pessoalmente, ora por comunicado no SIGA, ora por email: informatica@faculdadesantaluzia.edu.br.