



INSTRUÇÃO NORMATIVA Nº 23-AGETIC/RTR/UFMS, DE 25 DE SETEMBRO DE 2026.

Estabelece normas para a implantação, manutenção e descontinuidade de soluções tecnológicas externas na Universidade Federal de Mato Grosso do Sul.

O DIRETOR DA AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO da Fundação Universidade Federal de Mato Grosso do Sul, no uso da atribuição que lhe confere o art. 9º, caput, inciso VI, do Regimento Geral da UFMS, aprovado pela Resolução Coun nº 137, de 29 de outubro de 2021, e tendo em vista o disposto na Lei nº 13.709, de 14 de agosto de 2018, e na Lei nº 14.129, de 29 de março de 2021, e na Resolução Coun nº 333, de 21 de março de 2024, e considerando o contido no Processo nº 23104.025687/2026-71, resolve:

Art. 1º Ficam estabelecidas as normas para a implantação, manutenção e descontinuidade de sistemas, aplicações e aplicativos externos ou desenvolvidos por servidores e estudantes da UFMS no ambiente tecnológico da Fundação Universidade Federal de Mato Grosso do Sul.

CAPÍTULO I DAS DISPOSIÇÕES GERAIS

Art. 2º São objetivos desta Instrução Normativa:

- I – assegurar que as soluções implantadas atendam ao interesse institucional;
- II – preservar a segurança da informação, a continuidade dos serviços e a integridade do ambiente tecnológico institucional;
- III – promover a interoperabilidade entre soluções tecnológicas;
- IV – estabelecer responsabilidades das Unidades Demandantes, dos responsáveis técnicos e da Agência de Tecnologia da Informação e Comunicação; e
- V – assegurar que a implantação de sistemas externos ocorra de forma planejada, documentada e alinhada às normas institucionais.

CAPÍTULO II DA SOLICITAÇÃO DE IMPLANTAÇÃO

Art. 3º A implantação de qualquer sistema externo dependerá de solicitação formal da Unidade Demandante, mediante processo no Sistema Eletrônico de Informações – SEI.

Art. 4º Previamente à solicitação de implantação de qualquer software, aplicativo ou sistema desenvolvido no âmbito de projetos acadêmicos (pesquisa, extensão, inovação ou ensino) da UFMS, inclusive aqueles desenvolvidos no âmbito dos cursos de tecnologia da UFMS, o servidor responsável deverá submeter a solução à análise de Propriedade Intelectual pela Agência de Inovação – Aginova da UFMS.

Parágrafo único. A implantação em ambiente de produção ficará estritamente condicionada ao registro formal do programa de computador ou ao parecer de conformidade de Propriedade Intelectual emitido pelo Agência de Inovação, de forma a resguardar os ativos intelectuais da universidade contra pirataria, plágio e transferência indevida de tecnologia.

Art. 5º A solicitação deverá conter, no mínimo:

- I – identificação da Unidade Demandante;
- II – descrição da solução;
- III – finalidade institucional;
- IV – justificativa da necessidade;
- V – indicação dos usuários ou público-alvo;
- VI – identificação do servidor responsável, que será considerado o responsável técnico;
- VII – indicação das integrações pretendidas com sistemas institucionais, alinhadas ao interesse institucional, quando houverem;
- VIII – estimativa do impacto institucional;
- IX – informações sobre hospedagem, infraestrutura e requisitos operacionais; e
- X – documentação técnica disponível.

Parágrafo único. Deverão acompanhar a solicitação:

- I – documentação de arquitetura da solução;
- II – documentação das interfaces de integração, quando houver integração;
- III – política de privacidade e termo de uso, quando houver tratamento de dados pessoais;
- IV – plano de sustentabilidade;
- V – plano de manutenção e evolução da solução; e
- VI – demais documentos solicitados pela Agência de Tecnologia da Informação e Comunicação durante a instrução do processo.

Art. 6º A apresentação da solicitação não gera direito à implantação da solução, ficando sua aprovação condicionada à análise técnica prevista nesta Instrução Normativa.

Art. 7º A ausência das informações ou documentos necessários, que inviabilize a análise técnica, poderá ensejar diligência para complementação ou indeferimento da solicitação.

