PLANO DE CONTINGÊNCIA DOS SERVIÇOS INFORMÁTICOS DA INTRANET UPRA

CENTRO DE TECNOLOGIAS DA INFORMAÇÃO

1. OBJETIVO

Falhas nos serviços de TI (Tecnologia da Informação) impactam diretamente todos os setores administrativos e académicos da *INTRANET UPRA*. Pretende-se com este plano definir procedimentos, ações e medidas rápidas para os processos críticos de TI. Este plano deve ser seguido para garantir os serviços essenciais em caso de emergências que possam ocorrer durante as atividades do *Campus*, visando aplicar as ações necessárias para correção e/ou eliminação do problema.

2. APLICAÇÃO

Este documento se aplica a todos os serviços e sistemas de Tecnologia da Informação que são providos na INTRANET *UPRA*.

3. DEFINIÇÕES

Áreas Sensíveis: Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas encontram-se os laboratórios de informática, salas administrativas, DataCenter 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 e equipamentos, e que ocorrendo se transformará em uma situação de emergência. Diz respeito a uma eventualidade; possibilidade de ocorrer.

Backup: Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento.

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 do Campus.

Incidente: É o evento inesperado ou situação que altera a ordem normal das coisas, capaz de causar danos leves ou graves aos sistemas e aos equipamentos de TI do Campus. 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 Campus.

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

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.

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 Campus.

TI: Tecnologia da Informação.

VM: Máquina Virtual, virtualizada no servidor (PROXMOX).

Zabbix : Ferramenta que pode ser utilizada para monitoramento da infraestrutura de rede e sistemas e aplicações.

4. RESPONSABILIDADES

4.1 EQUIPE DO SETOR DE TECNOLOGIA DA INFORMAÇÃO

Devem mitigar os impactos que por ventura venham a ocorrer decorrentes de emergências ou situações de emergência que afetem os sistemas, equipamentos ou infraestrutura de TI do *Campus*.

4.2 SERVIDORES DO *CAMPUS*

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

5. NÍVEIS DE INCIDENTES

Nível I – Hipótese acidental que pode ser controlada pela equipe de TI do *campus* 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 sistema e 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 todo o *campus*, impedindo assim o desenvolvimento do trabalho de todos os servidores do *campus*. Ex: Falha na conexão com a internet ou queda de energia elétrica no *campus* ou ainda problema técnico em algum servidor de rede que controla a conexão interna do *campus*.

6. PRINCIPAIS RISCOS

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

Riscos	Parâmetros
01- 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 com curto-circuito, incêndio e infiltrações.
02- Falha na climatização do DataCenter	Superaquecimento dos ativos devido a falha no sistema de refrigeração
03 - Indisponibilidade de rede	Rompimento de cabos decorrente de execuções de obras internas, desastres ou acidentes.
04 - Falha humana	Acidente ao manusear equipamentos
05 - Ataques internos	Ataque aos ativos[1] 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 externo	Ataque virtual que comprometa o desempenho, acesso aos os dados ou configuração dos serviços essenciais

7. POLÍTICA E PROCEDIMENTOS PARA BACKUP

7.1 BACKUP

Os servidores foram configurados para que diariamente, entre meia-noite e 06:00 horas, sejam realizadas as atividades de Backup de arquivos localizados no Data Center da INTRANET UPRA *p*ara um NAS interno com réplica para um servidor externo ao Data Center.

Além do backup local, o *campus* conta com um outro servidor para receber os arquivos de backup, como um plano de contingência, armazenando os backups por até 7 (sete) dias.

7.2 RESTAURAÇÃO E TESTE

A restauração de dados deve ser solicitada na área de administração de redes de TI e será realizada de acordo com os procedimentos específicos do mesmo. 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.

8. PRINCIPAIS INCIDENTES E AÇÕES DE CONTINGÊNCIA

8.1 PROBLEMAS COM COMPUTADORES NOS LABORATÓRIOS

As máquinas passam por manutenções periódicas a cada 6 meses 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;

Professores que estão utilizando ou que irão utilizar o referido laboratório, informam o problema ao Setor de TI do *campus* através do Sistema de tickets por meio da URL (https://canal.upra.ao:89);

O Sistema envia um e-mail para o setor de TI alertando para um novo chamado, o chamado é atribuído a um técnico que ficará responsável pelo atendimento;

Após o atendimento o solicitante é informado da conclusão/resolução do problema;

Caso o problema impeça o andamento da aula, o Setor de TI vai até o local fazer uma primeira verificação do problema e tenta solucioná-lo *in sitos*.

8.2 PROBLEMAS COM COMPUTADORES ADMINISTRATIVOS

O servidor que está utilizando o equipamento, informa o problema ao Setor de TI do Campus através do Sistema de Suporte (https://canal.upra.ao:89);

O Sistema envia um e-mail para o setor de TI alertando para um novo chamado, o chamado é atribuído a um técnico que ficará responsável pelo atendimento;

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 tenta solucioná-lo *in-loco*.

Caso não seja possível a resolução imediata do problema, O servidor é encaminhado a outa estação de trabalho que não esteja sendo utilizada, em uma eventual falta de estações livres a TI providenciara uma máquina backup em caráter emergencial para continuidade dos trabalhos.

