MANUAL DE CONTINGÊNCIA DA INFRAESTRUTURA TECNOLÓGICA

NÚCLEO DE TECNOLOGIA DIGITAL DA INFORMAÇÃO E COMUNICAÇÃO

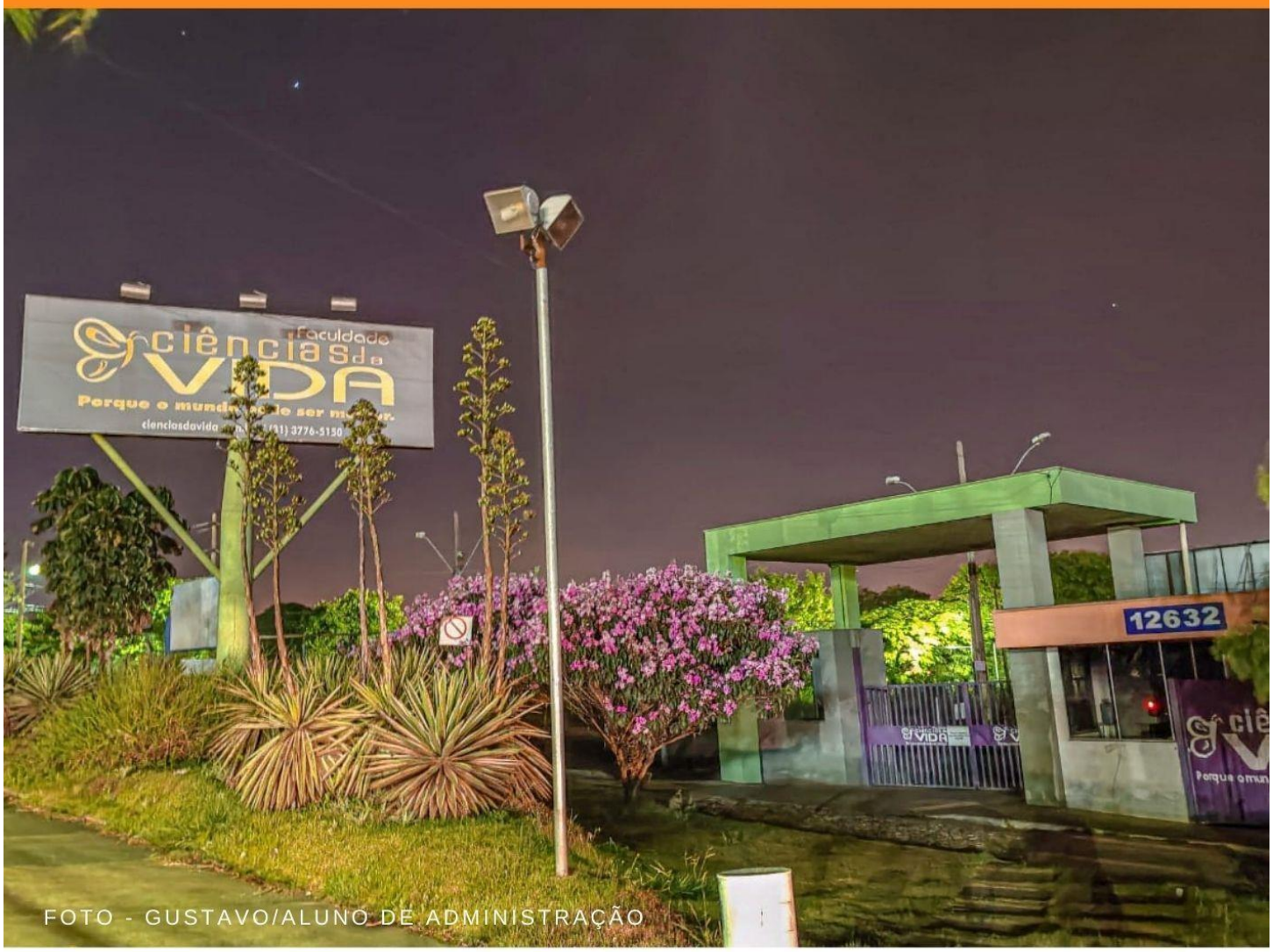


FOTO - GUSTAVO/ALUNO DE ADMINISTRAÇÃO

Faculdade ciências da VIDA
Porque o mundo pode ser melhor.

