MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI

RESOLUÇÃO Nº 16, DE 05 DE MARÇO DE 2026

Estabelece diretrizes e critérios para a realização de testes técnicos controlados na infraestrutura de Tecnologia da Informação da UFVJM, no âmbito de atividades acadêmicas, administrativas ou de pesquisa, e dá outras providências.

O COMITÊ DE GOVERNANÇA INTEGRIDADE, RISCOS E CONTROLE DA UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI, no uso das atribuições legais e regulamentares,

CONSIDERANDO que a infraestrutura de Tecnologia da Informação da UFVJM é essencial para o funcionamento dos serviços acadêmicos, administrativos e científicos da instituição;

CONSIDERANDO a necessidade de viabilizar a realização de testes técnicos - como análises de vulnerabilidades, auditorias de segurança, simulações de ataques (pentests) e avaliações de desempenho - no contexto de projetos acadêmicos e de pesquisa;

CONSIDERANDO que a realização desses testes pode envolver riscos à segurança da informação, à integridade dos sistemas e à continuidade dos serviços institucionais;

CONSIDERANDO a importância de garantir que tais testes sejam conduzidos de forma segura, autorizada, controlada e em conformidade com a legislação vigente, especialmente o Art. 154-A do Código Penal, a Lei nº 12.737/2012 e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018);

CONSIDERANDO deliberação tomada em sua Reunião nº 48, de 27 de fevereiro de 2026.

CONSIDERANDO o constante dos autos do processo no 23086.135440/2025-46;

RESOLVE

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Estabelecer diretrizes e critérios para solicitação, aprovação e realização de testes técnicos controlados na infraestrutura de Tecnologia da Informação da UFVJM, com foco na segurança, legalidade e minimização de riscos operacionais.

CAPÍTULO II
DA SOLICITAÇÃO E APROVAÇÃO DOS TESTES

Art. 2º Os testes técnicos só poderão ser realizados mediante autorização prévia da Pró-Reitoria de Tecnologia da Informação (PROTIC).

Art. 3º A solicitação deverá ser realizada pelo servidor responsável (orientador), via processo SEI, do tipo "TI : Gestão de Segurança da Informação", e deverá conter:

I – objetivos e justificativa;

II – metodologia a ser aplicada;

III – identificação dos sistemas e/ou redes envolvidos;

IV – medidas de mitigação de riscos;

V – identificação dos responsáveis e autorização do orientador, quando se tratar de projeto acadêmico.

Art. 4º – Sempre que os testes de vulnerabilidade ou atividades de pesquisa técnica envolver o tratamento de dados pessoais, conforme definido pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), ou o acesso a bases de dados que permita a identificação direta ou indireta de indivíduos, o protocolo do teste deverá:

I. Ser obrigatoriamente submetido e aprovado pelo Comitê de Ética em Pesquisa (CEP) antes de sua execução quando se tratar de projeto de pesquisa acadêmica; e

II. Ser obrigatoriamente submetido e aprovado pelo Encarregado de Dados (DPO) antes da sua execução quando se tratar de desenvolvimento técnico-administrativo.

§1º – A obrigatoriedade estende-se a testes que utilizem técnicas de engenharia social, coleta de dados em tráfego de rede contendo informações de usuários ou acesso a ambientes de produção que não possuam camadas efetivas de anonimização.

§2º – O pesquisador ou responsável técnico deverá apresentar ao Comitê o plano de mitigação de riscos, detalhando as medidas de segurança adotadas para garantir a confidencialidade, a integridade e o descarte seguro dos dados protegidos após a conclusão do estudo.

§3º – Estão dispensados da submissão ao CEP apenas os testes realizados em ambientes sintéticos (sandboxes) ou sobre dados comprovadamente anonimizados, onde não haja qualquer possibilidade de reversão da anonimização ou impacto a direitos de terceiros.

CAPÍTULO III

DA EXECUÇÃO E PUBLICAÇÃO DOS RESULTADOS

Art. 5º A execução dos testes deverá:

I – respeitar os limites definidos no plano aprovado;

II – ocorrer preferencialmente em ambientes controlados ou isolados;

III – ser acompanhada e/ou monitorada pela PROTIC.

Parágrafo único. A ação de que trata o inciso III poderá ser dispensada, desde que devidamente fundamentada, justificada e documentada.

Art. 6º Os resultados somente poderão ser publicados após correção das vulnerabilidades identificadas e deverão omitir informações sensíveis que possam comprometer a segurança da instituição.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 7º É dever do solicitante:

I – guardar o sigilo das informações obtidas durante os testes;

II – seguir estritamente o plano aprovado;

III – comunicar imediatamente qualquer incidente identificado às autoridades institucionais competentes :

Gestor de Segurança da Informação (seguranca@ufvjm.edu.br)

Encarregado de Dados (encarregado.lgpd@ufvjm.edu.br)

Art. 8º É de responsabilidade da PROTIC:

I – analisar e aprovar ou não as solicitações;

II – acompanhar testes considerados sensíveis;

III – aplicar medidas corretivas com base nos resultados.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 9º Os casos omissos serão avaliados pela PROTIC e, quando necessário, encaminhados ao CGIRC para deliberação.

Art. 10º Esta Resolução entra em vigor na data de sua publicação.

HERON LAIBER BONADIMAN

Presidente CGIRC

Documento assinado eletronicamente por **Heron Laiber Bonadiman**, **Reitor**, em 10/03/2026, às 16:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.