8.3 PROBLEMAS DE CONEXÃO COM A REDE INTERNA

O Setor de TI identificará por meio de um sistema de monitoramento (Zabbix), que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual bloco do *campus* está ocorrendo o problema;

Identificar e corrigir a causa do problema;

Caso o problema de conexão seja em todo o campus, verifica se os servidores de endereços DHCP (protocolo de configuração dinâmica de host) e de autenticação estão funcionando adequadamente.

Informar a previsão do conserto ou solução aos demais servidores.

8.4 PROBLEMAS DE CONEXÃO COM A INTERNET

O Setor de TI identificará por meio de um sistema de monitoramento do Firewall que irá comutar automaticamente para o Link Backup e pelo (*Zabbix*), ambos emitirão alertas com a descrição do incidente, os dispositivos envolvidos e em qual bloco do Campus está ocorrendo o problema;

Verificar se o Firewall comutou automaticamente para o Link de Backup;

Identificar a causa do problema:

Detectado problema externo de internet, abrir um chamado de suporte com a operadora, visando o reestabelecimento do serviço.

Informar a previsão do conserto ou solução aos demais servidores.

8.5 PROBLEMAS COM ACESSO AOS SISTEMAS INTERNOS DO CAMPUS

O Setor de TI identificará por meio de um sistema de monitoramento (*Zabbix*), que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual bloco do Campus está ocorrendo o problema;

Verificar se a VM onde o mesmo está instalado está em execução;

Caso esteja em execução, verificar as conexões de rede da VM;

Caso não esteja em execução, iniciá-la no servidor PROMOX e testar seu acesso novamente;

Caso seja necessário acionar o sistema de backup para a recuperação da máquina ou arquivos;

Informar a previsão do conserto ou solução aos demais servidores.

8.6 PROBLEMAS COM EQUIPAMENTOS DE REDE

O Setor de TI identificará por meio de um sistema de monitoramento (*Zabbix*), que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual bloco do Campus está ocorrendo o problema;

Caso tenha garantia, acionar a garantia;

Caso possível, realizar a manutenção do mesmo;

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 Campus.

8.7 PROBLEMAS FÍSICOS COM CABEAMENTO DA REDE INTERNA

O Setor de TI identificará por meio de um sistema de monitoramento (*Zabbix*), que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual bloco do Campus está ocorrendo o problema;

Detectar a causa do problema por meio de testes no cabeamento;

Detectado problema de cabeamento de rede, refazer a conexões;

Verificar as demais ligações caso seja em um rack com switch e testá-lo;

Caso haja necessidade, agendar ou efetuar a troca do(s) cabo(s) que estão apresentando falhas;

Detectado problema de cabeamento de fibra, contingenciar com cabeamento de rede UTP.

8.8 PROBLEMAS COM FALTA DE ENERGIA ELÉTRICA

Caso seja identificada queda ou falta total de energia elétrica no *campus* informar a CAP Coordenadoria de Almoxarifado e patrimônio para as devidas providências;

Verificar se a queda foi interna ou externa;

Verificar se o controle remoto para o restabelecimento da energia foi acionado;

Se a falta de energia for de curta e larga duração, os sistemas e servidores de rede continuam em funcionamento, os mesmos estão ligados a baterias com fontes alimentadas por paneis solares;

Caso a falta de energia dure mais de 16 horas, os sistemas deverão ser desligados, bem como todos os equipamentos e serão religados novamente assim que a energia for reestabelecida.

8.9 ORDEM PARA O DESLIGAMENTO DOS SERVIDORES

Acessar o ambiente virtual e desligar primeiramente os servidores virtuais de serviços/web;

Desligar os servidores virtuais de Autenticação;

Desligar os servidores físicos;

Desligar os demais dispositivos, Central Wi-Fi, PABX e Firewall.

8.10 ORDEM PARA RELIGAR OS SERVIDORES

Ligar os equipamentos Rack 1, Central Wi-FI, PABX e Firewall;

Ligar os servidores físicos;

Verificar se as Máquinas Virtuais (VM´s) Ligaram automaticamente;

Caso não tenham sido ligadas verificar a causa e ligar manualmente;

Realizar testes de acesso à internet, autenticação e demais sistemas web do *campus*.

8.11 OUTROS PROBLEMAS

Para qualquer outro tipo de problema que envolva a TI, como impressoras, problemas de acesso que envolvam login e senha e etc.

Os passos a serem seguidos são:

Informar o problema ao Setor de TI do Campus através do Sistema de Suporte (https://canal.upra.ao:89);

O Sistema envia um e-mail para o setor de TI alertando para um novo chamado, o chamado é atribuído a um técnico que ficará responsável pelo atendimento;

Após o atendimento o solicitante é informado da conclusão/resolução do problema.

9. COMUNICAÇÃO

9.1 QUEM DEVE COMUNICAR

Qualquer funcionário que detecte qualquer tipo de problema ou anomalia, referente aos sistemas, equipamentos e/ou infraestrutura de TI.

9.2 A QUEM COMUNICAR

A comunicação deve ser feita para o Setor de TI do *campus*.

9.3 COMO COMUNICAR

Através do Sistema de Suporte (https://canal.upra.ao:89), Whatapp ou Telephone;

Na indisponibilidade do sistema indicado acima: enviar um e-mail para o endereço suporte@upra.ao;

Ou pelo Telefone do setor: 925753897

Eng. Rouget J. Fundora Ruano. MSc.	Prof. Doutor Carlos Pinto de Sousa. PhD
_____	_____
Director do CTI	Magnifico Reitor da UPRA