



**MINISTÉRIO DA EDUCAÇÃO  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E  
TECNOLOGIA DE SÃO PAULO  
Câmpus Bragança Paulista**



**INSTITUTO  
FEDERAL**  
São Paulo  
Câmpus  
Bragança Paulista

# **PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO**

**COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO  
IFSP - CÂMPUS BRAGANÇA PAULISTA**

Plano de Contingência e Continuidade dos  
Serviços de Tecnologia da Informação da  
Coordenadoria de Tecnologia da  
Informação - CTI do Instituto Federal de  
Educação, Ciência e Tecnologia de São  
Paulo - Câmpus Bragança Paulista

### HISTÓRICO DE VERSÕES

<b>Versão</b>	<b>Descrição</b>	<b>Responsável</b>
1.0	Criação da primeira versão	Tiago Minoru Taguchi
1.0	Aprovação	André Marcelo Panhan

## Sumário

1. OBJETIVO.....	3
2. APLICAÇÃO .....	3
3. ESCLARECIMENTOS / DEFINIÇÕES .....	3
4. CENÁRIO .....	5
4.1. Estrutura Organizacional.....	5
4.2. Serviços e sistemas .....	6
4.3. Infraestrutura física .....	8
4.4. Infraestrutura tecnológica.....	9
5. RESPONSABILIDADES .....	9
5.1. Equipe da Coordenadoria de Tecnologia da Informação .....	9
5.2. Servidores (docentes e técnicos administrativos), discentes, estagiários e terceirizados do câmpus .....	10
6. NÍVEIS DE INCIDENTES .....	10
7. PRINCIPAIS RISCOS.....	10
8. POLÍTICA E PROCEDIMENTOS DE BACKUP .....	11
8.1. Backup .....	11
8.2. Restauração e teste .....	11
9. PRINCIPAIS PROBLEMAS, INCIDENTES E DEVIDAS AÇÕES DE CONTINGÊNCIA.....	12
9.1. Problemas com computadores nos laboratórios .....	12
9.2. Problemas com computadores administrativos.....	12
9.3. Problemas de conexão com a rede interna.....	13
9.4. Problemas de conexão com a Internet.....	13
9.5. Problemas no acesso aos sistemas internos .....	14
9.6. Problemas com equipamentos de rede.....	14
9.7. Problemas físicos com cabeamento da rede interna .....	14
9.8. Problemas com falta de energia elétrica .....	15
9.9. Ordem para desligamento dos servidores .....	15
9.10. Ordem para religar os servidores.....	15
9.11. Outros problemas .....	16
10. COMUNICAÇÃO .....	16

10.1. Quem deve comunicar .....	16
10.2. A quem comunicar .....	16
10.3. Como comunicar .....	16
11. REVISÃO .....	16
12. EQUIPE .....	17

## 1. OBJETIVO

Os serviços de Tecnologia da Informação - TI são essenciais tanto para as atividades acadêmicas quanto para as atividades administrativas do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - IFSP - Câmpus Bragança Paulista, por isso é imprescindível assegurar a continuidade e a alta disponibilidade desses serviços. O Plano de Contingência e Continuidade dos Serviços de Tecnologia da Informação tem por objetivo planejar e implementar ações e medidas de redução de riscos e de recuperação.

## 2. APLICAÇÃO

Este documento se aplica a todos os serviços e sistemas de TI que são disponibilizados no IFSP - Câmpus Bragança Paulista.

## 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, Centro de Processamento de Dados e demais locais que possuam equipamentos de TI.

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

**Asterisk:** Sistema de Central telefônica VoIP (Voice over IP ou Voz sobre IP).

**Centro de Processamento de Dados - CPD:** é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados e ativos de rede (switches, roteadores, racks, entre outros).

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

**Firewall:** É uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

**GLPI (Gestão Livre de Parque de Informática):** Sistema de código aberto de gerenciamento de ativos de TI, de projetos e de incidentes e requisições.

**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 do câmpus.

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

**Intervenção:** É a atividade de atuar durante a emergência, seguindo planos de ações para corrigir ou minimizar os possíveis danos aos equipamentos e sistemas de TI do câmpus.

**Rack:** Estrutura que permite armazenar e organizar os ativos de rede como servidores, sistemas de armazenamento, switches, cabos, entre outros equipamentos.

**Sala de equipamentos:** Ambiente climatizado onde estão alocados os racks dos equipamentos das empresas fornecedoras dos links de Internet, o rack do servidor de telefonia (Asterisk) e o rack de rede.

