	PLANO DE CONTINGÊNCIA PARA TECNOLOGIA DA INFORMAÇÃO (TI) E PROCEDIMETOS PARA BACKUP	
CIFRÃO Fundação de Previdência da Casa da Moeda do Brasil	**APROVAÇÃO:** **ATA 09/2020 DIREX**	**INÍCIO DE VIGÊNCIA:** **17/04/2020**
	DATA DE APROVAÇÃO: **17/04/2020**	**CODIFICAÇÃO:** **IN013.00**

1. FINALIDADE

1.1. Este instrumento normativo tem por finalidade preparar a CIFRÃO para possíveis falhas nos serviços de Tecnologia da Informação - TI que impactam diretamente em todos os setores administrativos da Fundação, bem como recomendar procedimentos para a realização de backup's diários, semanais e mensais, de forma a garantir que os serviços essenciais da Entidade, mesmo em casos de emergência, possam ocorrer normalmente durante as atividades de reparo e das ações necessárias para correção e/ou eliminação do problema.

2. APLICAÇÃO

2.1. Este normativo se aplica a todos os serviços e sistemas de Tecnologia da Informação - TI que são providos na CIFRÃO.

3. DEFINIÇÕES

3.1. Para fins de aplicabilidade deste normativo são estabelecidas as seguintes definições:

a) **Áreas Sensíveis:** Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas encontram-se as salas administrativas, o Data Center e demais locais que possuam equipamentos de informática;

b) **Área Vulnerável**: Área atingida pela extensão dos efeitos provocados por um evento de falha;

c) **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;

d) **Backup**: Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento;

e) **Data Center ou Centro de Processamento de Dados:** Ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores, e outros da CIFRÃO;

f) **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 da CIFRÃO. 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 da CIFRÃO;

g) **Intervenção:** É a atividade de atuar durante a emergência, seguindo planos de ações para corrigir ou minimizar os possíveis danos aos equipamentos e sistemas de TI da CIFRÃO;

h) **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;

i) **GLPI Gestão Livre de Parque de Informática):** Sistema de abertura de chamados técnicos;

j) **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 dos empregados da CIFRÃO;

k) **TI**: Tecnologia da Informação; e

l) **VM**: Máquina Virtual, virtualizada no servidor VirtualBox.

4. RESPONSABILIDADES

4.1. Equipe do setor de Tecnologia da Informação

4.1.1. Deverão 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 da CIFRÃO.

4.2. Funcionários da CIFRÃO

4.2.1. Serão responsáveis por informar ao Setor de TI da CIFRÃO, caso detectem algum tipo de emergência ou hipótese acidental que ocorram em alguma das áreas sensíveis da CIFRÃO.

5. NÍVEIS DE INCIDENTES

5.1. Os incidentes que por ocasião possam ocorrer no âmbito da CIFRÃO são classificados em 03 (três) níveis de impacto, conforme especificados nas alíneas a seguir:

a) **Nível I:** Hipótese acidental que pode ser controlada pela equipe de TI da CIFRÃO e que não afeta o andamento do trabalho do empregado da CIFRÃO. Exemplo: Problemas com equipamentos periféricos de computadores.

b) **Nível II:** Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo empregado da CIFRÃO. Exemplo: Problema com o

funcionamento do computador (não liga, travado, etc.) ou ainda sistemas off-line impedindo o uso do mesmo.

c) **Nível III:** Hipótese acidental que impede o uso de sistemas ou equipamentos de toda a CIFRÃO, impedindo assim o desenvolvimento do trabalho de todos os empregados da CIFRÃO. Exemplo: Falha na conexão com a internet ou queda de energia elétrica na empresa ou ainda problema técnico em algum servidor de rede que controla a conexão interna da CIFRÃO.

6. PRINCIPAIS RISCOS

6.1. O Plano de Contingência da CIFRÃO foi desenvolvido para ser acionado quando da ocorrência de cenários que apresentam risco à continuidade dos serviços essenciais. O quadro a seguir define estes 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 Data Center	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 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. PRINCIPAIS INCIDENTES E AÇÕES DE CONTINGÊNCIA

7.1. Problemas com Computadores no Datacenter

7.1.1. As máquinas deverão passar por manutenções periódicas a cada 03 (três) meses nos intervalos dos trimestres, onde são feitas imagens com atualizações do sistema e softwares solicitados pelas áreas. Durante este período, cabos e conexões também deverão testados e reparados.

7.1.2. O empregado da CIFRÃO que estiver utilizando o equipamento e verificar alguma deficiência nos computadores do Datacenter, deverá informar o problema ao Setor de TI da CIFRÃO, através do Sistema de Suporte GLPI (http://www.mdmac.com.br/suporte), e consequentemente, deverão ser realizados os seguintes procedimentos:

a) O Sistema deverá enviar um e-mail para o Setor de TI da CIFRÃO alertando para um novo chamado, no qual será atribuído a um técnico que ficará responsável pelo atendimento;

b) Após o atendimento o solicitante deverá ser informado da conclusão/resolução do problema; e

c) Caso o problema impeça o andamento das atividades, o setor de TI da CIFRÃO deverá ir até o local fazer uma primeira verificação do problema e tentar solucioná-lo *in loco*.

