PLANO DE CONTINGÊNCIA, REDUNDÂNCIA E EXPANSÃO DE RECURSOS DE TI - DINF

1. OBJETIVO.

As atividades da Fundação Universidade Estadual de Mato Grosso do Sul possuem grande dependência dos recursos e serviços de Tecnologia da Informação que lhes prestam suporte no dia a dia, de maneira que falhas ocorridas durante o seu fornecimento impactam diretamente a Universidade, seja em seus setores administrativos ou em suas atividades relacionadas ao ensino.
É objetivo deste plano fornecer procedimentos previamente definidos como resposta aos problemas e interrupções nos serviços de TI que podem prejudicar ou paralisar as atividades desta instituição, bem como prover medidas de contingência aos eventos que ofereçam risco aos processos e sistemas de TI da UEMS.
Este plano também tem como intuito fornecer procedimentos para comunicação e resposta contribuindo com o controle de emergências que venham a atingir os ativos de TI desta Universidade.

2. APLICAÇÃO.

Este plano se aplica a todos os serviços e recursos de TI utilizados pela Sede e Unidades Universitárias da UEMS.

3. ESCLARECIMENTOS / DEFINIÇÕES.

Áreas Sensíveis: Áreas que podem sofrer os efeitos negativos quando atingidas pelas consequências da emergência ocorrida, podendo ser laboratórios de aula, setores administrativos, *Data Center* e outros locais que possuam equipamentos de informática.

Canal de Atendimento do *Help Desk*: É o canal de comunicação entre o usuário e a equipe de TI da UEMS, onde é possível a abertura de chamados de suporte de TI através do envio de e-mail ou por telefone.

Contingência: Situação de risco com possibilidade de vir a ocorrer, inerente às atividades, serviços e equipamentos. Após a sua ocorrência torna-se uma situação de emergência.

Data Center: é um ambiente para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores, entre outros.

Incidente: evento não programado de grande proporção capaz de causar danos graves aos sistemas e aos equipamentos de TI.

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.

Help Desk: Serviço de *Help Desk* instalado em um servidor web da sede, onde é possível receber através de e-mail ou chamado telefônico, organizar e manter o solicitante/servidor informado sobre o andamento do chamado de suporte.

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 da Sede ou Unidade Universitárias da UEMS.

TI: Tecnologia da Informação.

Virtual Machine (V M): Máquina Virtual, uma máquina virtualizada em um servidor físico.

4. RESPONSABILIDADES.

4.1 Equipe da Diretoria de Informática:
Devem reduzir os possíveis impactos ocorridos durante emergências ou situações de emergência que afetem os recursos de TI da UEMS.

4.2 Funcionários da UEMS:
Devem informar a DINF, ou os responsáveis de TI das Unidades Universitárias, caso detectem algum tipo de emergência ou hipótese acidental que ocorra em alguma das áreas sensíveis da UEMS.

4.3 Responsáveis pela TI das Unidades Universitárias:
Devem reduzir os possíveis impactos ocorridos durante emergências ou situações de emergência que afetem os recursos de TI da UEMS. Quando não for possível solucionar o incidente em nível local, serão responsáveis por comunicar a DINF através do canal de atendimento da UEMS.

5. NÍVEIS DE INCIDENTES.

Nível I – Hipótese acidental que pode ser controlada pela equipe de suporte da UEMS 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 afeta equipamento ou sistema e impossibilita o andamento do trabalho de um grupo de servidores ou setores, sem que interrompa o trabalho de todos os servidores da Sede ou Unidade Universitária da UEMS. Ex: o Bloco D da Unidade Universitária de Dourados está sem internet; Um sistema Recursos Humanos está sem funcionar, prejudicando mais

de um setor da UEMS; Problema que afete acesso ao sistema de rematrícula ou de inscrição de processos seletivos oferecidos pela UEMS.

Nível IV – Hipótese acidental que impossibilita o uso de sistemas ou equipamentos, interrompendo assim o desenvolvimento do trabalho de todos os servidores da Sede ou de Unidade Universitária da UEMS. Ex: Interrupção no fornecimento de energia elétrica, ou falha em servidor que faz a autenticação dos serviços internos da UEMS.

