MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais
Reitoria

PORTARIA Nº 4000/IFMG, DE 07 DE JULHO DE 2025

Dispõe sobre a instituição da Política de Backup e Restauração de Dados Digitais, que trata sobre diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela área de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda no IFMG.

O **REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS**, no uso das atribuições que lhe são conferidas pelo Estatuto da Instituição, republicado com alterações no Diário Oficial da União do dia 08/05/2018, Seção 1, Páginas 09 e 10, e pelo Decreto de 11 de setembro de 2023, publicado no DOU de 12 de setembro de 2023, Seção 2, Edição nº 174, página 01

Considerando a Portaria SGD/MGI nº 852, de 28 de março de 2023 que Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI;
Considerando a Política de Segurança da Informação do IFMG;

Considerando a deliberação do Comitê de Segurança da Informação do IFMG e o que consta no Processo nº **23208.003392/2024-13**,

RESOLVE

Instituir a Política de Backup e Restauração de Dados Digitais do IFMG

Política de Backup e Restauração de Dados Digitais

1. Objetivo

1. A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela área de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda no IFMG, para se manter a continuidade do negócio.

2. No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. O presente documento apresenta a Política de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais, visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da informação e Comunicação - PoSIC – IFMG.

2. Escopo

3. Esta política se aplica a todos os servidores, sistemas e soluções de TI que são instaladas e operadas dentro da própria infraestrutura física da instituição, incluindo dados que foram armazenados em um serviço de nuvem pública ou privada gerenciado pelo IFMG.

4. A definição de dados críticos e o escopo desta norma de backup serão revisados sempre que necessário ou a cada 2 anos, após a data de aniversário da publicação desta Norma.

5. Esta política se aplica a todos os servidores do IFMG que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e usam sistemas e equipamentos de TI ou que criam, processam ou

armazenam dados de propriedade do IFMG.

6. A salvaguarda dos dados em formato digital pertencentes a serviços de TI do IFMG, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

7. Não serão salvaguardados nem recuperados dados:

■ Armazenados localmente, nos microcomputadores dos usuários;

■ Armazenados em quaisquer outros dispositivos móveis ou mídias externas/removíveis; e

■ Armazenados em data centers de terceiros (inclusive nuvem) que não são armazenados e administrados pela equipe da TI.

8. Em todos os casos referentes ao item 7, os dados ficam sob a responsabilidade do indivíduo que usa o(s) dispositivo/recurso(s) ou presta o serviço externo para o IFMG.

3. Termos e Definições

BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

CUSTODIANTE DA INFORMAÇÃO - Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

INFRAESTRUTURA PRIMÁRIA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

Recovery Point Objective (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

Backup Completo (Full): modalidade de backup na qual os dados são copiados em sua totalidade;

Backup completo sintético (Full Sintético): modalidade de backup na qual é gerado um arquivo semelhante ao Backup Completo a partir dos dados incrementais e Full realizados anteriormente, poupando recursos de rede e armazenamento;

Backup Diferencial: modalidade de backup na qual somente os

arquivos novos ou modificados desde o último backup completo são copiados;

Backup Incremental: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup – seja completo, diferencial ou incremental - são copiados.

Clientes de backup: todo equipamento servidor no qual é instalado o agente de backup;

Recuperação de Desastre: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

Formatação de baixo nível: tipo de método de limpeza de HD que apaga todos os vestígios de arquivos do disco por meio de ação mecânica

MI-TI Backup e Restore

Documento padrão para a descrição dos procedimentos operacionais para a execução do Backup e restore.

4. Referência legal e de boas práticas quando aplicável

[**Orientação**	**Seção**
Acórdão 1.109/2021-TCU-Plenário	Em sua íntegra
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra

Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI;	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Guia do Framework de Privacidade e Segurança da Informação	Controle 11
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

5. Declarações da política

Dos princípios gerais

9. Esta Política de Backup e Restauração de Dados deve estar alinhada com as políticas internas do IFMG.

10. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

11. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

12. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

13. O armazenamento de backup deve ser realizado em um prédio/unidade distinta da infraestrutura crítica. É desejável que se tenha um site de backup em um local distinto remoto ao da unidade da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

14. Recomenda-se que a infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

15. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.