7.2. Problemas com Computadores Administrativos

7.2.1. O empregado da CIFRÃO que estiver utilizando o equipamento e verificar alguma deficiência nos computadores administrativos, deverá informar o problema ao responsável pelo TI da CIFRÃO, através do Sistema de Suporte GLPI (http://www.mdmac.com.br/suporte), e consequentemente, deverão ser realizados os seguintes procedimentos:

a) O Sistema deverá enviar um e-mail para o responsável pelo TI da CIFRÃO alertando para um novo chamado, o chamado é atribuído a um técnico que ficará responsável pelo atendimento;

b) Após o atendimento o solicitante deverá ser informado da conclusão/resolução do problema informado;

c) Caso o problema impeça o andamento do trabalho do usuário, o Setor de TI deverá ir até o local fazer uma primeira verificação do problema e tenta solucioná-lo *in loco*; e

d) Caso não seja possível a resolução imediata do problema, o empregado da CIFRÃO deverá encaminhado a outra 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.

7.3. Problemas de Conexão com a Rede Interna

7.3.1. O Setor de TI deverá identificar eventuais problemas de conexão com a rede interna por meio de um sistema de monitoramento, e deverá emitir um alerta com a descrição do incidente, os dispositivos

envolvidos e em qual bloco da CIFRÃO está ocorrendo o problema para identificar e corrigir a causa do problema.

7.3.2. Caso o problema de conexão seja em todo a CIFRÃO, será verificado se os servidores de endereços DHCP (protocolo de configuração dinâmica de host) e de autenticação estão funcionando adequadamente.

7.3.3. O Setor de TI deverá informar a previsão do conserto ou solução aos demais empregados da CIFRÃO.

7.4. Instabilidade e Problemas de Conexão com a Internet

7.4.1. O Setor de TI da CIFRÃO deverá identificar eventuais instabilidade e problemas de conexão com a internet por meio de um sistema de monitoramento do Firewall, edeverá emitir um alerta para o e-mail suporte@cifrao.com.br com a descrição do incidente, os dispositivos envolvidos da CIFRÃO que está ocorrendo o problema.

7.4.2. Detectado problema externo de internet, deverá ser aberto um chamado de suporte com a operadora, visando o reestabelecimento do serviço.

7.4.3. O Setor de TI deverá informar a previsão do conserto ou solução aos demais empregados da CIFRÃO.

7.5. Problemas com Acesso aos Sistemas Internos da CIFRÃO

7.5.1. O Setor de TI da CIFRÃO deverá identificar eventuais problemas de acesso aos sistemas internos da CIFRÃO por meio de um sistema de monitoramento, e deverá ser emitido um alerta com a descrição do incidente, identificando quais são os dispositivos envolvidos da CIFRÃO estão ocorrendo o problema. Após essa etapa, deverão ser realizados os seguintes procedimentos:

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

b) Caso esteja em execução, deverá ser verificado as conexões de rede da VM;

c) Caso não esteja em execução, deverá iniciá-la no servidor *VirtualBox* e testar seu acesso novamente;

d) Caso seja necessário, deverá ser acionado o sistema de backup para a recuperação da máquina ou arquivos; e

e) Deverá informar a previsão do conserto ou solução aos demais empregados da CIFRÃO.

7.6. Problemas com Equipamentos de Rede

7.6.1. O Setor de TI deverá identificar por meio de um sistema de monitoramento, e deverá ser emitido um alerta com a descrição do incidente, identificando quais são os dispositivos envolvidos da CIFRÃO que está ocorrendo o problema. Após essa etapa, deverão ser realizados os seguintes procedimentos;

a) Caso o equipamento esteja na garantia, deverá ser acionado a assistência técnica do fabricante; e

b) Caso o equipamento não tenha como consertar e não esteja em garantia, deverá ser realizada a troca do equipamento de forma que haja o menor transtorno possível no desempenho das atividades dos demais empregados da CIFRÃO.

7.7. Problemas Físicos com Cabeamento da Rede Interna

7.7.1. O Setor de TI deverá identificar problemas físicos com cabeamento da rede interna por meio de um sistema de monitoramento, que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos da CIFRÃO que está ocorrendo o problema. Após essa etapa, deverão ser realizados os seguintes procedimentos;

a) Deverá ser detectado a causa do problema por meio de testes no cabeamento;

b) Caso detectado problema de cabeamento de rede, refazer as conexões;

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

d) Caso haja necessidade, agendar ou efetuar a troca dos cabos que estão apresentando falhas; e

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

7.8. Problemas com Falta de Energia Elétrica

7.8.1. Caso seja identificada queda ou falta total de energia elétrica na CIFRÃO, deverá ser informado ao setor responsável pela mesma ou a empresa fornecedora de energia elétrica para que tome as devidas providências. Após essa etapa, deverão ser realizados os seguintes procedimentos:

a) Verificar se a queda foi interna ou externa;

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

c) Se a falta de energia for de curta duração, máximo 25 minutos, os sistemas e servidores de rede continuam em funcionamento, os mesmos estão ligados a nobreaks com fonte redundante; e

d) Caso a falta de energia dure mais de 25 minutos, os sistemas deverão ser desligados, bem como todos os equipamentos e serão religados novamente assim que a energia for reestabelecida.

