Ministério da Educação
Universidade Federal de Viçosa
Campus Viçosa
Secretaria de Órgãos Colegiados

RESOLUÇÃO CONSU/UFV Nº 26, DE 18 DE AGOSTO DE 2025

Aprova o Regimento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da Universidade Federal de Viçosa.

O CONSELHO UNIVERSITÁRIO da Universidade Federal de Viçosa, órgão superior de administração, no uso das atribuições que lhe confere o art. 9º do Estatuto da Instituição, tendo em vista o disposto no art. 14 da Resolução Consu/UFV nº 12, de 17 de setembro de 2024, e considerando o que consta do Processo nº 23114.906951/2025-79 e o que foi deliberado em sua 503ª reunião, realizada em 14 de agosto de 2025,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Fica aprovado o Regimento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – Etir da Universidade Federal de Viçosa – UFV, nos termos desta Resolução.

Art. 2º O âmbito de atuação da Etir compreende todos os sistemas de informação, redes de computadores, serviços de Tecnologia da Informação – TI e demais ativos institucionais sob responsabilidade da UFV.

Art. 3º A Etir observará, em sua atuação, a legislação e as normas aplicáveis à matéria, notadamente a Lei nº 13.709, de 14 de agosto de 2018, no que se refere a incidentes envolvendo dados pessoais.

§ 1º A atuação da Etir será pautada pelos atos normativos, padrões e procedimentos técnicos expedidos pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov, pela Política de Segurança da Informação e da Comunicação da UFV – Posic, aprovada pela Resolução Consu/UFV nº 12, de 17 de setembro de 2024, e pelas políticas, pelas normas e pelos procedimentos internos da UFV relacionados à segurança da informação e à proteção de dados pessoais.

§ 2º A Etir alinhará suas ações com as diretrizes e as melhores práticas da Administração Pública federal em segurança da informação, de modo a manter aderência aos órgãos de controle e às orientações do Governo Federal.

Art. 4º A Etir reportará ao Gestor de Segurança da Informação e da Comunicação da UFV e comunicará imediatamente a ocorrência dos incidentes de segurança identificados em sua área de atuação ao CTIR Gov, conforme o padrão definido por esse órgão central.

§ 1º A comunicação de incidentes ao CTIR Gov visa possibilitar a geração de estatísticas federais e a adoção de soluções integradas no âmbito da Administração Pública federal, nos termos das normas vigentes.

§ 2º Quando cabível, a Etir também encaminhará notificações e informações sobre incidentes a outras instâncias pertinentes, de acordo com regulamentações superiores.

CAPÍTULO II

DAS COMPETÊNCIAS

Art. 5º Compete à Etir, no âmbito do tratamento e resposta a incidentes de segurança da informação:

I - receber, registrar e analisar prontamente as notificações ou detecções de incidentes de segurança no âmbito da UFV, classificando o incidente conforme sua natureza, criticidade e alcance, e adotar a priorização adequada em cada caso;

II - coletar evidências e informações relevantes logo após a identificação de um incidente, preservando-as adequadamente para análise detalhada e eventual uso em providências legais ou disciplinares;

III - conter e mitigar os efeitos do incidente, adotando as medidas imediatas necessárias para interromper ou limitar o dano, como isolamento de sistemas afetados, bloqueio de acessos indevidos ou remoção de artefatos maliciosos, coordenando a execução dessas ações em conjunto com os responsáveis pelos sistemas ou serviços impactados;

IV - comunicar tempestivamente aos responsáveis pelas unidades, pelos sistemas ou pelos dados afetados sobre a ocorrência do incidente e orientá-los quanto às ações de contenção, correção e recuperação a serem empreendidas;

V - acionar, quando necessário, outras equipes de apoio ou autoridades competentes, internas ou externas, em função da gravidade e da natureza do incidente;

VI - realizar análise pós-incidente, investigando as causas raízes do problema, os vetores de ataque ou as falhas exploradas e os impactos resultantes, de forma a obter um diagnóstico completo do ocorrido;

VII - coordenar e supervisionar a recuperação dos sistemas e a implementação de medidas de correção após o incidente, assegurando que vulnerabilidades exploradas sejam devidamente corrigidas ou mitigadas e que os serviços afetados retornem ao pleno funcionamento com segurança;

VIII - elaborar relatório detalhado de cada incidente atendido, com a descrição do incidente, sua causa, extensão dos danos, ações tomadas durante o tratamento, tempo de resolução e

recomendações para evitar ocorrências semelhantes;

IX - encaminhar os relatórios de que trata o inciso VIII ao Gestor de Segurança da Informação e da Comunicação da UFV e às demais instâncias pertinentes, como o Comitê Permanente de Governança de Dados, se envolver dados pessoais, para conhecimento e providências cabíveis; e

X - fornecer retorno (*feedback*) aos usuários ou às unidades que reportaram o incidente quanto às providências adotadas e aos resultados obtidos, sempre que possível, de modo a estimular a cultura de reporte de incidentes e a transparência na gestão de segurança.

