Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais
IFSULDEMINAS

INTE Nº1/2025/DTI/IFSULDEMINAS

Diretrizes para o processo de desenvolvimento de softwares do IFSULDEMINAS - versão 1
Diretoria de Tecnologia da Informação - DTI
IFSULDEMINAS

A DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA REITORIA DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SUL DE MINAS GERAIS - IFSULDEMINAS, no uso das atribuições legais que lhe são conferidas.

CONSIDERANDO:

- O Plano de Desenvolvimento Institucional do IFSULDEMINAS 2024-2028;
- A Política de Governança de Tecnologia da Informação do IFSULDEMINAS - Resolução Nº 308/2022 de 21 de dezembro de 2022;
- O Plano Diretor de Tecnologia da Informação do IFSULDEMINAS 2024-2026 - Resolução Nº 365/2023 de 14 de dezembro de 2023;
- A Política de Segurança da Informação do IFSULDEMINAS - Resolução N.º 355/2023 de 13 de novembro de 2023;
- A Política de Privacidade e Proteção de Dados do IFSULDEMINAS - Resolução N° 131/2021 de 15 de setembro de 2021.
- Política de Solicitação e Sustentação de Software do IFSULDEMINAS - Resolução N° 482/2025 de 29 de outubro de 2025.
- O Programa de Privacidade e Segurança da Informação (PPSI) da Secretaria de Governo Digital - Portaria SGD/MGI Nº 852, de 28 de março de 2023.
- O Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para Aplicações Web - versão 2.0.

RESOLVE:

CAPÍTULO I - DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Instrução Técnica estabelece diretrizes para o Processo de desenvolvimento de software do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais (IFSULDEMINAS), visando a garantia e melhoria contínua dos atributos de arquitetura, qualidade, acessibilidade, interoperabilidade, segurança e privacidade, governança, transparência e conformidade dos processos de software.

Art. 2º Esta Instrução Técnica deve ser aplicada a todas as soluções de software desenvolvidas ou mantidas pelas Unidades Provedoras de Solução (UPS) do IFSULDEMINAS, conforme as disposições da Política de Governança de Tecnologia da Informação (PGTI) e da Política de Segurança da Informação (PSI) da Instituição e demais resoluções e políticas relacionadas.

Art. 3º Qualquer solução de software desenvolvida no escopo de projetos de ensino, pesquisa ou extensão no IFSULDEMINAS e que venha a ser utilizada como solução institucional de abrangência comum ou exclusiva, nos termos do inciso IV, § 1º, do artigo 7º da PGTI, deverá ser aprovada pela UPS da unidade onde a solução será implantada, de forma que sejam alinhados aspectos como atendimento e suporte ao usuário, manutenção e sustentação da solução.

§1º Para esses casos, deve-se ainda determinar uma Unidade Gestora de Solução (UGS).

§2º Uma vez aprovada, a solução deve atender os requisitos previstos nesta Instrução Técnica, no prazo de até 12 (doze) meses.

§3º Os eventuais responsáveis docentes e/ou estudantes pela solução, assim como a UGS e interlocutores, deverão ser designados por meio de portaria publicada pelo dirigente máximo da unidade da UPS onde a solução será implantada.

CAPÍTULO II – DOS OBJETIVOS

Art. 4º São objetivos desta Instrução Técnica:

I. Assegurar que o processo de desenvolvimento de software esteja alinhado às políticas institucionais, incluindo a PGTI e a PSI e demais políticas aplicáveis à Administração Pública Federal.

II. Padronizar o processo de desenvolvimento de software a fim de assegurar aspectos relacionados à segurança, acessibilidade, interoperabilidade, confidencialidade, integridade, conformidade legal e qualidade.

III. Assegurar o cumprimento de requisitos técnicos mínimos estabelecidos pela Instituição.

IV. Dar transparência ao processo de desenvolvimento de modo a garantir que os interessados acompanhem as informações sobre as etapas que o constituem.

CAPÍTULO III – DOS REQUISITOS DE PRIVACIDADE E SEGURANÇA

Art. 5º As aplicações devem adotar os princípios de segurança e privacidade desde a concepção (*Security By Design* e *Privacy By Design*), garantindo que estes atributos sejam elementos centrais em todas as etapas do ciclo de vida do software.

§1º Esses princípios asseguram que as medidas protetivas de dados pessoais e de segurança da informação sejam implementadas de forma preventiva e contínua, minimizando riscos desde a concepção do projeto.

