

GUIA PRÁTICO DE DESENVOLVIMENTO DE SISTEMAS COM IA

Diretrizes de Programação, Engenharia de Software, Segurança e Conformidade com a LGPD

Elaborado por Alison Rafael Polpeta Freitas (NPD/PAD/UEM), com o apoio da ferramenta de Inteligência Artificial Gemini Notebook (Google), revisado em 19 de outubro de 2026

A IDEIA CENTRAL, EM UMA FRASE:

A Inteligência Artificial pode apoiar a escrita de código, a automação e a documentação, mas a responsabilidade técnica, a proteção de dados confidenciais e a revisão linha a linha do código-fonte continuam sendo 100% do desenvolvedor humano. [1, 2, 3]

1. Apresentação e Âmbito de Aplicação

A Universidade Estadual de Maringá (UEM) instituiu a Instrução Normativa GRE nº 1/2026, regulamentando o uso responsável de ferramentas de Inteligência Artificial nas atividades de ensino, pesquisa, extensão e gestão [1]. No contexto do desenvolvimento de software e sistemas corporativos da UEM, o uso de IA é classificado como uma atividade técnica assistida (Art. 4º, XIII) [1]. Isso significa que a tecnologia opera estritamente como instrumento auxiliar, permanecendo a autoria, a tomada de decisão e a responsabilidade civil e administrativa integralmente sob domínio do servidor ou equipe técnica encarregada [1, 2].

2. As Três Regras de Ouro da TI na UEM

1. A IA alucina e pode gerar código vulnerável: modelos de linguagem não possuem compreensão lógica de negócios; geram sequências de código com base em probabilidades estatísticas. Podem introduzir falhas graves de segurança (como vulnerabilidades a *Prompt Injection*, falta de sanitização de dados, vazamentos de memória) e importar dependências ou bibliotecas obsoletas ou problemáticas [1, 3, 5].

2. Revisão Linha a Linha Obrigatória: todo código, script de automação, consulta SQL ou estrutura arquitetural sugerida por IA deve ser meticulosamente revisado, testado e validado por um desenvolvedor antes de qualquer *commit* em repositórios oficiais ou implantação em ambientes de homologação e produção [1, 2, 4].

3. Proteção Absoluta de Dados (*Privacy by Design*): é expressamente vedado colar dados pessoais, credenciais de acesso, tokens de API, chaves privadas ou bases de dados institucionais em ferramentas de IA abertas/públicas sem prévia autorização e isolamento de ambiente [1, 2, 3].

3. O Semáforo do Desenvolvedor de Sistemas

Antes de submeter qualquer requisição ou trecho de código a uma ferramenta de IA, a equipe técnica deve avaliar a classificação de risco da atividade:

SINAL VERDE: USO PERMITIDO COMO APOIO TÉCNICO [1, 2]

Atividades permitidas: explicar sintaxe e algoritmos complexos; sugerir padrões de projeto (*Design Patterns*); auxiliar na documentação (*docstrings*/comentários); gerar dados de teste fictícios (*mock data*) sem vínculo com dados reais de cidadãos ou servidores da UEM [1, 2, 4].

SINAL AMARELO: CUIDADO REDOBRADO (REVISÃO E TESTE OBRIGATÓRIOS) [1, 3]

Atividades condicionalmente permitidas: gerar rotinas de código e scripts de automação; refatorar e otimizar rotinas existentes; modelar estruturas conceituais de banco de dados [1, 2].

Regra de Ouro: exige teste unitário, validação técnica linha a linha e garantia de que não houve exposição de lógica proprietária [1, 3, 5].

