Plano de Contingência Infraestrutura Tecnológica

"Tipo de plano preventivo, preditivo e reativo. Apresenta uma estrutura estratégica e operativa que ajudará a controlar uma situação de emergência e a minimizar as suas consequências negativas. O plano de contingência propõe uma série de procedimentos alternativos ao funcionamento normal de uma organização, sempre que alguma de suas funções usuais se vê prejudicada por uma contingência interna ou externa. Essa classe de plano procura, portanto, garantir a continuidade do funcionamento da organização face a quaisquer eventualidades, sejam estas, materiais ou pessoais. Um plano de contingência inclui quatro etapas básicas: a avaliação, a planificação, as provas de viabilidade e a execução" **(Instrumento de Avaliação Inep/MEC)**

A Direção Geral da **Faculdade de Botucatu - FDB**, no uso de suas atribuições legais, a fim de instituir o Plano de Contingência da Infraestrutura Tecnológica, delibera pelo presente regulamento, para efeito de implantação gradativa do referido plano no âmbito institucional.

I- DOS OBJETIVOS

Art. 1º. O principal objetivo do Plano de Contingência da Infraestrutura Tecnológica da **FDB** 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.

II- DA NATUREZA

Art. 2º. O Plano de Contingência da **FDB** identifica duas variáveis para o funcionamento adequado da instituição: Infraestrutura e Processos.

Art. 3º. A Infraestrutura engloba todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática, multimídia, sistemas internos. Para cada um dos itens que compõem a infraestrutura deverá existir uma ação a ser adotada.

Art. 4º. 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.

Art. 5º. 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.

III- DO GRUPO GESTOR DE CRISE

Art. 6º. O Plano de Contingência contará com um **Grupo Gestor de Crise** que ordinariamente reunir-se-á uma vez por semestre, e, extraordinariamente, em caso de evento significativo, a fim de analisar os planos e os cenários adversos que poderão influenciar a instituição.

§ 1º. A Presidência do Grupo Gestor de Crise será exercida pelo Diretor Geral e, na sua ausência ou impedimento pelo Coordenador da CPA.
§ 2º. Das reuniões ordinárias e extraordinárias serão lavradas Atas e suas deliberações amplamente divulgadas ao Corpo Social.

Art. 7º. O Grupo Gestor de Crise será constituído pelos seguintes membros:
a) Diretor Geral;
b) Responsável pelo Setor de Tecnologia e Informação (TI);
c) Responsável pelo Setor Financeiro (gerenciamento de risco);
d) Responsável pelo Setor de Infraestrutura;
e) Coordenador da CPA;
f) Um Coordenador de Curso designado pela Direção Geral.

Art. 8º. Basicamente são as atribuições do Grupo Gestor de Crise:
a) Identificar e avaliar as principais situações de emergência e os períodos críticos do Calendário Acadêmico, atividades essenciais da Instituição;
b) mensurar e gerenciar riscos, monitorar pontos frágeis, tangíveis e intangíveis e criar regras, procedimentos e controle;
c) avaliar o custo de cada risco depois de multiplicá-los pela probabilidade de ocorrência desses riscos;
d) assegurar o funcionamento dos serviços essenciais da Instituição em situações de emergência, como greves, falta de funcionários, falta de infraestrutura física e computacional ou de inoperância de servidores, equipamentos, sistemas de redes elétrica e de conectividade, de banco de dados;
e) relacionar as instalações e serviços da instituição nos diversos setores acadêmico e administrativo;
f) determinar quais são as partes da estrutura da instituição são essenciais e não podem parar;
g) desenvolver uma política de segurança e um ciclo de tratamento de risco na qual envolve a identificação dos ativos, as vulnerabilidades destes ativos, quais os riscos identificados e quais os riscos que serão de fato tratados;
h) prever ou analisar o problema/fato ocorrido, definindo estratégia(s), metas, e ações a serem adotadas que durem até o retorno à situação normal de funcionamento da Instituição;
i) propor procedimentos, controles e regras que possibilitem a ininterrupção das intervenções;
j) ter autoridade e autonomia para articular e atuar em nome da instituição, especialmente nos casos de sinistro;
k) ter sempre um segundo plano para cada procedimento de crise;
l) acompanhar e orientar os relatórios das equipes envolvidas nos processos;
m) agir com ética e responsabilidade social para com a comunidade interna e o meio ambiente no qual a Instituição atua, num esforço contínuo, abrangente e integrado.

Art. 8º. O Grupo Gestor de Crise deverá, inclusive, em conjunto com os setores administrativos e acadêmicos, atuar na execução das seguintes ações:

a) Mapeamento de Impacto:
Estimativa dos impactos financeiros e operacionais resultantes da interrupção e de cenários de desastres que podem afetar a Instituição, bem como as técnicas para quantificar e qualificar esses impactos. O

Mapeamento também servirá como justificativa para investimentos em prevenção e contenção, estratégias de continuidade e no próprio desenvolvimento;

b) Coleta de informações:

Referentes aos processos, e tais questionamentos devem ser feitos aos líderes de nível intermediário, ou seja, quem realmente conhece o processo. As informações serão coletadas pelo preenchimento de um questionário cujo foco é o negócio e não a tecnologia. Com esse questionário devemos obter as seguintes informações:

- ✓ Impactos e exposições financeiras;
- ✓ Impactos e exposições operacionais;
- ✓ Interdependências entre os processos de negócios;
- ✓ Grau de dependência de TI;
- ✓ Tempo máximo para retorno à operação;
- ✓ Recursos necessários à recuperação do processo de negócio.

