Política de Cópia de Segurança e Restauração de Dados

STI
SUPERINTENDÊNCIA DE
TECNOLOGIA DA INFORMAÇÃO

Universidade Federal Fluminense

Serviço Público Federal
Ministério da Educação
Universidade Federal Fluminense
Superintendência de Tecnologia da Informação

Política de Cópia de Segurança e

Restauração de Dados

O REITOR DA UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições legais, estatutárias e regimentais,

Considerando a implantação do Sistema Eletrônico de Informações (SEI);

Considerando a implantação do Sistema de Gestão Eletrônica de Documentos (Sigadoc);

Considerando o que consta na Portaria 55.749, de 29 de fevereiro de 2016 referente a criação da Infraestrutura de Chaves Públicas da Universidade Federal Fluminense, denominada ICP-UFF;

Considerando o vasto uso de sistemas administrativos e acadêmicos;

Considerando as diretrizes estratégicas da Governança Corporativa da Universidade Federal Fluminense, do Comitê de Gestão da Informação (CGI) e do Comitê de Tecnologia da Informação (COTI) a saber:

1. Alinhamento da estratégia de Tecnologia da Informação com o Planejamento Estratégico Institucional e com as diretrizes e normas do COTI;
2. Incentivo ao desenvolvimento e capacitação de servidores lotados na Superintendência de Tecnologia da Informação (STI), promovendo a gestão do conhecimento e competências, com foco em resultados e na comunicação interna e externa;
3. Fomento às boas práticas de gestão de Tecnologia da Informação e à implantação, monitoramento do desempenho, por intermédio da Governança de TI, precedidas de aconselhamento do Tribunal de Contas da União intervenientes e estratégicas desta Superintendência;
4. Fomento à Política de Segurança da Informação da Universidade Federal Fluminense;
5. Elaboração, controle de projetos de TI e planos de ação para o alcance das metas do PDTIC;
6. Revisão das metas de TI não atingidas, para o alcance dos objetivos do Planejamento Estratégico de Tecnologia da Informação e Comunicação e do Planejamento Estratégico Participativo;

Considerando o tema estratégico “Gestão de Riscos” e “Segurança da Informação”, objetiva-se identificar, analisar e mitigar, de forma continuada, os riscos presentes nos ativos de dados vinculados à TI, evitando a ruptura dos preceitos de integridade,

confidencialidade e disponibilidade das informações, para atender a um modelo de continuidade do negócio e minimizar perdas em caso de desastre e viabilizar a recuperação de dados através do processo de restauração;

Considerando a necessidade de assegurar o plano de continuidade de negócios desta Universidade, por meio de uma política de cópia de segurança que observe criteriosamente o modo e a periodicidade de cópia dos dados pertencentes aos serviços computacionais;

Considerando o portfólio de projetos aprovados junto a Governança Corporativa;

Considerando que a perda dos ativos de dados pode significar graves dificuldades administrativas e de prestação jurisdicional, podendo ocasionar a paralisação de atividades essenciais da Universidade;

Considerando a necessidade de definir procedimentos para solicitação por parte do serviço de recuperação dos ativos de dados eventualmente indisponíveis;

Considerando que deve ser estabelecida a periodicidade, o agendamento e a forma de tratamento das cópias de segurança conforme necessárias à recuperação dos ativos de dados;

Considerando que deve ser definido o período de tempo que as mídias de cópia de segurança permanecerão guardadas até serem reutilizadas ou destruídas;

Considerando o que consta no ofício 0449/2016-TCU/Sefti, de 19/4/2016, que trata do questionário eletrônico de Governança de Tecnologia da Informação junto ao TCU, questão 5.4 “Políticas e Responsabilidades”, item e: “a organização dispõe de política de cópias de segurança (backup) formalmente instituída como norma de cumprimento obrigatório” e, consequentemente, tal cumprimento requer uma política de restauração capaz de garantir um nível de recuperação às cópias de segurança efetuadas.

R E S O L V E:

1 - **Aprovar** a política de **Cópia de Segurança e Restauração dos Dados** junto ao CGI, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados a serem executadas pelo o referido órgão, visando garantir a segurança, integridade e recuperação das informações.

