



**PLANO DE CONTIGÊNCIA DA  
TECNOLOGIA DA INFORMAÇÃO**

**FADISP**  
FACULDADE AUTÔNOMA DE DIREITO

## FACULDADE AUTÔNOMA DE DIREITO

Recredenciamento pela Portaria MEC N<sup>o</sup>. 1.211, de 26 de outubro de 2016  
Publicada no Diário Oficial da União N<sup>o</sup> 208, Seção I, de 28/10/2016, pág. 24

**RESOLUÇÃO n<sup>o</sup> 014/2023, de 16 de janeiro de 2023.**

*Aprova o Plano de Contingência  
da Tecnologia de Informação,*

**O Diretor Superintendente da Faculdade Autônoma de  
Direito – FADISP, no uso de suas atribuições regimentais,**

### **RESOLVE:**

**Art. 1<sup>o</sup>** Aprovar o Plano de Contingência da Tecnologia de Informação da Faculdade Autônoma de Direito – FADISP.

**Art. 2<sup>o</sup>** Esta Resolução entra em vigor na data de sua assinatura.

São Paulo, 16 de janeiro de 2022.



**Dr. Nelson de Carvalho Filho**  
Diretor Superintendente da Faculdade Autônoma de Direito

## PLANO DE CONTINGÊNCIA DA TECNOLOGIA DE INFORMAÇÃO

### 1. OBJETIVO

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

Este plano objetiva também 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 nesta IES.

### 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 Contingência.

**Áreas Sensíveis:** Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas encontram-se os

laboratórios de informática, salas administrativas, Data Center 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, equipamentos, e que ocorrendo se transformará em uma emergência. Diz respeito a uma eventualidade; possibilidade de ocorrer.

**Data Center:** 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 da IES.

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

**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 equipamentos e sistemas de TI da IES.

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

**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 da IES.

**TI:** Tecnologia da Informação

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

## 4. RESPONSABILIDADES

### 4.1 Equipe do Setor de Tecnologia da Informação

Devem mitigar os impactos que porventura venham a acontecer decorrentes de emergências ou situações que afetem os sistemas, equipamentos ou infraestrutura de TI da FADISP.

### 4.2 Servidores da FADISP

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

## 5. NÍVEIS DE INCIDENTES

**Nível I** – Hipótese acidental que pode ser controlada pela equipe de TI a IES 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 sistemas 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 toda a IES, impedindo assim o desenvolvimento do trabalho de todos os servidores.

Ex: Falha na conexão com a internet ou queda de energia elétrica 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:

<b>Evento</b>	<b>Possíveis Causas</b>
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 curtos-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 equipamentos
05 - Ataques internos (usuários insatisfeitos)	Ataque aos ativos do Data Center 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 DECONTINGÊNCIA

### 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 da IES através do Sistema de Suporte, enviando um e-mail para o endereço [csti@unialfa.com.br](mailto:csti@unialfa.com.br) ou [ld-alfa-audiovisual@unialfa.com.br](mailto:ld-alfa-audiovisual@unialfa.com.br);
- 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 solucioná-lo *in-loco*.

### 7.2 Problemas com computadores administrativos

- O servidor que está utilizando o equipamento, informa o problema ao Setor de TI da IES através do Sistema de Suporte, enviando um e-mail para o endereço [csti@unialfa.com.br](mailto:csti@unialfa.com.br) ou [ld-alfa-audiovisual@unialfa.com.br](mailto:ld-alfa-audiovisual@unialfa.com.br). Caso não seja possível acessar o e-mail, o chamado pode ser aberto através do ramal telefônico do Setor de TI 5005 ou 5118;
- 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 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 bloco da IES 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 toda a IES, 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 da IES 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 da FADISP

- Identificar qual o sistema está apresentando problema de acesso;
- Identificar o servidor que atende este sistema e efetuar os testes necessário para validar o seu funcionamento;
- Caso não esteja em execução, iniciá-la no servidor e testar seu acesso novamente;
- Caso esteja em execução, verificar a conexão de rede ao qual este servidor está conectado;
- Por fim, identificar e resolver o problema informando a solução no encerramento do chamado.

## 7.6 Problemas com equipamentos de rede

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

## 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 ponteiros;
- 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 na IES, informar o Departamento de Infraestrutura para as devidas providências;
- O Data Center conta com proteção de nobreak com autonomia de 30 minutos;
- O grupo gerador tem seu acionamento automaticamente após 30 segundos da falta de energia.

## 7.9 Ordem para o desligamento dos servidores

- Acessar o ambiente virtual e desligar primeiramente os servidores virtuais deserviços/web;
- Desligar os servidores virtuais de Autenticação;
- 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 os demais servidores virtuais;
- Realizar testes de acesso à internet, autenticação e demais sistemas web da IES.

## 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, etc. Os passos a serem seguidos são os seguintes:

- Informar o problema ao Setor de TI da IES através do Sistema de Suporte, enviando um e-mail para um dos endereços dependendo do problema [csti@unialfa.com.br](mailto:csti@unialfa.com.br) ou [ld-alfa-audiovisual@unialfa.com.br](mailto:ld-alfa-audiovisual@unialfa.com.br);
- 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 colaborador da IES 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 FADISP.

## 8.3 Como comunicar

Os problemas detectados devem ser informados através do Sistema de Suporte, enviando um e-mail dos endereços: [csti@unialfa.com.br](mailto:csti@unialfa.com.br) ou [ld-alfa-audiovisual@unialfa.com.br](mailto:ld-alfa-audiovisual@unialfa.com.br).