6. PRINCIPAIS RISCOS

Este Plano de Contingência foi criado para fazer frente a situações que interrompam os serviços essenciais da UEMS.

Abaixo são definidos estes riscos e situações.

Evento Possíveis

01- Interrupção de energia elétrica:
Pode ser causada por fatores externos ou internos à rede elétrica da UEMS e que tenham duração superior a 25 minutos (tempo estimado de duração das baterias do *no-break* do *Data Center*).

02- Falha na climatização do Data Center:
Falha no sistema de climatização do *Data Center*, ocasionando superaquecimento do *hardware* dos servidores da UEMS.

03 - Indisponibilidade de rede/circuitos:
Interrupção do funcionamento da rede ocasionada por rompimento ou deterioração de seu cabeamento ou falha de equipamentos.

04 – Falha de Hardware:
Falha de equipamento de *hardware*, causada por falha humana, acidente, desgaste natural ou força maior que implique na paralisação de serviço ou recurso de TI.

05 – Falha de humana:
Erro causado por ação humana que implique em diminuição ou interrupção de serviço ou recurso de TI.

06 - Ataques internos(usuários insatisfeitos):
Ataques/Sabotagem ao *Data Center* e equipamentos de laboratórios, salas de aula e de uso administrativo/ensino

07 – Indisponibilidade de peças de reposição:
Falha em equipamento que implique a necessidade de aquisição de componentes, ou novo equipamento, através de procedimento licitatório.

08 - Ataque cibernético:
Ataque externo que atrapalhe/interrompa o desempenho, funcionamento ou integridade dos ativos de TI que suportam os serviços essenciais da instituição.

7. PRINCIPAIS PROBLEMAS, INCIDENTES E DEVIDAS AÇÕES DE CONTINGÊNCIA.

7.1 Problemas com computadores nos laboratórios de informática (Unidade Universitária):

- O responsável pela atividade desenvolvida, informam o problema a equipe de suporte da Unidade Universitária deste laboratório;
- o responsável pela TI adota as medidas necessárias para a solução do problema em conformidade com a sua organização de trabalho;
- após o atendimento o solicitante é informado da conclusão/resolução do problema informado;

7.2 Problemas com computadores administrativos (Unidade Universitária):

- o servidor que detectou o problema, aciona o responsável de TI da Unidade Universitária, enviando um e-mail ou ligando para o ramal de atendimento do responsável de TI local.
- o atendimento é agendado;
- em caso de interrupção do trabalho do servidor, o responsável de TI vai até o local e tenta solucioná-lo in-loco.

7.3 Problemas com computadores administrativos (sede):

- o servidor que detectou o problema informa o problema a DINF através do canal de atendimento do Help Desk, enviando um e-mail para o endereço informatica@uems.br. Caso não seja possível acessar o e-mail, o chamado pode ser aberto através do ramal telefônico do Help Desk – 67 3902-1837;
- o chamado é distribuído e é agendado pela DINF;
- ao final do atendimento o solicitante é informado sobre a conclusão do chamado;
- em caso de interrupção do trabalho do servidor, o responsável de TI vai até o local e tenta solucioná-lo in-loco.

7.4 Problemas de conexão com a rede interna (Unidade Universitária):

- o responsável local pela TI da Unidade Universitária identificará em qual problema da unidade está ocorrendo o problema;
- analisar a conexão do servidor central até o bloco afetado;
- identificar a causa do problema;
- caso o problema de conexão seja em toda a unidade, o responsável deverá comunicar imediatamente ao setor de infraestrutura de redes da UEMS, através dos contatos do Help Desk.

7.5 Problemas de conexão com a rede interna (sede):

- o Setor de Infraestrutura de Redes identificará em qual bloco está ocorrendo o problema;
- analisar a conexão do servidor central até o bloco afetado;
- identificar a causa do problema;
- em seguida, adotará as medidas necessárias para a resolução do problema.

