

UNIVERSIDADE FEDERAL DE ALFENAS – UNIFAL-MG
COMITÊ DE GOVERNANÇA DIGITAL (CGD)
RESOLUÇÃO Nº 03, DE 09 DE OUTUBRO DE 2019

Estabelece, no âmbito da Universidade Federal de Alfenas – UNIFAL-MG, diretrizes para gerenciamento e execução de cópias de segurança (backup), seu armazenamento e restauração.

O Comitê de Governança Digital (CGD) da Universidade Federal de Alfenas – UNIFAL-MG, no uso de suas atribuições regimentais e considerando a necessidade de se estabelecer diretrizes para gerenciamento e execução, de forma automatizada, de cópias de segurança (backup), seu armazenamento e restauração resolve estabelecer norma de cópias de segurança nos seguintes termos:

Art. 1º Esta norma tem por objetivo estabelecer, no âmbito da Universidade Federal de Alfenas – UNIFAL-MG, diretrizes para o serviço automatizado de cópias de segurança (backup), armazenamento e restauração (restore) dos dados, estruturados e não estruturados, sob a guarda do Núcleo de Tecnologia da Informação – NTI, visando garantir a segurança, integridade e disponibilidade dos mesmos, evitando que informações sejam permanentemente perdidas ou danificadas em caso de algum incidente, seja ele físico, lógico, ambiental ou falha humana.

Art. 2º Para efeito desta normativa, entende-se por:

I – Administrador de Backup: servidor efetivo do quadro da UNIFAL-MG responsável por quaisquer dos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de cópia, armazenamento e restauração de dados;

II – Dado: qualquer registro de conteúdo armazenado em meio magnético. Pode compreender aplicativos/sistemas, dados propriamente ditos (documentos, mensagens de correio eletrônico - e-mails, arquivos, bancos de dados), conteúdo multimídia (imagem, vídeo, áudio) ou qualquer outro conteúdo passível de armazenamento em meio magnético no formato digital;

III - Dado Estruturado: dado que passou por processo de modelagem, geralmente residente em tabelas componentes de bancos de dados ou arquivos acessados por aplicações;

IV - Dado não Estruturado: arquivos, documentos, mensagens de correio eletrônico (e-mails), conteúdo multimídia;

V – Backup: cópia de segurança gerada e armazenada para possibilitar o acesso ou recuperação futura de dados. O termo também pode ser associado ao processo como um todo: backup (cópia), armazenamento e restore (restauração);

VI – Backup Completo (full): modalidade de backup na qual todos os dados são copiados integralmente;

VII – Backup Diferencial: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo são copiados;

VIII – Backup Incremental: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup (de qualquer tipo) são copiados;



IX – Restore: procedimento no qual os dados armazenados em um backup são restaurados para um disco ou outra mídia através da qual podem ser acessados por usuários ou aplicações;

X - Mídia: meio físico no qual efetivamente armazenam-se os dados de um backup (discos, storages, fitas, cartuchos, servidores);

XI - Software de Backup: conjunto de programas especializados no processamento e controle dos backups;

XII - Janela de Backup: período de tempo requerido para a geração de um backup (completo, diferencial ou incremental);

XIII – Período de Retenção: tempo em que o conteúdo da mídia de backup deve ser preservado;

XIV – Serviços de missão crítica: Serviços cuja perda de dados, por menor que seja, gere prejuízo incalculável à instituição.

Art. 3º Os seguintes princípios e diretrizes deverão ser adotados na gestão do serviço de backup:

I – Deve ser executado regularmente para minimizar e sempre que possível evitar as perdas de trabalho executado caso algo indesejado aconteça;

II - O serviço deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restauração de dados;

III - Utilizar recursos adequados para a geração de cópias de segurança para garantir que toda informação e sistemas essenciais possam ser recuperados após uma perda de dados;

IV - Registrar informações completas e exatas das cópias de segurança em documentação apropriada;

V - Todas as aplicações corporativas sob a responsabilidade do NTI, com arquivos e/ou dados armazenados nos servidores e bancos de dados disponibilizados na infraestrutura do NTI, terão asseguradas a execução de rotina de backup, de acordo com esta política;

VI - Esta norma não se aplica aos dados e sistemas locais, computadores de usuários ou máquinas virtuais, mesmo que hospedadas na infraestrutura do NTI, cabendo a responsabilidade do backup ao usuário responsável pelo dado, a não ser que explicitado em contrário em documento complementar;

VII – O armazenamento dos backups deve obrigatoriamente possuir redundância em local fora do Datacenter do NTI.