Capítulo I

Definições e Funções

Art. 1 Para o disposto neste ato considera-se:

I. **Administrador de Banco de Dados:** responsável técnico pelo serviço de instalação, configuração e gerenciamento do ambiente de banco de dados;
II. **Administrador da Virtualização:** responsável técnico pelo serviço de instalação, configuração e gerenciamento dos ambientes virtuais baseados em virtualização;
III. ***Backup* Completo:** modalidade de *backup* na qual todos os dados são copiados integralmente;
IV. ***Backup* Diferencial:** modalidade de *backup* na qual somente os arquivos novos e modificados desde o último *backup* completo são copiados;
V. ***Backup* Incremental:** modalidade de *backup* na qual somente os arquivos novos e modificados desde o último *backup* realizado;
VI. ***Backup* de primeiro nível:** armazenamento do *backup* em disco local;
VII. ***Backup* de segundo nível:** armazenamento do *backup* em mídia externa;
VIII. **Backup *off-site*:** estratégia de *backup* que abrange a replicação de dados do backup em um local geograficamente separado do local dos sistemas de produção;
IX. **Catálogo de Serviços:** Listagem com todos os serviços ativos oferecidos pela STI, que necessitam de backup;
X. **Colaborador:** integrante do quadro de funções da STI.
XI. **Equipe de *backup*:** equipe técnica responsável pelos procedimentos de configuração, execução, monitoramento e testes de *backup* e restauração;
XII. **Mídia:** meio físico no qual efetivamente armazenam-se os dados de um *backup* (fita magnética e DVD);
XIII. **Retenção:** período de tempo em que o conteúdo da mídia de *backup* deve ser preservado;
XIV. **Recuperação de desastre:** estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;
XV. **Responsável pelo Serviço:** colaborador da STI responsável pela operação de determinados serviços ou recursos computacionais da Universidade;
XVI. **RPO**:(do inglês,*Recovery Point Objective*) diz respeito à quantidade de informação que é tolerável perder, no caso de indisponibilidade nos serviços.
XVII. **RTO**:(do inglês, *Recovery Time Objective*) diz respeito à quantidade de tempo que as operações levam para estarem acessíveis, após uma indisponibilidade;
XVIII. **Serviço de *backup*:** todo ativo que possui informações ou dados e foi incluído nos serviços de *backup* em conformidade com as regras de inclusão;

Capítulo II

Domínios de dados

Art. 2 Os serviços que serão contemplados nesta política de *backup* e restauração estarão divididos em quinze categorias, para que cada tipo de dado possa ser tratado com maior especificidade, atendendo da melhor forma, cada tipo de serviço.

I. Arquitetura
II. Banco de Dados
III. Compartilhamento de Arquivos
IV. E-mail
V. Equipe NDC
VI. Hospedagem
VII. Infraestrutura
VIII. LDAP
IX. Plataformas WEB
X. Sistemas Acadêmicos
XI. Sistemas Java
XII. Sistemas Legados
XIII. Sistemas PHP
XIV. Sistemas Rails
XV. Virtualização

Capítulo III

Atribuições e Responsabilidades

Art. 3 O responsável pela Área de Operações da STI será o responsável pela Equipe de *backup*, delegando assim as atribuições de manter a política e procedimentos relativos aos serviços de *backup* e restauração, bem como de guardar as mídias e assegurar o cumprimento das normas aplicáveis.

Parágrafo único. O responsável pela Área de Operações deve: definir os modelos de documentos envolvidos em todo o processo de *backup*, e a periodicidade de relatórios técnicos, os quais avaliem todo o processo de restauração efetuado, além de reportar ao CGI relatório mensal.

Art. 4 São atribuições da Equipe de *Backup* e *Restore*:

I. Propor modificações visando o aperfeiçoamento da política de Cópia de Segurança e Restauração de Dados;
II. Criar e manter os backups;
III. Executar os procedimentos de restauração;
IV. Configurar a ferramenta de backup conforme os serviços;
V. Configurar e operar os serviços e os ambientes de Restauração;
VI. Criar e testar procedimentos a fim de operacionalizar as atividades;
VII. Gerenciar mídias;
VIII. Criar notificações e relatórios de backup;
IX. Criar Relatório de Execução de Restauração;
X. Criar Modelo de Notificação conforme cenário de restauração;
XI. Cumprir os cenários de restauração de acordo com anexo III (Classificação das Categorias de Serviço);
XII. Verificar periodicamente os relatórios gerados pela ferramenta de backup;
XIII. Restaurar os *backups* em caso de necessidade;
XIV. Gerenciar mensagens e logs diários dos *backups*, fazendo o tratamento dos erros de forma que o procedimento de *backup* tenha sequência e os erros na sua execução sejam eliminados;
XV. Fazer manutenções periódicas dos dispositivos de *backup*;
XVI. Fazer o carregamento dos *backups* programados para as mídias necessárias;
XVII. Comunicar ao Responsável pelo Serviço as falhas e ocorrências de anomalias durante os procedimentos de *backup* e restauração;
XVIII. Fazer o armazenamento das mídias de *backup* em cofre;
XIX. Definir o documento para Solicitação do Serviço de *Backup*;
XX. Definir o documento para Solicitação do Serviço de Restauração;
XXI. Gerar relatórios gerenciais semanalmente, para o Gerente da Área de Operações.

