Universidade Federal de São João del-Rei

PORTARIA NORMATIVA N° 105, DE 06 DE FEVEREIRO DE 2025

Dispõe sobre a Política de *Backup* e Recuperação de Dados Digitais no âmbito da Universidade Federal de São João del-Rei - UFSJ.

O REITOR DA UNIVERSIDADE FEDERAL DE SÃO JOÃO DEL-REI – UFSJ, no uso de suas atribuições legais e estatutárias, e considerando:

- Decreto nº. 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação.

- Decreto nº. 10.332, de 28 de abril de 2020 - Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.

- Decreto nº. 12.069, de 21 de junho de 2024 - Dispõe sobre a Estratégia Nacional de Governo Digital e a Rede Nacional de Governo Digital – Rede Gov.br e institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027.

- Instrução Normativa Nº 01/GSI/PR, de 27 de maio de 2020 - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

- Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021 - Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

- Lei nº. 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD.

- Lei nº. 12.527, de 18 de novembro de 2011 – Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

- Lei nº. 14.129, de 29 de março de 2021 - Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017.

- Norma ABNT NBR ISO/IEC 27002:2013. Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.

- Norma ABNT NBR ISO/IEC 27001:2013. Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos.

- Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.

Portaria GSI/PR Nº 93, de 18 de outubro de 2021 - Aprova o glossário de segurança da informação.

- Norma complementar nº. 04/IN01/DSIC/GSI/PR, Gestão de Riscos de Segurança da Informação e Comunicações

- Norma complementar nº. 06/IN01/DSIC/GSIPR, Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações

- Norma complementar nº. 07/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF,

- o que consta do Processo nº 23122.017301/2024-77,

RESOLVE:

Art. 1º **Disciplinar**, regulamentar, no âmbito da UFSJ, e nos termos do Anexo I a esta portaria, a Política de Backup e Recuperação de Dados Digitais.

Art. 2º. Os casos omissos nesta portaria serão resolvidos pelo Comitê Gestor de Tecnologia da Informação - CGTI - da UFSJ.

Art. 3º. Esta portaria entra em vigor no primeiro dia útil do mês subsequente à data de sua publicação

PROF. MARCELO PEREIRA DE ANDRADE
Reitor

ANEXO I

Política de Backup e Recuperação de Dados Digitais

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Seção I
Do Objetivo

Art. 1º A Política de *Backup* e Recuperação de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo Núcleo de Tecnologia da Informação (NTInf) e formalmente definidos como de necessária salvaguarda na UFSJ, para manter a continuidade do negócio. No sentido de assegurar a missão da instituição, 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.

Seção II
Dos Termos e Definições

Art. 2º Para os efeitos desta Política de *Backup* e Recuperação de Dados Digitais e de suas regulamentações, aplicam-se as seguintes definições:

I - Administrador de *Backup*: pessoa física que administra os serviços correspondentes à área de abrangência do backup;

II - Ativos: tudo que tenha valor para a organização, material ou não;

III - Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

IV - *Backup*: 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;

V - Computação em Nuvem: modelo de fornecimento e entrega de

tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o Provedor de Serviços de Nuvem (PSN);

VI - Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

VII - Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

VIII - Gestão de Continuidade de Negócios em Segurança da Informação: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

IX - Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

X - Mídia: mecanismo 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;

XI - Provedor de Serviços de Nuvem (PSN): ente, público ou privado, que fornece uma plataforma, infraestrutura, aplicativo, serviços de armazenamento ou ambientes de tecnologia da informação baseados em nuvem;

XII - Serviços de Tecnologia da Informação (TIC): provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação;

Seção III
Do Escopo

Art. 3º Esta política se aplica a todos os dados no âmbito da UFSJ, sob governança e responsabilidade do NTInf.

Parágrafo único. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos datacenters mantidos pelo NTInf, ficando estes sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).

Art. 4º A salvaguarda dos dados em formato digital pertencentes a serviços de Tecnologia da Informação e Comunicação (TIC) da UFSJ poderá ser realizada por meio de contratação de Provedor de Serviços de Nuvem (PSN) e deverá estar garantida no instrumento jurídico formalizado entre a UFSJ e outras entidades, públicas ou privadas.

Art. 5º Os serviços de TIC críticos da UFSJ devem ser formalmente aprovados pelo Comitê Gestor de Tecnologia da Informação (CGTI) da UFSJ.

