MINISTÉRIO DA EDUCAÇÃO
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
COMITÊ DE GOVERNANÇA DIGITAL

RESOLUÇÃO CGOVD/DTI/CEFET-MG Nº 1, DE 31 DE MARÇO DE 2023

Aprovar a Política de Backup e restauração de Dados Digitais do CEFET-MG, na forma do Anexo a esta deliberação.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL DO CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS, autarquia de regime especial vinculado ao Ministério da Educação, no uso das atribuições legais e regimentais que lhe são conferidas, considerando: i) a Instrução Normativa GSI/PR 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências; ii) o Decreto Nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética (E-CIBER), Item 2.3.4 do Anexo, que estabelece ação estratégica para elevar o nível de proteção do Governo; iii) a Política de Segurança da Informação e Comunicação (POSIC) do CEFET-MG; iv) o plano de metas e ações do PDTIC 2022-2026 do CEFET-MG, Ação A-4.1.4, que prevê a elaboração de atos normativos para a gestão de operações; v) a Norma Técnica ABNT NBR ISO/IEC 27002:2022, Item 8.13 *Backup* das informações, que tem como propósito a recuperação da perda de dados ou sistemas; vi) o Framework de segurança cibernética do CIS, versão 8, Controle 11 Recuperação de dados, que recomenda o estabelecimento e manutenção de práticas de recuperação de dados; vii) o que foi deliberado na 1ª Reunião Ordinária de 2023 do Comitê de Governança a Digital (CGOVD) realizada em 10 de fevereiro de 2023,

RESOLVE:

Art. 1º Aprovar a Política de Backup e restauração de Dados Digitais do CEFET-MG, na forma do Anexo a esta deliberação.

Art.2 º Esta Política entra em vigor na data de sua publicação.

Publique-se e cumpra-se.

(Assinado digitalmente em 31/03/2023 18:47)
FLAVIO ANTONIO DOS SANTOS
PRESIDENTE - TITULAR
CGOVD (11.47.04)
Matrícula: 980644

ANEXO

POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º 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 pelas unidades de tecnologia da informação (TI) e formalmente definidos como de necessária salvaguarda no CEFET-MG, para se manter a continuidade do negócio.

Art. 2º A Política de que trata este documento aplica-se a todas as unidades do CEFET-MG que tenham sob sua guarda dados em suporte digital, incluindo dados fora da Instituição armazenados em um serviço de nuvem Pública ou Privada.

Art. 3º A salvaguarda e restauração dos dados digitais do CEFET-MG abrange exclusivamente repositórios institucionais custodiados pelas unidades de TI, armazenados nos centros de processamento de dados.

Parágrafo único. 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 sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).

Art. 4º A salvaguarda dos dados em formato digital pertencentes a serviços de TI do CEFET-MG 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.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para os fins desta Política, considera-se:

I - administrador de backup: responsável pelo planejamento de soluções de backup, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas;

II - área técnica: unidade responsável pela operação técnica dos ativos e serviços de TI;

III - ativo crítico: equipamento físico, unidade de armazenamento e dados que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização;

IV - backup: cópia de segurança de dados computacionais, que pode ser utilizada ou consultada após sua restauração, em caso de indisponibilidade, perda ou alteração dos dados originais;

V - backup completo: modalidade de backup em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup;

VI - backup incremental: modalidade de backup em que são salvaguardados apenas os dados novos ou modificados desde o último backup de qualquer modalidade efetuado;

VII - backup diferencial: modalidade de backup em que são salvaguardados apenas dados novos ou modificados desde o último backup completo efetuado;

VIII - criticidade: grau de importância dos dados para a continuidade das atividades e serviços da organização;

IX - descarte: eliminação correta de dados, documentos, unidades de armazenamento e acervos digitais;

X - disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa física ou determinado serviço de TI, órgão ou entidade devidamente autorizados;

XI - gestor da informação: agente público formalmente responsável pela operação do serviço ou sistema de TI e pelas informações produzidas em seu processo de trabalho;

XII - imagem de backup: arquivo gerado pela solução de backup, não necessariamente no formato original dos arquivos que contêm os dados salvaguardados;

XIII - janela de backup: período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XIV - operador de backup: responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de backup, realização de restaurações de arquivos de usuários, manutenção de troca de fitas no robô e gerenciamento de estoque de fitas locais;

XV - plano de continuidade de negócios (PCN): plano que define as etapas necessárias para recuperação dos processos de negócio logo após uma interrupção, identificando também os gatilhos para invocação, as pessoas a serem envolvidas, as comunicações, etc.

XVI - restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de backup;

XVII - retenção: período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

XVIII - *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;

XIX - *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;

XX - rotina de backup: procedimento utilizado para se realizar um backup;

XXI - serviço de TI: sistema de informação ou qualquer solução de tecnologia da informação que armazene informações em formato digital;

XXII - unidade de armazenamento: dispositivo para armazenamento de dados em suporte digital;

XXIII - unidade de armazenamento de backup: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais.

CAPÍTULO III
DOS PADRÕES OPERACIONAIS

Seção I

Dos princípios gerais

Art. 6º A Política de Backup e Restauração de Dados deve ser alinhada com a Política de Segurança da Informação da Instituição.