Art. 5 Todo e qualquer serviço de responsabilidade da STI deverá ser ponderado e estudado antes de sua inclusão no *backup*. Após incluído, obrigatoriamente deverá seguir os procedimentos de restauração.

§1º Serão abrangidos por esta política de backup e restauração, todos os serviços classificados com criticidade alta, no Catálogo de Serviços e, no mínimo, oitenta por cento dos serviços que possuírem criticidade média.

§2º O responsável por cada serviço deverá definir quais servidores e respectivos diretórios e arquivos serão incluídos no *backup*, tendo como prioridade:

I. Arquivos de configurações de ambientes e aplicativos referentes a serviços deste servidor em questão;
II. Arquivos de *log* dos aplicativos, inclusive *log* da ferramenta de *backup* e restauração;
III. Dados e configurações de banco de dados;
IV. Arquivos de usuários (documentos e e-mail).

§3º A Equipe de *backup* deverá definir quais diretórios e arquivos não serão incluídos no *backup*, tendo como referência:

I. Arquivos do sistema operacional ou de aplicações que podem ser obtidos através de uma nova instalação;
II. Arquivos temporários;
III. Arquivos salvos nas unidades locais das estações de trabalho;
IV. Arquivos da área de transferência;
V. Arquivos particulares dos usuários.

§4º Para os aplicativos e/ou bancos de dados de terceiros devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante, desde que estas não infrinjam nenhum dos artigos e parágrafos aqui descritos.

Art. 6 Os procedimentos de *backup* deverão ser atualizados quando houver:

I. Novas aplicações desenvolvidas;
II. Novos locais de armazenamento de dados;
III. Novos arquivos com relevância para funcionamento do serviço;
IV. Novas instalações de bancos de dados;
V. Novos aplicativos instalados;
VI. Outras informações que necessitem de proteção através de *backups* deverão ser informadas a Equipe de *Backup*, pelo Responsável pelo Serviço.

Art. 7 Para a especificação de um *backup*, o Responsável pelo Serviço deverá efetuar uma solicitação de *backup* contendo as informações necessárias de acordo com modelo de solicitação adotado, mediante inciso XV do Art. 3., conforme Anexo I.

§1º O *backup* deverá ser programado na ferramenta de *backup*, seguindo as orientações do documento de solicitação de *backup*;

§2º Todos os *backups* criados deverão ser testados antes de aplicar a programação solicitada. Estes testes deverão incluir uma restauração para comprovar a eficácia do *backup*, que deverá incluir um atestado de aprovação do Responsável pelo Serviço, conforme Anexo II.

Art. 8 A configuração e monitoração das funcionalidades relativas ao *backup* de banco de dados será de responsabilidade do Administrador de Banco de Dados.

Art. 9 A Universidade Federal Fluminense deverá disponibilizar uma implantação e uma infraestrutura capaz de atender ao modelo de continuidade da instituição em nível de

recuperação de desastres, a fim de que se torne viável à STI a implementação de uma estratégia de backup *off-site.*

Capítulo IV

Procedimento de *backup*

Art. 10 Os *backups* de dados serão efetuados da seguinte forma:

I. O procedimento padrão para as Categorias de Dados que não possuírem especificação própria, seguirá a seguinte estratégia:

A. O *Backup* Completo de todas as aplicações, será executado entre os 10 primeiros dias de cada mês e será copiado em dois locais diferentes. O primeiro será em *storage*, para facilitar o acesso rápido, em pequenas restaurações e terá sua retenção de 30 dias. O segundo será fita magnética e terá sua retenção detalhada no próximo capítulo.

B. O *Backup* Incremental será executado durante os demais dias do mês e será copiado diariamente em dois locais diferentes. O primeiro será em *storage* e terá sua retenção finalizada após a realização do próximo *backup* Completo. O segundo será fita magnética e terá retenção de 3 meses.

II. O procedimento para a Categoria de Banco de Dados seguirá a seguinte estratégia:

A. O *Backup* Completo será executado diariamente e será copiado em dois locais diferentes. O primeiro será em *storage* e terá sua retenção de 30 dias. O segundo será fita magnética e terá sua retenção detalhada no próximo capítulo.