§1º Ficam previamente estabelecidos como serviços de TIC críticos da UFSJ: os bancos de dados, os códigos fontes de sistemas desenvolvidos pela UFSJ e os servidores de arquivos.

§2º O NTInf deve designar um servidor efetivo como responsável técnico por cada serviço de TIC crítico da UFSJ, que deve auxiliar o Administrador de *Backup* na implantação e manutenção da política de *backup*.

Art. 6º A salvaguarda dos dados em formato digital pertencentes a serviços de TIC da UFSJ, 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
OPERAÇÕES
Seção I
Dos Princípios Gerais

Art. 7º Esta política é norteada pelos princípios básicos da Política de Segurança da Informação e Comunicação (POSIC) da UFSJ, que considera os princípios da confidencialidade, da disponibilidade, da integridade, e da autenticidade.

Art. 8º Esta Política de *Backup* e Recuperação de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 9º As rotinas de *backup* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TIC críticos da UFSJ.

Parágrafo único. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelos responsáveis pelos serviços de TIC.

Art. 10. As rotinas de *backup* devem possuir requisitos mínimos, diferenciados de acordo com o tipo de serviço de TIC ou dado salvaguardado, dando prioridade aos serviços de TIC críticos da UFSJ.

Art. 11. Cabe aos responsáveis prever a realização de testes periódicos de restauração, no intuito de averiguar os processos de *backup* e estabelecer melhorias.

Art. 12. Deve-se inutilizar as mídias defeituosas, ou aquelas que não serão mais utilizadas, antes do descarte, a fim de impossibilitar a recuperação dos dados por terceiros.

§ 1º O NTInf deve garantir que a mídia não contenha mais imagens de *backup* ativas e que os conteúdos, atuais ou anteriores, não possam ser lidos ou recuperados por terceiros não autorizados.

§ 2º O NTInf deve providenciar a destruição física da mídia antes do descarte.

Art. 13. Em situações em que a confidencialidade é importante e a encriptação é tecnicamente viável, as cópias de segurança devem ser protegidas por meio de encriptação.

Art. 14. As rotinas de *backup* devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 15. Os ativos envolvidos no processo de *backup* são considerados ativos críticos para a UFSJ.

§ 1º Compete ao NTInf providenciar, com as justificativas pertinentes, a aquisição de equipamentos necessários para manter o parque de ativos atualizado e em quantidade necessária ao atendimento das demandas da UFSJ.

§ 2º 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 NTInf.

§ 3º 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 de recuperação de dados - *Recovery Time Objective* (RTO);

V - o custo de aquisição da unidade de armazenamento de *backup*; e

VI - a vida útil da unidade de armazenamento de *backup*.

§ 4º A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 16. 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.

Seção II
Da Frequência e Retenção dos Dados

Art. 17. Os *backups* dos serviços de TIC da UFSJ devem ser realizados utilizando ao menos uma das seguintes frequências temporais:

I – diária;

II – semanal;

III – mensal; ou

IV – anual.

Art. 18. Os serviços de TIC da UFSJ devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I - Diária: 1 mês;

II - Semanal: 2 meses;

III - Mensal: 6 meses;

IV - Anual: 2 anos.

Parágrafo único. Especificidades dos serviços de TIC podem demandar frequência e tempo de retenção diferenciados, que devem ser determinados pelo Administrador de *Backup*.

Art. 19. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais, encaminhadas ao Administrador de *Backup* da UFSJ.

Parágrafo único. A aprovação para execução da alteração referida no *caput* depende da anuência do CGTI.

Art. 20. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança.

Parágrafo único. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

Art. 21. 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.

Art. 22. Salvo indicação em contrário, aprovada pelo Administrador de *Backup*, o *backup* dos dados dos serviços de TIC da UFSJ deve ser feito de acordo com a seguinte programação padrão:

I - *Backup* incremental diário (sábado a quinta-feira), armazenado no local.

II - *Backup* diferencial semanal (sexta-feira), armazenado local e externamente.

III - *Backup* completo mensal, armazenado local e externamente.

Art. 23. O Administrador de *Backup* deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da UFSJ, garantindo que o tráfego necessário às atividades de backup não ocasione indisponibilidade dos demais serviços de TIC da UFSJ.

Art. 24. A execução do *backup* deve concentrar-se, preferencialmente, no período de janela de *backup*.