16. Em situações em que são usadas mídias externas (Fitas ou HD’s) ou nuvem para armazenar backups, e dados confidenciais, as cópias de segurança devem ser protegidas através de encriptação.

Da frequência e retenção dos dados

17. Os backups dos serviços de TI primários e secundários do IFMG devem ser realizados utilizando-se as seguintes frequências temporais, que estarão definidas no MI – Backup e Restore:

I. Diária;

II. Semanal;

III. Mensal;

IV. Anual.

18. Especificidades dos serviços críticos e não críticos podem demandar

frequência e tempo de retenção diferenciados.

19. Os ativos envolvidos no processo de backup são considerados ativos primários para a organização.

20. A solicitação de salvaguarda dos dados referentes aos serviços de TI primários e aos serviços de TI secundários, deve ser realizada pelos responsáveis, com a anuência prévia e formal da gestão, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I. Escopo (dados digitais a serem salvaguardados);

II. Tipo de *backup* (completo, incremental, diferencial);

III. Frequência temporal de realização do backup (diária, semanal, mensal, anual);

IV. Retenção;

V. RPO;

VI. RTO.

21. A alteração das frequências e tempos de retenção definidos no MI – Backup e Restore deve ser precedida de solicitação e justificativa formais encaminhadas aos responsáveis pela execução do Backup. A aprovação para execução da alteração depende da anuência Infraestrutura de TI.

22. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

Do uso da rede

23. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do IFMG, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI do IFMG.

24. A execução do backup deve concentrar-se, preferencialmente, no

período de janela de backup.

25. O período de janela de backup deve ser determinado pela equipe de Infraestrutura em conjunto com a área técnica responsável pela administração da rede de dados do IFMG.

Do transporte e armazenamento

26. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

I. A criticidade do dado salvaguardado;

II. O tempo de retenção do dado;

III. A probabilidade de necessidade de restauração;

IV. O tempo esperado para restauração;

V. O custo de aquisição da unidade de armazenamento de backup;

VI. A vida útil da unidade de armazenamento de backup.

27. O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

28. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.

29. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

30. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura,

umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

31. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutiliza-los, atentando-se ao descarte sustentável e ambientalmente correto.

Dos testes de backup

32. Os backups serão verificados periodicamente:

I. Diariamente, os logs de backup serão revisados conforme alertas recebidos via e-mail e/ou diretamente na ferramenta, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.

II. Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.

III. A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.

IV. Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

33. Os testes de restauração dos backups devem ser realizados, por amostragem anualmente, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção e para os sistemas críticos pelo menos semestralmente, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.

34. Verificar se foi atendido os níveis de serviço pactuados, em condições normais do ambiente, tais como os Recovery Time Objective – RTOs.

35. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso

36. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo Comitê de Segurança da Informação.

37. Para a execução dos testes de restore, que deve ser realizada ao menos uma vez ao ano para cada sistema crítico, todas as evidências devem ser armazenadas.

Do Descarte da Mídia

38. A mídia de backup será retirada e descartada conforme descrito neste documento:

I. A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.

II. Deve ser garantida a sanitização (formatação) de mídias de acordo com o tipo de equipamento e nível de sensibilidade dos dados.

III. A TI garantirá a destruição física da mídia antes do descarte.

IV. O uso de terceiros para descarte e certificação segura de descarte é recomendado

V. Deve ser garantida a sanitização (formatação) de mídias de acordo com o tipo de equipamento e nível de sensibilidade dos dados.paráveis

Das Responsabilidades

39. São atribuições e responsabilidades da Alta Administração do IFMG.

I. Acompanhar e auxiliar no preenchimento dos documentos de operacionalização do backup fornecidos pelo Setor de Tecnologia da Informação;

II. Prover apoio administrativo e, se possível, financeiro para os servidores responsáveis pela administração e operacionalização dos backups.

40. São atribuições e responsabilidades da equipe de administração do Sistema de Backup da DTI:

I. Configurar e administrar as ferramentas (sistema/software) de backup;

II. Definir os procedimentos de criação e restore das rotinas de backup, a criticidade, escalabilidade e prioridade dos JOBS de backup;

III. Pesquisar e propor novas soluções de sistemas de backups com tecnologia de ponta e que atendam melhor aos objetivos da instituição, bem como prever renovações de licenças de software utilizados nos backups.

