MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI

RESOLUÇÃO Nº 06 - CGIRC, DE 17 DE OUTUBRO DE 2022

Estabelece a política de retenção de arquivos de backup dos sistemas institucionais da UFVJM mantidos pela STI.

O COMITÊ DE GOVERNANÇA INTEGRIDADE, RISCOS E CONTROLE DA UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI, no uso das atribuições legais e regulamentares, tendo em vista o que consta do processo 23086.012079/2022-38 e o que fora deliberado na 39ª reunião,

CONSIDERANDO o vasto uso de sistemas administrativos e acadêmicos;

CONSIDERANDO que a quantidade de dados produzida nesses sistemas é vultosa, demandando grande volume de recursos computacionais de armazenamento;

CONSIDERANDO que os recursos computacionais para armazenamento das cópias de segurança são limitados.

CONSIDERANDO as diretrizes estratégicas do Comitê de Governança, Integridade, Riscos e Controle, a saber:

1. Institucionalizar estruturas adequadas de governança, integridade, gestão de riscos e controles internos;

2. Garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;

3. Monitorar e avaliar a implementação das ações, o uso dos recursos e a entrega dos serviços inseridos no PDTIC, com o objetivo de atender às estratégias e aos objetivos institucionais;

4. 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;

5. Fomento à Política de Segurança da Informação da Universidade Federal dos Vales do Jequitinhonha e Mucuri;

6. Elaboração, controle de projetos de TI e planos de ação para o alcance das metas do PDTIC;

7. Coordenar e implementar políticas, diretrizes e normas que assegurem a adoção de boas práticas de governança de tecnologia da informação.

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 elaboração e a necessidade de assegurar conformidade com 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 ao CGIRC;

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 307/2020-TCU/Sefti, de 24/10/2020, 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.

CONSIDERANDO ainda que a instituição não possui sistema de combate à incêndio na infraestrutura de data center, estando assim em alto risco a danos e perdas de dados em caso de incidente do gênero.

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Estabelecer a Política de Backup e Restauração de Dados dos sistemas institucionais da UFVJM, 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, mantidos na infraestrutura de Tecnologia da Informação (TI) sob responsabilidade da STI.

Art. 2º Para fins desta resolução, são considerados os seguintes termos:

I – Backup: cópia de dados de uma mídia de armazenamento principal em outra mídia, a partir da qual seja possível a restauração dos dados caso necessário, correspondente a um momento passado (ano, mês, dia, hora e minuto).

II – Backup completo (full): cópia completa de uma base de dados em uma execução da rotina de backup.

III – Backup incremental: cópia da porção nova da base de dados (arquivos novos ou modificados) em relação ao último backup.

IV – Responsável pelo Serviço: colaborador da UFVJM responsável pela operação de determinados serviços ou recursos computacionais da Universidade;

V - 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;

VI - Catálogo de Sistemas: Listagem com todos os serviços ativos oferecidos pela STI, que necessitam de backup;

VII - Colaborador: integrante do quadro de funções da STI;

VIII - Equipe de backup: equipe técnica responsável pelos procedimentos de configuração, execução, monitoramento e testes de backup e restauração;

IX - Retenção: período em que o conteúdo da mídia de backup deve ser preservado;

X - Recuperação de desastre: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

XI - RPO: (do inglês, Recovery Point Objective) quantidade de informação cuja perda é tolerável, no caso de indisponibilidade nos serviços.

XII - RTO: (do inglês, Recovery Time Objective) quantidade de tempo que as operações levam para estarem acessíveis, após uma indisponibilidade;

XIII - Serviço com backup: todo ativo que possui informações ou dados e incluído nos serviços de backup conforme as regras de inclusão;

CAPÍTULO II

DAS GOVERNANÇA E RESPONSABILIDADES

Art. 3º. A governança e a responsabilidade na garantia do pleno funcionamento do serviço de backup dos sistemas institucionais da UFVJM deverá ser da STI.