CAPÍTULO III DOS REQUISITOS TÉCNICOS

Art. 8º O sistema deverá possuir documentação técnica completa, incluindo:

- I – manuais de implantação e operação;
- II – documentação de arquitetura e dicionário de dados;
- III – especificação de dependências técnicas;
- IV – documentação de Application Programming Interfaces - APIs (padrão OpenAPI/Swagger ou equivalente);

V – evidências de testes de software (unitários, integração ou equivalentes); e

VI – documentação de manutenção preventiva e evolução a longo prazo.

Art. 9º O sistema externo deverá ser implementado usando as seguintes linguagens e tecnologias:

I – Linguagens:

- a) PHP;
- b) Java;
- c) JavaScript / TypeScript; ou
- d) Python;

II – Frameworks:

- a) CakePHP;
- b) Laravel;
- c) Spring; ou
- d) Vue.js;

III – Desenvolvimento Mobile:

- a) Flutter; ou
- b) Dart;

IV – Banco de dados:

- a) PostgreSQL; ou
- b) MariaDB; e

V – Infraestrutura:

- a) Docker;
- b) Kubernetes; ou
- c) CI/CD institucional.

§ 1º A utilização das linguagens e ferramentas deve priorizar versões com suporte de longo prazo (Long Term Support - LTS).

§ 2º É vedada a utilização de tecnologias que atingiram o estado de End of Life - EOL ou que possuam vulnerabilidades críticas conhecidas sem correção.

§ 3º Poderá ser exigido um plano de atualização tecnológica.

§ 4º Poderá ser implantado sistema externo desenvolvido em linguagem ou tecnologia diferente das listadas no caput, desde que seja aprovada pela Agência de Tecnologia da Informação e Comunicação.

Art. 10. O sistema externo deverá adotar, em sua interface, os padrões, componentes e diretrizes estabelecidos pelo Padrão Digital de Governo (Design System Gov.br), incluindo os

requisitos aplicáveis de identidade visual, experiência do usuário, responsividade e acessibilidade, disponível no endereço eletrônico <https://www.gov.br/ds/home>.

Art. 11. Todo sistema externo deverá disponibilizar uma seção ou página denominada "Sobre", acessível de forma clara ao usuário, contendo obrigatoriamente:

- I – identificação dos desenvolvedores e coordenadores do projeto;
- II – no caso de projetos vinculados à núcleos de desenvolvimento vinculados aos cursos de computação e de tecnologia, a indicação do Edital de Seleção de Proposta correspondente;
- III – número do protocolo de registro no Sistema de Informação e Gestão de Projetos - Sigproj da UFMS;
- IV – versão atual da aplicação; e
- V – links para a Política de Privacidade e Termos de Uso, conforme Política de Privacidade e Proteção de Dados Pessoais vigente e Lei nº 13.709, de 14 de agosto de 2018.

Art. 12. Os aplicativos móveis, desenvolvidos para sistemas operacionais Android e iOS, vinculados a sistemas externos deverão ser publicados exclusivamente por meio de contas institucionais nas lojas oficiais, sob responsabilidade da Agência de Tecnologia da Informação e Comunicação.

§ 1º O código-fonte dos aplicativos deverá ser integralmente disponibilizado pelo responsável técnico, incluindo histórico de versionamento, para fins de armazenamento em repositório institucional de controle de versão.

§ 2º A criação, configuração e gerenciamento das contas nas lojas Google Play e Apple App Store serão realizados exclusivamente pela Agência de Tecnologia da Informação e Comunicação.

§ 3º Compete ao responsável técnico fornecer:

- I – nome do Aplicativo (até 50 caracteres);
- II – descrição breve do aplicativo (até 80 caracteres);
- III – descrição completa do aplicativo (até 4.000 caracteres)
- VI – Política de Privacidade ou Termo de Uso;
- V – logomarca da aplicação;
- VI – ícone do aplicativo para exibição nas lojas; e
- VII – telas de apresentação (splash screen e imagens institucionais).

§ 4º Poderá ser exigida adequação dos materiais gráficos e descritivos de acordo com o Manual de Identidade Visual oficial da UFMS antes da publicação nas lojas oficiais.

