DECISÃO N° Decisão 2/2024 - CGD/RT/IFMS

Campo Grande, 12 de setembro de 2024.

Processo nº 23347.006356.2024-17

Referência: **Aprovação da Política de Backup e Restauração de Dados Digitais do IFMS .**

Vistos,

1. A Presidente do Comitê de Governança Digital do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul - IFMS, no uso de suas atribuições legais e tendo em vista os documentos que instruem o presente processo;

2. APROVAR, Política de Backup e Restauração de Dados Digitais do IFMS, conforme deliberado na **3ª Reunião do Comitê de Governança Digital,** ocorrida no dia 22/08/2024.

Elaine Borges Monteiro Cassiano
Presidente do Comitê de Governança Digital - CGD/IFMS

Documento assinado eletronicamente por:

- **Elaine Borges Monteiro Cassiano**, **REITOR(A)** - **CD1** - **IFMS**, em 12/09/2024 11:10:17.

Este documento foi emitido pelo SUAP em 11/09/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifms.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 473733
Código de Autenticação: dce9f5e97d

Política de *Backup* e Restauração de Dados Digitais

Versão 1.0

Campo Grande, janeiro de 2024

Histórico de Versões

Data	Versão	Descrição	Autor
23/1/2024	1.0	Minuta da Política de *Backup*	Dirti

ÍNDICE

INTRODUÇÃO

A tecnologia desempenha um papel crucial em assegurar a disponibilidade e confiabilidade das informações, uma vez que as soluções de *backup* e restauração de dados evoluíram significativamente, oferecendo alternativas mais eficientes e seguras.

O Instituto Federal de Mato Grosso do Sul deve buscar utilizar tecnologias de ponta que atendam às suas necessidades específicas, garantindo a proteção dos dados e a rápida recuperação em caso de incidentes.

Além disso, a boa prestação de serviços ao cidadão está diretamente relacionada à política de *backup* e restauração de dados. Ao manter a integridade das informações, a instituição pode oferecer um atendimento mais ágil e preciso, contribuindo para a satisfação e confiança dos cidadãos que interagem com o IFMS.

Em resumo, a política de *backup* e restauração de dados digitais do IFMS está alinhada com as melhores práticas em tecnologia, visando a garantir a segurança e disponibilidade das informações, ao mesmo tempo em que contribui para a excelência na prestação de serviços à comunidade.

Política de *Backup* e Restauração de Dados Digitais

Responsável	Coordenação de Infraestrutura, Redes e Telecomunicações (Coirt)
Aprovado por	Comitê de Governança Digital (CGD) e Conselho Superior (Cosup)
Políticas Relacionadas	Política de Segurança da Informação e Comunicação do IFMS
Localização de armazenamento	https://www.ifms.edu.br/centrais-de-conteudo/documentos-institucionais/politicas <URL DO SITE>
Data da Aprovação	<Entra em vigor a partir da data de sua aprovação>
Data de revisão	-

Propósito

Art. 1º A Política de *Backup* e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam a segurança, proteção e disponibilidade dos dados digitais custodiados no Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul (IFMS) e formalmente definidos como de necessária salvaguarda.

Art. 2º Para se manter a continuidade do atendimento e prestação dos serviços públicos e internos desta Instituição e 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.

Art. 3º 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.

Art. 4º Ela envolve as diretrizes que visam proteger os dados contra perda, corrupção ou acesso não autorizado e seus procedimentos estão descritos no Manual de Instruções de *Backup* e *Restore* do IFMS.

Art. 5º O objetivo principal dessa política é assegurar a disponibilidade e confiabilidade das informações, tanto para o bom funcionamento interno da instituição quanto para a prestação de serviços de qualidade aos cidadãos.

Escopo

Art. 6º Esta política se aplica a todos os dados no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul, incluindo dados fora de suas dependências físicas, eventualmente, armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, nesse contexto, incluem documentos e arquivos institucionais, arquivos pessoais sob guarda da instituição (aqui, excluem-se os arquivos pessoais não ligados ao exercício da função pública dos servidores da Instituição, estejam eles em servidores de arquivo e, principalmente, nas estações de trabalho), bancos de dados e arquivos de

sistemas institucionais. A definição de dados críticos e o escopo desta política de *backup* serão revisados anualmente, sob a responsabilidade do CGD – CSTIC.

Art. 7º Os serviços de TI críticos do IFMS devem ser formalmente elencados pelo Comitê de Governança Digital (CGD).

Art. 8º Já ficam previamente estabelecidos o serviço de *e-mail* (*Google Workspace*), *Domain Name Server* (DNS), *links* de Internet, Microsoft *Active Directory*, servidores de arquivo do datacenter, redes sem fio e os sistemas Suap, Sistema Acadêmico, Portal Institucional, Central de Seleção, AVEA/Moodle, Sistema de Matrícula e Questionário Socioeconômico, como serviços críticos do IFMS.

Art. 9º Esta política se aplica aos servidores e estudantes que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e utilizam sistemas e/ou equipamentos de TI do IFMS ou que criam, processam e/ou armazenam dados de propriedade do IFMS.