7.6 Problemas de conexão com a internet (Unidade Universitária):

- o responsável local pela TI Unidade Universitária deverá identificar em qual bloco da Unidade Universitária está ocorrendo o problema;
- analisar a conexão do servidor central até o bloco afetado
- identificar a causa do problema;
- detectado problema externo de internet, avisar imediatamente o setor de infraestrutura de redes da UEMS através do serviço de Help Desk.
- atenção: **somente a DINF** deverá abrir chamado de suporte com a operadora, visando o reestabelecimento do serviço.

7.7 Problemas de conexão com a internet (sede):

- o Setor de Infraestrutura de Redes deverá identificar em qual bloco está ocorrendo o problema;
- analisar a conexão do servidor central até o bloco afetado e identificar a causa do problema;
- detectado problema externo de internet, abrir chamado de suporte com a operadora, visando o reestabelecimento do serviço
- atenção: **somente a DINF** deverá abrir chamado de suporte com a operadora, visando o reestabelecimento do serviço.

7.8 Problemas com acesso aos sistemas internos:

- atenção: somente o **Setor de Infraestrutura de ~~Redes e~~ Servidores** deverá realizar este procedimento.
- identificar qual o sistema está apresentando problema de acesso;
- verificar se a VM onde o mesmo está instalado está em execução;
- caso esteja em execução, verificar a conexão de rede da VM;
- caso não esteja em execução, corrigir o problema e iniciá-la no servidor de virtualização e testar seu acesso novamente;
- por fim, identificar e resolver o problema informando a solução adotada.

7.9 Problemas com equipamentos de rede (Unidade Universitária)

- o responsável local pela TI Unidade Universitária deverá identificar qual equipamento está apresentando problema;
- caso possível, realizar a manutenção do mesmo;
- caso não haja possibilidade de realizar a manutenção/reparo, realizar a troca do equipamento, avisando ao Gerente da unidade para que sejam tomadas as devidas

providências, de forma que haja o menor transtorno possível no desempenho das atividades da Unidade Universitária.

7.10 Problemas com equipamentos de rede (sede):

- o setor de infraestrutura de redes deverá identificar qual equipamento está apresentando problema;
- caso possível, realizar a manutenção do mesmo;
- caso não haja possibilidade de realizar a manutenção/reparo, realizar a troca do equipamento de forma que haja o menor transtorno possível no desempenho das atividades da Sede.

7.11 Problemas físicos com cabeamento da rede interna (Unidade Universitária):

- o responsável local pela TI da Unidade Universitária deverá identificar qual o problema e onde este ocorre;
- detectado problema no cabeamento de rede, refazer a conexões e ponteiras;
- verificar as ligações (switches) do cabeamento que está com defeito e testá-lo, bem como os conectores RJ45;
- caso haja necessidade, efetuar a troca do cabo ou cabos que estão apresentando falhas;
- detectado problema de cabeamento de fibra, contingenciar com cabeamento de rede UTP.
- caso haja necessidade, avisar o Gerente para as devidas providências.

7.12 Problemas físicos com cabeamento da rede interna (sede):

- o setor de infraestrutura de redes deverá identificar qual o problema e onde está ocorrendo;
- detectado problema de cabeamento de rede, refazer a conexões e ponteiras;
- verificar as ligações (switches) do cabeamento que está com defeito e testá-lo, bem como os conectores rj45;
- caso haja necessidade, efetuar a troca do cabo ou cabos que estão apresentando falhas;
- detectado problema de cabeamento de fibra, contingenciar com cabeamento de rede UTP.

7.13 Problemas com falta de energia elétrica (sede):

Caso seja identificada queda ou falta total de energia elétrica na sede, informar a Diretoria de Infraestrutura (DINFra) para as devidas providências;

- se a falta de energia for de curta duração, máximo de 25 minutos, os sistemas e servidores de rede continuam em funcionamento, pois estão ligados em um *no-break* no *Data Center*;
- caso a falta de energia perdure por período superior a 25 minutos, os sistemas são desligados, bem como os demais equipamentos, e serão religados assim que a energia for restabelecida.

Caso seja necessário o desligamento manual do *Data Center* a ordem de desligamento será:

- desligar o *rack* de servidores;
- desligar o *rack* de telecomunicações;
- desligar os *no-breaks*;
- desligar ar condicionado.