7.9. Ordem para o Desligamento dos Servidores

1. Deverá ser acessado o ambiente virtual e desligar primeiramente os servidores virtuais de serviços/web;
2. Desligar os servidores virtuais de Autenticação;
3. Desligar os servidores físicos Rack 2; e
4. Desligar os demais dispositivos Rack 1, Central Wi-Fi, PABX e Firewall.

7.10. Ordem para Religar os Servidores

1. Ligar os equipamentos Rack 1, Central Wi-Fi, PABX e Firewall.
2. Ligar os servidores físicos.
3. Verificar se as Maquinas Virtuais (VM) ligaram automaticamente.
4. Caso não tenham sido ligadas verificar a causa e ligar manualmente.
5. Realizar testes de acesso à internet, autenticação e demais sistemas web da CIFRÃO.

7.11. Outros Problemas

7.11.1. Para qualquer outro tipo de problema que envolva a TI, como problemas de acesso que envolvam login e senha e etc, os passos a serem seguidos são:

1. Informar o problema ao Setor de TI da CIFRÃO através do Sistema de Suporte GLPI (http://www.mdmac.com.br/suporte);

2. 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;

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

8. PROCEDIMENTOS PARA BACKUP

8.1 Backup

8.1.1. Os servidores deverão ser configurados para que diariamente, entre 19:00 h e 5:00 h sejam realizadas as atividades de Backup de arquivos localizados no Data Center da CIFRÃO para um Hard Drive-1 interno e um Hard Drive-2 externo.

8.1.2. Além do backup local, a CIFRÃO deverá contar com um outro servidor externo para receber os arquivos de backup, como plano de contingência, armazenando os backups semanais por até 04 (quatro) semanas.

8.2. Modo e Dia de Execução

8.2.1. Os procedimentos de backup's dos dados da CIFRÃO deverão compreender os seguintes cronogramas:

a) **Backup diário:** Os backups diários deverão ser executados de segunda à sexta-feira, em modo incremental;

b) **Backup semanal:** Os backups semanais deverão ser executados aos finais de semana, iniciando aos sábados, em modo completo; e

c) **Backup mensal:** Os backups mensais serão executados no primeiro sábado do mês, em modo completo.

8.2.2. Não deverá haver backup semanal quando o sábado coincidir com a mesma data do backup mensal.

8.2.3. Os backups deverão ser processados, preferencialmente, durante a noite ou dias não úteis, em horário que gere menor impacto nas demais rotinas e no Centro de Processamento de Dados da CIFRÃO.

8.2.4. Para execução de ações de contingências, o responsável pelo TI da CIFRÃO deverá realizar manutenções periódicas a cada 03 (três) meses nos equipamentos, e atualizações do sistema e software, bem como testes e reparos nos cabos e conexões.

8.3. Restauração e Teste

8.3.1. A restauração de dados deverá ser solicitada ao responsável pelo TI e será realizada de acordo com os procedimentos específicos do mesmo. A verificação e o teste de restauração, serão realizados sempre após o termino do backup através do mesmo software gerador dos backups, configurado para verificar automaticamente as condições do backup.

8.4. Em Caso de Falha

8.4.1. Caso o sistema de backup falhe na primeira camada (Hard Drive-1), ele automaticamente deverá tentará executar na segunda camada (Hard Drive-2), caso a falha persista, o sistema de backup automaticamente deverá reportar-se ao responsável pelo TI da CIFRÃO descrevendo todo ocorrido e logo passará para a terceira camada (Servidor Cloud) de backup.

8.4.2. Se novamente houver falha de algum procedimento de backup ou impossibilidade da sua execução, o administrador de backup deverá adotar as providências necessárias para promover a salvaguarda das informações através de outro mecanismo, como por exemplo: nova execução do backup em horário de comercial ou cópia dos dados para outro servidor.

9. COMUNICAÇÃO

9.1. Quem deve Comunicar

9.1.2. Qualquer empregado da CIFRÃO que detecte algum tipo de problema ou anomalia, referente aos sistemas, equipamentos e/ou infraestrutura de TI.

9.2 A Quem Comunicar

9.2.1. A comunicação deve ser feita para ao responsável pelo TI da CIFRÃO através do Sistema de Suporte GLPI (http://www.mdmac.com.br/suporte) ou pelo e-mail suporte@cifrao.com.br.

9.3 Como Comunicar

9.3.1. Preferencialmente pelo e-mail suporte@cifrao.com.br ou pelo telefone indicado pelo responsável pelo TI da CIFRÃO.