Art. 10. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sob a responsabilidade do indivíduo que usa o(s) dispositivo(s). Também não é considerado de responsabilidade da Instituição manter ou ter o cuidado sobre os dados ali armazenados, considerando a natureza e objetivo institucional dos equipamentos em patrimônio do IFMS. A Dirti fortemente recomenda a utilização e armazenamento de quaisquer dados pessoais somente em dispositivos pessoais com constante zelo por cópias de segurança de seus arquivos.

Art. 11. Também não serão salvaguardados os dados armazenados/mantidos nos serviços de armazenamento (Google Drive, *e-mail* etc.) em nuvem. A Google dispõe de recurso de recuperação de arquivos deletados em definitivo no Google Drive e Gmail que pode ser utilizado em até 30 dias após a exclusão, porém mediante solicitação ao Suporte Google. Neste caso, solicita-se o contato com o Service Desk de TI do IFMS pelo *e-mail* sd@ifms.edu.br.

Art. 12. Os serviços críticos de servidor de arquivos em cada campus do IFMS terão a responsabilidade de salvaguarda/gestão por cada equipe de Tecnologia da Informação local.

Art. 13. Arquivos protegidos por direitos autorais como músicas, videoaulas, *softwares* etc., que não tenham sua devida autorização de uso, armazenados em dispositivos institucionais não só não serão salvaguardados como terão seu armazenamento removido sem aviso prévio.

Art. 14. Em casos diversos de armazenamento dos dados em formato digital pertencentes a serviços de TI do IFMS por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve-se deixar de forma garantida seus meios de proteção por meio de acordos ou contratos que formalizam a relação entre os envolvidos.

Termos e Definições

Art. 15. Para efeito desta Política, entende-se por:

I - *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.

II - 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.

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

IV - 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.

V - INFRAESTRUTURA CRÍTICA – 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, sejam da Instituição ou da sociedade.

VI - *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.

VII - *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.

VIII - *BACKUP* INCREMENTAL - Cópia de segurança que armazena apenas as alterações feitas nos dados desde o último *backup* realizado, seja ele completo ou incremental. Esse método otimiza o tempo de *backup* e o uso de espaço de armazenamento, uma vez que evita a duplicação de dados inalterados. Para restaurar o sistema, é necessário combinar o *backup* completo inicial com todos os *backups* incrementais subsequentes até o ponto desejado.

IX - *BACKUP* SINTÉTICO COMPLETO - Método de *backup* em que um *backup* completo é criado a partir de um *backup* completo inicial e subsequentes *backups* incrementais, sem a necessidade de acessar os dados de origem novamente. Esse processo ocorre no servidor de *backup* ou na infraestrutura de armazenamento, onde os dados incrementais são combinados com o *backup* completo inicial para formar uma nova cópia completa. Isso resulta em *backups* completos atualizados de forma eficiente, economizando tempo e largura de banda de rede, ao mesmo tempo em que facilita a restauração de dados.

X - *BACKUP* DIFERENCIAL - Cópia de segurança que armazena todos os dados alterados desde o último *backup* completo. Ao contrário do *backup* incremental, que só inclui as mudanças desde o último *backup* de qualquer tipo, o *backup* diferencial acumula todas as modificações desde o último *backup* completo.

Referência legal e de boas práticas

Orientação	Seção
Acórdão nº 1.109/2021-TCU-Plenário	Em sua íntegra
Decreto nº 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2º, 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 e 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 do PPSI	v1.1.2: 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;	5.1.3 Gerenciamento da Segurança da Informação
Instrução Normativa nº 01/GSI/PR, de 27 de maio de 2020	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 (LGPD)	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

Declarações da política

Princípios gerais

Art. 16. A Política de *Backup* e Restauração de Dados está alinhada com a Política de Segurança da Informação do IFMS.

Art. 17. As rotinas de *backup* estão orientadas para a restauração dos dados no menor tempo possível, principalmente, quando da indisponibilidade de serviços de TI.

Art. 18. As rotinas de *backup* devem utilizar soluções próprias e especializadas para este fim, preferencialmente, de forma automatizada.

Art. 19. 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.

Art. 20. O armazenamento de *backup*, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais *backups*, a exemplo dos *backups* de dados de serviços críticos.

Art. 21. A infraestrutura de rede de *backup* deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Art. 22 Em situações em que a confidencialidade seja primordial, convém que cópias de segurança sejam protegidas através de encriptação.

Frequência e retenção dos dados

Art. 23. Os *backups* dos serviços de TI críticos do IFMS devem ser realizados utilizando-se as seguintes frequências temporais:

I - *Backup* incremental diário.
II - *Backup* sintético completo semanal.

Art. 24. Os serviços de TI do IFMS devem ser resguardados (política de retenção) por um prazo mínimo de 6 dias.

Art. 25. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

Art. 26. Os ativos envolvidos no processo de *backup* são considerados ativos críticos para a organização.

Art. 27. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelos servidores responsáveis por tais serviços, com a anuência prévia e formal dos responsáveis por esta política, 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.

Art. 28. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas aos responsáveis por esta política. A aprovação para execução da alteração depende da anuência do Administrador de *Backup* e do Comitê de Governança Digital (CGD).