Em caso de religamento manual, a ordem para religar o *Data Center* será:

- religar o ar condicionado;
- religar os *no-breaks*;
- religar o *rack* de telecomunicações;
- religar o *rack* de servidores.

7.14 Em caso de incidente que cause a indisponibilidade nos servidores do Data Center da Sede, ficarão indisponíveis para toda a UEMS os serviços que contam com hospedagem ou autenticação interna. Este incidente será classificado como de nível IV, afetando os seguintes serviços:

- autenticação na Comunidade Café;
- *Webmail*;
- páginas da UEMS;
- Moodle da UEMS;
- serviço de armazenamento de arquivos;
- SAU;
- SIGPOS;
- Lotação;
- Plano de Atividades Docente;
- Biblioteca;
- Recursos Humanos;
- IntraUEMS;
- SiSU UEMS;
- Controle de Estoque do Laboratório de Química;
- Periódicos UEMS;
- Anais UEMS;
- Sistema de Gerenciamento de Sistemas;
- acesso à internet na Sede e Unidade Universitária de Dourados.

Os serviços que dependem de hospedagem externa, tais como as redes sociais oficiais da UEMS (Facebook, Instagram, Twitter e canais de vídeo do Youtube) continuarão funcionando normalmente desde que haja conexão com a internet e conforme disponibilidade dos próprios serviços.

7.15 - Outros Problemas:

Para qualquer outro tipo de problema que envolva a TI, como configurações de e-mail, impressoras, outros tipos de *harware* e etc.
Os passos a serem seguidos são os seguintes:

- informar o problema ao setor de TI através do canal de atendimento Help Desk, enviando um *e-mail* para o endereço informatica@uems.br;
- o chamado de suporte chega até o setor de TI e o atendimento é agendado;
- após o atendimento o solicitante é informado da conclusão/resolução do problema reclamado.

8. COMUNICAÇÃO

8.1 Quem deve comunicar:
Todo servidor que detecte qualquer tipo de problema que diga respeito a sistemas, equipamentos e/ou infraestrutura de TI.

8.2 A quem comunicar:
A comunicação deve ser feita para os Responsáveis de TI das Unidades ou para a DINF, seguindo os procedimentos elencados neste plano.

8.3 Como comunicar:
Nas Unidades Universitárias a comunicação deve ser feita primeiro ao responsável de TI local, na sua ausência, as comunicações devem ser dirigidas ao responsável indicado pelo Gerente da Unidade.
Os problemas detectados devem ser informados através do canal de atendimento do Help Desk, enviando um *e-mail* para o endereço informatica@uems.br ou, na impossibilidade de acesso ao *e-mail*, ligando para o telefone 67 3902-1837.

8.4 Manutenções programadas em Ativos de TI:
As manutenções programadas pela DINF, outros setores da UEMS ou por agentes externos e que causem interrupção nos serviços de informática devem ser comunicadas com antecedência aos usuários que serão afetados pela interrupção do serviço, através dos canais e serviços oficiais da UEMS.

8.5 Comunicação de incidentes, hipóteses acidentais e situações de emergência:

8.5.1 Indisponibilidade do Data Center de Dourados:
Nos casos de incidentes de Nível IV em que os servidores alocados *Data Center* da Sede da UEMS estiverem indisponíveis (ver 7.8.1), a informação sobre a indisponibilidade e suas causas (quando identificadas) será repassada à Reitoria, e caberá a esta informar os Gerentes das Unidades Universitárias por meio de um grupo de WhatsApp.

8.5.2 Indisponibilidade de sistemas de TI destinadas ao corpo discente ou ao público externo:
Em situações em que o incidente Nível III afetar de maneira prolongada o acesso a sistemas destinados ao corpo discente ou comunidade externa, um aviso na própria página de acesso ao serviço indicará a sua indisponibilidade (**quando tecnicamente possível)**, podendo ser replicado nos canais oficiais de comunicação da UEMS.