SETE LAGOAS - 2021

DADOS DA INSTITUIÇÃO

INFORMAÇÕES E CONTATOS
Faculdade Ciências da Vida
Avenida Prefeito Alberto Moura , 12.632 – Distrito Industrial
Sete Lagoas – MG
Cep: 35702-383
WebSite : www.faculdadecienciasdavida.com.br

DIREÇÃO GERAL

Valcir Marcílio Farias

EQUIPE DE ELABORAÇÃO

Camila Alves Martins

Darliane de Cássia Gonçalves de Oliveira

Ione Aparecida Neto Rodrigues

Marcos José Moreira Ferreira

CAPA

Tatiane Guimarães de Carvalho

FICHA CATALOGRÁFICA

Faculdade de Ciências da Vida
Manual de contingência da infraestrutura tecnológica / Instituto Vida e Saúde. – Sete Lagoas – MG, 2021

Documento desenvolvido pelo Núcleo de Tecnologia Digital da Informação e de Comunicação da Faculdade de Ciências da Vida, situada na cidade de Sete Lagoas-MG, 2021.

Orientador: Prof MSc. Valcir Marcílio Farias.

1. Documento institucional. 2. Crises e contingencias. 3. Administrativo, discentes e docentes. I. Título. II. Farias, Valcir Marcílio. III. Instituto Vida e Saúde – Faculdade de Ciências da Vida.

CDU - 047.3

Ficha catalográfica por Stênio Clemente CRB6 - 3282

Sumário

LISTAS DE FLUXOGRAMAS

LISTAS DE FIGURAS

1 APRESENTAÇAO

Este instrumento tem por finalidade estabelecer orientações à comunidade da Faculdade de Ciências da Vida (FCV) sobre o Plano de Contingência da Infraestrutura Tecnológica (PCIT). O principal objetivo do PCIT da FCV é possibilitar a continuidade do funcionamento da instituição diante a quaisquer eventualidades, sejam estas, materiais ou pessoais, além de estabelecer escopos estratégicos e ações para cumprir as metas estabelecidas nessa área, bem como nortear a prevenção de incidentes e recuperação em caso de desastres e em momentos de crise.

Ele deve ser atualizado a qualquer momento em que se mostrar necessário, mediante aprendizado organizacional ou por necessidade de adaptação ao cenário imediato, o PCIT identifica duas variáveis para o funcionamento adequado da instituição: Infraestrutura e Processos.

A Infraestrutura engloba todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática, multimídia, sistemas internos, sistemas externos e de terceiros. Para cada um dos itens que compõem a infraestrutura deverá existir uma ação a ser adotada.

Os processos são concebidos como atividades realizadas para operacionalizar a Instituição, e dependem da infraestrutura toda ou de parte da estrutura em funcionamento. Com os processos em andamento pode-se definir se o plano de ação foi bem ou não executado.

O Plano de Contingência da Infraestrutura Tecnológica será composto pelos seguintes planos:

a) **Administração de Crise**: ações preventivas, análise de riscos, sistemas de emergência preparados, ou seja, procedimentos que serão acionados no momento em que a crise de fato ocorrer. Na ocasião, é fundamental manter a equipe preparada para colocá-lo em prática até que a situação seja normalizada;

b) **Continuidade Operacional**: relacionado aos ativos da instituição, sejam eles, humanos ou não, o objetivo é mantê-los sempre disponíveis para que possam dar o fulcro necessário à continuidade dos processos. Sua missão maior é a de restabelecer os serviços no menor tempo possível caso haja uma interrupção nos sistemas de informação ou nos serviços prestados, de forma que o impacto causado seja o mínimo possível;

c) **Recuperação de Desastre**: tem a finalidade de agir no momento de um desastre. Vários são os tipos de eventos causadores de falhas e interrupções, como por exemplo de uma inundação, um vendaval, incêndios, blecautes, invasão de sistemas, interrupção de comunicação de dados e voz, roubos, atos de vandalismo, sabotagens, que afetem a estrutura física e tecnológica da Instituição.

