SERVIÇO PÚBLICO FEDERAL

PORTARIA Nº 03 DE 13 DE NOVEMBRO DE 2019

Dispõe sobre a Política de Cópias de Segurança (Backup) e Restauração de Dados da Universidade Federal de Lavras.

O Diretor de Gestão de Tecnologia da Informação da UNIVERSIDADE FEDERAL DE LAVRAS, no uso de suas atribuições legais e regimentais, e,

Considerando a Portaria Nº 1.327, de 13 de Novembro de 2019, que atualiza a Política de Segurança da Informação e Comunicações da Universidade Federal de Lavras, conforme disposto no Art. 19 que trata da necessidade de normas complementares para estabelecer procedimentos que visem garantir a integridade, a confidencialidade e a disponibilidade das informações, incluindo procedimentos para a criação, manutenção e verificação dos ativos de informação e de suas cópias de segurança;

Considerando a Portaria Nº 1062, de 20 de Setembro 2019, que trata da Política de Gestão de Riscos da Universidade Federal de Lavras;

Considerando o Plano Diretor de Tecnologia da Informação e Comunicações da Universidade Federal de Lavras - triênio - 2017-2020,

Considerando o disposto no inciso VI do Art. 3º do Decreto Nº 8.638 de 15, de janeiro de 2016, que trata do princípio da segurança e privacidade no âmbito da Política de Governança Digital;

Considerando o disposto no artigo 5º, incisos IV e VI, da

SERVIÇO PÚBLICO FEDERAL

Instrução Normativa GSI nº 1, de 13/6/2008, do Gabinete de Segurança Institucional da Presidência da República, publicada na seção 1 do D.O.U. nº 115, de 18/6/2008,

Considerando o disposto na Lei Nº 12.965, de 23 de abril de 2014, Marco Civil da Internet,

Considerando o Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação - PNSI, no âmbito da administração pública federal,

Considerando as Boas Práticas em Segurança da Informação do Tribunal de Contas da União - 4ª Edição.

Resolve:

Art. 1º Estabelecer a Política de Cópias de Segurança (Backup) e Restauração de Dados no âmbito da Universidade Federal de Lavras - UFLA, disponível em meio digital no endereço https://dgti.ufla.br/pt/politicas-e-normas.

Art. 2º Esta portaria entra em vigor na data de sua publicação revogadas as disposições em contrário.

SERVIÇO PÚBLICO FEDERAL

Anexo

Política de Cópias de Segurança (Backup) e Restauração de Dados

da Universidade Federal de Lavras (UFLA)

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Seção I
Do Objetivo

Art. 1º Este documento tem por objetivo estabelecer uma política de backup de dados estruturados e não estruturados a fim de evitar que os arquivos sejam permanentemente perdidos ou danificados em caso de algum incidente, seja ele físico, lógico, ambiental, ou como na maioria dos casos, uma falha humana. Os arquivos de backup ajudam a evitar ou minimizar as perdas de trabalho executado caso algo indesejado aconteça, sendo sua criação necessária periodicamente.

Seção II
Do Escopo

Art. 2º Essa política se limita a toda informação ou dado armazenado nos servidores institucionais sob a tutela e guarda da Diretoria de Gestão de Tecnologia da Informação (DGTI).

Art. 3º Os dados de máquinas locais e individuais não estão cobertos por essa política, sendo que a proteção e cópia de segurança (backup) dos dados são de responsabilidade do seu usuário.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 4º Esta política é norteada pelos princípios básicos da Política de Segurança da Informação e Comunicação da UFLA (POSIC), que considera os preceitos básicos da segurança da informação: a confidencialidade, a legalidade, a autenticidade, o não-repúdio, a conformidade, o controle de acesso, a auditabilidade, a integridade e a disponibilidade. Sendo esses dois últimos, fundamentos para todas as ações e diretrizes dessa política.