§ 5º Aplicativos que realizam tratamento de dados pessoais deverão:

- I – atender integralmente à Lei nº 13.709, de 14 de agosto de 2018;
- II – informar de forma clara as permissões solicitadas ao usuário;

III – coletar apenas os dados estritamente necessários (princípio da minimização);

IV – garantir o armazenamento seguro dos dados;

V – possibilitar, quando aplicável, a revogação de consentimento e exclusão de dados; e

VI – informar o uso de serviços de terceiros (como por exemplo analytics, notificações push).

§ 6º A assinatura, publicação e atualização de versões do aplicativo deverão seguir procedimentos institucionais, sendo vedada a publicação direta por terceiros.

CAPÍTULO IV DA ANÁLISE TÉCNICA

Art. 13. Recebida a solicitação, a Agência de Tecnologia da Informação e Comunicação realizará análise técnica da solução, considerando, conforme a natureza e a complexidade do sistema:

I – o interesse institucional;

II – a aderência ao planejamento institucional e às estratégias de transformação digital;

III – a compatibilidade com a arquitetura tecnológica da UFMS;

IV – a viabilidade operacional da implantação;

V – a interoperabilidade com os sistemas institucionais;

VI – os impactos sobre a infraestrutura tecnológica, o desempenho e a continuidade dos serviços;

VII – os requisitos de acessibilidade e usabilidade;

VIII – os aspectos relacionados à segurança da informação

IX – os requisitos relativos à proteção de dados pessoais; e

X – outros aspectos técnicos considerados necessários pela Agência de Tecnologia da Informação e Comunicação.

§ 1º O nível de interesse institucional será avaliado com base em critérios qualitativos, podendo considerar:

I – alinhamento com o planejamento estratégico institucional;

II – contribuição para melhoria de serviços prestados à comunidade acadêmica ou à sociedade;

III – abrangência de público atendido (número de usuários ou unidades impactadas);

IV – relevância acadêmica, administrativa ou social da solução;

V – potencial de integração com sistemas institucionais existentes;

VI – impacto na eficiência operacional ou redução de custos;

VII – inovação tecnológica ou metodológica introduzida;

VIII – risco associado à não implantação da solução;

IX – possibilidade de reutilização por outras unidades da instituição; e

X – aderência a políticas institucionais de tecnologia da informação e segurança da informação.

§ 2º O nível de interesse institucional poderá ser classificado como:

- I – Alto: quando houver impacto institucional amplo, estratégico ou crítico;
- II – Médio: quando houver impacto relevante, porém restrito a unidades ou processos específicos; e
- III – Baixo: quando o uso for limitado, experimental ou de interesse localizado.

Art. 14. A análise técnica deverá envolver outras unidades administrativas ou instâncias de governança da Universidade, quando a matéria exigir manifestação especializada ou decisão colegiada, podendo a Agência de Tecnologia da Informação e Comunicação solicitar, quando aplicável, manifestação da unidade responsável pela proteção de dados pessoais, da unidade de segurança da informação ou de outras áreas técnicas competentes.

Art. 15. Quando a solução demandar integração com sistemas institucionais, a análise técnica considerará, além dos critérios previstos no art. 8º:

- I – a compatibilidade com arquitetura tecnológica atual;
- II – os impactos sobre sistemas já implantados;
- III – o uso de APIs institucionais e padrões de interoperabilidade;
- IV – o consumo de dados institucionais;
- V – os impactos em desempenho, recursos e infraestrutura;
- VI – os requisitos de acessibilidade, conforme o Modelo de Acessibilidade em Governo Eletrônico - eMAG e a Lei nº 13.146, de 6 de julho de 2015.
- VII – a consistência e integridade dos dados compartilhados; e
- VIII – os mecanismos de autenticação, autorização e rastreabilidade das integrações.

Art. 16. Durante a análise técnica, a Agência de Tecnologia da Informação e Comunicação poderá solicitar esclarecimentos, documentação complementar, demonstrações da solução ou acesso a ambientes de homologação, quando necessários à formação de seu entendimento técnico.