2 GESTÃO DE CRISE

2.1 O QUE É CRISE

A crise pode ser considerada como qualquer situação ou ação negativa que escape ao controle da instituição e ganhe visibilidade, podendo impactar negativamente a imagem e reputação da instituição.

Com o gerenciamento de riscos, espera-se evitar decisões improvisadas e informações distorcidas, disseminadas sem embasamento ou orientação adequada. Ao adotar um planejamento preventivo, a FCV busca desenvolver uma cultura organizacional voltada para a abordagem das situações de incerteza que possam desencadear ameaças à segurança ou comprometer os objetivos organizacionais, evitando assim, que tais ocorrências tomem proporções mais graves e ocasionem uma crise.

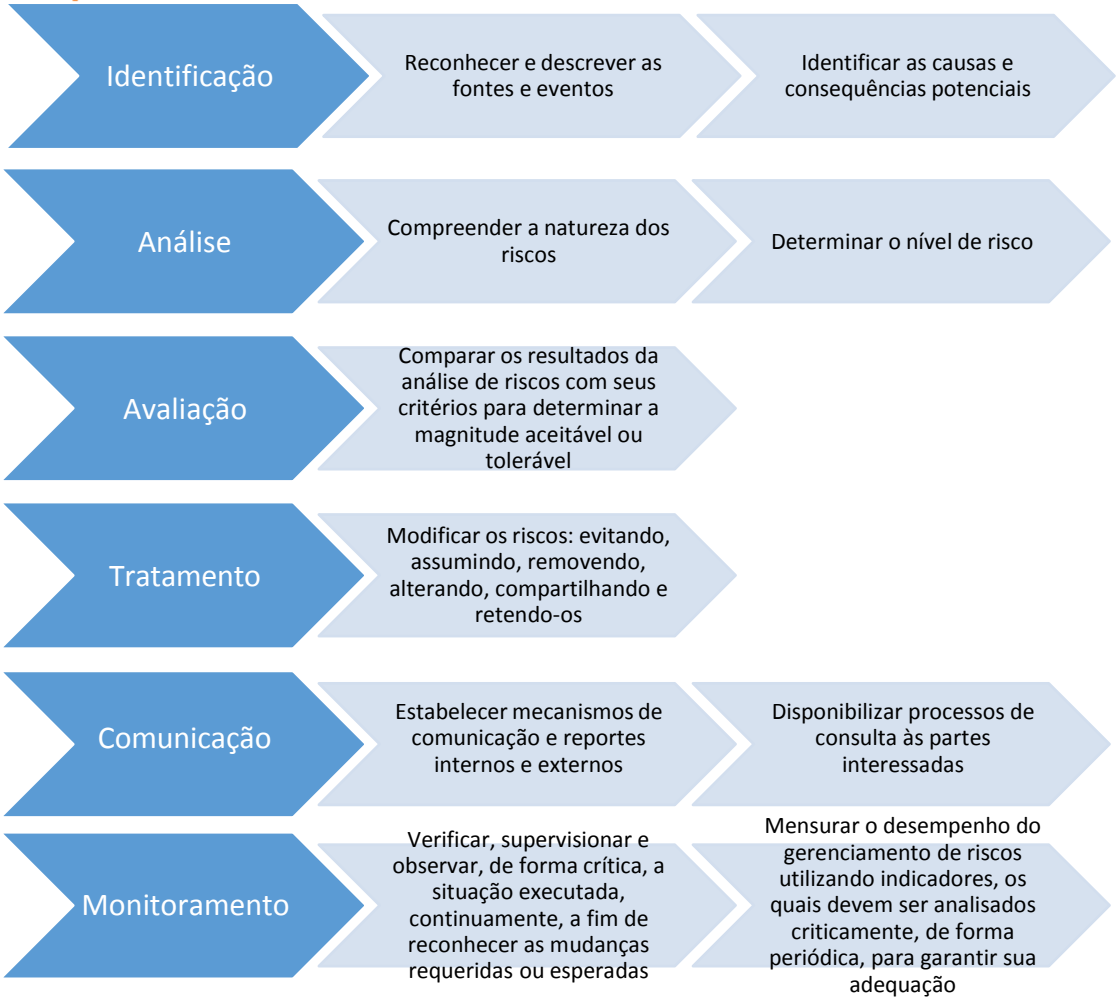
Entre os principais benefícios do gerenciamento de riscos, destacam-se:

- otimização de procedimentos em situações de riscos;
- adoção de metodologia própria no gerenciamento de riscos e crises;
- alinhamento junto aos funcionários para os devidos encaminhamentos em situações de riscos;
- mitigação dos impactos, caso se instale a crise;
- mais atenção ao desempenho de segurança e proteção;• proteção e preservação da imagem institucional.

2.2 COMITÊ DE CRISE

O comitê tem a responsabilidade de acompanhar as informações/notícias que podem desencadear uma crise e acionar as pessoas responsáveis em cada caso; gerenciar as situações, determinando as ações mais indicadas a cada caso; definir o posicionamento da instituição e lidar com todos os públicos envolvidos, garantindo a distribuição das informações e controlar o fluxo de informações até que o problema seja solucionado e esclarecido, auxiliando a comunicação no acompanhamento e análise da cobertura da imprensa.

Fluxograma 1 - Etapas do Plano de Gerenciamento de Riscos



Fonte: Elaborado pelos autores

2.3 AÇÕES DE COMUNICAÇÃO

A FCV busca garantir a transparência e o acesso à informação aos seus públicos. Baseado nessa premissa, o Grupo de Gerenciamento de Crises (GGC) tem como um de seus princípios assegurar a rapidez na divulgação de informações sobre incidentes que venham a ocorrer, prevenindo assim, reflexos negativos na imagem da Instituição. Em todas as situações, o Setor de Comunicação, sempre deverá estar envolvido.

2.3.1 Comunicação Preventiva

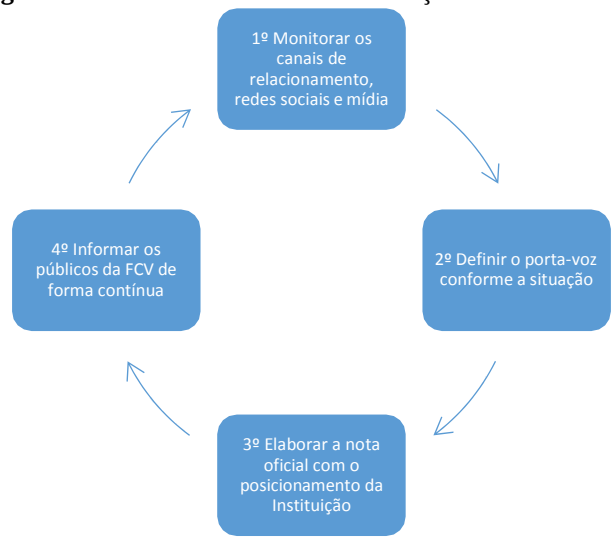
Entre as ações, destacam-se as seguintes medidas: monitorar de forma contínua a mídia, os canais de relacionamentos e as redes sociais, a fim de identificar riscos ou detectar fatores que

possam gerar uma crise; facilitar a comunicação com os públicos de interesse da Instituição, promovendo o diálogo e o bom relacionamento com eles.