III. Quando um serviço for descontinuado a equipe de *backup* deverá ser notificada e então providenciará um *Backup* completo final, envolvendo seu banco de dados e arquitetura quando necessário. Este *backup* deve ser gravado em fita magnética e guardada no cofre por tempo indeterminado.

Capítulo V

Guarda dos dados

Art. 11 Os *backups* do tipo Completo, realizados em fita magnética devem ser guardados mensalmente em cofre de segurança anti-chamas designado pela STI sempre no dia 10 (dez) de cada mês, ou no dia útil consecutivo, juntamente com uma identificação física do conjunto de fitas.

Parágrafo único. Deverá ser guardado no cofre, juntamente com as fitas, uma planilha ou identificação física com o objetivo de viabilizar a restauração em caso de desastres.

Art. 12 Visando atender a grande diversidade de naturezas dos serviços, contemplados por legislações, que definem diferentes prazos obrigatórios para guarda de documentos e conhecendo o baixo custo para o armazenamento de mídias, os dados serão armazenados atendendo os requisitos deste artigo.

§1º As fitas armazenadas nos meses de janeiro de cada ano terão tempo de guarda indeterminado, servindo como base de dados consolidada do ano imediatamente anterior, tendo seus dados transcritos para novas mídias quando necessário, respeitando as diretrizes deste documento.

§2º As fitas dos demais meses terão sua informação descartada após 12 meses e a fita magnética será encaminhada para sobrescrita ou para descarte, caso já tenha excedido 2/3 da sua vida útil ou apresente sinais de degradação.

§3º Em caso de limitação de capacidade do cofre, deve-se providenciar um novo local igualmente seguro, para que o processo não seja interrompido.

Capítulo VI

Da transcrição de dados e do Descarte de mídias

Art. 13 A fita magnética só será considerada confiável durante os dois primeiros terços da vida útil estabelecida pelo fabricante. Após expirado este prazo, as informações nela contidas deverão ser transcritas para uma nova mídia, a fim de zelar pela integridade dos dados.

Art. 14 O descarte das mídias de *backup* não confiáveis deverá ser feito mediante proposta apresentada pela Equipe de *Backup* e dirigida à Superintendência de Tecnologia da Informação.

Parágrafo único. As fitas a serem descartadas deverão ser destruídas fisicamente, seguindo orientações do fabricante quanto a vida útil, de forma a impedir a sua reutilização ou acesso indevido às informações por pessoas não autorizadas.

Capítulo VII

Procedimento de Restauração

Art. 15 A recuperação dos *backups* deverá obedecer às seguintes orientações:

I. Todo e qualquer usuário que precise recuperar arquivos deve entrar em contato com o Setor de Suporte ao Usuário, que registrará a solicitação na ferramenta de controle de atendimento;

II. A equipe responsável pelo cadastramento do chamado técnico solicitará o nome e setor do usuário, o(s) arquivo(s) a ser(em) recuperado(s), subdiretório(s) em que se encontra(m) e a data da versão que deseja recuperar, sendo esta última informação obrigatória para viabilizar a recuperação do arquivo;

III. O chamado técnico será encaminhado à Equipe de *Backup*, que após a conclusão da tarefa, realizará o fechamento do chamado indicando a restauração do(s) arquivo(s);

IV. Deverá ser mantido registro de todos os arquivos cuja restauração foi solicitada, juntamente com as informações relativas ao solicitante, nome do arquivo, data da versão restaurada e data e hora da solicitação;

V. A restauração dos arquivos somente será possível nos casos em que o arquivo tenha sido atingido pela estratégia de *backup* que ocorre todos os dias com início às 22h, ou seja, os arquivos criados e eventualmente apagados ou alterados não serão passíveis de recuperação no mesmo dia da criação.

Capítulo VIII

Dos Testes de Restauração

Art. 16 As cópias de segurança armazenadas deverão ser testadas mensalmente, e a cada mês serão testados domínios de dados distintos, a fim de percorrer anualmente todos os itens descritos no Capítulo II.

§1º. A equipe de *backup* deverá definir quais domínios de dados serão testados a cada mês.

§2º. O teste será realizado com o intuito de validar a suficiência dos dados armazenados e a integridade das mídias de *backup*.

§3º. O responsável pelo serviço terá total responsabilidade pela validação de todos os dados restaurados pela equipe de *backup*.

§4º Eventuais dados que não tenham sido incluídos no *backup* por falta de sinalização do responsável pelo serviço, deverão ser informados a equipe de *backup* durante o período de testes.

Art. 17 Após a restauração dos dados a recuperação do serviço deverá ser realizada pelo responsável pelo serviço com auxílio de áreas correlacionadas, como Governança de dados ou arquitetura.