§2º Todo o processo de desenvolvimento, manutenção e operação de aplicações deverá observar as disposições contidas no **Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para Aplicações Web (BRASIL, 2023)** do Programa de Privacidade e Segurança da Informação - PPSI **(BRASIL, 2023)**, bem como normas complementares aplicáveis, além das práticas de desenvolvimento seguro listadas a seguir:

I. validação de dados;
II. proteção contra injeções;
III. controle de acesso robusto;
IV. bibliotecas atualizadas;
V. armazenamento seguro de senhas;
VI. uso de comunicação segura (HTTPs);
VII. registro e auditoria de todo acesso ou tentativa de acesso realizado;
VIII. tratamento adequado de erros e exceções;
IX. autenticação em duplo fator ou via GovBR, quando aplicáveis;
X. revisão de código e testes de segurança.

Art. 6º As aplicações deverão respeitar os requisitos relacionados à coleta, uso e retenção de dados pessoais, previstos na Política de Privacidade e Proteção de Dados do IFSULDEMINAS, além dos requisitos listados a seguir:

I. Limitar os dados pessoais coletados ao mínimo necessário para atingir o objetivo da aplicação, conforme o princípio da minimização de dados;
II. Informar claramente aos usuários sobre a Política de Privacidade e Proteção de Dados;
III. Implementar mecanismos para obter o consentimento do usuário sempre que necessário.

Art. 7º Por padrão, os desenvolvedores deverão utilizar bancos de dados anonimizados durante os

processos de desenvolvimento e testes. Caso seja necessário a utilização de banco de dados com dados sensíveis, o desenvolvedor deverá justificar e notificar o coordenador da Unidade Provedora da Solução via e-mail.

Art. 8º Sempre que um requisito da solução entrar em conflito com as diretrizes e requisitos de privacidade e segurança, estes terão prioridade sobre os demais, ainda que gerem impactos negativos no negócio, usabilidade ou qualquer outro requisito.

Art. 9º Para garantir a segurança das aplicações, estas deverão ser submetidas a testes de segurança baseados no *OWASP Top Ten* (https://owasp.org/www-project-top-ten/), com o objetivo de identificar e mitigar os riscos mais comuns associados a vulnerabilidades em aplicações web.

Art. 10º Os desenvolvedores e a UGS deverão garantir que todas as diretrizes de privacidade e segurança sejam cumpridas, com suporte da CGDTI/DTI para auditorias técnicas.

Art. 11º Os requisitos de privacidade e segurança serão revisados periodicamente para garantir conformidade com atualizações da LGPD e normativas governamentais.

CAPÍTULO IV – DOS REQUISITOS DE ARQUITETURA

Art. 12º As aplicações devem ser versionadas em *GIT*.

§1º As aplicações de abrangência comum, nos termos do artigo 7º da PGTI, devem ser versionadas no *GitLab* institucional do IFSULDEMINAS, na DTI.

§2º As aplicações de abrangência exclusiva, nos termos do artigo 7º da PGTI, devem ser versionadas no *GitLab* da unidade provedora da solução.

Art. 13º As aplicações devem utilizar a tecnologia *Docker* para conteinerização dos serviços necessários.

Art. 14º As aplicações devem prover mecanismos de *CI/CD* (*Continuous Integration / Continuous Delivery*) automatizados para homologação e produção por meio da ferramenta *GitLab*.

Art. 15º As aplicações deverão ser desenvolvidas utilizando *frameworks* e arquiteturas reconhecidas no mercado, com foco em modularidade, manutenibilidade e segurança.

§1º Deverá ser adotado, preferencialmente, o Django como *framework* principal de aplicações web. No caso de aplicações PHP, deverá ser adotado, preferencialmente, o *framework CodeIgniter*.

CAPÍTULO V – DOS REQUISITOS DE AUTENTICAÇÃO

Art. 16º As aplicações desenvolvidas deverão possuir mecanismo de autenticação integrado com a base de autenticação única (provedor de identidade) do SUAP, seguindo o modelo de SSO (*Single Sign On*).

§1º Admitirá-se que o SSO do SUAP não seja utilizado em casos em que, justificadamente, essa não seja a melhor solução.

Art. 17º A integração com o Login Único (GOV.BR) deverá, sempre que possível, ser implementada para aplicações que possuam público externo (usuários não vinculados à Instituição) e recomendada para aplicações que possuam apenas público interno de acordo com a **Lei nº 14.534/2023** (BRASIL, 2023) e **Roteiro de Integração do Login Único** (BRASIL, 2025).

§1º Ao utilizar a API do GOV.BR, poderá ser exigido mecanismo de autenticação multifator (MFA) e estabelecido o nível mínimo de conta que o cidadão deve possuir, de acordo com a finalidade da aplicação.

