UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA STI/POSIN 13 – CÓPIAS DE SEGURANÇA (BACKUP)

Esta instrução normativa tem por objetivo estabelecer diretrizes para o processo de cópia e armazenamento de dados dos sistemas da Ufes, visando garantir a sua integridade e disponibilidade, bem como evitar que informações sejam permanentemente perdidas em caso de algum incidente físico, lógico ou ambiental.

O mero procedimento de backup não pode ser confundido ou utilizado como uma estratégia de temporalidade – guarda ou preservação de longo prazo – mas para a recuperação de desastres, perda de dados originados por apagamentos acidentais ou corrupção de dados.

1. CONCEITOS

Para o disposto nesta Instrução Normativa, considera-se:

- **Administrador de Backup:** servidor responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e *restore*;
- **Ativos de Informação:** base de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;
- **Ativos de Software:** aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- **Backup:** cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais;
- **Backup *full* ou completo:** modalidade de backup na qual todos os dados são copiados;
- **Backup incremental:** modalidade de backup na qual somente os arquivos modificados desde o último backup são copiados;
- **Gestor de Ativo de Informação:** proprietário ou custodiante de ativo de informação;
- **Log:** histórico de avisos, erros e mensagens de aplicativos e sistemas;
- **Mídia:** meio físico no qual efetivamente se armazena o backup;

- ***Restore*:** recuperação dos arquivos existentes em um backup;
- **Retenção:** período em que o conteúdo da mídia de backup deve ser preservado; e
- **Sistemas Críticos:** sistemas, incluindo seus dados, cuja indisponibilidade afetem a execução das principais atividades acadêmicas e administrativas da Ufes.

2. RESPONSABILIDADES

As unidades responsáveis pelos sistemas ficam encarregadas de indicar os administradores de backup, servidores responsáveis pela administração dos procedimentos relativos aos serviços de backup e *restore*.

São atribuições dos administradores de backup:

1. Propor modificações visando o aperfeiçoamento da política de backup;
2. Criar e manter os backups;
3. Configurar a ferramenta de backup, com no mínimo, periodicidade, conteúdo e relatórios;
4. Preservar as mídias de backup;
5. Testar os procedimentos de backup e *restore*;
6. Executar procedimentos de *restore*;
7. Gerenciar mensagens e logs diários dos backups, através dos relatórios, fazendo o tratamento dos erros de forma que o procedimento de backup tenha sequência e os erros na sua execução sejam eliminados;
8. Realizar manutenções periódicas dos dispositivos de backup;
9. Comunicar o gestor sobre os erros e ocorrências nos backups dos ativos de informação e de software sob sua responsabilidade;
10. Documentar os procedimentos dos itens 2 a 9; e
11. Registrar a execução dos procedimentos, visando a manutenção de histórico de ocorrências.

3. PROCEDIMENTOS DE BACKUP

Todo e qualquer ativo de informação ou de software deverá ter sua inclusão nos procedimentos de backup avaliada.

O gestor de cada ativo de informação, em conjunto com os administradores de backup,

deverá definir e registrar formalmente, através de documento ou sistema, o que será incluído no backup, bem como a periodicidade e o período de retenção.

A disponibilização do serviço de backup para um dado ativo, e em quais termos, fica condicionada tanto a necessidade da preservação do ativo quanto a disponibilidade de recursos na infraestrutura para atender a demanda.

A oferta do serviço de backup deve ser garantida para os serviços críticos da Ufes.

Os procedimentos de backup devem ser atualizados sempre que necessário.

A periodicidade e a retenção dos backups deverão observar os seguintes prazos:

- Periodicidade diária – retenção: sete últimos dias – mídia: disco;
- Periodicidade semanal – retenção: quatro últimas semanas – mídia: disco;
- Periodicidade mensal – retenção: doze últimos meses – mídia: fita; e
- Periodicidade anual – cinco últimos anos – mídia: fita.

Em casos especiais, o gestor do ativo de informação poderá definir, em conjunto com os administradores de backup, prazos diferenciados para retenção dos backups.

Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada.

A criação e operação de backups deverão obedecer às seguintes diretrizes:

- O backup deverá ser programado para execução automática em horários de menor ou nenhuma utilização dos sistemas e da rede;
- Os administradores de backups deverão certificar-se da conclusão bem-sucedida dos backups, analisando, se for o caso, os arquivos de log, para garantir o resultado da operação;
- Em caso de problemas na operação de backups, as causas deverão ser analisadas, reparadas e, quando necessário, um novo backup deverá ser imediatamente realizado;
- As mídias utilizadas no processo de realização do backup deverão possuir identificação suficiente para permitir, direta ou indiretamente, a localização e extração das informações nelas armazenadas;
- Os backups deverão ser armazenados em, pelo menos, duas cópias, em mídias diferentes;

- Os backups dos sistemas críticos, deverão ter cópias mantidas em locais fisicamente distintos, bem como deverá ser mantida uma cópia offline, em dispositivo de proteção de mídia.
- Quando as cópias de segurança forem armazenadas em mais de um local físico, a distância entre os dois locais deve ser suficiente para escapar dos danos decorrentes de desastre ocorrido em um deles;
- Nas situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação; e
- As cópias de segurança deverão ser armazenadas em um local diferente do servidor físico onde são utilizadas em produção.

O backup deverá ser realizado com base nas seguintes disposições:

1. Os backups quinzenais, mensais e anuais deverão ser realizados, preferencialmente, na modalidade *full*, de forma a poderem recuperar integralmente todas as informações sem a necessidade de outros backups;
2. O backup semanal ocorrerá, preferencialmente, aos sábados, referindo-se à semana que se encerra;
3. O backup mensal ocorrerá, preferencialmente, no primeiro dia de cada mês, referindo-se ao mês anterior;
4. O backup diário ocorrerá, preferencialmente, fora do horário de expediente, na modalidade *full*+incremental de forma a poder reverter os dados recentes de forma mais rápida;
5. Em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, os administradores de backup deverão adotar as providências no sentido de salvaguardar as informações através de outro mecanismo, como por exemplo, cópia dos dados para outro servidor ou execução do backup em horário de produção; e
6. As bases de dados dos sistemas críticos deverão ser realizadas pelo menos uma vez ao dia, na modalidade incremental, para reduzir a perda de transações.

4. PROCEDIMENTOS DE RESTORE

O procedimento de *restore* deverá obedecer ao seguinte processo:

1. O gestor do ativo de informação que precise recuperar informações deverá solicitar formalmente, por meio definido pela unidade responsável pelo setor onde o ativo se encontra, justificando o motivo da solicitação; e
2. A solicitação prevista no item anterior será encaminhada aos administradores de backup para que realizem a recuperação e comuniquem o resultado do procedimento.

É vedado o *restore* diretamente nos ambientes de produção, exceto em situações de recuperação de desastre ou plano de contingência.

5. TESTES DE BACKUP E RESTORE

Os procedimentos de backup e *restore* deverão ser testados sempre que necessário.

Os backups mensais e anuais deverão ser testados no prazo máximo de uma semana após a sua execução e, caso seja detectada falha no backup, ou se este estiver incompleto, novo backup deverá ser executado com vistas ao seu armazenamento.

Os backups mensais e anuais deverão ser testados regularmente a fim de verificar a integridade da mídia.

6. DESCARTE E SUBSTITUIÇÃO DAS MÍDIAS DE BACKUP

Os administradores de backup deverão respeitar os critérios definidos pelos fabricantes para assegurar a validade e a qualidade das mídias utilizadas na realização de backups.

No caso de substituição da solução utilizada nos backups, as informações contidas nas mídias da antiga solução deverão ser transferidas em sua totalidade para as mídias da nova solução.

A solução antiga somente poderá ser desativada após a confirmação, através de teste de *restore*, de que todas as informações foram transferidas para a nova solução implementada.

O descarte das mídias utilizadas para backup deve ser realizado de forma a impossibilitar a recuperação total ou parcial das informações.