2.3.2 Comunicação quando Instalada a Crise

Uma vez determinada pelo GGC a existência de uma situação de crise, cuja magnitude possa causar impacto à imagem da Instituição, devem ser realizados os seguintes procedimentos:

Fluxograma 2 – Procedimentos da comunicação da crise instalada



Fonte: Elabora pelos autores

2.3.3 Processos de Comunicação e Reporte Internos

A fim de evitar boatos e informações distorcidas que possam prejudicar a imagem da instituição, a FCV utiliza alguns canais de comunicação:

• Site Institucional;

• Informativo Interno via e-mail, grupos de whatsapp e mensagens via CRM;

• Encontros presenciais e reuniões em remoto de acordo com a gravidade do fato;

2.3.3.1 Recomendações:

Geralmente as pessoas têm dificuldade para distinguir e separar o lado pessoal do profissional. Assim, um comentário ou opinião pessoal emitida por algum funcionário da FCV pode ser interpretado como a posição social da Instituição. Por isso, para evitar essas situações, este Manual aponta algumas recomendações.

Mantenha em sigilo as informações que ainda não foram divulgadas oficialmente pela FCV. Comunique ao setor de Comunicação se perceber informações negativas sobre a Instituição. No caso de algum jornalista entrar em contato com o setor onde está o foco do problema, a orientação é encaminhá-lo ao setor de Comunicação.

Evite falar em público sobre situações do seu trabalho que possam comprometer a imagem da Instituição. Se você tem discordâncias ou críticas aos processos da FCV, resolva internamente por meio dos canais abertos para isso.

2.3.3.2 Cuidado nas Redes Sociais

Tudo o que você posta pode ser interpretado pelos usuários das redes como uma manifestação da FCV. Evite postar qualquer conteúdo que possa causar dano à imagem da Instituição. Comunicações de caráter interno não devem ser compartilhadas com outros colegas por redes sociais.

Evite fazer parte de comentários especulativos a respeito de posicionamentos ou ações da Instituição em situações de crise. Pense bem sobre o que você vai publicar a respeito da FCV nas redes sociais, pois seus comentários podem ser compartilhados por um número imensurável de usuários das redes.

Lembre-se: em todas situações, a FCV definirá um porta-voz para responder oficialmente pela Instituição. Entretanto, se você publicar informações e comentários nas redes sociais referindo-se a essa situação, sua rede de relacionamento poderá considerar que você fala em nome da Instituição.

2.3.3.3 O que não se pode fazer

- ✓ Falar ou escrever em nome da FCV sem estar autorizado para isso.
- ✓ Representar a Instituição sem a devida autorização.
- ✓ Criticar publicamente as decisões institucionais.
- ✓ Divulgar informações confidenciais.
- ✓ Antecipar decisões que ainda não foram divulgadas oficialmente.

2.3.4 Processos de Comunicação e Reporte Externos

O setor de Comunicação será o responsável pela elaboração do material de divulgação, como notas, releases ou informativos. Em uma situação de crise, a Instituição estabelecerá comunicação com seu público externo por meio dos seguintes canais:

- Site;
- E-mails;
- Redes sociais;
- Mídia paga;
- Imprensa;
- Release;
- Nota oficial;
- Coletiva;

A comunicação deverá ser simples, direta e transparente: o que aconteceu; por que aconteceu; e o que será feito para solucionar o caso e evitar que tal situação ocorra novamente.

2.3.4.1 O que fazer em casos de emergência?

Se você presenciar alguma situação de risco ou emergência, comunique o fato para o whastapp Oficial da Faculdade ciências da Vida através deste link. E ainda poderá acessar a todos os setores através do site: http://www.cienciasdavida.com.br e clique em Fale Conosco e novamente em Fale Conosco.

Figura 1 - Fale Conosco

Fonte: Site www.cienciasdavida.com.br (2021)

E no formulário selecione o setor, digite seu nome completo, e-mail, cidade, telefone e digite a sua mensagem, após clique em Enviar, você receberá o retorno para o e-mail preenchido no formulário.

Figura 2 - Formulário de preenchimento do fale conosco

Fonte: Site www.cienciasdavida.com.br (2021)

3 PLANO DE CONTINUIDADE E RECUPERAÇÃO DE DESASTRES

3.1 OBJETIVO

Estabelecer um plano para recuperação após desastres, que busque assegurar o reestabelecimento dos negócios da FCV 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.