CAPÍTULO VI – DOS REQUISITOS DE INTERFACE E ACESSIBILIDADE

Art. 18º As aplicações desenvolvidas deverão adotar como modelo de interface o Padrão Digital de Governo (GOV.BR *Design System*) **conforme a Portaria MCOM nº 540/2020**, salvo em situações em que este, justificadamente, não possa ser utilizado.

Art. 19º São requisitos obrigatórios de interface:

I. Responsividade para dispositivos móveis;
II. Atendimento aos critérios do Modelo de Acessibilidade em Governo Eletrônico (eMAG) e às diretrizes WCAG (*Web Content Accessibility Guideline*), versão 2 ou superior, garantindo no mínimo o nível A de acessibilidade web do *WCAG* nas aplicações, sendo desejável garantir o nível AA ou AAA;
III. Compatibilidade *cross-browser*, ou seja, funcionamento adequado nos navegadores mais utilizados;
IV. Facilidade de navegação: uso de menus intuitivos e caminhos simplificados, a fim de entregar uma boa experiência ao usuário;
V. *Feedback* claro ao usuário: mensagens e indicações visuais claras em caso de ações, erros ou sucesso.

CAPÍTULO VII – DOS REQUISITOS DE INTEROPERABILIDADE

Art. 20º As aplicações deverão adotar protocolos de comunicação amplamente reconhecidos para garantir interoperabilidade entre sistemas internos e externos.

Art. 21º As informações públicas das aplicações deverão utilizar padrões de dados abertos e formatos estruturados, adotando formatos abertos como JSON, XML ou CSV, conforme a Política de Dados Abertos do IFSULDEMINAS, e a do Poder Executivo Federal e suas atualizações e ramificações.

Art. 22º Quando aplicável, conforme estabelecido na resolução dos **Registros de Referência da Infraestrutura Nacional de Dados (BRASIL, 2021)**, as aplicações deverão estar integradas com as APIs do programa Conecta GOV para o consumo de dados de usuários, tais como:

I. Cadastro Base do Cidadão (CPF Light);
II. CadÚnico Serviços;
III. Cadastro Base de Endereço (CEP);
IV. Consulta CNPJ;
V. Faixa de Renda de Grupo Familiar;
VI. Pessoa com Deficiência;
VII. Situação Militar;
VIII. PagTesouro;
IX. SIAPE Consultas;
X. API DOU - Diário Oficial da União;
XI. Registro de Referência - Estruturas Organizacionais do Poder Executivo Federal (SIORG);

CAPÍTULO VIII – DOS REQUISITOS DE DESEMPENHO

Art. 23º As funcionalidades das aplicações devem ser massivamente testadas para garantir conformidade com os requisitos de negócio. Para isto, podem ser realizados testes de unidade em código e testes ponta-a-ponta (*end-to-end* - E2E), quando aplicável.

§1º Os testes E2E deverão, preferencialmente, ser automatizados, utilizando-se de ferramentas como *Selenium* e *Cypress*.

§2º No caso de novos sistemas ou novas funcionalidades, a UGS demandante deverá realizar os testes com o objetivo de homologar a entrega da demanda.

Art. 24º As aplicações deverão passar por testes de carga e desempenho, sendo recomendado o uso da ferramenta *JMeter*.

Art. 25º Para que seja assegurada a qualidade da aplicação, especialmente os requisitos elencados no Capítulo III, as aplicações deverão ser testadas em ferramentas específicas, como por exemplo, o Google Lighthouse ou ferramenta equivalente.

CAPÍTULO IX – DOS REQUISITOS DE MONITORAMENTO E AUDITORIA

Art. 26º Todos os sistemas deverão possuir mecanismos de *logging* para auditoria, diagnóstico e monitoramento de desempenho.

§1º Os logs, especialmente de eventos críticos como tentativas de acesso, alterações de dados e falhas, devem ser registrados e persistidos em ferramenta de armazenamento, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

§2º As aplicações devem prover mecanismo de monitoramento de erros e exceções, por exemplo, a ferramenta *Sentry*.

§3º As aplicações devem prover mecanismo de monitoramento de acessos, como as ferramentas *Graylog* e Google Analytics.

Art. 27º As aplicações deverão possuir gerenciamento de perfis e níveis de acesso, sendo responsabilidade da UGS a definição das atribuições dos níveis aos usuários, conforme previsto na PGTI.

CAPÍTULO X – DOS DEMAIS REQUISITOS

Art. 28º As aplicações deverão ter mecanismos de *backup* de acordo com a Política de Backup e Restauração de dados digitais do IFSULDEMINAS.