IV. Propor à Direção da DTI ou ao seu Conselho Consultivo, alterações, correções ou anulações, na sua totalidade ou em parte, da Norma de Backup vigente na Instituição.

V. Solicitar à Direção da DTI, sempre que necessário, treinamentos e técnicas para a equipe de operação do Sistema de Backup da DTI.

VI. Responder, de forma institucional as instâncias superiores do IFMG, sobre o serviço de backup além de manter a Diretoria de Tecnologia da Informação, ciente sobre o andamento do serviço e das futuras necessidades de expansão do mesmo a fim de que os serviços de backup sejam mantidos de forma ininterrupta e que atenda a toda a Comunidade acadêmica do IFMG.

41. São atribuições e responsabilidades da equipe de operação:

I. Criar, testar e implantar os scripts (JOBS) de backups;

II. Efetuar periodicamente rotinas de testes de todo o sistema de backup com o objetivo de manter todo o sistema e seus periféricos em perfeito funcionamento;

III. Criar, etiquetar, gerenciar e manter a guarda das mídias magnéticas em local próprio e seguro, seguindo as condições físicas e ambientais explicitadas pelo fabricante dos equipamentos, tanto para a fitoteca local quanto para a fitoteca de segurança externas.

IV. Fazer a troca das mídias de backup no robô de backup retirando as mídias com armazenamento cheio por outras scratchs;

V. Quando identificado, fazer a troca das mídias defeituosas ou inservíveis por novas dentro do sistema;

VI. Mídias magnéticas descartadas após a certeza de que os dados

inseridos não são possíveis de ser recuperados por terceiros;

VII. Executar, programar a execução (data/hora) e restaurar as rotinas e os *JOBS* de backups;

VIII. Verificar diariamente os relatórios e arquivos de logs de execução dos backups gerados pelas ferramentas (softwares) de backups;

IX. Executar rotinas de testes do sistema de backup e de restore dos backups em disco e mídias magnéticas. Estas necessárias com o objetivo de validar que o backup realizado foi feito com sucesso e que sua recuperação/restore foi realizada para garantir que o processo obteve êxito.

42. Dos usuários do Servidor de Arquivos Institucional do IFMG (Controlador de Domínio):

I. É de inteira e única responsabilidade do usuário local, armazenar todo o conteúdo de informação digital relevante ao trabalho institucional nas unidades de armazenamento remotas (pastas de rede) mapeadas virtualmente nas estações de trabalho (quando houver), pois somente os dados contidos nestas pastas terão backup realizados pelo setor de TI.

II. O usuário responsável pela estação de trabalho local é o único responsável pela salvaguarda dos arquivos e dados digitais contidos no disco rígido local e portanto, o setor TI se exime da responsabilidade sobre a salvaguarda destes dados, os quais não são abarcados no Sistema de Backup administrado pelo setor de TI.

6. Procedimentos

43. Os documentos complementares relacionados a procedimentos e planos de backup/restore, deverão ser elaborados em até 90 dias após a publicação desta portaria.

7. Não conformidade

44. Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

ANEXO I

Concordância

Eu, _____, SIAPE nº _____, lotado(a) no setor _____, declaro, para os devidos fins, que:

1. **Li e entendi** a Política de Backup e Restauração de Dados Digitais do Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais (IFMG), e estou ciente das diretrizes, responsabilidades e procedimentos nela estabelecidos.

2. **Comprometo-me** a cumprir integralmente os termos dessa política, zelando pela correta utilização dos sistemas institucionais, bem como pela preservação e recuperação dos dados sob minha responsabilidade, conforme definido no documento.

3. Estou ciente de que o descumprimento das normas descritas poderá implicar em sanções administrativas, conforme previsto nas normativas internas do IFMG e demais legislações aplicáveis.

Local e data: _____

Assinatura: _____

Publicação: Transparência Ativa em 07 de julho de 2025

Documento assinado eletronicamente sob fundamentação, por:
RAFAEL BASTOS TEIXEIRA | Reitor

Data da Assinatura:
07 de julho de 2025 as 16:59 (America/Sao_Paulo)

Tipo de Documento:
Portaria

Autenticidade