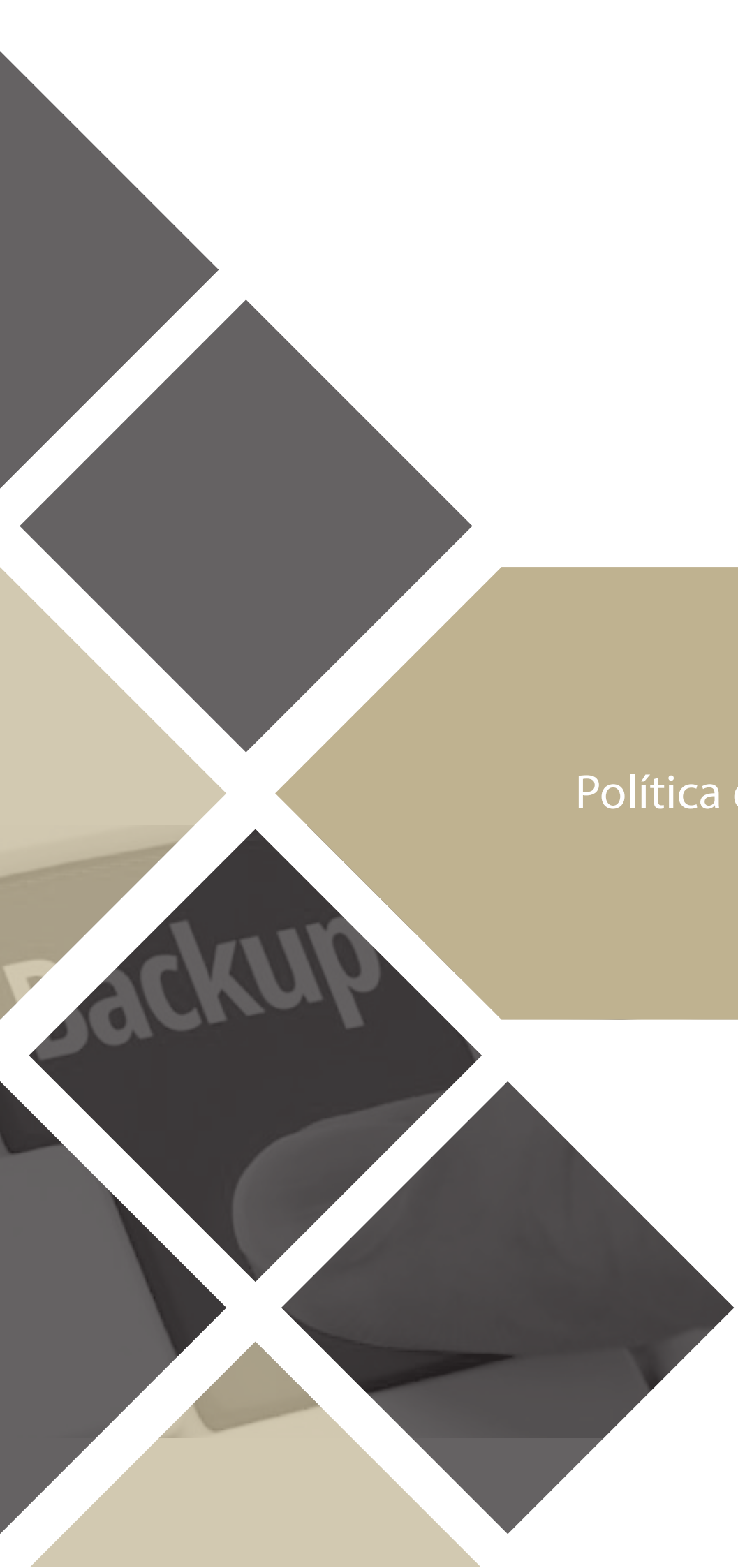

Política de backup

UNIFESSPA
Universidade Federal do Sul e Sudeste do Pará

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Autor
01/11/2018	1.0	Documento de referência 1, Versão inicial	Fábio de oliveira Torres
01/12/2018	1.1	Revisão	Luiz Felipe de Sousa, Vitor de Souza Castro
01/02/2019	1.2	Revisão	Luiz Felipe de Sousa, Vitor de Souza Castro
13/03/2019	2.0	Revisão e padronização da norma	Ralfh Alan Gomes Machado, Luiz Felipe de Sousa, Vitor de Souza Castro

Apresentação

O presente documento estabelece uma política de cópias de segurança (*backup*) e restauração de arquivos digitais armazenados no parque tecnológico da Universidade Federal do Sul e Sudeste do Pará – Unifesspa.

Orientações Gerais

Art. 1°- As diretrizes desta instrução normativa devem considerar, prioritariamente, os requisitos legais, os objetivos estratégicos, a estrutura e finalidade da Instituição.