§1º. O responsável pelo serviço deverá informar a equipe de *backup* se a recuperação do serviço foi bem-sucedida ou se será necessária a inclusão de novos arquivos.

§2º. Para todos os testes realizados deverá ser gerado um relatório, com parecer do Gerente da Área de Segurança da Informação, e em seguida deverá ser enviado ao Gerente da Área de Operações da STI, para posteriormente ser publicado em portal de conteúdo referente à Administração do Backup.

Capítulo IX

Diretrizes de Operação

Art. 18 A criação e operação dos backups deverá obedecer às seguintes orientações:

I. Criação de backups:
   I. o backup deverá ser programado para execução automática em horários de menor ou nenhuma utilização dos sistemas e da rede.

II. Operação de backups:
   I. o backup deverá ser monitorado pela Equipe de Backup;
   II. Para todos os backups realizados com sucesso, deve ser gerado um extrato automatizado pela própria ferramenta de backup, confirmando a execução do mesmo;
   III. Aos backups que apresentarem falhas, a Equipe de Backup deverá criar um relatório de “Acompanhamento de backup”, no qual deverá constar a data,

os horários de início e término, os objetos e o responsável pelo serviço, a causa da falha, a ação corretiva adotada e qual parte do backup ficou comprometida.

Art. 19 Os backups deverão ser realizados seguindo as regras de acordo com cada nível de serviço, levando em conta a classificação dos dados.

I. Em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, a Equipe de Backup deverá adotar as providências no sentido de guarda das informações através de outro mecanismo, como por exemplo: cópia dos dados para outro servidor, execução do backup em outro horário de agendamento e etc.

Art. 20 Os backups mensais de todas as categorias deverão ser testados, no prazo máximo de um ano, após a sua execução.

Art. 21 Quaisquer procedimentos programados nos servidores e que impliquem riscos de funcionamento em quaisquer serviços ou equipamento da instituição, somente deverão ser executados após a realização de backup dos seus dados.

Art. 22 O backup *off-site* deverá armazenar os dados em fita ou *storage*, em qualquer unidade da UFF, atendendo os requisitos deste artigo.

§1º A armazenagem do backup *off-site* deve estar obrigatoriamente fora do campus onde encontra-se o *data center* de produção.

§2º Os dados que serão transportados ao backup *off-site* deverão estar criptografados.

§3º O armazenamento *off-site* deve estar em conformidade com padrões acordados entre a STI e o CGI, e aprovado pelo COTI.

Art. 23 O procedimento de criptografia das cópias de segurança deverá ser feito em conformidade com um utilitário (recomendação: GnuPG).

Capítulo X

Das Considerações Finais

Art. 24 Fica estabelecido o prazo de 60 (sessenta) dias, a contar da data de publicação desta portaria para a adoção das providências necessárias para prover uma infraestrutura à implementação plena desta política de backup pela Universidade Federal Fluminense.

Art. 25 Este ato entra em vigor na data de sua publicação.

Capítulo XI

Das Referências Normativas

Art. 26 Este documento se ampara em referência pelos instrumentos normativos apresentados conforme segue:

I. Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário. Disponível em<www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20080814/008-380-2007-1-GP.doc>. Acesso em: 12 ago.2016.

II. Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário. Disponível em<http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20120528/AC_1233_19_12_P.doc>. Acesso em: 12 ago.2016.

III. BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Disponível em <www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 12 ago.2016.

Anexo I

Matriz de Responsabilidades de Cópia de Segurança

Atividade	Operação de Backup	Detentor do Serviço	Arquitetura	Superintendência de Tecnologia da Informação
Identificar necessidade de backup para novo serviço	C	R	I	A
Classificar o novo serviço em uma categoria existente	R	I		A
Informar diretórios e bancos que necessitam de backup	I	R	I	A
Criar rotinas de backup	R	I		A
R - **R**esponsável; **A** - Prest**a**dor de Contas; **C** - **C**onsultado; **I - I**nformado				

Anexo II

Matriz de Responsabilidades para Teste e Restauração de Dados

Atividade	Operação de Back up	Detentor do Serviço	Arquitetura	Superintendência de Tecnologia da Informação
Restaurar periodicamente os serviços de cada categoria.	R			A
Disponibilizar os arquivos restaurados ao detentor do serviço.	R	I		A
Verificar integridade e suficiência dos arquivos restaurados.	I	R	C	A
Validar backup.	I	R	I	A
R: **R**esponsável; **A**: Prest**a**dor de Contas; **C**: **C**onsultado; **I: I**nformado				