Art. 4º A equipe de backup será a responsável pelo serviço de backup, podendo delegar 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. A Equipe de Backup deve definir os modelos de documentos a serem produzidos em todo o processo de backup e restauração. Também determinará a periodicidade de relatórios técnicos, os quais avaliem todo o processo de restauração efetuado, além de reportar ao dirigente máximo da STI, relatório mensal.

Art. 5º 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, juntamente com os responsáveis pelo serviço, os procedimentos de restauração;

IV. Configurar a ferramenta de backup conforme necessidade dos serviços;

V. Configurar e operar, juntamente com os responsáveis pelo serviço, os ambientes de Restauração;

VI. Criar e testar procedimentos a fim de operacionalizar as atividades;

VII. Gerenciar dispositivos e mídias de backup;

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, juntamente com os responsáveis pelos serviços, os cenários de restauração;

XII. Verificar periodicamente os relatórios gerados pelas ferramentas 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 destinadas aos mesmos;

XVII. Comunicar ao Responsável pelo Serviço as falhas e ocorrências de anomalias durante os procedimentos de backup e restauração;

XVIII. Definir o procedimento para Solicitação do Serviço de Backup;

XIX. Definir o procedimento para Solicitação do Serviço de Restauração;

Art. 6º 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 conforme o Anexo I.

§2º Poderá ocorrer adição ou remoção de serviços, conforme normativos internos e legislações futuras.

§3º 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).

§4º 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.

§5º 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. 7º Os procedimentos de backup deverão ser atualizados, ou novos poderão ser criados, 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 à Equipe de Backup, pelo Responsável pelo Serviço.

Art. 8º Para a especificação de um backup, o Responsável pelo Serviço deverá efetuar uma solicitação de backup, contendo as informações necessárias, no sistema de Controle de Chamados (GLPI) para a Equipe de backup.

§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. 9º A configuração e monitoração das funcionalidades relativas ao backup de banco de dados será de responsabilidade do Responsável pelo Serviço.

Art. 10 A UFVJM deverá disponibilizar 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.

Art. 11 A STI deverá realizar monitoramento ativo dos recursos computacionais existentes quanto à disponibilidade de espaço, em se tratando de armazenamento on-premise (local).

§1º. A STI deverá tomar providências para aumento dos recursos computacionais quando o nível de utilização da capacidade de armazenamento se aproximar de sua capacidade total, considerando o limite mínimo de 80%.

§2º. Na situação de utilização da infraestrutura computacional em nuvem pública, a UFVJM deve garantir o cumprimento do Art. 10.

CAPÍTULO III

DA FREQUÊNCIA E RETENÇÃO DOS DADOS

Art. 12. Os backups dos serviços de TIC da UFVJM mantidos pela STI deverão ser realizados utilizando-se uma das seguintes frequências temporais:

I – diária;

II – semanal;

III – mensal; ou

IV – anual.

Art. 13 As definições de retenção de arquivos de backup se diferenciam de acordo com o conjunto e tamanho de dados a serem alvos de backup, além de considerar os sistemas aos quais tais dados estão relacionados.

Art. 14 As categorias de sistemas estão definidas da seguinte maneira:

I - Categoria 1: serviços de infraestrutura de TI e desenvolvimento de sistemas, tais como relacionados a redes e segurança da informação, virtualização de servidores, telefonia, armazenamento, backup, gestão de projetos, versionamento de código.

II - Categoria 2: serviços destinados à comunidade acadêmica de maneira ampla, tais como sistemas de gestão acadêmica e administrativa, controle de frequência, gestão eletrônica de processos, portal institucional e de acervo acadêmico institucional.

III - Categoria 3: serviços de menor abrangência, relacionados a demandas específicas de alguma unidade administrativa, acadêmica ou outro órgão da UFVJM.