8.5.3 Indisponibilidade nos demais sistemas de TI:

Nos incidentes de Nível III que afetarem de maneira prolongada os demais sistemas da UEMS, duas medidas serão adotadas concomitantemente:
a.) um aviso na página de acesso ao serviço indicará a sua indisponibilidade (**quando tecnicamente possível)**.
b.) A informação sobre a indisponibilidade e suas causas (quando identificadas) será repassada à Reitoria, e caberá a esta informar os Gerentes das Unidades Universitárias por meio de um grupo de WhatsApp.

9. REDUNDÂNCIA

9.1 O Centro de processamento de dados:

Está em fase de implantação a redundância de alguns serviços computacionais mais críticos entre os datacenters da Unidade Universitária de Dourados e a UEMS Centro, faltando a aquisição de alguns equipamentos para darmos continuidade com a adequada implantação desse serviço. Será necessário aquisição de um servidor, nobreak e roteadores, a fim de garantir alta disponibilidade, processamento, armazenamento e backup, propiciando a capacidade de expansão para futuras implementações de serviços de TIC.

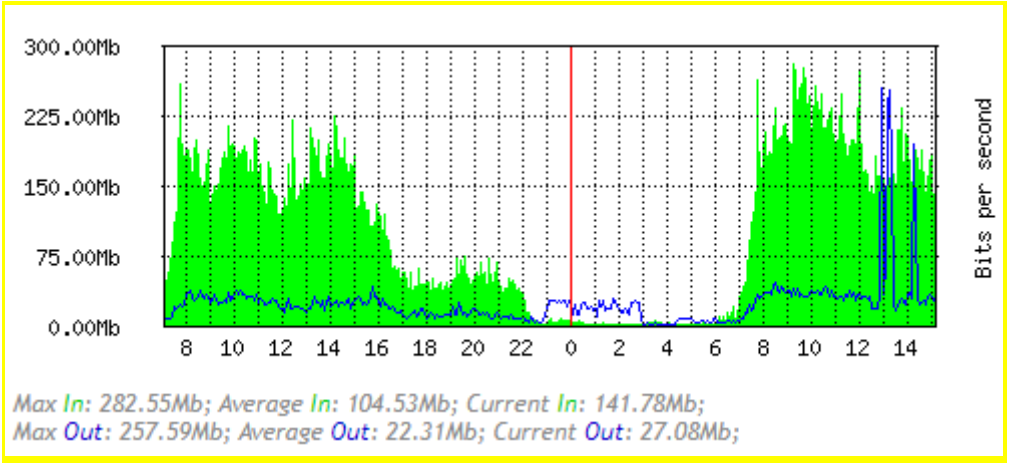
9.2 Plano de redundância da disponibilidade de Internet

Quanto à conectividade e redundância para a internet, a UEMS dispõe de dois links com à internet, sendo uma da Rede Nacional de Ensino e Pesquisa (RNP), com capacidade de 1000 Mbps e outra do Provedor Oi, com capacidade de 600Mbps, garantindo alta velocidade com largura de banda unificada em 1600 Mbps. Ressalta-se, uma vez que a instituição possui duas saídas para a internet, ela têm a garantia de alta disponibilidade no acesso à internet e certificando que em momentos de falhas em um dos provedores, o outro atenderá a instituição automaticamente, visto que os equipamentos de redes monitoram o fornecimento de ambos os serviços, ativando ou desativando a fonte de acesso à internet quando indisponível.

9.3 Estimativa do consumo institucional de internet

Apesar da UEMS possuir 600 Mbps de velocidade no acesso à internet, o consumo institucional para atender Ensino, Pesquisa e Extensão não vem ultrapassando ao longo dos meses 50% do link disponível, como mostrado na Figura 1. Isso garante maior eficiência para a comunidade acadêmica no acesso à internet, uma vez que existe o dobro de disponibilidade para expansão no consumo de internet pela universidade sem a necessidade de novos investimentos.