Art. 5º No ambiente de Tecnologia da Informação, o backup e a proteção dos dados são utilizados para prover continuidade de negócios, replicação de dados, recuperação de desastres e redução nos custos de infraestrutura tecnológica.

Art. 6º Para a proteção das informações e para atenderem a padrões de segurança e regulamentações governamentais, as organizações estabelecem políticas de segurança. Ainda assim, as organizações não estão livres de erros humanos, ataques de vírus, catástrofes naturais, e outras ameaças. E caso ocorram perdas de informações é preciso recuperá-las, e isto se torna possível se o processo de backup e recuperação de dados for seguro.

CAPÍTULO III
CONCEITOS E DEFINIÇÕES
Seção I
Da Terminologia

Art. 7º São termos e definições utilizados nesta Política:

I – Agente Público: Toda e qualquer pessoa que exerce uma atribuição pública em sentido lato, seja estagiário, ocupante de função, cargo ou de emprego público.

II – Prestador de Serviço: Toda e qualquer pessoa que possui uma relação contratual com a UFLA em período determinado.

III – Usuário de TIC: agente público ou prestador de serviço que fazem uso de serviço de TIC.

IV – Dado - Qualquer registro de conteúdo armazenado em meio magnético. Pode compreender software, dados propriamente ditos (arquivos, bancos de dados), conteúdo multimídia ou qualquer outro passível de armazenamento em meio magnético.

V – Dado estruturado - dado que passou por processo de modelagem; geralmente residente em tabelas componentes de bancos de dados ou arquivos acessados por aplicações.

VI – Dado não estruturado - documento, mensagens de correio eletrônico, conteúdo multimídia (imagem, vídeo, áudio) armazenado em formato digital. Em conjunto, têm como características grande volume, rápido crescimento e dificuldade de manipulação pelas ferramentas de gerenciamento de bancos de dados ou aplicações que processam arquivos de dados.

VII – Backup - Cópia de segurança gerada para possibilitar o acesso ou recuperação futura de dados existentes no Data Center da DGTI. O termo também pode ser

associado ao processo de geração da cópia de segurança.

VIII – Janela de Backup - Período de tempo requerido para a geração do backup (total, diferencial ou incremental).

IX - Mídia de Backup - Suporte magnético ou óptico utilizado para armazenamento de dados. Dentre as mídias de backup destacam-se as fitas e cartuchos magnéticos e os discos ópticos.

X - Restore - Cópia eventual de dados armazenados em backup para um disco ou outra mídia através da qual podem ser acessados pelos usuários ou aplicações.

XI - Servidor - Computador responsável por gerenciar e oferecer serviços para uma rede de computadores clientes.

XII- Storage - Equipamento composto por conjuntos de discos magnéticos, especializado no armazenamento e disponibilização de grandes volumes de dados.

XIII - Software de backup - Conjunto de programas especializados no planejamento, identificação do backup, processamento e controle do backup de servidores, storage e demais dispositivos que armazenam dados.

XIV. Disaster Recovery: plano de recuperação de dados em função de incidentes de segurança de graves proporções que impactem na disponibilidade, integridade e autenticidade dos dados.

XV. Retenção: período de tempo em que o conteúdo da mídia de backup deve ser preservado.

Seção II
Das Instâncias Administrativas

Art. 8º Para os efeitos desta Política e das normas dela originadas, entende-se por:

I – Reitoria: é o órgão executivo superior, ao qual compete dirigir, administrar, planejar, coordenar, estabelecer parcerias e fiscalizar as atividades da universidade;

II – Comitê Interno de Governança (CIGOV): Art 1° da portaria 1.499 de 2018 da

Reitoria. Comitê responsável por elaborar e revisar periodicamente a POSIC e normas relacionadas, submetendo à aprovação da Reitoria, entre outras competências; tem entre suas atribuições principais: participar e orientar o planejamento dos investimentos em Tecnologia da Informação e Comunicações de acordo com as diretrizes do Plano de Desenvolvimento Institucional (PDI) em execução; estabelecer as políticas, diretrizes e prioridades na área de Tecnologia da Informação e Comunicações (TIC); promover e estimular o desenvolvimento da Tecnologia da Informação e Comunicações no âmbito da UFLA; elaborar, acompanhar e avaliar um Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) para a UFLA; elaborar, acompanhar e avaliar as Políticas de Segurança da Informação e Comunicações para a UFLA;