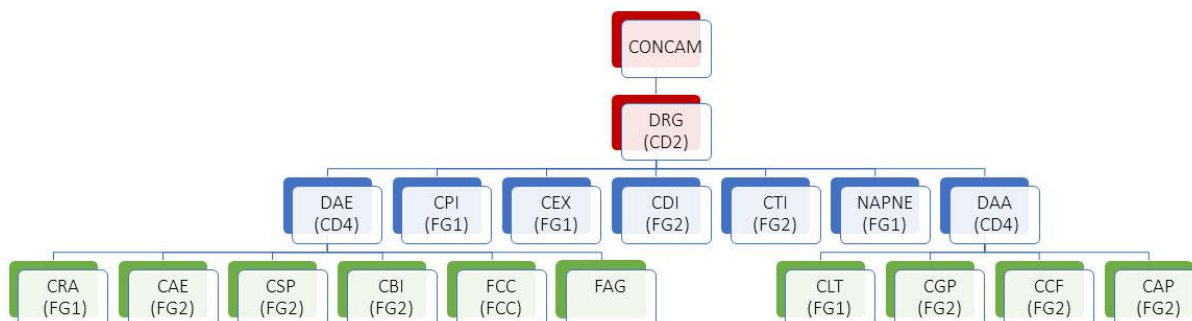
**Situação de Emergência:** Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos ou ao desempenho do trabalho de servidores do câmpus.

**Usuário:** É quem utiliza os equipamentos, sistemas ou serviços disponíveis no câmpus. Pode ser qualquer indivíduo do público interno (servidores técnicos administrativos e docentes, terceirizados, estagiários, discentes, visitantes ou convidados).

**VM (Virtual Machine ou Máquina Virtual):** São computadores virtuais que possuem a mesma funcionalidade de computadores físicos.

## 4. CENÁRIO

### 4.1. Estrutura Organizacional



Sigla	Setor
CONCAM	Conselho de Câmpus
DRG	Direção Geral
CPI	Coordenadoria de Pesquisa e Inovação
CEX	Coordenadoria de Extensão
CDI	Coordenadoria de Apoio à Direção
CTI	Coordenadoria de Tecnologia da Informação
NAPNE	Núcleo de Apoio às Pessoas com Necessidades Educacionais Específicas
DAE	Diretoria Adjunta Educacional
CAE	Coordenadoria de Apoio ao Ensino
CRA	Coordenadoria de Registros Acadêmicos
CSP	Coordenadoria Sociopedagógica
CBI	Coordenadoria de Biblioteca
FCC-ECA	Coordenação do curso de Engenharia de Controle e Automação
FCC-MAT	Coordenação do curso de Licenciatura em Matemática
FCC-TEEL	Coordenação do curso Técnico Integrado em Eletroeletrônica



FCC-TINF	Coordenação do curso Técnico Integrado em Informática
FCC-TMEC	Coordenação do curso Técnico Integrado em Mecânica
FCC-MCI	Coordenação do curso de Tecnologia em Mecatrônica Industrial
FCC-TMCT	Coordenação do curso Técnico Concomitante ou Subsequente em Mecatrônica
FCC-ADS	Coordenação do curso de Tecnologia em Análise e Desenvolvimento de Sistemas
FAG-GETI	Coordenação do curso de Especialização em Gestão Estratégica de Tecnologia da Informação
DAA	Diretoria Adjunta de Administração
CLT	Coordenadoria de Licitações e Contratos
CGP	Coordenadoria de Gestão de Pessoas
CCF	Coordenadoria de Contabilidade e Finanças
CAP	Coordenadoria de Almoxarifado, Manutenção e Patrimônio

#### 4.2. Serviços e sistemas

Serviços e sistemas de TI essenciais utilizados no Câmpus Bragança Paulista:

Nome	Descrição
Portal (bra.ifsp.edu.br) <sup>1</sup>	Portal institucional do Câmpus Bragança Paulista
SUAP	O Sistema Unificado de Administração Pública (SUAP) é utilizado nos processos administrativos e acadêmicos de todo o IFSP. Por ser um sistema unificado, vários módulos (que são os sistemas informatizados das áreas administrativas e acadêmicas) se relacionam entre si, como uma engrenagem.
Moodle <sup>1</sup>	O Moodle é um ambiente virtual de aprendizado (AVA) onde o aluno tem a possibilidade de acompanhar atividades do curso pela internet. Através da plataforma, o aluno terá acesso, utilizando as credenciais do SUAP, aos conteúdos disponibilizados pelos professores, além de postar atividades, debater o tema em

	fóruns de discussão, tirar suas dúvidas via mensagens, entre outros recursos.
Pergamum	Catálogo online das obras do acervo físico da biblioteca, bem como da Biblioteca Virtual Universitária Pearson.
E-mail (Gmail)	O IFSP utiliza o Google Workspace for Education como serviço de e-mail institucional e acadêmico.
Serviços Google	Além do e-mail, o Google Workspace for Education oferece ferramentas como o Drive (armazenamento em nuvem), Documentos (ferramentas de escritório) e o Meet (conferências).
Microsoft Office 365	Conjunto de ferramentas. O IFSP por ser uma instituição de ensino, possui licença onde é possível a utilização de ferramentas de escritório para criação e edição de documentos (Word), planilhas (Excel), apresentações (Power Point), entre outros, de forma online. Além dessas ferramentas, a licença permite a utilização do Microsoft Teams e o OneDrive.
Helios Voting	Sistema de eleição online.
Sistemas de certificados <sup>1</sup>	Sistemas de emissão de certificados eletrônicos (cursos e eventos). O câmpus possui dois sistemas: SGCE (Sistema de Gestão de Certificados Eletrônicos) de código livre e outro sistema desenvolvido no próprio câmpus.
Mostra de Ensino Pesquisa e Extensão <sup>1</sup>	Utilizando a ferramenta de código aberto BookStack é um Sistema para exibição e interação com os projetos de ensino, pesquisa e extensão desenvolvidos no câmpus,
Hospedagem de sites de eventos e projetos <sup>1</sup>	Espaço disponibilizado para a hospedagem dos sites dos eventos realizados no câmpus e de projetos desenvolvidos pelos alunos.
GLPI <sup>1</sup>	Sistema de código aberto de gerenciamento de ativos de TI, de projetos e de incidentes e requisições.
ZoneMinder <sup>1</sup>	Sistema com código aberto de circuito fechado de TV (CFTV) para monitoramento e armazenamento de imagens das câmeras de vigilância.
DMP AccessII	Sistema de controle de acesso que possui

(Catracas) <sup>1</sup>	comunicação com as catracas.
Sistemas governamentais	Além dos sistemas do IFSP, nas atividades administrativas são utilizados diversos outros sistemas do Governo como o SouGov (gestão de pessoas) e o ComprasNet (Portal de compras do Governo Federal).
Internet <sup>1</sup>	O câmpus possui link dedicado fornecido pela RNP (Rede Nacional de Pesquisa) e link auxiliar contratado <sup>2</sup> (link de backup).
Wi-Fi <sup>1</sup>	Rede sem fio de acesso à Internet disponibilizada para todo o público interno do câmpus.
Telefonia <sup>1</sup>	Serviço telefônico contratado que possui 20 ramais externos (ligação externa), cuja administração é feita através do sistema Asterisk.
ConferênciaWeb RNP	Sistema de videoconferências disponibilizado pela RNP que possui integração com o Moodle.

<sup>1</sup> Sistemas e serviços hospedados, disponibilizados e administrados no próprio câmpus.

<sup>2</sup> A contratação do link auxiliar será limitada à disponibilidade orçamentária do câmpus.

#### **4.3. Infraestrutura física**

O prédio do Câmpus Bragança Paulista é dividido em dois blocos: A e B. O bloco A possui 3 (três) andares e o bloco B, 5 (cinco). O câmpus possui:

- A. 8 (oito) salas de aula;
- B. 24 (vinte e quatro) laboratórios;
- C. 21 (vinte e uma) salas para atividades administrativas (setores, coordenações e coordenadorias);
- D. 1 (uma) biblioteca;
- E. 1 (uma) sala de eventos;
- F. 1 (um) laboratório de pesquisa;
- G. 1 (uma) sala de videoconferência;
- H. 1 (uma) sala dos professores;
- I. 6 (seis) gabinetes de professores;

- J. 1 (um) CPD;
- K. 1 (uma) sala de equipamentos.