A Política de Segurança elaborada pela equipe de Tecnologia e Informação será reavaliada continuamente e inclui as seguintes regras:

a) O backup do sistema SIG é feito diariamente em servidor local da Empresa responsável contratada por atualização, criação e hospedagem do sistema;

b) O backup do AVA (Moodle) é feito diariamente no servidor na nuvem dedicado na Hostgator;

c) O backup do servidor de arquivos é feito diariamente em servidor local, conforme ferramenta do sistema Windows Server 2012;

d) Renovação anual dos domínios cienciasdavida.com.br e faculdadecienciasdavida.com.br;

e) A Instituição conta com linhas de telefone digitais, em caso de falhas nas linhas telefônicas, os funcionários ainda possuem celulares que podem substituir a telefonia fixa.

f) Falha no fornecimento de energia, a Instituição possui nobreak para suportar o funcionamento dos servidores locais. A unidade de quebra de fornecimento de energia conta com capacidade de processamento ininterrupto das operações por 20 minutos por um no-break (unidades de UPS - Uninterruptiple Power Supply).

g) O plano de recuperação de desastres permite o gerenciamento de crises. Em caso de efetiva necessidade de utilização da estrutura de contingência, a equipe de Tecnologia e Informação deverá ficar à disposição para suporte aos funcionários técnico-administrativos. Com os procedimentos descritos acima, a Instituição pode continuar a funcionar com a equipe administrativa mesmo que não possa ter acesso físico ao Campus.

h) Lista de Informações deverá ser disponibilizada ao corpo técnico-administrativo, de comunicação e marketing e de gestão acadêmica relação de acesso às informações de contato do corpo social da Instituição, bem como dos prestadores de serviço contratados. (E-mails, telefones e CRM's).

i) Procedimentos de Contingência na impossibilidade de se utilizar o espaço físico da Instituição, os funcionários envolvidos no processo de contingência (nomes serão disponibilizados com número dos celulares) deverão comparecer a um local de encontro do plano de contingência, indicado.

Se a impossibilidade de se utilizar o espaço físico ocorrer quando os funcionários estiverem na Instituição, o corpo técnico-administrativo deverá dirigir-se ao ponto de encontro.

1º. Os alunos serão dispensados das atividades escolares e as aulas serão repostas em datas e horários estipulados pelas coordenadorias de cursos e divulgados ao corpo estudante por notificação no aluno-online, e-mails e grupos de whatsapp.

2º. Chegando no Ponto de Encontro estabelecido, o responsável pela tecnologia e Informação, será responsável por recuperar os arquivos no back-up diário realizado no servidor local. A lista dos arquivos que necessitam de recuperação consta no Manual de Administração de Crises.

Além do processo de recuperação de arquivos do servidor local, o responsável pela tecnologia e informação é o responsável pelo acesso à Internet da Instituição, que sem fio poderá ser acessada utilizando o ticket pelo facebook e que com fio será providenciado um usuário e senha de acesso.

3.2 RESTAURAÇÃO DE SERVIDORES EM CASO DE DESASTRE

3.2.1 Sistema Sig

O sistema SIG é da Empresa Stharparanet e caso venha dar problema como: sair do ar, estar instável e/ou outro motivo, o contato é feito pelo sistema de mensagem (CRM) e/ou entrar em contato pelo suporte técnico via WhatsApp ou telefone fixo.

3.2.2 Sistema AVA-Moodle

Se o sistema AVA-Moodle der problemas de sair do ar, e/ou instabilidade e/ou qualquer outro motivo a solicitação do suporte técnico é feito por abertura de chamado no site cliente da Hostgator, e/ou pelo chat online. A Administradora do Moodle tem acesso ao painel de controle do servidor ao qual poderá reiniciado caso seja este o problema.

3.2.3 Servidores de Firewall (6 HORAS)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Providenciar um novo servidor para que o serviço seja instalado;
3. Proceder com a instalação do Debian 8;
4. Instalar os serviços necessários para o funcionamento do firewall (iptables, squid3, bind9, etc);
5. Restaurar, através de backup, os scripts de firewall;
6. Configurar e testar todos serviços.