Art. 4º São atribuições do Administrador de Backup:

I - Propor modificações visando o aperfeiçoamento desta política de backup;

II – Criar, manter e monitorar os backups;

III - Configurar o software de backup bem como tudo o que for necessário para a sua execução e a realização correta das cópias de segurança;

IV - Criar e manter as mídias de armazenamento;

V - Testar periodicamente os procedimentos do backup e restore;

VI - Criar notificações e relatórios administrativos;

VII - Verificar periodicamente os relatórios gerados pelo software de backup;

VIII – Restaurar os backups em caso de necessidade;



IX - 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;

X - Fazer manutenções periódicas dos dispositivos de backup;

XI – Definir de maneira formal, juntamente com o responsável pelo dado a ser copiado, quais diretórios, arquivos e dados devem ou não ser incluídos nos backups.

Parágrafo único. As atribuições do Administrador de Backup ficarão a cargo dos servidores lotados na Gerência de Segurança da Informação/NTI, podendo ser delegadas formalmente em comum acordo a outro servidor lotado na Gerência de Redes e Infraestrutura/NTI, quando necessário.

Art. 5º Os procedimentos de backup deverão ser atualizados formalmente junto ao Administrador de Backup quando houver:

I - Novos aplicativos/sistemas desenvolvidos e/ou instalados.

II - Novos locais de armazenamento de dados ou arquivos.

III - Novas instalações de bancos de dados ou servidores.

IV - Novos serviços de Tecnologia da Informação disponibilizados formalmente pelo NTI à comunidade de usuários;

V - Novas informações que necessitem de proteção através de backups.

Art. 6º A execução do backup obedecerá as seguintes regras:

I - O backup deverá ser programado para execução automática preferencialmente em horários de menor ou nenhuma utilização dos sistemas e da rede, sendo entre 22:00 e 06:00h, de segunda à sexta e, aos sábados e domingos durante todo o dia;

II - Para todos os backups realizados com sucesso, deverá ser gerado um extrato automatizado pela própria ferramenta de backup, confirmando a execução do mesmo e enviado, via e-mail, ao Administrador de Backup para sua conferência;

III – Para os backups que apresentarem falhas, o administrador 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 os clientes de backup, a causa da falha, a ação corretiva adotada e qual parte do backup ficou comprometida;

IV - Os backups serão realizados de maneira contínua em mídias próprias e exclusivas para armazenamento de dados;

V – Os backups poderão ter a periodicidade contínua, diária, semanal, mensal e anual;

VI - Os backups semanais, mensais e anuais devem ser realizados na modalidade completo, para que os dados possam ser recuperados integralmente sem a necessidade de outros backups. Estes deverão ser testados no prazo máximo de uma semana após a sua execução. A execução destes backups se dará:

a) no sábado, para backups semanais, referindo-se à semana que se encerra;

b) no primeiro dia de cada mês, para backups mensais, referindo-se ao mês anterior;

c) no primeiro dia do mês de janeiro, para backups anuais, referindo-se ao ano anterior.

VII - Em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, o Administrador de Backup deverá adotar as providências no sentido de salvaguardar as informações através de outro mecanismo, como por exemplo: cópia dos dados para outro servidor, execução do backup em horário de produção, entre outros, sempre priorizando a segurança dos dados.

VIII – As solicitações para inclusão de dados no backup deverão ser feitas formalmente através de processo. A solicitação deverá conter informações que identifiquem corretamente o dado, como: o(s) nome(s) do(s) arquivo(s) e/ou diretório(s), banco(s) de dado(s), servidor(es) etc, bem como a periodicidade dos backups e o período de retenção das cópias. Todos os backups criados deverão ser testados assim que forem criados. Os testes deverão incluir um backup e uma restauração para comprovar a eficácia do backup.

§ 1º Entende-se por backup de periodicidade contínua aquele executado continuamente na menor janela possível, respeitando-se o limite máximo de um backup por hora;

§ 2º Os casos que necessitem de periodicidades diferentes deverão ser protocolados para análise pela Gerência de Segurança da Informação. As solicitações deverão conter a descrição completa da necessidade do backup, tipo e local do dado, modalidade do backup, periodicidade, período de retenção e demais informações que forem necessárias.

Art. 7º São passíveis de execução de backup:

I - Arquivos de configurações de sistemas operacionais e aplicativos/sistemas instalados em servidores;

II - Arquivos de aplicativos/sistemas desenvolvidos pela UNIFAL-MG ou quaisquer outros não descritos neste, mas que a perda de suas informações gere prejuízo para a instituição;

III - Dados e configurações de banco de dados;

IV - Arquivos de usuários e institucionais (documentos e e-mails);

V - Arquivos de LOG dos aplicativos/sistemas, inclusive LOG da ferramenta de backup.