#### **4.4. Infraestrutura tecnológica**

Atualmente o parque tecnológico do IFSP - Câmpus Bragança Paulista é composto pelos seguintes ativos:

- A. 1 CPD;
- B. 1 Sala de equipamentos;
- C. 6 racks com equipamentos de rede;
- D. 3 racks para servidores;
- E. 41 switches gerenciáveis;
- F. 1 Firewall (Stonegate);
- G. 2 servidores Dell;
- H. 2 servidores IBM;
- I. 2 servidores HP;
- J. 1 storage de grande porte;
- K. 2 nobreaks de grande porte;
- L. 7 impressoras de rede;
- M. 430 computadores (desktops e notebooks)<sup>3</sup>;
- N. 150 usuários administrativos (técnicos administrativos, docentes, terceirizados e estagiários)<sup>3</sup>;
- O. 1200 usuários acadêmicos (discentes)<sup>3</sup>.

<sup>3</sup> Valores aproximados.

## **5. RESPONSABILIDADES**

### **5.1. Equipe da Coordenadoria 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 do câmpus.

## 5.2. Servidores (docentes e técnicos administrativos), discentes, estagiários e terceirizados do câmpus

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

## 6. NÍVEIS DE INCIDENTES

Nível	Descrição	Exemplos
<b>Nível I</b>	Hipótese acidental que pode ser controlada pela equipe de TI do câmpus e que não afeta o andamento do trabalho do servidor.	Problemas com equipamentos periféricos de computadores.
<b>Nível II</b>	Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo servidor.	Problema com o funcionamento do computador (não liga, travado, etc) ou ainda sistemas offline impedindo o uso do mesmo.
<b>Nível III</b>	Hipótese acidental que impede o uso de sistemas ou equipamentos de todo o câmpus, impedindo assim o desenvolvimento do trabalho de grande parte e/ou todos os servidores do câmpus.	Falha na conexão com a internet ou queda de energia elétrica no câmpus ou ainda problema técnico em algum servidor de rede que controla a conexão interna do câmpus.

## 7. PRINCIPAIS RISCOS

O quadro abaixo define os principais riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência:

Riscos	Parâmetros
Interrupção de energia elétrica	Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 60 (sessenta) minutos.
	Causada por fator interno que comprometa a rede elétrica do prédio como curto-circuito, incêndio ou infiltrações.
Falha na climatização do CPD	Superaquecimento dos ativos devido a falha no sistema de refrigeração.

Indisponibilidade de rede/circuitos	Rompimento de cabos decorrente de execuções de obras internas, desastres ou acidentes.
	Falha ou defeito nos ativos de rede (servidores, switches, roteadores, patch panels, etc.).
Falha humana	Acidentes no manuseio de equipamentos.
Falha de hardware	Falha que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo licitatório.
Desatualização ou descontinuidade	Falha ou travamento do equipamento ou serviço devido a incompatibilidades, falta de atualizações ou descontinuidade necessitando nova contratação ou aquisição.
Ataques internos	Ataque aos ativos do CPD e/ou equipamentos de TI dos laboratórios, salas de aula e de uso administrativo/ensino.
Ataque externo	Ataque virtual que comprometa o desempenho, acesso aos dados ou configuração dos serviços essenciais.

## 8. POLÍTICA E PROCEDIMENTOS DE BACKUP

### 8.1. Backup

Os servidores foram configurados para diariamente realizar as atividades de backup fora do período de atividade do câmpus. Os backups são armazenados em unidades de armazenamento externos (storages) localizados no CPD.

Além do backup automático, mensalmente os backups são salvos em unidades armazenadas em outro local do câmpus.

Caso seja necessário (manutenções emergenciais, atualizações, procedimentos do setor, etc.), os backups podem ser realizados a qualquer momento pela CTI.

### 8.2. Restauração e teste

A restauração de dados deve ser solicitada a CTI e será realizada de acordo com os procedimentos específicos do setor. A verificação e o teste de restauração, serão realizados sempre que possível por meio de um software de backup, configurado para verificar automaticamente as condições do backup.

Devido a possíveis falhas nos serviços e sistemas, a CTI poderá realizar restaurações para correções.

## **9. PRINCIPAIS PROBLEMAS, INCIDENTES E DEVIDAS AÇÕES DE CONTINGÊNCIA**

### **9.1. Problemas com computadores nos laboratórios**

- A. As máquinas passam por manutenções periódicas nos intervalos dos semestres, onde são feitas imagens com atualizações do sistema e softwares solicitados pelas áreas. Durante este período cabos e conexões são testados e reparados;
- B. Docentes que estão utilizando ou que irão utilizar o referido laboratório, deverão informar o problema à CTI (a comunicação deverá ser realizada conforme o item 10 deste documento);
- C. A CTI irá abrir um chamado no GLPI que será atribuído à um dos integrantes do setor que ficará responsável pelo atendimento;
- D. Após o atendimento o solicitante será informado da conclusão/resolução do problema;
- E. Caso o problema impeça o andamento da aula, a CTI irá até o local fazer uma primeira verificação do problema e tentará solucioná-lo *in loco*;
- F. Caso seja necessário, o equipamento será levado para a CTI para análise e correção do problema;
- G. Caso não seja possível o conserto, a CTI providenciará, se possível, outro equipamento para substituição.

