IPREM	Manual – 012 Plano de Contingência TI

HISTÓRICOS DAS ALTERAÇÕES		
Revisão	**Data**	**Descrição**
0	20/01/2021	Elaboração Inicial
1	13/05/2021	Revisão do Mapeamento e Manual

OBJETIVO:
A proteção e controle de acesso da informação deve existir para garantir a continuidade dos serviços, ações que previna contra incidentes que possam causar danos à uma organização ou provocar alterações nos planos elaborados previamente, minimizado os riscos dentro de patamares aceitáveis.

O Plano de Contingência é estruturado a partir da previsão de falhas associadas aos planos de trabalho ordinários e tem por objetivo tomar as ações para a continuidade dos serviços e para a recuperação dos recursos que foram danificados.

O Controle de Acesso é usado para identificar, registrar e rastrear os acessos de cada pessoa.

REGULAMENTAÇÃO:

1. Lei Federal 8.159/1991, de 08/01/1991 - Dispõe sobre a política nacional de arquivos públicos e privados;

2. Lei Federal 9.610/1998, de 19/02/1998 - Dispõe sobre o direito autoral;

3. Lei Federal 9.279/1996, de 14/05/1996 - Dispõe sobre marcas e patentes;

4. Lei Federal 10.406/2002, de 10/01/2002 - Institui o Código Civil brasileiro;

5. Decreto-Lei 2.848/1940, de 07/12/1940 - Institui o Código Penal brasileiro.

TERMOS UTILIZADOS:

BACKUP – é uma cópia de segurança dos seus dados (física ou em nuvem) de um dispositivo de armazenamento ou sistema. Se você está aqui é porque algum software ou aplicativo está recomendando que você faça backup dos seus dados;

CONTROLE DE ACESSO – é qualquer sistema, mecanismo ou equipamento que limite o acesso a um determinado ambiente ou informação. O objetivo é garantir a segurança de dados sigilosos, dos bens e das pessoas. Impedindo assim, o acesso de pessoas não autorizadas aos ambientes;

HARDWARE - é a parte física do computador, ou seja, o conjunto de aparatos eletrônicos, peças e equipamentos que fazem o computador funcionar. O monitor, impressora e o mouse são exemplos de hardware;

SOFTWARE – são os programas que fazem com que a máquina funcione, como os

Thaís Gabrielle da Rocha Silva

aplicativos e sistemas operacionais. São os elementos físicos de um computador ou eletrônico;

DOWNLOAD - é o mesmo que baixar um arquivo;

UPLOAD - é o mesmo que enviar um arquivo, mesmo que seja por e-mail;

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.

1. PROCESSO DE IDENTIFICAÇÃO DOS RISCOS E AÇÕES PARA CONTIGENCIAR:

1.1. Todos os servidores do IPREM que utilizam o sistema de informática e processamento de dados deverão seguir os planos de contingenciamento conforme orientação abaixo:

2. ESTRUTURA GLOBAL:

2.1. Cabe a qualquer servidor, que identificar alguma situação que venha comprometer as instalações do prédio da sede do IPREM, deverá acionar as medidas de contingencia de acordo com cada ocorrência.

I. Interrupção da energia elétrica

a. Acionar a CEMIG para manutenção de energia elétrica.

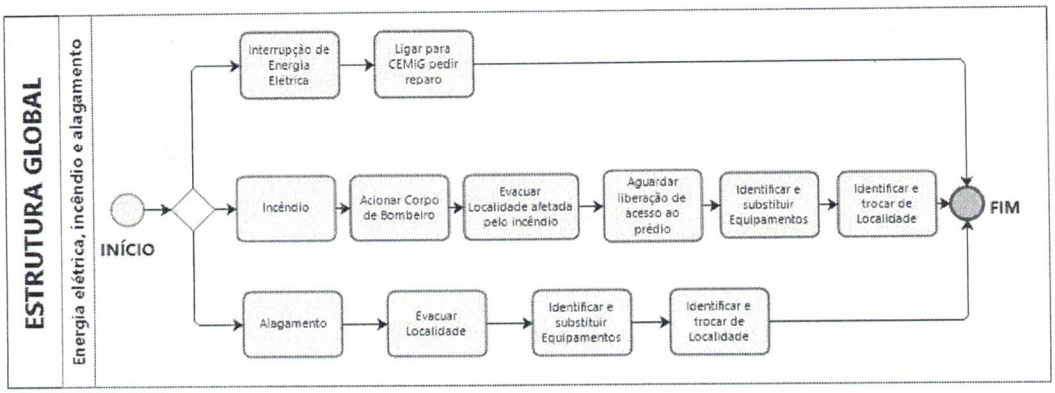
II. Incêndio

a. Acionar Corpo de Bombeiro para conter o incêndio;
b. Evacuar localidade;
c. Substituir equipamentos danificados;
d. Trocar localidade.

