*Autorizada pela Portaria Ministerial nº 552 de 22 de março de 2001 e publicada no Diário Oficial da União de 26 de março de 2001.*
*Endereço: Rua Juracy Magalhães, 222 – Ponto Central CEP 44.032-620*

# RESOLUÇÃO CONSAD 002/2019

*Aprova o Plano de Contingências para as unidades físicas e tecnológicas da Faculdade Anísio Teixeira de Feira de Santana, nos termos do Regimento Geral.*

O CONSELHO DE ADMINISTRAÇÃO da Faculdade Anísio Teixeira, no uso das atribuições que lhe confere o Regimento Geral desta mesma Faculdade, **RESOLVE:**

Artigo 1º. Aprovar o Plano de Contingência para as unidades físicas e tecnlógicas da Faculdade Anísio Teixeira de Feira de Santana, que, em anexo e devidamente autenticado, passa a integrar a presente Resolução.

Artigo 2º. Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Gabinete do Diretor, 15 de fevereiro de 2019.

*Antônio Walter Moraes Lima*

*Diretor Geral*

# PLANO DE CONTINGÊNCIA

## Tecnologias da Informação e Comunicação

## 1. OBJETIVO

Uma vez que falhas nos serviços de TI impactam diretamente nos setores administrativos e de ensino, tanto nas unidades físicas como tecnológicas, este plano busca prover medidas de proteções rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais.

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

## 2. APLICAÇÃO

Este documento se aplica a todos os serviços de Tecnologia da Informação que são executados nas unidades da Faculdade Anísio Teixeira.

## 3. ESCLARECIMENTOS / 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 Contigência.

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

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

**Contingência:** Situação de risco com potencial de ocorrer, inerente as atividades, serviços e equipamentos, e que ocorrendo se transformará em uma situação de emergência. Diz respeito a uma eventualidade; possibilidade de ocorrer.

**DataCenter:** ou 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.

**Incidente:** É o evento não programado de grande proporção capaz de causar danos graves aos sistemas e aos equipamentos de TI da Faculdade.

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

**Intervenção:** É a atividade de atuar durante a emergência, seguindo ações planejadas, visando minimizar os possíveis danos aos equipamento e sistemas de TI da IES.

**Sistema de Suporte:** Sistema GLPI instalado em um servidor web da Faculdade, onde é possível receber, organizar e manter o solicitante/servidor informado sobre o andamento do chamado de suporte.

**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.

**TI:** Tecnologia da Informação

**VM:** Máquina Virtual, virtualizada no servidor.

## 4. RESPONSABILIDADES

### 4.1 Equipe do Setor de Tecnologia da Informação

Devem mitigar os impactos que porventura venham a ocorrer decorrentes de emergências ou situações de emergência que afetem os sistemas, equipamentos ou infraestrutura de TI das unidades da FAT.

### 4.2 Servidores das Unidades

Responsáveis por informar o Setor de TI, caso detectem algum tipo de emergência ou hipótese acidental que ocorram em alguma das áreas sensíveis da FAT.

## 5. NÍVEIS DE INCIDENTES

**Nivel I –** Hipótese acidental que pode ser controlada pela equipe de TI do FAT 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 servidor.
Ex: Problema com o funcionamento do Computador (não liga, travado, etc) ou ainda sistemas offline impedindo o uso do mesmo.

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

## 6. 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.<br>Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndio e infiltrações. |
| 02- Falha na climatização do DataCenter | 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 equipamentos |
| 05 - Ataques internos (usuários insatisfeitos) | Ataque aos ativos do DataCenter e equipamentos de TI dos laboratórios, salas de aula e de uso administrativo/ensino |
| 06- Falha de hardware | Falha que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo licitatório |
| 07- Ataque cibernético | Ataque virtual que comprometa o desempenho, os |

| | |
|---|---|
| | dados ou configuração dos serviços essenciais |

## 7. PRINCIPAIS PROBLEMAS, INCIDENTES E DEVIDAS AÇÕES DE CONTINGÊNCIA

### 7.1 Problemas com computadores nos laboratórios de informática

- Professores que estão utilizando ou que irão utilizar o referido laboratório, informam o problema ao Setor de TI do Campus através do Sistema de Suporte.
- O chamado de suporte chega até o setor de TI e o atendimento é agendado;
- Após o atendimento o solicitante é informado da conclusão/resolução do problema informado;
- 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*.