Art. 17. A análise técnica observará, sempre que aplicável:

- I – a Política de Segurança da Informação da UFMS;
- II – a Política de Inteligência Artificial da UFMS;
- III – a Instrução Normativa que disciplina o inventário de soluções de software, as listas de softwares e bibliotecas autorizadas e o tratamento de software não autorizado;
- IV – a legislação relativa à proteção de dados pessoais;
- V – as normas internas de arquitetura, interoperabilidade, desenvolvimento de software e infraestrutura tecnológica; e
- VI – os demais instrumentos de governança digital editados pela Agência de Tecnologia da Informação e Comunicação.

Art. 18. A análise técnica observará a natureza, a complexidade, a criticidade e os riscos associados à solução tecnológica externa, podendo a Agência de Tecnologia da Informação e

Comunicação estabelecer procedimentos diferenciados para soluções de baixo, médio ou alto impacto institucional.

Art. 19. Ao término da análise técnica, a Agência de Tecnologia da Informação e Comunicação emitirá parecer técnico, podendo concluir pelo:

- I – deferimento da implantação;
- II – deferimento condicionado ao atendimento de exigências técnicas;
- III – necessidade de complementação de informações; ou
- IV – indeferimento da solicitação.

§ 1º O parecer técnico deverá apresentar, de forma motivada, os fundamentos da decisão.

§ 2º O indeferimento poderá ocorrer, entre outras hipóteses, quando houver:

- I – incompatibilidade com a arquitetura tecnológica institucional;
- II – riscos relevantes à segurança da informação ou à proteção de dados pessoais;
- III – duplicidade injustificada em relação a solução institucional existente;
- IV – inviabilidade operacional ou técnica;
- V – ausência de responsável técnico ou de plano mínimo de manutenção da solução; ou
- VI – desconformidade com as normas institucionais aplicáveis.

Art. 20. Todas as imagens, fontes, logomarcas, entre outros, utilizados no sistema, aplicação ou aplicativo deverão estar de acordo com o Manual de Identidade visual da UFMS vigente, e caso necessário, após análise técnica, passará por uma análise conjunta entre a Agência de Tecnologia da Informação e Comunicação e a Agência de Comunicação Social e Científica.

CAPÍTULO V DA IMPLANTAÇÃO

Art. 21. A implantação da solução somente poderá ocorrer após a conclusão favorável da análise técnica prevista nesta Instrução Normativa e o atendimento das eventuais condicionantes estabelecidas no parecer técnico, observados os requisitos e as verificações previstos no Checklist de Implantação, constante do Anexo I a esta Instrução Normativa.

Parágrafo único. A implantação inicial será responsabilidade da unidade solicitante, com o servidor responsável técnico, sob supervisão da Agência de Tecnologia da Informação e Comunicação.

CAPÍTULO VI DA MANUTENÇÃO E EVOLUÇÃO

Art. 22. A manutenção corretiva, adaptativa, evolutiva e preventiva da solução permanecerá sob responsabilidade do servidor responsável técnico indicado no processo administrativo.

Art. 23. A Unidade Demandante deverá assegurar a existência de servidor responsável técnico durante todo o período de utilização da solução.

Parágrafo único. A substituição de servidor responsável técnico deverá ser comunicada à Agência de Tecnologia da Informação e Comunicação no prazo de até trinta dias, acompanhada da identificação do novo responsável.

Art. 24. Alterações que possam modificar significativamente a arquitetura, a infraestrutura, os mecanismos de integração, o tratamento de dados pessoais ou os requisitos de segurança da solução poderão ser submetidas a nova análise técnica, a critério da Agência de Tecnologia da Informação e Comunicação.

CAPÍTULO VII DA DESCONTINUIDADE

Art. 25. A Agência de Tecnologia da Informação e Comunicação poderá recomendar a descontinuidade da solução quando verificada, entre outras hipóteses:

- I – inexistência de servidor responsável técnico;
- II – ausência de manutenção que comprometa a continuidade da solução;
- III – riscos relevantes à segurança da informação ou à proteção de dados pessoais;
- IV – incompatibilidade superveniente com a arquitetura tecnológica institucional;
- V – substituição por solução institucional equivalente; ou
- VI – perda do interesse institucional.