Art. 2°- Cabem aos administradores preverem a realização de testes periódicos de restauração, no intuito de averiguar os processos de *backup* e estabelecer melhorias.

Art. 3°- A administração dos *backups* também deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 4°- As mídias (ou dispositivos de armazenamento) deverão ser armazenados em cofre corta-fogo, ou em localidade diversa da origem dos dados (*backup off-site*).

Art. 5°- As mídias defeituosas ou inservíveis serão encaminhadas para picotamento, incineração, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros.

Art. 6°- As solicitações de restauração de arquivos deverão ser abertas formalmente através de ferramentas de abertura de chamados e/ou formulário que deverá conter os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso.

Conceitos e Definições

Art. 7°- Para o disposto neste ato considera-se:

I. Administrador de *backup*: responsável pelos procedimentos de configuração, execução e monitoramento de backup e pelo acompanhamento dos testes nos procedimentos de *restore*;

II. Administrador de recurso: responsável pela operação de serviços ou equipamentos do CTIC, bem como pela realização dos testes de *restore*;

III. *Backup full*: cópia de segurança de dados computacionais;

IV. *Backup* total: *backup* em que todos os dados são copiados integralmente (cópia de segurança completa);

V. *Backup* incremental: *backup* em que somente os arquivos novos ou modificados são copiados;

VI. *Backup* diferencial: *backup* em que os arquivos novos ou modificados da base de dados incremental são copiados;

VII. Clientes de *backup*: todo equipamento servidor no qual é instalado o cliente de *backup*;

VIII. *Disaster Recovery*: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

IX. Mídia: meio físico no qual se armazenam os dados de um *backup*;

X. Retenção: período de tempo em que o conteúdo da mídia de *backup* deve ser preservado;

XI. *Restore*: restauração de arquivos computacionais.

XII. Cofre corta fogo: Equipamento para manter a guarda das mídias magnéticas ou digitais.

Das Atribuições dos Responsáveis

Art. 8° **-** O gestor do departamento de Segurança da Informação será o administrador do b*ackup*, ficando responsável pela política e procedimentos relativos aos serviços de *backup* e *restore*, bem como de guardar as mídias móveis e assegurar o cumprimento das normas aplicáveis.

Art. 9° - São atribuições do administrador de b*ackup*:

I – Providenciar a criação e manutenção dos *backups*;

II – Configurar a ferramenta de *backup*;

III – Manter as mídias preservadas, funcionais e seguras;

IV – Efetuar testes de *backup* e auxiliar nos procedimentos de *restore*;

V – Verificar diariamente os eventos gerados pela ferramenta de *backup*, tomando as providências necessárias para remediação de falhas;

VI – Restaurar os *backups* em caso de necessidade;

VII – Gerenciar mensagens e *logs* diários dos *backups*;

VIII – Comunicar ao administrador de recurso os erros e as ocorrências nos *backups* e

IX – Propor modificações visando o aperfeiçoamento da política de *backup*.

Parágrafo Único – O serviço de *backup* deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de *restore*.

Art. 9° - É atribuição do administrador de recurso:

I – Preencher documento de solicitação de *backup* e *restore* com as informações relativas ao *backup*, como servidor e dados a serem incluídos;

II – Dar permissão ao administrador de *backup* para configurar e modificar a ferramenta cliente de *backup* no servidor;

III – Validar o resultado do *restore*.

Estratégia geral de backup

Art. 10° - De acordo com a natureza dos dados trazemos a seguinte classificação:

I. Arquivos dos sistemas operacionais;
II. Arquivos de configurações de *firewall*;
III. Arquivos de configurações dos sistemas pertencentes aos sistemas de Informação de Unifesspa;
IV. Arquivos de configurações de centrais telefônicas;
V. Arquivos de configurações dos s*witches* e roteadores;
VI. Servidores de arquivos;
VII. Servidores de e-mail;
VIII. Servidores de sincronização de relógios;
IX. Servidores Web;
X. Servidores de monitoramento de infraestrutura de redes (Nagios, Zabbix e Ridgeline)
XI. Servidor de acesso à federação Cafe;
XII. Servidores DNS;
XIII. Servidores de acesso aos sistemas de rede *Wi-Fi*;
XIV. *Anti-spam*;
XV. Bancos de Dados (MySQL, PostgreSQL);
XVI. Máquinas Virtuais (imagem);

Art. 11° - Por padrão será adotada o seguinte esquema de realização de *backups*:

I – Backups Full (denominados semestrais) das máquinas virtuais serão realizados pelo software “Virtual Data Protection”, com armazenamento no disco do Appliance, com 2 meses de retenção; Serão armazenados ainda em fita a cada 6 meses, com retenção de 1 ano.