III. Alagamento

a. Evacuar a localidade;
b. Substituir equipamentos danificados;
c. Trocar localidade.

Fluxograma da Estrutura Global:



Thaís Gabrielle da Rocha Silva

3. REDE DO INSTITUTO:

3.1. Qualquer servidor, que perceber alguma falha no funcionamento da rede do Instituto, deverá observar em qual das situações se encontra o problema, deverá comuniciar ao Técnico de Informática para que sejam tomadas as medidas equiparadas com a situação em ocorrência.

I. Falha de Acesso à internet

a. Acionar o setor responsável para manutenção da internet ou utilização de um link de internet paralelo.

II. Falha em Softwares

a. Atualizar o software para a versão recente ou restaurar imagem no backup diário.

III. Interrupção do serviço de e-mail

a. Acesso ao servidor de email para as devidas configurações;

b. Reinstalação do Software de email;

c. Restauração de backup diário.

IV. Falha de acesso à rede (Falha lógica)

a. Abrir chamado para configurar computador à rede com as devidas permissões.

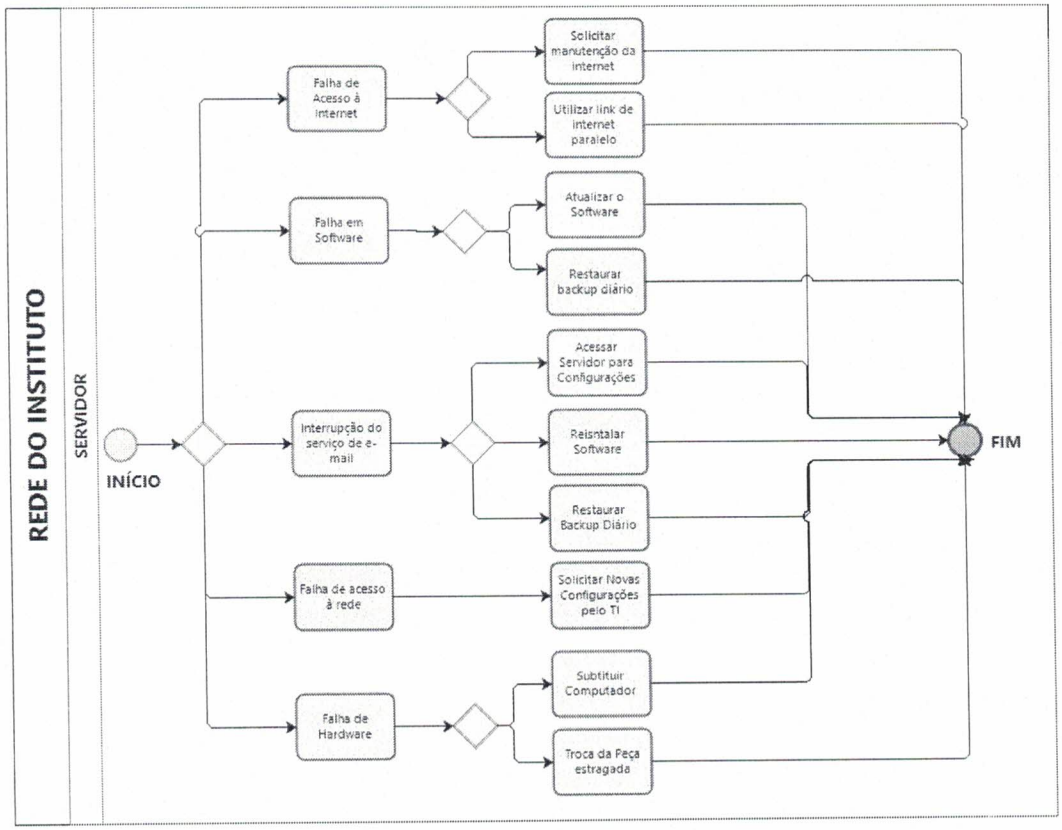
V. Falha de Hardware

a. Substituição imediata do computador para o colaborador;

b. Troca da peça com falha.