### **9.2. Problemas com computadores administrativos**

- A. O usuário que está utilizando o equipamento, informará o problema à CTI (a comunicação deverá ser realizada conforme o item 10 deste documento);
- B. A CTI irá abrir um chamado no GLPI que será atribuído à um dos integrantes do setor que ficará responsável pelo atendimento;
- C. Após o atendimento o solicitante é informado da conclusão/resolução do problema;
- D. Caso o problema impeça o andamento do trabalho, a CTI irá até o local fazer uma primeira verificação do problema e tentará solucioná-lo *in loco*.

- E. Caso seja necessário, o equipamento será levado para a CTI para análise e correção do problema e o usuário será orientado a utilizar outro equipamento temporariamente;
- F. Caso não seja possível o conserto, a CTI providenciará, se possível, outro equipamento para substituição.

### **9.3. Problemas de conexão com a rede interna**

- A. Os usuários podem comunicar a CTI quando detectarem problemas na rede interna em seus setores (a comunicação deverá ser realizada conforme o item 10 deste documento);
- B. A própria CTI, através de ferramentas, poderá identificar falhas na rede;
- C. A CTI irá fazer o possível para identificar e corrigir a causa do problema;
- D. Caso o problema de conexão seja em todo o câmpus, verificará se os servidores de endereços DHCP (protocolo de configuração dinâmica de host) e de autenticação e os equipamentos de rede estão funcionando adequadamente;
- E. A CTI informará, se possível, a previsão do conserto ou solução aos demais servidores.

### **9.4. Problemas de conexão com a Internet**

- A. Os usuários podem comunicar a CTI quando detectarem problemas de conexão com a Internet em seus setores (a comunicação deverá ser realizada conforme o item 10 deste documento);
- B. A própria CTI, através de ferramentas, poderá identificar problemas na conexão com a Internet;
- C. A CTI verificará se o Firewall comutou automaticamente para o link de backup;
- D. A CTI irá fazer o possível para identificar e corrigir a causa do problema;
- E. Caso detectado problema externo, será aberto chamado técnico na operadora e/ou fornecedora do link visando o restabelecimento do serviço;
- F. Caso detectado problema interno, a CTI verificará a rede cabeada e os equipamentos de rede;
- G. A CTI informará, se possível, a previsão do conserto ou solução aos demais servidores.



#### **9.5. Problemas no acesso aos sistemas internos**

- A. Os usuários podem comunicar a CTI quando detectarem problemas de acesso aos sistemas internos em seus setores;
- B. A própria CTI, através de ferramentas, poderá identificar falhas de acesso;
- C. Verificar se a VM onde o mesmo está instalado está em execução;
- D. Caso esteja em execução, serão verificadas as conexões de rede da VM;
- E. Caso não esteja em execução, a VM será iniciada e serão realizados testes de acesso;
- F. Caso seja necessário, a VM será recuperada através do backup;
- G. A CTI informará, se possível, a previsão do conserto ou solução aos demais servidores.

#### **9.6. Problemas com equipamentos de rede**

- A. A CTI, através de ferramentas e/ou procedimentos, identificará problemas nos equipamentos de rede;
- B. Caso identificado problema no equipamento, será verificado se o mesmo está na garantia. Se estiver, a garantia será acionada;
- C. Caso possível, a CTI irá realizar manutenção do mesmo (se necessário, a CTI solicitará auxílio dos técnicos de eletroeletrônica do câmpus);
- D. Caso não tenha como consertar e não esteja em garantia, realizar a troca do equipamento de forma que haja o menor transtorno possível no desempenho das atividades dos demais servidores do câmpus.

#### **9.7. Problemas físicos com cabeamento da rede interna**

- A. A CTI, através de ferramentas e/ou procedimentos, identificará problemas no cabeamento de rede;
- B. A CTI tentará detectar a causa do problema por meio de testes no cabeamento;
- C. Detectado problema de cabeamento de rede, as conexões serão refeitas;
- D. Verificar as demais ligações caso seja em um rack com switch e testá-las;
- E. Caso haja necessidade, agendar ou efetuar a troca do(s) cabo(s) que estão apresentando falhas.