Após a análise das respostas, a Instituição terá um relatório gerencial detalhado contendo os impactos financeiros e operacionais quantificados, processos prioritários para recuperação, interdependências existentes, recursos mínimos para recuperação e definição do tempo máximo de recuperação.

c) Estratégias de continuidade:

Definição e orientação da seleção de estratégias operacionais alternativas para a recuperação dos processos e componentes de negócio, dentro dos prazos de recuperação desejados, enquanto os processos corporativos críticos são mantidos em atividade. Esta é possivelmente a etapa mais desafiadora, pois vai requerer experiência técnica e conhecimento das atividades da Instituição, incluindo a escolha de estratégias que tenham a melhor relação Custo X Benefício, que reduzam os riscos e as exposições e que atendam às necessidades da Instituição e não só de Tecnologia e Informação.

d) Desenvolvimento e Implantação de Planos:

Planejamento e elaboração de vários planos componentes que, em conjunto, comporão um grande programa corporativo, os quais deverão garantir todo o ciclo de uma interrupção expressiva, contendo as ações e procedimentos necessários à recuperação dos processos de negócio, inventário dos recursos críticos, listas de contato dos responsáveis e demais informações essenciais. Os planos aprovados deverão conter no mínimo:

- ✓ As atividades devem ser escritas como ordens de comando, curtas e simples, com maior detalhamento para as atividades diferentes do dia-a-dia. Se necessário, inserir comentários e/ou informações adicionais;
- ✓ Todos os passos a serem executados pelos colaboradores durante a recuperação de um processo de negócio, de suporte ou recurso crítico;
- ✓ Listas de acionamento com nome, telefone de contato, endereço etc. dos funcionários envolvidos;
- ✓ Relatório de Contatos Telefônico e eletrônico da Comunidade Acadêmica: Docentes e Discentes;
- ✓ Relação de acionamento de fornecedores e parceiros;
- ✓ Inventário de recursos necessários para recuperação.

Os planos também devem estar armazenados em local único, para que possam ser acessados mesmo no pior cenário; o acesso às informações deve ser controlado, garantindo a sua confidencialidade.

IV- DA POLÍTICA DE SEGURANÇA

Art. 9º. A **Política de Segurança** elaborada pela equipe de Tecnologia e Informação será reavaliada continuamente e inclui as seguintes regras:

a) Política e procedimentos para *back-up:*

O backup dos servidores e sistemas é feito usando um STORAGE e a NUVEM como armazenamento.

Os *Backups são* realizados utilizando um *software* de *backup* dedicado apropriado para o sistema operacional utilizado.

b) Status do *backup*:
O *software* de *backup* é configurado para alertar automaticamente o administrador para o status de qualquer *backup* realizado. O status do *backup* é analisado em uma base diária e quaisquer falhas identificadas são corrigidas.

c) Verificação e teste de restauração:
O *software* de *backup* é configurado para verificar automaticamente o *backup*. A verificação será realizada por meio da comparação do conteúdo da cópia de segurança com os dados no disco.
A restauração de informações a partir do *backup* é testada periodicamente a cada sete dias.

d) Ciclos de backup:
Repositório de Dados - O *backup* completo dos sistemas importantes é realizado diariamente.
Esquema de rotação - É utilizado o método simples de rotação diária, sendo que, no mínimo, 7 (sete) *backups* são mantidos.
Backups diários - O *backup* é feito todos os dias, como parte de uma rotação diária simples.

e) Armazenamento de *backup*:
Os *backups* dos sistemas locais são armazenados de forma segura em 2 (dois) STORAGES. Os backups dos sistemas que ficam alocados no datacenter, são armazenados em um STORAGE no próprio datacenter. Para resiliência, um dos STORAGES é sempre removido do local. No mínimo, uma cópia do mais atualizado *backup* de dados local é armazenado fora do local uma vez por semana. A programação para o armazenamento externo é detalhada em um log.