Parágrafo único. O período de janela de backup deve ser determinado pelo Administrador de *Backup*, em conjunto com servidor designado pelo chefe do Setor de Internet e Redes (SETIR).

Seção III
Dos Testes de Backup

Art. 25. Os *backups* devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

§ 1º Os *backups* devem ser validados e certificados, preferencialmente de maneira automática, imediatamente após a execução da cópia.

§ 2º O responsável técnico pelo serviço de TIC deve confirmar a integridade do *backup*.

§ 3º Em caso de falha, o responsável técnico pelo serviço de TIC deve tomar as devidas providências.

§ 4º Diariamente, os logs de *backup* devem ser revisados em busca de erros ou durações anormais, e em busca de
oportunidades para melhorar o desempenho do *backup*.

§ 5º O NTInf deve manter registros de *backups* e testes de restauração para demonstrar conformidade com esta política.

§ 6º Os testes devem ser realizados para todos os *backups* dos ambientes de produção.

Art. 26. Além das validações automatizadas, os pontos de restauração dos sistemas institucionais devem passar por inspeção e validação manual sempre que o responsável técnico julgar necessário.

Seção IV
Dos Procedimentos de Restauração do *Backup*

Art. 27. 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 dados deve sempre partir do responsável pelo recurso ou responsável pelo serviço de TIC que gera, manipula e armazena os dados, por meio de registro de chamado no Sistema de Abertura de Chamados (SAC) do NTInf.

II - A restauração de dados somente será possível nos casos em que estes tenham sido atingidos pela estratégia de *backup*.

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

IV - O Administrador de *Backup* terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, sendo permitido ao gestor da unidade do demandante apresentar recurso da negativa ao CGTI.

Art. 28. O tempo de restauração é proporcional ao volume de dados necessários para a restauração e à capacidade de processamento dos ativos de *backup* da UFSJ.

CAPÍTULO III
DA GOVERNANÇA E RESPONSABILIDADES

Art. 29. A governança e a responsabilidade na garantia do pleno funcionamento do serviço de *backup* da UFSJ devem ser do NTInf.

Art. 30. O Administrador de *Backup* deve ser capacitado para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Parágrafo único. O Administrador de *Backup* deve ser designado, dentre os servidores efetivos do NTInf, pelo diretor do NTInf.

Art. 31. São atribuições do Administrador de *Backup*:

I - propor soluções de cópia de segurança dos dados gerados ou manipulados pelos serviços de TIC críticos, mantidos
pela UFSJ;

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 auxiliar a sua execução;

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 à Direção do NTInf 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 - configurar a execução dos testes de restauração;

XII - restaurar ou recuperar os *backups* em caso de necessidade; e

XIII - operar e manusear as unidades de armazenamento de *backups*.

Art. 32. São atribuições dos responsáveis pelos serviços de TIC críticos da UFSJ:

I - identificar os dados (bancos de dados, códigos fontes, servidores de arquivos etc.), relacionados a cada serviço de TIC sob sua responsabilidade, que deverão ser salvaguardados por meio de rotinas de *backup*;

II - solicitar a implementação de rotina de backup para cada serviço de TIC sob sua responsabilidade, por meio do registro de chamado no Sistema de Abertura de Chamados (SAC) do NTInf;

III - dar permissão ou fornecer usuário de acesso ao Administrador de *Backup* para instalar e configurar as ferramentas no ambiente onde residem os dados que serão incluídos na rotina de *backup*;

IV - auxiliar o Administrador de *Backup* na definição dos procedimentos de restauração de *backups* relacionados aos serviços de TIC sob sua responsabilidade;

V - auxiliar o Administrador de *Backup* na configuração ou implementação dos testes de restauração de *backups* relacionados aos serviços de TIC sob sua responsabilidade;

VI - validar o resultado dos testes de restauração de *backups* relacionados

a cada serviço de TIC sob sua responsabilidade e comunicar ao Administrador de *Backup* sobre o resultado das validações realizadas;

VII - solicitar inclusões ou remoções de dados das rotinas de *backup* dos serviços de TIC sob sua responsabilidade, sempre que necessário;

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 33. Os casos omissos e as dúvidas surgidas na aplicação do disposto nesta Política de *Backup* e Recuperação de Dados Digitais deverão ser tratados pelo NTInf da UFSJ.

Art. 34. A Política de *Backup* e Recuperação de Dados Digitais deve ser revisada pelo NTInf no período máximo de 4 (quatro) anos de sua publicação.