#### **9.8. Problemas com falta de energia elétrica**

- A. Caso seja identificada queda ou falta total de energia elétrica no campus, a CTI irá informar a Coordenadoria de Almojarifado e Patrimônio - CAP para as devidas providências;
- B. A CTI verificará com a CAP se a queda foi interna ou externa;
- C. A CTI irá verificar se os nobreaks estão ativos e acompanhará a carga das baterias;
- D. Se a falta de energia for de curta duração, antes das baterias dos nobreaks atingirem 20% da carga, os sistemas e servidores de rede continuarão em funcionamento;
- E. Caso a falta de energia perdurar até os nobreaks atingirem 20% de carga, os sistemas deverão ser desligados, bem como todos os equipamentos e serão religados novamente assim que a energia for restabelecida.

#### **9.9. Ordem para desligamento dos servidores**

- A. Acessar o ambiente virtual e desligar primeiramente os servidores virtuais de serviços/web;
- B. Acessar o ambiente virtual e desligar o servidor das VMs dos laboratórios;
- C. Desligar fisicamente os servidores que hospedam as VMs;
- D. Desligar servidor do ZoneMinder e o storage;
- E. Desligar os servidores físicos (câmeras D-Link, catracas, Asterisk, gerenciador de domínio, entre outros) dos racks do CPD;
- F. Desligar o Firewall e a controladora Wi-Fi.

#### **9.10. Ordem para religar os servidores**

- A. Ligar o Firewall e a controladora Wi-Fi;
- B. Ligar os servidores físicos (câmeras D-Link, catracas, Asterisk, gerenciador de domínio, entre outros) dos racks do CPD;
- C. Ligar os servidores físicos onde estão hospedados as VMs;
- D. Verificar se as VMs ligaram automaticamente;
- E. Caso não tenham sido ligadas verificar a causa e ligar manualmente;
- F. Ligar o storage;
- G. Ligar o servidor do ZoneMinder e verificar mapeamento do storage;

- H. Verificar conexão e gravação das câmeras de vigilância no ZoneMinder/Storage;
- I. Realizar testes de acesso à Internet, ao domínio, aos sistemas hospedados no câmpus;
- J. Realizar testes no serviço de telefonia.

#### **9.11. Outros problemas**

Para demais problemas de TI não relacionados neste documento, o usuário deverá comunicar a CTI. A comunicação deve ser realizada conforme o item 10 deste documento.

### **10. COMUNICAÇÃO**

#### **10.1. Quem deve comunicar**

Qualquer usuário que detecte qualquer tipo de problema ou anomalia nos sistemas, equipamentos e/ou infraestrutura de TI.

#### **10.2. A quem comunicar**

A comunicação deve ser feita, assim que possível, para a CTI do câmpus.

#### **10.3. Como comunicar**

Deve ser enviado um e-mail para o endereço [cti.bra@ifsp.edu.br](mailto:cti.bra@ifsp.edu.br) relatando o máximo possível de informações do incidente e/ou requisição. Caso seja necessário, é possível realizar a comunicação através de chamada telefônica no número (11) 4034-7815 ou pelos ramais internos ou ainda ir presencialmente ao setor.

### **11. REVISÃO**

Este documento poderá ser revisado a qualquer momento pela CTI. As revisões poderão alterar, atualizar ou até excluir quaisquer pontos do documento.

## 12. EQUIPE

<b>Nome</b>	<b>Cargo</b>	<b>E-mail</b>	<b>Ramal interno</b>
Tiago Minoru Taguchi (Coordenador da CTI)	Técnico de Laboratório	tiagotaguchi@ifsp.edu.br	8151
Evanilton Marques de Lima	Técnico de Laboratório	evanilton@ifsp.edu.br	8152
Luiz Nelson Viana Filho	Técnico de Laboratório	luiznelson@ifsp.edu.br	8153
Sandra Cristina Martins de Oliveira	Técnica de TI	sandra.martins@ifsp.edu.br	8154
Vanderlei Benedito da Silva Filho	Técnico de TI	vanderlei_filho@ifsp.edu.br	8155

Elaborado por

**Coordenadoria de Tecnologia da Informação – CTI  
IFSP - Câmpus Bragança Paulista**