III – Diretoria de Gestão de Tecnologia da Informação (DGTI): instância administrativa/executiva responsável pelo desenvolvimento, implantação e manutenção dos ativos de sistemas de informação;

IV – Coordenadoria de Segurança da Informação: responsável por monitorar e analisar o cumprimento das políticas, normas e procedimentos de segurança dos sistemas de informação e comunicações, além de elaborar estratégias para comunicação, publicação e divulgação das políticas, normas e procedimentos de segurança dos sistemas de informação e comunicações;

V – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): portaria da reitoria nº 275, 15 de março de 2019. Equipe mantida pela Diretoria de Tecnologia da Informação (DGTI) que possui a missão de realizar o tratamento de vulnerabilidades e incidentes de segurança, emissão de alertas e advertências relativos à rede computacional da UFLA;

VI – Coordenadoria de Administração de Redes:

VI – Coordenadoria de Sistemas de Informação:

CAPÍTULO IV
COMPETÊNCIAS E RESPONSABILIDADES

Art. 9º A DGTI é a unidade responsável por assegurar a execução das rotinas de backup e seus testes no âmbito da UFLA, sendo que:

Art. 10 Compete à Coordenadoria de Segurança da Informação:

I – Zelar pelo cumprimento política e procedimentos relativos aos serviços de backup e restore e assegurar o cumprimento das normas aplicáveis.

II – Propor modificações visando o aperfeiçoamento desta política de backup e restauração.

III – Auditar quanto à existência de procedimentos de backup dos sistemas, sites e bases de dados institucionais;

IV – Auditar quanto à existência e execução dos planos de testes dos backups dos sistemas, sites e bases de dados institucionais;

Art. 11 Compete à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR):

I – Receber, analisar e responder eventos de indisponibilidade de serviços e incidentes de segurança da informação.

II – Comunicar a ocorrência de incidentes de segurança informação, que afetem a disponibilidade de dados e serviços de TIC, às áreas de administração de redes, sistemas de informação e segurança da informação para que as mesmas tomem providências necessárias de disaster recovery e recuperação de dados.

Art. 12 Coordenadoria de Administração de Redes e Sistemas:

I – Operacionalizar e executar a política de backup das bases de dados dos sistemas e sites institucionais;

II – Configurar e gerenciar as ferramentas de backup;

III – Manter os dispositivos e mídias armazenamento, funcionais e seguros;

IV – Verificar diariamente os eventos gerados pela ferramenta de backup, tomando as providências necessárias em caso de de falhas;

V – Providenciar a restauração das bases de dados dos sistemas e sites institucionais o mais rápido possível, de forma a não comprometer o nível de acordo de serviço;

VI – Gerenciar eventos e logs diários das ferramentas de backups.

VII – Operacionalizar e executar a política de backup das máquinas virtuais;

VIII – Executar periodicamente testes para verificação da consistência dos backups dos bancos de dados e máquinas virtuais.

Art. 13 Coordenadoria de Sistemas de Informação:

I – Gerenciar o sistema de controle de versões (GIT e SVN) no intuito de manter as diferentes versões, bem como o histórico e desenvolvimento dos códigos-fontes e documentações dos ambientes de Produção, Teste e Homologação dos sistemas institucionais desenvolvidos e mantidos pela DGTI;

II – Sempre que necessário, solicitar formalmente a restauração de bases de dados e máquinas virtuais a Coordenadoria de Administração de Redes.