Art. 29. 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.

Tipos de *backup*

Art. 30. Salvo indicação em contrário, o *backup* dos dados será feito de acordo com a seguinte programação padrão:

I - *Backup* incremental diário (segunda a sábado), armazenado local e remotamente.
II - *Backup* sintético completo semanal (sábado a domingo), armazenado local e remotamente.

Uso da rede

Art. 31. O administrador de backup deve considerar o impacto da execução das rotinas de *backup* sobre o desempenho da rede de dados do IFMS, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI do IFMS.

Art. 32. A execução do *backup* deve concentrar-se, preferencialmente, no período de janela de *backup*.

Art. 33. O período de janela de *backup* deve ser determinado pelo administrador de *backup* em conjunto com a área técnica responsável pela administração da rede de dados do IFMS.

Transporte e armazenamento

Art. 34. 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*.

Art. 35. 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.

Art. 36. 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.

Art. 37. A execução das rotinas de *backup* deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 38. No caso de desligamento do usuário (de forma permanente ou temporária), o *backup* de seus arquivos em nuvem deverá ser mantido por um período mínimo de 90 dias para servidores e 180 dias para estudantes. Após esse período, os arquivos poderão ser excluídos a qualquer tempo.

Art. 39. 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.

Art. 40. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

Testes de *backup*

Art. 41. Os *backups* serão verificados periodicamente:

I - Semestralmente, os logs de *backup* serão revisados em busca de erros, 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.

Art. 42. Os testes de restauração dos *backups* devem ser realizados, por amostragem, a cada seis meses, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de

produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar *backups* bem-sucedidos.

Art. 43. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.

Art. 44. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do *backup* e se o procedimento foi concluído com sucesso.

Procedimento de restauração de *backup*

Art. 45. O atendimento de solicitações de restauração de arquivos, *e-mails* e demais formas de dados deverá obedecer às seguintes orientações:

I - A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de envio de chamado técnico para sd@ifms.edu.br.

II - A restauração de objetos somente será possível nos casos em que este tenha sido atingido por esta Política.

III - A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

IV - O operador de *backup* terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

Art. 46. O cronograma de restauração de dados:

I - O tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço entre as áreas de negócio e de TIC, é proporcional ao volume de dados necessários para o *restore*. A cada 70GB de dados, o tempo de restauração médio é de uma hora. Esta estimativa é do tempo de atendimento da Diretoria de Gestão de Tecnologia da Informação, não contemplando o tempo antes ou após o pedido à equipe.
II - *Backups* externos serão disponibilizados em aproximadamente 15 dias de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um;
III - *Backups* externos serão disponibilizados em aproximadamente 24 horas de uma falha não catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.

Art. 47. Diretrizes para restauração de dados:

I - Estabelecer critérios para priorizar a restauração de dados, determinando quais conjuntos de dados são mais críticos e devem ser restaurados primeiro em caso de falha.

II - Realizar testes automatizados regulares de restauração para garantir que os procedimentos estejam atualizados e que a recuperação de dados seja eficiente, ajudando a identificar e corrigir problemas antes que ocorram emergências.
III - Realizar testes manuais em prazos pré-determinados de restauração para garantir que os procedimentos de recuperação de dados estejam funcionais de modo prático, contribuindo com o treinamento procedural a fim de aumentar a eficiência durante situações reais de emergência.

Descarte da Mídia

Art. 48. 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, através de procedimentos '*zero fill'* ou formatação de baixo nível.

II - Os procedimentos citados acima serão aplicados em mídias tanto mecânicas quanto de tipo *flash*, como discos rígidos ou SSDs, por exemplo.

Responsabilidades

Art. 49. O administrador de *backup* e o operador de *backup* devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de *backup*.

Art. 50. São atribuições do administrador de *backup*:
I - Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;
II - Providenciar a criação e manutenção dos *backups*;
III - Configurar as soluções de *backup*;
IV - Manter as unidades de armazenamento de *backups* preservadas, funcionais e seguras;
V - Definir os procedimentos de restauração e neles auxiliar;

Art. 51. São atribuições do operador de *backup*:

I - Executar e monitorar o *status* das operações de *backup*, identificando e resolvendo quaisquer problemas que possam surgir durante o processo.
II - Realiza rotinas de manutenção, como troca de fitas, gerenciamento de armazenamento de mídia, limpeza de dispositivos de *backup* etc.
III - Gerir os relatórios e manter os registros detalhados de todas as operações de *backup*, incluindo falhas e sucesso.
IV - Comunicar o administrador sobre quaisquer problemas críticos, como falhas de *backup*.
V - Executar procedimentos de recuperação conforme necessário.

Procedimentos Relevantes

Art. 52. Os procedimentos relacionados ao *backup* e *restore* estão tecnicamente descritos no Manual de Instruções de *Backup* e *Restore* do IFMS.

Não conformidade

Art. 53. Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

Disposições Finais

Art. 54. Eventuais situações não abrangidas por esta política devem ser abordadas pelo administrador de *backup*, que, caso considere pertinente, deve submeter a questão a uma consulta junto ao Comitê de Governança Digital (CGD).