§ 1º Sempre que possível, a Unidade Demandante será previamente comunicada para apresentação de plano de adequação ou de transição.

§ 2º A descontinuidade deverá observar medidas destinadas à preservação da continuidade dos serviços, da integridade das informações e da destinação adequada dos dados institucionais.

Art. 26. Confirmada a descontinuidade da solução, deverão ser adotadas, conforme aplicável, as seguintes ações:

- I – comunicar formalmente aos responsáveis pela solução a decisão de descontinuidade, indicando a data prevista para sua efetivação e as providências necessárias à transição;
- II – realizar, previamente à descontinuidade, a preservação das informações institucionais armazenadas na solução, mediante cópia de segurança ou outro mecanismo tecnicamente adequado;
- III – realizar o desligamento do servidor de aplicação, máquina virtual, serviço ou demais componentes de infraestrutura relacionados à solução, após a conclusão das providências de preservação e transição;
- IV – realizar a extração ou dump das bases de dados, arquivos e demais informações institucionais pertinentes, quando necessário, assegurando sua integridade e disponibilidade para a Unidade Demandante ou para a unidade responsável pela custódia das informações;
- V – revogar ou desabilitar contas, credenciais, chaves, certificados, integrações, acessos e demais mecanismos de autenticação ou comunicação associados à solução;
- VI – interromper as integrações, rotinas automatizadas, agendamentos e demais serviços vinculados à solução, de modo a evitar seu funcionamento indevido após a data de

descontinuidade; e

VII – providenciar a destinação adequada dos dados, arquivos e demais informações da solução, observados os prazos de retenção, as regras de classificação da informação, a legislação aplicável e as normas institucionais de segurança da informação e proteção de dados pessoais.

CAPÍTULO VIII DA PROTEÇÃO DE DADOS

Art. 27. Soluções que realizem o tratamento de dados pessoais deverão demonstrar conformidade com a Lei nº 13.709, de 14 de agosto de 2018, e observar as diretrizes institucionais relativas à privacidade e à proteção de dados.

Parágrafo único. Sempre que necessário, poderão ser solicitadas informações adicionais destinadas à análise dos riscos relacionados ao tratamento de dados pessoais.

Art. 28. A análise de conformidade e segurança da informação será realizada de forma compatível com a criticidade, a abrangência e os riscos da solução e deverá considerar, entre outras medidas, os seguintes quesitos:

- I – finalidade e base legal para o tratamento;
- II – aplicação dos princípios de minimização de dados e de armazenamento seguro;
- III – mecanismos de controle de acesso e trilhas de auditoria;
- IV – registro de atividades de tratamento (log de operações); e
- V – análise de vulnerabilidades.

Parágrafo único. A Agência de Tecnologia da Informação e Comunicação poderá exigir a realização de testes de segurança ou outras avaliações especializadas antes da implantação da solução, sempre que a natureza ou o risco do sistema assim justificar.

CAPÍTULO IX DA SEGURANÇA DA INFORMAÇÃO

Art. 29. Antes da implantação, o sistema deverá passar por análise de segurança.

Art. 30. Será obrigatória a realização de testes de segurança (pentest) ou análise de vulnerabilidades.

Art. 31. A implantação somente ocorrerá após correção de vulnerabilidades críticas e parecer favorável da Agência de Tecnologia da Informação e Comunicação.

Art. 32. Para permitir a auditoria e investigação de incidentes, o sistema deverá registrar logs de:

- I – acesso;
- II – autenticação;
- III – operações relevantes; e
- IV – falhas e exceções.

Art. 33. O Sistema deverá possuir mecanismo de controle de acesso baseado em perfis ou papéis (Role-Based Access Control - RBAC), quando aplicável.

CAPÍTULO X DAS COMPETÊNCIAS

Art. 34. Compete à Unidade Demandante:

- I – assegurar que as informações prestadas durante a instrução do processo permaneçam atualizadas;
- II – disponibilizar os recursos necessários para implantação da solução, quando de sua responsabilidade;
- III – acompanhar a implantação e homologar o atendimento dos requisitos funcionais da solução; e
- IV – comunicar à Agência de Tecnologia da Informação e Comunicação alterações relevantes que possam impactar a operação, a segurança ou a integração do sistema.