Art. 8º Não são passíveis de execução de backup:

I - Arquivos de sistemas operacionais ou de aplicativos/sistemas que podem ser recolocados através de uma nova instalação;

II – Arquivos contidos na pasta padrão de arquivos temporários do sistema operacional;

III - Arquivos salvos nas unidades locais das estações de trabalho dos usuários;

IV - Arquivos da área de transferência e lixeira.

Art. 9º As solicitações de restauração de dados deverão ser feitas formalmente através do Sistema de Ordem de Serviço – SOS. A solicitação deverá conter informações que identifiquem corretamente o dado, como: o(s) nome(s) do(s) arquivo(s) e/ou diretórios(s), banco(s) de dado(s), servidor(es) e demais dados que se fizerem necessários, além da data do dado que se pretende ter acesso, respeitando-se os períodos de retenção definidos nesta política e a janela de backup.

Art. 10º A restauração de um dado respeitará a seguinte referência:

I - Arquivos de configurações de sistemas operacionais e LOGs serão recuperados e entregues à Gerência de Redes e Infraestrutura para que esta recupere a informação no respectivo servidor;

II - Dados, configurações de bancos de dados e arquivos de aplicativos/sistemas serão restaurados e entregues à Gerência de Desenvolvimento e Gestão da Informação para que esta recupere a informação no banco de dados ou no respectivo servidor;

III - Arquivos de usuários e institucionais serão restaurados e colocados nos locais indicados pelo

usuário, sempre que possível;

IV - E-mails serão restaurados para as suas respectivas contas no servidor de e-mails institucional.

Art. 11. Qualquer solicitação que envolva outros equipamentos e/ou dados, software de backup, local de armazenamento de mídias, alteração na frequência e/ou periodicidade do backup, horário de geração da(s) cópia(s) ou no tempo de retenção de um backup deverá ser analisada previamente pelo NTI, quanto à sua viabilidade, em prazo negociado entre as partes.

Art. 12. Quaisquer procedimentos programados nos equipamentos servidores ou em quaisquer dispositivos de armazenamento, bem como atualização de aplicativos/sistemas ou banco de dados que impliquem riscos à integridade de algum tipo de dado, somente deverão ser executados após a realização de um backup ou a confirmação da existência de um backup atual dos dados do equipamento, aplicativo/sistema ou banco de dados. O Administrador do Backup deverá ser avisado antecipadamente para que possa, caso seja necessário, realizar um backup prévio dos dados, antes da execução do procedimento.

Art. 13. O período de retenção dos backups obedecerá os seguintes prazos:

I – Periodicidade Contínua: três últimas cópias;

II – Periodicidade Diária: sete últimos dias;

III – Periodicidade Semanal: quatro últimas semanas;

IV – Periodicidade Mensal: doze últimos meses;

V – Periodicidade Anual: cinco últimos anos.

§ 1º Expirado o prazo de retenção dos backups armazenados, a mídia poderá ser reutilizada ou destruída;

§ 2º Retenções diferentes do padrão definido nesta normativa deverão ser formalizadas através de processo para análise pela Gerência de Segurança da Informação/NTI.

Art. 14. Por padrão, os backups serão executados da seguinte maneira:

I – Para arquivos de configurações de sistemas operacionais e aplicativos/sistemas instalados em servidores será executado backup completo com periodicidade diária;

II – Para arquivos de aplicativos e sistemas desenvolvidos pela UNIFAL-MG ou quaisquer outros não descritos neste, mas que a perda de suas informações gere prejuízo para a instituição, será executado backup completo com periodicidade diária;

III – Para dados e configurações de banco de dados, será executado backup completo com periodicidade diária e backup completo com periodicidade mensal;

IV – Para arquivos institucionais e de usuários:

a) Documentos: backup completo com periodicidade semanal e backup incremental com periodicidade diária;

b) e-mails: backup completo 3 (três) vezes por semana com retenção semanal.

V – Para arquivos de LOG dos aplicativos/sistemas, inclusive LOG da ferramenta de backup e restore, será executado backup completo com periodicidade semanal e backup incremental com

periodicidade diária;

VI – Para os arquivos de aplicativos/sistemas e/ou bancos de dados não desenvolvidos pela UNIFAL-MG o backup deverá seguir as recomendações sugeridas pelo desenvolvedor e/ou fabricante e, caso não exista nenhuma recomendação, o backup seguirá o descrito nos incisos II e III deste artigo;

VII – Para os sistemas e/ou dados considerados de missão crítica pelo Comitê de Governança Digital, o backup será executado de maneira contínua concomitantemente ao backup diário.

Art. 16. Esta norma faz parte da Política de Segurança da Informação da UNIFAL-MG.

Art. 17. Casos omissos a este documento devem ser tratados pelo Comitê de Governança Digital.



Prof. Sandro Amadeu Cerveira

Presidente do CGD