Art. 15 Os procedimentos de retenção de backups relacionados aos sistemas enquadrados em cada uma das categorias listadas no art. 4.º se encontram assim definidas:

I - Categoria 1: uma cópia de backup completo por dia, dos últimos 7 dias; uma cópia de backup completo por semana, das últimas 4 semanas; uma cópia de backup completo por mês, dos últimos 3 meses.

II - Categoria 2: uma cópia de backup completo por dia, nos últimos 7 dias; uma cópia de backup por semana, das últimas 4 semanas; uma cópia de backup por mês, dos últimos 6 meses.

III - Categoria 3: uma cópia de backup completo por dia, nos últimos 7 dias; uma cópia de backup completo por semana, das últimas 4 semanas; uma cópia de backup completo por mês, dos últimos 3 meses.

Art. 16 Excepcionalmente, poderá haver alguma regra de retenção diferenciada, para algum conjunto de arquivos, de algum sistema enquadrado em alguma das categorias mencionadas neste artigo.

Parágrafo único: a exceção mencionada no caput deste artigo deverá ser solicitada à Superintendência da STI, que analisará o pedido consultando as seções envolvidas, emitindo parecer a ser referendado pelo CGIRC.

CAPÍTULO IV

DA DEFINIÇÃO PARA SISTEMAS NÃO MANTIDOS PELA STI

Art. 17 Para os sistemas que não são mantidos na infraestrutura de TI sob responsabilidade da STI, mas que sejam mantidos por alguma unidade administrativa ou acadêmica da UFVJM, é responsabilidade da referida unidade realizar as cópias de backup e retê-las, de acordo com o necessário.

Parágrafo único: para os sistemas mencionados no caput deste artigo, recomenda-se a adoção no mínimo da política de retenção adotada para a Categoria III dos sistemas institucionais, conforme descrito no artigo 5º.

CAPÍTULO V

DO PROCEDIMENTO DE RESTAURAÇÃO

Art. 18 A recuperação dos backups deverá obedecer às seguintes orientações:

I. Havendo necessidade de recuperar arquivos, o usuário 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. Sendo o chamado aberto pelo usuário final, este será encaminhado ao Responsável pelo Serviço para indicação das informações necessárias à restauração dos dados.

IV. 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);

V. 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;

VI. A restauração dos arquivos somente será possível nos casos em que o arquivo tenha sido atingido pela estratégia de backup, conforme registro no Anexo II. Os arquivos criados e eventualmente apagados ou alterados dentro de um intervalo não compreendido pelo backup, não serão passíveis de recuperação.

CAPÍTULO VI

DOS TESTES DE RESTAURAÇÃO

Art. 19 As cópias de segurança armazenadas deverão ser testadas semestralmente, e a cada período serão testados domínios de dados distintos, a fim de percorrer anualmente todos os itens descritos no Capítulo II.

§1º. A equipe de backup, juntamente com o Responsável pelo Serviço, deverá definir quais domínios de dados serão testados a cada período.

§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 à equipe de backup durante o período de testes.

Art. 20 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 Dirigente da STI, para posteriormente ser publicado em portal de conteúdo referente à Administração do Backup.

CAPÍTULO VII

DIRETRIZES DE OPERAÇÃO

Art. 21 A criação e operação dos backups deverá obedecer às seguintes orientações:

I. Criação de backups:

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

II.Operação de backups:

a. o backup deverá ser monitorado pela Equipe de Backup;

b. Para todos os backups realizados com sucesso, deve ser gerado um extrato automatizado pela própria ferramenta de backup, confirmando a execução do mesmo;

c. Aos backups que apresentarem falhas, a Equipe de Backup deverá criar um relatório de "Acompanhamento de backup", em que deverá constar a data, os horários de início e término, e notificar o responsável pelo serviço, informando a causa da falha e a ação corretiva adotada.

Art. 22 Os backups deverão ser realizados seguindo as regras de acordo com cada nível de serviço, considerando a classificação dos dados.