Art. 35. Compete ao servidor responsável técnico:

- I – fornecer as informações técnicas necessárias durante o processo de análise;
- II – executar ou acompanhar as atividades técnicas de implantação, quando aplicável;
- III – manter documentação técnica atualizada;
- IV – apoiar a correção de falhas identificadas durante a implantação; e
- V – comunicar à Unidade Demandante alterações que possam impactar a operação da solução.

Art. 36. Compete à Agência de Tecnologia da Informação e Comunicação:

- I – coordenar as atividades técnicas necessárias à implantação no ambiente institucional;
- II – definir os procedimentos técnicos necessários para disponibilização da solução;
- III – acompanhar a execução das condicionantes estabelecidas no parecer técnico;
- IV – autorizar a entrada da solução em ambiente de produção; e
- V – registrar a implantação nos controles administrativos e tecnológicos institucionais, quando aplicável.

Parágrafo único. A autorização para implantação não transfere à Agência de Tecnologia da Informação e Comunicação a responsabilidade pelo desenvolvimento, evolução funcional ou manutenção da solução, salvo quando houver ato formal que disponha em sentido diverso.

CAPÍTULO XI DAS DISPOSIÇÕES FINAIS

Art. 37. As soluções disciplinadas por esta Instrução Normativa permanecem sujeitas às normas institucionais relativas à governança de software, segurança da informação, proteção de dados pessoais, gestão de riscos, continuidade dos serviços, desenvolvimento de software e governança digital.

Parágrafo único. A utilização de softwares, bibliotecas, frameworks, componentes, serviços e demais tecnologias observará as listas institucionais de autorização e os respectivos critérios



técnicos estabelecidos pela Agência de Tecnologia da Informação e Comunicação.

Art. 38. Os casos omissos serão resolvidos pela Agência de Tecnologia da Informação e Comunicação, podendo ser submetidos à instância de governança competente quando a matéria exigir deliberação institucional.

Art. 39. Esta Instrução Normativa entra em vigor na data de sua publicação.

ANEXO I – CHECKLIST DE IMPLANTAÇÃO
(INSTRUÇÃO NORMATIVA Nº 23-AGETIC/RTR/UFMS, DE 25 DE SETEMBRO DE 2026.)

1. Informações Gerais:

- ☐ Justificativa Institucional
- ☐ Responsável Técnico definido
- ☐ Unidade Demandante identificada

2. Documentação Técnica:

- ☐ Manual de Implantação
- ☐ Manual de Operação
- ☐ Arquitetura do Sistema

3. Integração com Sistemas Institucionais:

- ☐ Análise Técnica da TI
- ☐ Definição de APIs e Integrações

4. Proteção de Dados (LGPD):

- ☐ Identificação de Dados Pessoais Tratados
- ☐ Base Legal definida
- ☐ Controle de Acesso implementado

5. Segurança:

- ☐ Análise de Vulnerabilidades realizada
- ☐ Pentest executado
- ☐ Correção de Vulnerabilidades críticas

6. Infraestrutura:

- ☐ Compatibilidade com Tecnologias Institucionais
- ☐ Logs e Monitoramento configurados

7. Aplicativos Móveis (quando aplicável):

- ☐ Publicação em Conta Institucional

- ☐ Código-fonte entregue
- ☐ Política de Privacidade ou Termo de Uso disponível
- ☐ Conformidade com LGPD
- ☐ Identidade Visual validada

ANDERSON VIÇOSO DE ARAUJO

Diretor da Agência de Tecnologia da Informação e Comunicação

NOTA
MÁXIMA
NO MEC

UFMS
É 10!!!



Documento assinado eletronicamente por **Anderson Viçoso de Araujo, Diretor(a)**, em 26/09/2026, às 14:46, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.ufms.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6694107** e o código CRC **2482F6E9**.

AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Av Costa e Silva, s/nº - Cidade Universitária

Fone: (67)3345-7669

CEP 79070-900 - Campo Grande - MS