3.2.4 Servidor de Banco de Dados (12 HORAS)

1 Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2 Providenciar um novo servidor para que o serviço seja instalado;
3 Proceder com a instalação Windows Server 2012;
4 Instalar o banco de dados Oracle;
5 Configurar e testar o banco de dados.

3.2.5 Servidores de Aplicações

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Providenciar um novo servidor para que o serviço seja instalado;
3. Proceder com a instalação do Debian 8;
4. Instalar os serviços necessários para o funcionamento da aplicação;
5. Restaurar, através de backup, os arquivos da aplicação;
6. Configurar o acesso ao banco de dados;
7. Configurar e testar todos serviços.

3.2.6 Servidor de Autenticação/Controlador de Domínio/Arquivos (24 HORAS)

1. Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2. Providenciar um novo servidor para que o serviço seja instalado;

3. Proceder com a instalação do Windows Server 2012 R2;
4. Ativar os serviços necessários para o funcionamento do servidor;
5. Restaurar, através de backup, os dados do compartilhamento de arquivos;
6. Restaurar, através de backup, as configurações de diretivas de grupos;
7. Restaurar, através de backup, as configurações de impressoras;
8. Configurar e testar todos serviços.

3.2.7 ANTIVÍRUS (12 HORAS)

1 Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2 Providenciar um novo servidor para que o serviço seja instalado;
3 Proceder com a instalação do Antivírus, instalar todos os serviços de Antivírus necessários para o funcionamento;
4 Restaurar, através de backup, as configurações do antivírus;
5 Configurar e testar todos serviços.

3.2.8 Servidor de Controlador DE Wifi (6 HORAS)

1 Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2 Providenciar um novo servidor para que o serviço seja instalado;
3 Proceder com a instalação do PFSense, Mikrotik;
4 Instalar o serviço controlador de rádios Unifi;
5 Restaurar, através de backup, as configurações do controlador;
6 Configurar e testar o controlador;

3.2.9 Servidor do Software de Gestão de Rh (12 HORAS)

1 Comunicar todas Diretorias os serviços afetados e o prazo para restauração;
2 Providenciar um novo servidor para que o serviço seja instalado;
3 Proceder com a instalação do Windows Server 2012 R2;

4 Ativar os serviços necessários para o funcionamento do servidor;

5 Instalar o software da Alterdata;

6 Instalar o software SQL Server;

7 Conectar o software ao servidor de licenciamento;

8 Restaurar, através de backup. a base de dados;

9 Configurar e testar o software.

3.2.10 Serviço de Acesso à Internet (12 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;

3.2.11 Serviço de Webconferência Zoom (1 hora)

1 A equipe do Núcleo de Tecnologia Digital deverá entrar em contato com o suporte técnico através do painel de administrador e abrir o chamado;

2 Aguardar a resposta do suporte até a resolução do problema.

3.2.12 Serviço Unidades de Aprendizagem SAGAH (24 horas)

1 A equipe do Núcleo de Tecnologia Digital, coordenação de curso e professores deverão entrar em contato com o suporte técnico através do painel de administrador e abrir o chamado;

2 Aguardar a resposta do suporte até a resolução do problema.

Áreas Afetadas

- Diretoria;

- Administrativa;
- Educação Profissional.

NOTIFICAÇÕES

Internas (Telefone/E-mail):

- Diretoria;
- Administrativa;
- Educação Profissional.

Externas (Telefone/E-mail):

- Provedor de acesso a Internet (ALGAR);
- Paranet (SIG);
- Hostgator (Moodle);
- SAGAH
- Alterdata.
- Zoom

Backup Disponível

- Servidor com principais serviços pré-instalados (Windows Server 2012);
- Servidores com principais serviços (PFSense, Mikrotik);
- Nobreaks;
- Link ADSL de backup;
- Link dedicado de Backup;
- Cópias em HD Externo dos principais dados e serviços.