**PLANO DE CONTINGÊNCIA**

**INFRAESTRUTURA TECNOLÓGICA**

**SUMÁRIO**

**[OBJETIVO 3](#_Toc129884911)**

[**FUNCIONÁRIOS RESPONSÁVEIS 3**](#_Toc129884912)

[**RESPONSABILIDADES 3**](#_Toc129884913)

[**Anderson Oliveira: 3**](#_Toc129884914)

[**Heber Miranda: 4**](#_Toc129884915)

[**Peterson Nilton: 4**](#_Toc129884916)

[**Rodrigo Vilela 4**](#_Toc129884917)

[**Vinicius Carvalho: 5**](#_Toc129884918)

[**Restauração de servidores em caso de desastre 5**](#_Toc129884919)

[**Servidores de Firewall (2 horas) 5**](#_Toc129884920)

[**Servidor de Banco de Dados (4 horas) 5**](#_Toc129884921)

[**Servidores de Aplicações (4 horas) 6**](#_Toc129884922)

[**Servidor de Autenticação/Controlador de Domínio/Arquivos (2 horas) 6**](#_Toc129884923)

[**Servidor de E-mail (4 horas) 6**](#_Toc129884924)

[**Servidor de Controlador de Wifi (2 horas) 6**](#_Toc129884925)

[**Servidor de Gestão ERP (TOTVS) (4 horas) 6**](#_Toc129884926)

[**Servidor de Gestão Acadêmico e Financeiro 7**](#_Toc129884927)

[**(4 horas) 7**](#_Toc129884928)

[**Servidor de LMS – Moodle (4 horas) 7**](#_Toc129884929)

[**Serviço de acesso à rede e internet (6 horas) 7**](#_Toc129884930)

[**Áreas Afetadas 7**](#_Toc129884931)

[**Notificações 8**](#_Toc129884932)

[**Backup Disponível 8**](#_Toc129884933)

# OBJETIVO

Estabelecer um plano para recuperação após desastres, que busque assegurar o reestabelecimento das atividades da Faculdade de São Lourenço assim como seus objetivos. O plano constitui de um conjunto de procedimentos definidos formalmente para permitir que os serviços de processamento de dados continuem a operar, de forma que dependendo da extensão do problema, com certo grau de degradação, caso ocorra algum evento que não possibilite seu funcionamento normal.

# FUNCIONÁRIOS RESPONSÁVEIS

* Anderson Oliveira – Gerente de TI

(11) 99597-4421;

* Heber Miranda – Analista de Sistemas

(11) 99588-1254;

* Peterson Nilton – Analista de Sistemas

(11) 96962-6133;

* Rodrigo Vilela de Paulo – Analista de Sistemas

(35) 98879-4333;

* Vinicius Silveira de Carvalho

Técnico em Informática (35) 98703-3422;

# RESPONSABILIDADES

## Anderson Oliveira:

* Servidores de Firewall;
* Servidor de Banco de Dados;
* Servidores de Aplicações;
* Servidor de Autenticação/Controlador de Domínio/Arquivos;
* Servidor de E-mail;
* Servidor de Controlador Wifi;
* Servidor de Gestão ERP (TOTVS);
* Servidor de Gestão Acadêmico e Financeiro; 9. Servidor de LMS (Moodle).

## Heber Miranda:

* Servidores de Firewall;
* Servidor de Banco de Dados;
* Servidores de Aplicações;
* Servidor de Autenticação/Controlador de Domínio/Arquivos;
* Servidor Anti-vírus;
* Servidor de Controlador Wifi;
* Servidor de Gestão ERP (TOTVS); 8. Servidor de Gestão Acadêmico e Financeiro;
* Servidor de LMS (Moodle).

## Peterson Nilton:

* Servidor de Banco de Dados;
* Servidores de Aplicações;
* Servidor de E-mail;
* Servidor de Controlador Wifi;
* Servidor de Gestão ERP (TOTVS);
* Servidor de Gestão Acadêmico e Financeiro.

## Rodrigo Vilela

* Servidor de Banco de Dados;
* Servidores de Aplicações;
* Servidor de Controlador Wifi;
* Serviço de acesso à rede e internet.
* Servidor Antivírus.

## Vinicius Carvalho:

* Servidor de Banco de Dados;
* Servidores de Aplicações;
* Servidor de Autenticação/Controlador de Domínio/Arquivos;
* Serviço de acesso à rede e internet.

O plano de contingência prevê condições de funcionamento 24 horas por dia, 7 dias por semana.

# Restauração de servidores em caso de desastre

## Servidores de Firewall (2 horas)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Ativar servidor de backup;
3. Proceder com a ativação da VM Firewall;
4. Atualizar políticas de acessos atuais;
5. Testar todos serviços.

## Servidor de Banco de Dados (4 horas)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Abertura de ordem de serviço (OS) junto a prestadora do Datacenter;
3. Acompanhamento do andamento da OS;
4. Testar o banco de dados.

## Servidores de Aplicações (4 horas)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Abertura de ordem de serviço (OS) junto a prestadora do Datacenter;
3. Acompanhamento do andamento da OS;
4. Testar o Aplicações.

## Servidor de Autenticação/Controlador de Domínio/Arquivos (2 horas)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Ativar servidor de backup;
3. Proceder com a ativação da VM SAMBA/AD;
4. Atualizar políticas de acessos atuais;
5. Testar todos serviços.

## Servidor de E-mail (4 horas)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Abertura de ordem de serviço (OS) junto a prestadora do Datacenter;
3. Acompanhamento do andamento da OS;
4. Testar E-mails.

## Servidor de Controlador de Wifi (2 horas)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Ativar servidor de backup;
3. Proceder com a ativação da VM;
4. Atualizar políticas de acessos atuais;
5. Testar todos serviços.

## Servidor de Gestão ERP (TOTVS) (4 horas)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Ativar servidor de backup;
3. Proceder com a ativação da VM Totvs;
4. Restauração do banco de dados;
5. Testar todos serviços.

## Servidor de Gestão Acadêmico e Financeiro

## (4 horas)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Abertura de ordem de serviço (OS) junto a prestadora do Datacenter;
3. Acompanhamento do andamento da OS;
4. Testar Aplicação.

## Servidor de LMS – Moodle (4 horas)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Abertura de ordem de serviço (OS) junto a prestadora do Datacenter;
3. Acompanhamento do andamento da OS;
4. Testar Serviços.

## Serviço de acesso à rede e internet (6 horas)

1. Verificar a alimentação dos ativos de rede (Modens, Switchs, Roteadores, etc);
2. Identificar se o problema é local ou na operadora;
3. Entrar em contato com a operadora para solicitar reparo;
4. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
5. Testar os serviços de rede e internet.

## Áreas Afetadas

* Direção;
* CPD;
* Secretaria Geral;
* Coordenações de Curso;
* Laboratórios;
* Tesouraria;
* ISE/PAD;
* Biblioteca;
* Recursos Humanos;
* Wifi de alunos e professores.

## Notificações

* Internas (Telefone/E-mail):
* Direção
* CPD;
* Secretaria Geral;
* Coordenações de Curso;
* Laboratórios;
* Tesouraria;
* ISE/PAD;
* Biblioteca;
* Recursos Humanos.

## Backup Disponível

Servidor com cópia das máquinas virtuais com serviços pré-instalados XEN (Linux, Windows Server, Pfsense)

* Nobreaks;
* Link para Backup;
* Cópias dos principais dados e serviços.