Art. 29º Novas funcionalidades ou sistemas, preferencialmente, devem ser desenvolvidos sob o ambiente do SUAP, a fim de promover uma maior eficiência no uso dos recursos tecnológicos e humanos da Instituição e garantir maior integração, interoperabilidade e uniformidade nas soluções implementadas.

§1º Em casos excepcionais, onde a aplicação ou funcionalidade não seja desenvolvida no ambiente SUAP, uma justificativa deverá ser encaminhada juntamente com a solicitação de aprovação da solução junto ao CGTI.

Art. 30º Os requisitos elencados neste capítulo devem ser adotados como padrão institucional, no entanto, situações excepcionais poderão permitir alternativas, desde que devidamente fundamentadas, documentadas e aprovadas pela Diretoria de Tecnologia da Informação do IFSULDEMINAS.

Art. 31º As aplicações deverão seguir o processo de remediação e correção de vulnerabilidades de acordo com a Política de gestão de vulnerabilidades do IFSULDEMINAS.

CAPÍTULO XI – DO USO DE SOFTWARE LIVRE

Art. 32º As soluções de código aberto utilizadas no contexto do desenvolvimento de software deverão ser priorizadas sempre que viáveis tecnicamente.

§1º O uso de solução proprietária no contexto do desenvolvimento de software, mesmo que gratuito, deverá ser justificado e documentado.

CAPÍTULO XII – DO CICLO DE VIDA

Art. 33º O ciclo de desenvolvimento pode ser iniciado a partir de um dos 2 processos definidos pela PSS - Política de Solicitação e Sustentação de Software do Ifsuldeminas (IFSULDEMINAS, 2025) a seguir:

- Processo de Solicitação de Software (PSS, Anexo II);
- Processo de Sustentação de Software (PSS, Anexo VI).

§1º Uma vez iniciado o processo, todo o ciclo de vida envolve 3 processos nesta sequência:

- Processo de Planejamento e Execução (PSS, Anexo III);
- Processo de Testes (PSS, Anexo IV);
- Processo de Entrega (PSS, Anexo V).

Referências

IFSULDEMINAS. Resolução 482/2025/CONSUP/IFSULDEMINAS. Política de Solicitação e Sustentação de Software do Ifsuldeminas (PSS). Pouso Alegre: IFSULDEMINAS, 2025. Disponível em: https://portal.ifsuldeminas.edu.br/attachments/article/1010/Resolucao482-2025.pdf.pdf.

BRASIL. Secretaria de Governo Digital. *Programa de Privacidade e Segurança da Informação (PPSI).* Brasília, DF: Secretaria de Governo Digital, Instituído pela Portaria SGD/MGI nº 852, de 28 mar. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-atual. Acesso em: 25 jun. 2025.

BRASIL. Secretaria de Governo Digital. *Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para Aplicações Web.* Brasília, DF: Ministério da Economia, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_requisitos_minimos_web.pdf. Acesso em: 25 jun. 2025.

BRASIL. Secretaria de Governo Digital. *Guia de requisitos mínimos de segurança e privacidade para APIs.* Brasília, DF: Ministério da Economia; Secretaria de Governo Digital, set. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/guia-do-gestor/documentos/sessoes-tematicas-do-sisp-2021/sic-guia-api.pdf. Acesso em: 25 jun. 2025.

BRASIL. Secretaria de Governo Digital. *Registros de Referência da Infraestrutura Nacional de Dados.* Brasília, DF: Secretaria de Governo Digital, 25 jan. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/interoperabilidade/registros-de-referencia. Acesso em: 25 jun. 2025.

BRASIL. Ministério da Gestão e Inovação em Serviços Públicos; Secretaria de Governo Digital. *Design System do Governo Federal – Padrão Digital de Governo.* Portaria MCOM nº 540, de 2020, que disciplina a implantação e gestão do Padrão Digital de Governo dos órgãos e entidades do Poder Executivo federal. Brasília, DF, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/transformacao-digital/ferramentas/design-system. Acesso em: 25 jun. 2025.

BRASIL. Secretaria de Governo Digital. *Roteiro de Integração do Login Único*. Brasília, DF: Secretaria de Governo Digital, [ano]. Disponível em: https://acesso.gov.br/roteiro-tecnico/. Acesso em: 25 jun. 2025.

BRASIL. *Lei nº 14.534, de 11 de janeiro de 2023.* Altera as Leis nºs 7.116/1983, 9.454/1997, 13.444/2017 e 13.460/2017 para adotar número único para documentos e estabelecer o CPF como identificação suficiente nos bancos de dados de serviços públicos. Diário Oficial da União, Seção 1 (Extra), Brasília, DF, 11 jan. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14534.htm. Acesso em: 25 jun. 2025.