CAPÍTULO V
DIRETRIZES GERAIS

Art. 14 São diretrizes gerais da Política de Cópias de Segurança (Backup) da UFLA:

I – Utilizar recursos adequados para a geração de cópias de segurança para garantir que toda informação e sistemas essenciais possam ser recuperados após a perda de dados devida a desastres, erros, falhas de mídias ou outros fatores.

II – Registrar informações completas e exatas das cópias de segurança em documentação apropriada.

III – Todas as aplicações corporativas ou setoriais essenciais ou críticas para a UFLA devem armazenar os dados nos servidores de arquivos e nos servidores de bancos de dados, que deverão estar sob a guarda da DGTI, para os quais será assegurada a execução de rotina de backup, de acordo com esta política.

IV – Observar as boas práticas e procedimentos de Segurança da Informação e Comunicações recomendados por órgãos e entidades responsáveis pelo estabelecimento de padrões, bem como o que foi disposto pela POSIC da UFLA e suas normas.

Art. 15 As Diretrizes de Segurança da Informação definidas neste documento são aplicadas aos ativos de informação, de hardware, de software e intangíveis, fornecendo orientações para práticas de gestão de segurança da informação.

Seção I
Das Diretrizes e Procedimentos para o Realização da Cópia de Segurança (Backup)

Art. 16 Toda informação deverá ser classificada considerando seu nível de criticidade, importância e impacto para continuidade dos serviços, da integridade da informação e sua disponibilidade e a imagem da UFLA.

Art. 17 Definida sua classificação, deverá ser determinado quais os dados serão armazenados;

Art. 18 A seguir, deve-se definir quais sistemas e informações terão prioridade para criar backups e o intervalo de criação entre cada uma das cópias. A priorização deverá ser realizada de modo que cada solução de TIC e informação esteja relacionada aos processos de maior importância do negócio, investigando também quais os possíveis impactos em caso de falha.

Art. 19 Deve-se determinar os equipamentos e tecnologias que serão utilizados no backup, qualquer que seja o tipo de mídia a ser utilizada (fita magnética, disco, nuvem ou qualquer outra). A escolha da mídia poderá ser determinada pela janela de tempo de execução do backup, o volume de dados gerado, a velocidade para recuperar arquivos e as rotinas de trabalho do negócio.

Art. 20 Considerando a volatilidade da informação, deve-se estipular a frequência com que o processo será executado (diário, semanal, mensal e/ou anual).

Art. 21 Deve-se definir a melhor estratégia de backup a ser aplicada (diferencial, completo ou incremental) para cada tipo classificação de informação. As diretrizes a serem adotadas obedecerão o seguinte esquema de realização de backups:

I – Backups das máquinas virtuais serão realizados pelo software "Veeam", com armazenamento no storage da DGTI, obedecendo a seguinte política de retenção:

a) O Backup completo das máquinas virtuais como imagem (para fins de disaster recovery), será feito a cada atualização de segurança realizada ou em caso de alterações sensíveis no sistema, a pedido do responsável pelo serviço, com 12 meses de retenção;
b) Backups completos (mensais) das máquinas virtuais serão realizados com 6 meses de retenção.

c) Backups incrementais diários e semanais de todas as máquinas virtuais conforme procedimentos específicos definidos pela Coordenadoria de Administração de Redes e Sistemas

II – Backups dos bancos de dados deverão ser organizados em níveis de acordo com de acordo com o tamanho de cada backup e a frequência de modificação dos dados obedecendo a seguinte política de retenção:

a) Anual - Armazenar um backup de cada ano dos últimos 5 anos
b) Mensal - Armazenar um backup de cada mês dos últimos 12 meses
c) Semanal - Armazenar um backup de cada semana das últimos 4 semanas anteriores aos últimos 30 dias
d) Diário - Armazenar um backup de cada dia dos últimos 30 dias

III – Backup completo e incremental, com armazenamento em nuvem, via script, das pastas e documentos dos servidores de arquivos institucionais, com retenção mínima de 5 anos .