II – *Backups Full* dos bancos de dados e sites serão realizados diariamente por scripts localizados nos servidores de *backups*, com 2 meses de retenção;

III – *Backups Full* (denominados semanais) das caixas de e-mail vide Art.º 10 inciso VII serão realizados aos sábados a partir da 01:00, com 2 meses de retenção;

IV – *Backups* incrementais (denominados diários) das caixas de e-mail serão realizados a partir da 01:00, com 2 meses de retenção.

Necessidades especiais de backup para máquinas virtuais – imagem (exceções)

Art. 12º **–** O *backup* das máquinas virtuais como imagem (adequado para fins de *disaster recovery* – ou seja: restauração da máquina como um todo), será feito apenas na seguinte periodicidade:

I – *Backups* completos: a cada atualização de segurança realizada ou em caso de alterações sensíveis no sistema, a pedido do responsável pelo serviço, com um ano de retenção;

II – As máquinas virtuais terão o mesmo tratamento dispensado a máquinas físicas.

Art. 13º – A recuperação de *backups* deverá obedecer às seguintes orientações:

I – O usuário que necessitar recuperar arquivos deverá entrar em contato com o setor de suporte ao usuário, registrar a solicitação por meio do sistema de chamados do CTIC (https://atendimento.unifesspa.edu.br) com, obrigatoriamente, as informações sobre o usuário, o arquivo a ser recuperado, e a data da versão que deseja recuperar;

II – Deverá ser mantido registro de todos os arquivos restaurados acompanhado da solicitação inicial;

III – Os bancos de dados serão restaurados pelo administrador de recurso, devendo o administrador de *backup* auxiliá-lo na tarefa de *restore*;

IV – Só será possível a restauração dos arquivos criados ou alterados no dia anterior à janela de realização do *backup*.

Art. 14º- Os procedimentos de *backup* deverão ser atualizados quando houver:

I – Novas aplicações desenvolvidas ou instaladas;

II – Novos locais de armazenamento de dados ou arquivos;

III – Novas instalações de bancos de dados;

IV – Outras informações que necessitem de proteção através de *backups* deverão ser informadas ao administrador de *backup*, pelo administrador do recurso.

Art. 15º – Quaisquer procedimentos programados nos equipamentos computacionais físicos ou virtuais e que impliquem riscos de funcionamento com interrupção dos sistemas e serviços essenciais da Unifesspa somente deverão ser executados após a realização do *backup* dos seus dados.

Parágrafo Único – Em casos excepcionais em que a urgência justifique, desde que autorizados pelo diretor do centro de tecnologia da informação e comunicação, os procedimentos mencionados no caput deste artigo poderão ser executados sem a realização de *backup*.

Art. 16º – O descarte das mídias de *backup* inservíveis ou inutilizáveis deverá ser realizado mediante proposta apresentada pelo administrador de *backup* dirigida à unidade competente, conforme política de descarte vigente.

Parágrafo Único **–** As mídias a serem descartadas deverão ser destruídas de forma a impedir a sua reutilização ou acesso indevido às informações por pessoas não autorizadas.

Uso do Cofre Corta-fogo

Art. 17º – Proteger e armazenar mídias magnéticas de cópias de segurança de contingência de dados da Universidade Federal do Sul e Sudeste do Pará, em dispositivo próprio de segurança, que as proteja de acesso indevido, campos magnéticos, poeira, variações externas de temperatura, umidade e desastres que podem causar a distorção ou a perda de dados que impossibilite a recuperação do ambiente em situações de contingência.

Art. 18º – As fitas magnéticas devem ser armazenadas no cofre corta-fogo que garante a proteção em caso de incêndio, enchentes e vazamentos de gases.

Parágrafo Único – O cofre deve ser mantido trancado para garantir a hermeticidade das mídias armazenadas.

Art. 19º – Os *backups* realizados em mídias do tipo cartucho de fita e que necessitem de armazenamento para *Disaster Recovery* serão guardados no cofre-corta fogo da Universidade, observando a sua capacidade, de forma que seja priorizado o armazenamento dos sete últimos *backups* diários; quatro últimos *backups* semanais; doze últimos *backups* mensais e cinco últimos *backups* anuais.

Parágrafo Único – Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída.

Art. 20º – Casos omissos a esta normativa serão tratados pelo Centro de Tecnologia da Informação e Comunicação, cabendo recurso ao Comitê de Governança Digital da Universidade Federal do Sul e Sudeste do Pará.

Parágrafo Único – Os responsáveis pelos dados deverão ter ciência dos prazos de retenção aqui estabelecidos para cada tipo de informação e os administradores/operadores de *backup* deverão zelar pelo cumprimento das diretrizes aqui estabelecidas.

Art. 21º Não é dado aos responsáveis aqui descritos o direito de alegar desconhecimento da presente política.

Art. 22º – Esta resolução entra em vigor na data de sua publicação.