NORMA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS DA UNIVERSIDADE FEDERAL DE VIÇOSA (UFV)

O GESTOR DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DE VIÇOSA (UFV), NA CONDIÇÃO DE COORDENADOR DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO DA UFV, no uso de suas atribuições legais e regimentais, resolve aprovar a Norma de Backup e Restauração de Dados Digitais da Universidade Federal de Viçosa (UFV):

Da finalidade e do objeto

Art. 1º A Norma 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 Diretoria de Tecnologia da Informação (DTI) e formalmente definidos como de necessária salvaguarda na UFV, para se manter a continuidade do negócio. Na medida do possível, as recomendações aqui descritas, devem ser extensíveis a todos os campi da UFV.

Do escopo (objeto)

Art. 2º Esta norma se aplica a todos os dados no âmbito da UFV, armazenados e administrados pela DTI. Neste contexto, são incluídos: dados dos sistemas e sites acadêmicos, administrativos e de pessoal da UFV, armazenados nas máquinas servidoras administradas pela DTI. Uma atenção especial deve ser considerada para os dados críticos da instituição.
§ 1º A definição de dados críticos e o escopo desta norma de backup serão revisados sempre que necessário ou a cada um ano, após a data da publicação desta norma.
§ 2º Os serviços de TI críticos da UFV devem ser formalmente elencados pelo Comitê de Governança Digital (CGD) e validados pelo Comitê de Governança, Riscos e Controles (CGRC).

Art. 3º Esta norma se aplica a técnicos, docentes e estudantes que podem ser criadores e/ou usuários de tais dados. A norma também se aplica a terceiros que acessam e usam na UFV sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da instituição.

Art. 4º Não serão salvaguardados nem recuperados os dados:
I - discos locais das estações de trabalho das áreas administrativas e acadêmicas da UFV;
II - máquinas servidoras externas ao Data Center da DTI da UFV, incluindo quaisquer dados armazenados;

III - máquinas servidoras alocadas fisicamente ou virtualmente no Data Center da DTI/UFV que não são administradas e da responsabilidade da equipe técnica da DTI/UFV, incluindo quaisquer dados armazenados;
IV - Dados, sites e sistemas hospedados em serviços de nuvem externos ao Data Center da DTI da UFV, e não administrados pela equipe de TI da UFV.
Parágrafo único: A salvaguarda dos dados em formato digital pertencentes a serviços de TI da UFV, 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.

Das referências normativas

Art. 5º A presente Portaria Normativa tem como base as seguintes referências normativas:
I - Acórdão 1.109/2021-TCU-Plenário;
II - Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022;
III - Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD) - Art. 2, XXIII;
IV - Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER) - Anexo, Item 2.3.4 e 2.3.5;
V - Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) - Anexo, art.3, Inciso I, II e V;
VI - 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;
VII - 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;
VIII - Guia do Framework de Privacidade e Segurança da Informação - Controle 11;
IX - 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;
X - Instrução Normativa 01/GSI/PR - Art.12, Inciso IV, alínea g, h;
XI - Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021 - Capítulo IV;
XII - Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados - CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
XIII - Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)
XIV - 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;
XV - 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;

XVI - Portaria GSI/PR nº 93, de 18 de outubro de 2021

Dos termos e definições

Art 5º Para efeitos desta Portaria Normativa, aplicam-se as seguintes definições:

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;
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 Storage: Meio físico (equipamento) onde são armazenados os dados digitais contidos no backup.

IX Janela de Backup - período de tempo definido pelo menor uso de recursos computacionais dos ativos de uma determinada rede de dados, quando a execução de tarefas de backup não impacta os serviços e usuários. Geralmente, é o período fora do horário de trabalho e atendimento da empresa ou instituição.

Dos princípios gerais

Art 6º A norma de Backup e Restauração de Dados deve estar alinhada com a norma de Segurança da Informação e Comunicações da Universidade Federal de Viçosa.
Art 7º A norma de Backup e Restauração de Dados 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 utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
Art 10º 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 11º 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 12º Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
Art 13º Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Da frequência e retenção dos dados

Art 13º O administrador de backup, juntamente com o CGRC, deverá definir formalmente, em procedimento:
I - Os tipos de backups que serão realizados;
II - A frequência da realização de cada tipo de backup, para dados críticos;
III - A frequência da realização de cada tipo de backup, para dados não críticos;
IV - O tempo mínimo de retenção de cada tipo de backup, para dados críticos;
IV - O tempo mínimo de retenção de cada tipo de backup, para dados não críticos;
(parágrafo único ou)
Art 14º Caso os recursos físicos e tecnológicos disponíveis não permitam atender aos padrões mínimos de frequência e retenção de backup definidos anteriormente, admite-se uma redução nesses padrões, que deve ser previamente comunicada pela DTI aos responsáveis pelos dados.
Art 15º Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.
Art 16º A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelo responsável técnico do serviço ou ativo crítico, com a anuência prévia e formal da chefia do setor.

Art 17º A alteração das frequências e tempos de retenção deve ser precedida de solicitação e justificativa formais encaminhadas à DTI. A aprovação para execução da alteração será avaliada pelos administradores de backup.
Art 18º 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, transporte e armazenamento

Art 19º O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da UFV, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da organização.
§1º A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
§2º 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 da DTI/UFV.

Art 20º 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.
§1º 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.
§2º 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.
§3º A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
§4º 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.
§5º 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.

Dos testes de backup e restauração dos dados

Art 21º Os backups serão verificados periodicamente, por amostragem, mensalmente, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos e conformidade com esta norma.
§1º Quaisquer exceções a esta norma serão totalmente documentadas e aprovadas pelo Comitê de Governança, Riscos e Controles – CGRC.
Art 22º O atendimento de solicitações de restauração de arquivos e demais formas de dados deverá ser solicitado à DTI pelo responsável pelo ativo ou recurso.
§1º A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.
§2º A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.
§3º 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.
§4º 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 a restauração dos ativos.

Das responsabilidades

Art 23º O administrador de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

§1º 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;
VI - Definir as rotinas de testes de backups.

§2º São atribuições do operador de backup:

I - Criar, testar e implantar as rotinas de backups;
II - Efetuar periodicamente rotinas de testes de backups;

III - Quando identificado falha em ativos de backup, providenciar a manutenção ou comunicar ao administrador de backup;
IV - Verificar logs das rotinas de backup diariamente;
V - Atender e executar as solicitações de restauração de backups.

Não conformidade

Art 24º Em caso de violação desta norma poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis. As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

I - Processo Administrativo Disciplinar de acordo com a legislação aplicável
II - Exoneração.
III - Ação judicial de acordo com as leis aplicáveis e acordos contratuais.
IV - Rescisão contratual ao bem do serviço público.