Art. 22 A recuperação de backups deverá obedecer às seguintes orientações:
I – A área requisitante deverá registrar a solicitação por meio do sistema de chamados da DGTI com, obrigatoriamente, as informações sobre o usuário, o arquivo a ser recuperado, e a data da versão que deseja recuperar;
II – Deverá ser mantido registro de todos os arquivos restaurados acompanhado da solicitação inicial;
III – Os bancos de dados serão restaurados pelo administrador de banco de dados, devendo o administrador de backup auxiliá-lo na tarefa de restore;

Art. 23 Os procedimentos de backup deverão ser atualizados sempre que houver:

I – Novas aplicações desenvolvidas ou instaladas nos servidores institucionais administrados pelas DGTI;

II – Novos locais de armazenamento de dados ou arquivos;

III – Novas instalações de bancos de dados;

IV – Outras informações que necessitem de proteção através de backups deverão ser informadas ao administrador de backup, pelo administrador de banco de dados.

Art. 24 Quaisquer procedimentos programados na infraestrutura de armazenamento e processamento física ou virtual, que possua potenciais riscos de funcionamento com interrupção dos sistemas e serviços de TIC prestados pela DGT, somente deverão ser executados após a realização do backup dos seus dados.

Art. 25 Qualquer solicitação de serviços que envolva outros equipamentos, software de backup, local de armazenamento de mídias, alteração na frequência de geração ou no tempo de retenção do backup deverá ser analisada previamente pela Coordenadoria de Segurança da Informação, quanto à sua viabilidade, em prazo negociado entre as partes.

Art. 26 O backup deverá ser processado, preferencialmente, durante a noite, em horário que gere menor impacto nas demais rotinas e serviços do Data Center da DGTI. A instituição deverá adotar as medidas necessárias para que os responsáveis pelos backups possam geri-los adequadamente, cabendo ao gestor da informação solicitar os recursos necessários para tal.

CAPÍTULO VI
VIOLAÇÕES, PENALIDADES E SANÇÕES

Art. 27 As violações, penalidades e sanções, deverão estar em conformidade com o CAPÍTULO VII, Art. 43 da POSIC UFLA (Portaria Nº 1.327, de 13 de Novembro de 2019).

CAPÍTULO VII
FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

Art. 28 As referências legais e normativas utilizadas para a elaboração da POSIC da UFLA estão de acordo com:

I – a Portaria Nº 1.327, de 13 de Novembro de 2019, que dispõe sobre a Política de Segurança da Informação e Comunicações da UFLA;

II – o disposto no artigo 5º, incisos IV e VI, da Instrução Normativa nº 1, de 13/6/2008, do Gabinete de Segurança Institucional da Presidência da República, publicada na seção 1 do D.O.U. nº 115, de 18/6/2008;

III – a Lei 12.527, de 18 de novembro de 2011, Lei de Acesso da Informação;

IV – o Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação - PNSI, no âmbito da administração pública federal;

V – a Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais;

VI – a Lei 9.069, de 19 de fevereiro de 1998, Lei do Software;

VII – a Lei 12.965, de 23 de abril de 2014, Marco Civil da Internet;

VIII – a Portaria 1.499, de 19 de novembro de 2018, da Reitoria da UFLA, Institui o

Comitê Interno de Governança da Universidade Federal de Lavras (CIGOV-UFLA);

IX – a Portaria 275, de 15 de março de 2019, da Reitoria da UFLA, Institui a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR - UFLA;

X – as Boas Práticas em Segurança da Informação do Tribunal de Contas da União - 4ª Edição.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 29 Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Cópias de Segurança (Backup) dos Dados da UFLA deverão ser analisados pela DGTI.

Art. 30 A presente política passa a vigorar a partir da data de sua publicação, revogando-se as disposições em contrário.

ERASMO EVANGELISTA DE OLIVEIRA
Diretor de Gestão de Tecnologia da Informação