Figura 1 - Monitoramento do Link de Internet



9.4 Plano de melhoria da estabilidade elétrica

Em relação a estabilidade elétrica, a UEMS possui em seu *Data Center* 7 *nobreaks*, sendo um de 3Kva que acomoda a conexão dos ativos de rede (roteadores, switch core e distribuição) e outros 6 nobreaks que somam 35Kva que alimentam os servidores de rede, todos trabalhando simultaneamente, garantindo a alta disponibilidade energética mesmo em falha de um dos nobreaks.

9.5 Rede lógica

Todos os prédios da estão conectados ao Data Center através de fibra óptica na velocidade de 1Gbps, cada prédio distribui a conectividade recebida pela fibra por meio de cabo gigabit ethernet aos respectivos computadores, como também os mais de 92 *Access Points* distribuídos pela UEMS, provisionam total cobertura Wi-Fi em todos os prédios didáticos e laboratórios, contando com uma cobertura inteligente de deslocamento roaming e altíssima velocidade aos dispositivos móveis.

10. PLANO DE EXPANSÃO

10.1 Planejamento:

Cada Unidade Universitária possui infraestrutura necessária de laboratórios e de recursos tecnológicos para o desenvolvimento de atividades de ensino, ainda assim a expansão, implementação e implantação é programada conforme o planejamento exposto no PDI. Existe ainda a situação de expansão em decorrência de ajustes em diretrizes curriculares, portarias, resoluções e leis emanadas dos órgãos federais, por inovações tecnológicas ou necessidade institucional devido ao crescimento orgânico.

10.1 Estimativa de expansão por quantidade de alunos: CARLOS VIANA

Itens	Cenário atual	Possíveis cenários		
Quantidade de alunos	7850	8000	9000	10000
Quantidade de computadores para uso dos alunos	300	300	340	380

Links de internet	5 Mbps/por aluno	5 Mbps/por aluno	5 Mbps/por aluno	5 Mbps/por aluno
Quantidade de Pontos de acesso WIFI	92	120	140	160
Quantidade de Geradores	0	1	1	1

Os nobreaks atuais são de médio porte, não sendo o cenário ideal para acomodar os equipamentos de rede. O gerador é um item essencial para disponibilidade energética em caso de falta de energia da concessionária, sendo complementado por um banco de baterias conectadas a um nobreak de alta capacidade, proporcionando um cenário mais confortável para o plano elétrico do Data Center da UEMS.

Os Pontos de acesso Wi-Fi atuais estão desatualizados, o padrão Wi-Fi 4 já há muito tempo superado, não consegue atender a alta demanda das aplicações cotidianas da instituição. Faz-se necessário uma atualização de padrão para o Wi-Fi 6, que além de atingir altas velocidades, possui tecnologia de melhor aproveitamento de banda de tempo para os dispositivos móveis. Além disso, os APs que possuem tal tecnologia possuem boa capacidade de densidade de usuários, uma vez que, com mais usuários conectados ao mesmo tempo, com mais velocidade é possível diminuir a quantidade de APs instalados, reduzindo assim o custo da infraestrutura de rede.

Há a necessidade de aquisição de mais um servidor de rack de alta capacidade de processamento e armazenamento para melhorar a disponibilidade dos serviços computacionais oferecidos por esta diretoria, além da aquisição de roteadores para uma melhor conexão entre os datacenters da Unidade Universitária de Dourados e a unidade da UEMS Centro, e também a aquisição de mais um nobreak para possibilitar a redundância elétrica no datacenter da UEMS Centro.

11. REVISÃO E ATUALIZAÇÃO DO PLANO DE CONTINGÊNCIA

11.1 A quem cabe a revisão e atualização
Compete à DINF revisar e atualizar o Plano de Contingência dos Recursos de TI da UEMS.

11.2 Da revisão
A revisão deste plano será feita anualmente, a contar da data de sua primeira publicação.

11.3 Da atualização
A sua atualização será feita sempre que a evolução do parque de informática determinar a necessidade de manter este plano operacional e fiel a realidade das contingências que venham a ser enfrentadas pela UEMS. Por exemplo: a implementação de redundância de alguns serviços hospedados nos *Data Centers* da Sede, ou até mesmo alterações nas configurações de rede, criará a necessidade de atualização deste plano e das práticas aqui contidas.