Thaís Gabrielle da Rocha Silva

Fluxograma da Rede do Instituto:



4. CENTRO DE PROCESSAMENTO DE DADOS – CPD

I. Falha no Hardware

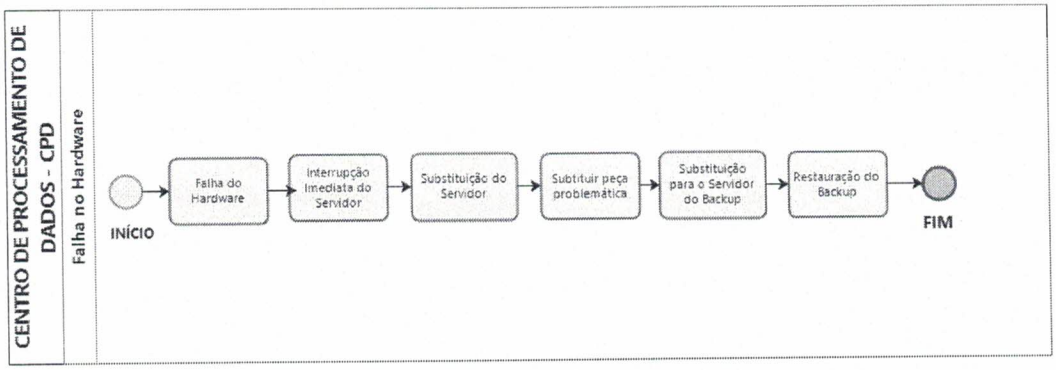
a. Interrupção imediata do servidor;

b. Substituição do servidor por servidor redundante ou outro backup;

c. Substituir peças problemáticas;

d. Caso dados estejam corrompidos, seguir coma restauração do backup.

Fluxograma do centro Processamento de dados – CPD:



Thaís Gabrielle da Rocha Silva

5. FIREWALL

I. Invasões Externas

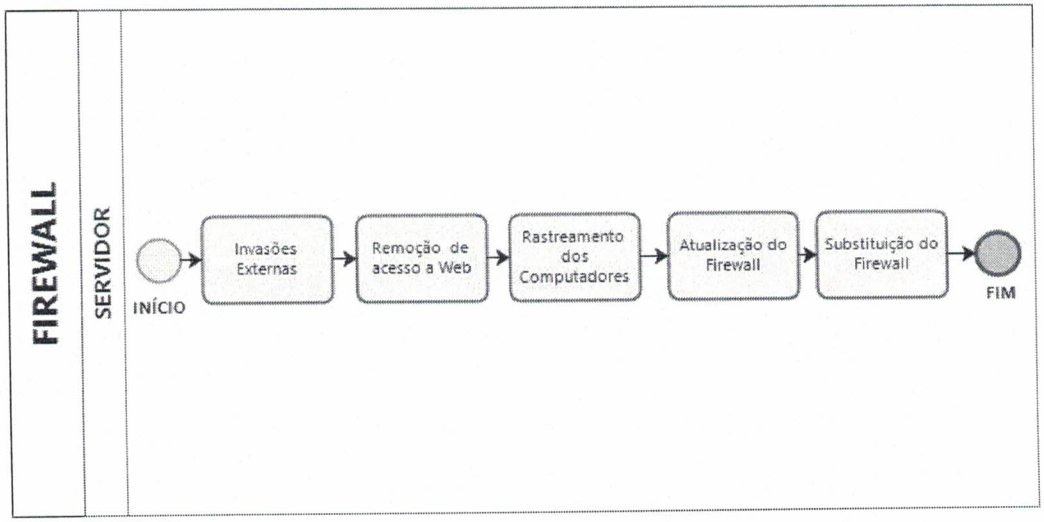
a. Remoção de acesso à web imediata;

b. Rastreamento dos computadores com dados corrompidos para backup e restauração

c. Atualização do Firewall;

d. Atualização do Firewall ou substituição imediata.

Fluxograma do Firewall:



Thais Gabrielle da Rocha Silva