Art. 7º A Política de Backup e Restauração de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 8º As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Art. 9º 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. 10. Os serviços de TI críticos do CEFET-MG, formalmente estabelecidos pelo Comitê de Governança Digital (CGD), são: o Sistema Integrado de Gestão Acadêmica e Administrativa (SIG), o Ambiente Virtual de Aprendizagem (AVA), as pastas compartilhadas em domínio e o Correio Eletrônico.

Parágrafo único. Compete ao Comitê de Governança Digital (CGD) deliberar sobre futuras atualizações da relação dos serviços críticos.

Seção II

Das ferramentas de backup

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

Art. 12. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

Parágrafo único. Compete à Diretoria de Tecnologia da Informação (DTI) solicitar, à Administração, com as justificativas pertinentes, as contratações necessárias para manter os ativos sempre atualizados e em quantidade necessária ao atendimento da demanda do CEFET-MG.

Seção III

Da frequência e retenção dos dados

Art. 13. Os backups dos serviços de TI críticos do CEFET-MG devem ser realizados utilizando-se as seguintes frequências temporais:

I - diária;

II - semanal;

III - mensal;

IV - anual.

Art. 14. Os serviços de TI críticos e não críticos devem ser resguardados sob um padrão mínimo, o qual deve observar uma correlação frequência/retenção de dados.

Parágrafo único. As frequências e retenções dos backups dos serviços de TI serão definidas em norma específica a ser elaborada pela DTI em conjunto com os gestores das informações.

Art. 15. O backup de serviços de TI não críticos deve ser formalmente solicitado ao administrador de backup pelo responsável técnico pelo serviço de TI.

Art. 16. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenções diferenciadas.

Art. 17. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelos responsáveis técnicos dos serviços de TI, com a anuência prévia e formal dos gestores das informações, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação 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. 18. A restauração de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

Art. 19. A alteração das frequências e tempos de retenção deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de backup. A aprovação para execução da alteração depende da anuência do gestor da informação.

Seção IV

Do uso da rede

Art. 20. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do CEFET-MG, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da Instituição.

Art. 21. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

Art. 22. 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 CEFET-MG.

Seção V

Das unidades de armazenamento de backups

Art. 23. 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. 24. 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. 25. 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. 26. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de backup.

Art. 27. 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.

Seção VI

Dos testes de backup

Art. 28. Os backups devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Art. 29. Os testes de restauração dos backups devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis em cada unidade do CEFET-MG.

Art. 30. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de backup serão definidos em norma específica a ser elaborada pela DTI em conjunto com os gestores das informações.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 31. O administrador de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup, mediante solicitação da DTI.

§ 1º O administrador e o operador de backup do CEFET-MG, no âmbito da Administração Central, serão formalmente indicados pelo diretor da DTI, entre os servidores lotados na DTI.

§ 2º Nas unidades do CEFET-MG, o administrador e o operador de backup serão formalmente designados pelo diretor de unidade ou pelo coordenador da Coordenação de Tecnologia da Informação e Comunicação (CTIC), quando houver.

§ 3º Caso não seja possível a indicação de servidores distintos, o mesmo servidor poderá exercer os papéis de administrador e operador de backup.

Art. 32. São atribuições do administrador de backup:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pelo CEFET-MG;

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;

VI - verificar diariamente os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;

VII - tomar medidas preventivas para evitar falhas;

VIII - reportar imediatamente ao setor a que está subordinado os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de backups;

IX - gerenciar mensagens e registros de auditoria (LOGs) diários dos backups;

X - disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;

XI - propor modificações visando ao aperfeiçoamento da Política de Backup e Restauração de Dados Digitais, objeto desta Política;

XII - providenciar a execução dos testes de restauração.

Art. 33. São atribuições do operador de backup:

I - restaurar ou recuperar os backups em caso de necessidade;

II - operar e manusear as unidades de armazenamento de backups;

III - informar ao administrador de backup qualquer problema que impossibilite a restauração de um backup.

Art. 34. São atribuições das áreas técnicas:

I - solicitar restaurações de dados, com anuência do gestor da informação;

II - sanar dúvidas técnicas do administrador de backup acerca das informações salvaguardadas;

III - validar, tecnicamente, o resultado das restaurações eventualmente solicitadas;

IV - validar, tecnicamente, o resultado dos testes de restauração dos backups.

Art. 35. São atribuições dos gestores da informação:

I - solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pela área técnica para restauração de dados;

II - validar, negocialmente, o resultado das restaurações eventualmente solicitadas;

III - validar, negocialmente, o resultado dos testes de restauração dos backups.

Art. 36. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

Parágrafo único. 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.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 37. Esta Política deverá ser amplamente divulgada no CEFET-MG, fazendo-se ainda constar, em destaque, na página da DTI.

Art. 38. Esta Política poderá ser revisada a qualquer tempo, para fins de eventual atualização, quando identificada a necessidade de alteração em qualquer de seus dispositivos.

Art. 39. A DTI, os CTICs e os gestores das informações tomarão as providências necessárias para a adequação das rotinas e dos procedimentos de backups definidos nesta Política.

Art. 40. Casos excepcionais não abordados nesta Política serão decididos pelo CGOVD, com análise da DTI, e, sendo necessário, pelas unidades de TI ou pelos gestores das informações.