f) Efetiva Contingência
Na impossibilidade de se utilizar o espaço físico da instituição a equipe de informática e técnico-administrativa poderá continuar a funcionar home office. O serviço de e-mail da Instituição é fornecido pelo(a) MICROSOFT, no caso Office 365 que é uma suíte de aplicativos para escritório online por assinatura que oferece acesso a vários serviços e softwares construídos em torno da plataforma Microsoft Office, com suporte 24 horas por dia da semana, serviço de AntiSpam, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A Instituição utiliza ainda o(a) Exchange da Microsoft que possibilita, via webmail, o acesso remoto de todas as mensagens pelos colaboradores. A Instituição conta com linhas de telefone digitais e linhas analógicas em caso de contingencia. Em caso de falhas nas linhas telefônicas, os funcionários ainda possuem celulares que podem substituir a telefonia fixa. As informações do portfólio além de estarem nos sistemas internos da Instituição são disponibilizadas diariamente pelo administrador dos fundos, que também informará qualquer movimentação no passivo dos fundos para adequação do caixa dos fundos. Em caso de falha de fornecimento de energia, a Instituição possui *nobreak* para suportar o funcionamento de seus servidores, rede corporativa, telefonia e estações de trabalho. 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) Estrutura de Suporte
Além dos mecanismos convencionais para garantir a integridade das informações, como *back-up* em servidores com *hardware* redundante, a Instituição replica diariamente todos os seus sistemas operacionais (Banco de Dados, Arquivos e E-mails) em servidores externos. Neste site, as empresas parceiras da Instituição possuem sistemas de armazenamento de alta disponibilidade para *backup* e arquivamento, além de servidores para a operação contínua *fail-over*. No caso de falha, o hardware redundante passa a operar

automaticamente. Tal *hardware* redundante está à disposição para substituição, assim que o original apresentar qualquer problema. No caso de ocorrer uma falha, o monitoramento automático irá detectar o problema e alertar a diretoria da Instituição. A detecção automática de falhas em *hardware* permite a recuperação automática de todo o hardware. O plano de recuperação de desastres permite o gerenciamento de crises. Além disso, o(s) fornecedor(es) MentorWeb e o Office 365 é uma suíte de aplicativos para escritório online por assinatura que oferece acesso a vários serviços e softwares construídos em torno da plataforma Microsoft Office possuem contratos de suporte em seu nível máximo. 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)

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 no **Manual de Administração de Crises**.

Art. 10. Se a impossibilidade de se utilizar o espaço físico ocorrer quando os funcionários estiverem na Instituição, o corpo técnico-administrativo deverá dirigir-se a sua home portando os notebooks da faculdade, que estão preparados com todas as ferramentas necessárias para o processo de contingência (MentorWeb, SKYPE, Outlook e Microsoft Office 365 que é uma suíte de aplicativos para escritório online por assinatura que oferece acesso a vários serviços e softwares construídos em torno da plataforma Microsoft Office).

§ 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 discente por SMS, e-mails.
§ 2º. Já se a impossibilidade de se utilizar o espaço físico ocorrer quando os funcionários não estiverem na Instituição, eles dirigir-se-ão ao Ponto de Encontro determinado pela direção portando seus notebooks, que estão preparados com todas as ferramentas necessárias para o processo de contingência (MentorWeb, SKYPE, Outlook e Microsoft Office 365 que é uma suíte de aplicativos para escritório online por assinatura que oferece acesso a vários serviços e softwares construídos em torno da plataforma Microsoft Office em nuvem).

§ 3º. Chegando no Ponto de Encontro estabelecido, o responsável pela tecnologia e Informação, e na sua ausência o técnico de informática, será responsável por recuperar os arquivos no back-up diário realizado na nuvem. A lista dos arquivos que necessitam de recuperação consta do Manual de Administração de Crises.

Art. 11. Além do processo de recuperação de arquivos da nuvem, o responsável pela tecnologia e informação é o responsável pelo acesso à Internet da Instituição, que sem fio poderá ser acessada utilizando somente o código do cartão de acesso da Instituição e que com fio será providenciado um usuário e senha de acesso do local de encontro determinado.

V- DO MANUAL DE ADMINISTRAÇÃO DE CRISE

Art. 12. O Manual de Administração de Crises será elaborado por uma Comissão Especial Acadêmico-Administrativa a ser especialmente nomeada pela Direção Geral para tal finalidade, para que no prazo máximo de cento e oitenta (180) dias seguidos e contados a partir da data de nomeação.

§ 1º. O Manual deverá ser apresentado à homologação do Conselho Superior da Instituição.

§ 2º. Outros Manuais poderão vir a ser elaborados a medida em que as necessidades apontem para tal fim.

§ 3º. Finalizados os trabalhos da Comissão Especial Acadêmico-Administrativa, a mesma será destituída por portaria.

VI- DA AVALIAÇÃO DO PLANO DE CONTINGÊNCIA

Art. 13. O Plano de Contingência da Infraestrutura Tecnológica será (re)avaliado semestralmente pela Comissão Própria de Avaliação – CPA, e extraordinariamente quando demandar.

§ 1º. Os diagnósticos serão preparados por meio de Relatórios contendo, inclusive, tabelas, gráficos, até mesmo figuras se couber.

§ 2º. O relatório será divulgado à comunidade acadêmica em página da CPA no portal institucional.

VII- DAS DISPOISIÇÕES GERAIS

Art. 14. Os casos omissos serão encaminhados à julgamento e deliberação da Direção Geral, ouvido o Conselho Superior.

FDB, agosto/2019.