SINAL VERMELHO: VEDAÇÕES EXPRESSAS (PROIBIDO) [1, 3]

Condutas proibidas (Art. 5º da IN GRE 01/2026):

1. Inserir dados pessoais (RA, CPF, notas, salários, dados de saúde) ou segredos de projeto em IAs externas [1, 3].
2. Submeter arquivos .env, senhas, tokens de API ou credenciais de banco de dados [1, 2, 4].
3. Implantar código em ambiente de produção sem revisão e testes de segurança por equipe humana [1, 5].
4. Isentar-se da responsabilidade técnica atribuindo falhas do sistema à ferramenta de IA [1, 2].

4. Segurança, Governança e LGPD no Ciclo de Vida do Software

Conformidade com a LGPD (Lei nº 13.709/2018): as soluções tecnológicas desenvolvidas com apoio de IA na UEM devem seguir os princípios de *Privacy by Design* e *Privacy by Default* [3]. O tratamento automatizado de dados pessoais exige transparência, finalidade legítima e garantia dos direitos dos titulares (Art. 20 da LGPD), incluindo o direito à explicação das decisões automatizadas [3, 7].

Hospedagem e Infraestrutura Interna: para sistemas que tratem informações sigilosas ou dados institucionais sensíveis, deve-se priorizar modelos de linguagem operados em infraestrutura própria (*On-Premises*) com segregação de rede e sem saída para serviços de nuvem públicos não homologados [1, 4, 5].

Sustentação e Ciclo de Vida (ISO/IEC 5338): a equipe de TI atua como sustentadora da aplicação, sendo responsável pelo monitoramento contínuo quanto a depreciação de desempenho (*model drift*), gestão de mudanças (GMUD) e encerramento seguro de componentes de IA [4, 5].

5. Checklist de Bolso para o Desenvolvedor

Antes de realizar qualquer *commit*, *pull request* ou implantação de código desenvolvido com apoio de IA, certifique-se de cumprir todos os itens abaixo:

- ☐ **Entendimento Total:** revisei o código linha a linha e compreendo perfeitamente sua lógica e funcionamento? [1, 2]
- ☐ **Higienização de Dados:** garanti que nenhum token, senha, chave privada ou dado pessoal real foi exposto nos prompts ou no código? [1, 3]
- ☐ **Validação de Segurança:** testei o código contra vulnerabilidades conhecidas e verifiquei que nenhuma biblioteca alucinada ou obsoleta foi importada? [1, 4, 5]
- ☐ **Testes Funcionais:** validei o comportamento da aplicação em ambiente isolado de desenvolvimento antes de submeter à homologação? [1, 4]
- ☐ **Responsabilidade Técnica:** assumo total responsabilidade pela autoria, precisão e segurança do código entregue? [1, 2]

6. Referências Normativas e Bibliográficas

[1] UNIVERSIDADE ESTADUAL DE MARINGÁ (UEM). Instrução Normativa GRE nº 1, de 6 de outubro de 2026. Dispõe sobre o uso responsável de ferramentas de Inteligência Artificial na UEM. Maringá: Gabinete da Reitoria, 2026.

[2] UNIVERSIDADE ESTADUAL DE MARINGÁ (UEM). Guia Prático para Estudantes e Comunidade: IA com Responsabilidade. Pró-Reitoria de Ensino (PEN) / Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação (PPG), 2026.

[3] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018.

[4] MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI / Gov.br). Guia Unificado de Inteligência Artificial para o Setor Público. Brasília: Secretaria de Governo Digital, 2024–2026.

[5] CONSELHO NACIONAL DE JUSTIÇA (CNJ). Resolução nº 615, de 14 de março de 2025. Estabelece diretrizes para o desenvolvimento e uso responsável de soluções de IA no setor público/judiciário. Brasília: CNJ, 2025.

[6] UNESCO. Recomendação sobre a Ética da Inteligência Artificial. Paris: Organização das Nações Unidas para a Educação, a Ciência e a Cultura, 2022.

[7] ESTADO DO PARANÁ. Plano Diretor de Inteligência Artificial do Estado do Paraná. Curitiba: Secretaria de Estado da Inovação e Inteligência Artificial, 2024.