I. Em caso de falha em algum procedimento de backup, a Equipe de Backup deverá adotar as providências para identificar a causa que motivou a falha, consultando o Responsável pelo Serviço quando necessário. Tão logo a causa da falha seja corrigida e demais condições para realizar o backup sejam reunidas, um novo procedimento deve ser realizado para averiguar se a falha foi resolvida.

Art. 23 Os backups mensais de todas as categorias deverão ser testados, no prazo máximo de um ano, após a sua execução.

Art. 24 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. 25 O backup off-site deverá armazenar os dados em fita ou storage, em qualquer unidade da UFVJM, atendendo os requisitos deste artigo.

§1º A armazenagem do backup off-site deve estar obrigatoriamente fora do campus onde se encontra 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 adotados pela STI, e aprovado pelo CGIRC.

Art. 26 O procedimento de criptografia das cópias de segurança deverá ser feito em conformidade com um utilitário (recomendação: GnuPG).

Art. 27 Fica estabelecido o prazo de 90 (noventa) dias, a contar da data de publicação desta resolução, para a adoção das providências necessárias para prover uma infraestrutura à implementação plena desta política de backup pela Universidade Federal dos Vales do Jequitinhonha e Mucuri.

Art. 28 Os casos omissos serão avaliados pela STI e caso necessário, encaminhando ao CGIRC para deliberação, no âmbito das suas competências.

Art. 29 Esta resolução entra em vigor na data de sua publicação

JANIR ALVES SOARES

Presidente do Comitê de Governança, Integridade, Riscos e Controles Internos

ANEXO I À RESOLUÇÃO Nº 06 - CGIRC, DE 17 DE OUTUBRO DE 2022

CATÁLOGO DOS SISTEMAS INSTITUCIONAIS POR CATEGORIA

Categoria	Identificação do Sistema
I (infraestrutura)	VmWare Vcenter
	ProxMox
	Avamar
	Gitlab
	Redmine
	Firewalls
	Serviço de Autenticação de Rede
	Rancher,
	Fone@RNP
	CFTV
II (sistemas de ampla abrangência)	Sistema de Controle de Chamados - GLPI
	SIP / SEI!
	Sistema de Gestão Integrada - e-CAMPUS
	REP
	Sistema de Controle de Chamadas de Ingresso Acadêmico - Pressiga
	Portais Institucionais
	Portal de Assinatura Digital - Assina@UFVJM

	Sistema de Analytics de Acessos - Matomo
	Portal de Documentação de Sistemas e Serviços
	Portal de Dados Abertos - CKAN
	Sistema de automação para envio de e-mails por fluxo - Mautic
	Sistemas de Inscrição e Seleção - Copese
	Sistemas de Inscrição e Seleção - PRPPG
	Sistema de Turmas Online - Moodle
	Portal de Gestão de Revistas Eletrônicas - OJS
III (demandas específicas)	SIEXC
	Sistema de Catalogação para Bibliotecas - Pergamum
	Sistema de Gestão de Dados Geoespaciais - Geonode

ANEXO II À RESOLUÇÃO Nº 06 - CGIRC, DE 17 DE OUTUBRO DE 2022

MODELO RELATÓRIO DE EXECUÇÃO DE RESTAURAÇÃO

1. Data de Execução da Restauração:
2. Sistema / serviços envolvidos:
3. Porção / Tipo de dados envolvidos: (banco de dados, sistemas de arquivos, discos virtuais, etc)
4. Atores Envolvidos:
    - 4.1. Responsável(is) da Equipe de Backup e Restore:
    - 4.2. Responsável(is) pela administração do Sistema / Serviço:
5. Horário de Início do Procedimento:
6. Horário de Término do Procedimento:
7. Resultado do procedimento:
    - 7.1. __ Concluído com Êxito
    - 7.2. __ Concluído com Ressalvas
    - 7.3. __ Concluído com Falha
8. Observações:
9. Data prevista para a próxima Execução de Restauração:

Criado por otavio.gabriel, versão 5 por otavio.gabriel em 17/10/2022 10:58:07.