### 7.2 Problemas com computadores administrativos

- O servidor que está utilizando o equipamento, informa o problema ao Setor de TI do Campus através do Sistema de Suporte, enviando um e-mail. Caso não seja possível acessar o e-mail, o chamado pode ser aberto através do ramal telefônico do Setor de TI;
- O chamado de suporte chega até o setor de TI e o atendimento é agendado;
- Após o atendimento o solicitante é informado da conclusão/resolução do problema informado;
- Caso o problema impeça o andamento do trabalho do servidor, 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 servidor poder continuar desenvolvendo suas atividades.

### 7.3 Problemas de conexão com a rede interna

- O Setor de TI identificará em qual prédio da Faculdade está ocorrendo o problema;
- Analisar a conexão do servidor central até o bloco afetado;
- Identificar a causa do problema;
- Caso o problema de conexão seja em todo o campus, verifica se os servidores de endereços DHCP e de autenticação estão funcionando adequadamente.

### 7.4 Problemas de conexão com a internet

- Identificar em qual bloco do Campus está ocorrendo o problema;
- Analisar a conexão do servidor central até o bloco afetado
- Identificar a causa do problema;

- Detectado problema externo de internet, ativar o link de internet de contingência.
- Abrir chamado de suporte com a operadora, visando o reestabelecimento do serviço

### 7.5 Problemas com acesso aos sistemas internos do campus

- Identificar qual o sistema está apresentando problema de acesso;
- Verificar se a VM onde o mesmo está instalado está em execução;
- Caso esteja em execução, verificar a conexão de rede da VM;
- Caso não esteja em execução, iniciá-la no servidor e testar seu acesso novamente;
- Por fim, identificar e resolver o problema informando a solução aos demais servidores.

### 7.6 Problemas com equipamentos de rede

- Identificar qual equipamento está apresentando problema;
- Caso possível, realizar a manutenção do mesmo;
- Caso não tenha como consertar, realizar a troca do equipamento de forma que haja o menor transtorno possível no desempenho das atividades dos demais servidores do Campus.

### 7.7 Problemas físicos com cabeamento da rede interna

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

### 7.8 Problemas com falta de energia elétrica

- Caso seja identificada queda ou falta total de energia elétrica no Campus informar o Departamento de Administração e Planejamento (DAP) para as devidas providências;
- Se a falta de energia for de curta de duração, máximo 30 minutos, os sistemas e servidores de rede continuam em funcionamento, pois estão ligados em um nobreak no DataCenter;
- Caso a falta de energia dure mais de 30 minutos, os sistemas são desligados, bem como os equipamentos e serão religados assim que a energia for reestabelecida.

### 7.9 – Ordem para o desligamento dos servidores

- Acessar o ambiente virtual e desligar primeiramente os servidores virtuais de serviços/web;
- Desligar os servidores virtuais de Autenticação;
- Desligar o servidor virtual do Firewall;
- Desligar os servidores físicos.

### 7.10 – Ordem para religar dos servidores

- Ligar os servidores físicos;
- Acessar o ambiente virtual e ligar os servidores de Autenticação;
- Ligar o servidor virtual do Firewall;
- Ligar os demais servidores virtuais;
- Realizar testes de acesso à internet, autenticação e demais sistemas web do campus.

### 7.11 - 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:
- Informar o problema ao Setor de TI do Campus através do Sistema de Suporte, enviando um e-mail para o gestor;
- O chamado de suporte chega até o setor de TI e o atendimento é agendado;
- Após o atendimento o solicitante é informado da conclusão/resolução do problema reclamado;

## 8. COMUNICAÇÃO

### 8.1 Quem deve comunicar

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

### 8.2 A quem comunicar

A comunicação deve ser feita para o Setor de TI da Faculdade.

### 8.3 Como comunicar

Os problemas detectados devem ser informados através do Sistema de Suporte, enviando um e-mail para o endereço **fat.junior@gmail.com**