Art. 6º Compete à Etir, no âmbito da prevenção de incidentes e da melhoria contínua da segurança:

I - monitorar de forma contínua a rede de dados, os sistemas e os serviços de TI da UFV, empregando ferramentas e procedimentos de detecção proativa, como sistemas de detecção de intrusão, analisadores de tráfego e monitoramento de *logs*, para identificar precocemente eventos anômalos ou indícios de incidentes de segurança;

II - realizar varreduras técnicas periódicas em servidores, equipamentos de rede, aplicações e demais ativos de TI institucionais, com o objetivo de identificar vulnerabilidades, configurações indevidas ou outras fragilidades de segurança;

III - formalizar e comunicar os resultados das varreduras de que trata o inciso II aos gestores ou responsáveis pelos ativos avaliados, acompanhando a correção das vulnerabilidades identificadas até sua resolução satisfatória;

IV - emitir alertas, avisos e comunicados de segurança para as unidades organizacionais e os usuários da UFV, em coordenação com a Diretoria de Comunicação Institucional, a Diretoria de Tecnologia da Informação e o Gestor de Segurança da Informação e da Comunicação, sempre que houver ameaças emergentes, vulnerabilidades críticas ou incidentes em andamento que exijam atenção ou ação imediata, contendo orientações claras sobre as medidas preventivas ou corretivas a serem adotadas, com vistas a reduzir riscos iminentes;

V - pesquisar e manter-se atualizada quanto a novas ferramentas, técnicas, ameaças e tendências em segurança da informação e comunicações, avaliando sua relevância no contexto institucional e propondo a adoção de melhorias tecnológicas, de procedimentos ou de controles de segurança na UFV;

VI - prospectar soluções inovadoras e acompanhar recomendações de órgãos oficiais, como o Gabinete de Segurança Institucional da Presidência da República, o CTIR Gov e a Secretaria de Governo Digital, para elevar o nível de proteção dos ativos de informação;

VII - implementar e manter mecanismos de detecção de intrusão e de monitoramento de segurança adequados, bem como estabelecer mecanismos de registro e auditoria (*logs*) nos sistemas críticos, de forma a possibilitar a identificação de atividades suspeitas e a posterior investigação de incidentes;

VIII - assegurar que os *logs* de segurança relevantes sejam coletados e armazenados com integridade e por período adequado, conforme as políticas internas;

IX - participar de ações de conscientização e capacitação em segurança da informação junto à comunidade acadêmica da UFV, em coordenação com a Diretoria de Comunicação Institucional, a Pró-Reitoria de Gestão de Pessoas, a Diretoria de Tecnologia da Informação e o Gestor de Segurança da Informação e da Comunicação;

X - disseminar boas práticas, lições aprendidas de incidentes, resguardando sigilo e privacidade, e orientações gerais que contribuam para a redução de riscos humanos, por meio de treinamentos, campanhas educativas, manuais ou outros meios adequados;

XI - apoiar os processos de governança de segurança da informação e de dados na UFV, fornecendo informações sobre vulnerabilidades identificadas e incidentes ocorridos para subsidiar a gestão de riscos e a atualização das políticas, das normas e dos controles de segurança; e

XII - colaborar com os comitês internos responsáveis de TI, segurança da informação ou governança de dados, para garantir que as lições extraídas de incidentes resultem em melhorias concretas nos mecanismos de proteção institucional.

CAPÍTULO III

DA COMPOSIÇÃO E DO VÍNCULO

Art. 7º A Etir será composta por servidores públicos efetivos da UFV, com capacitação técnica compatível com as atribuições da equipe.

§ 1º A Etir terá no mínimo três e no máximo cinco membros, indicados pelo Diretor de Tecnologia da Informação, ouvido o Gestor de Segurança da Informação e da Comunicação, e designados em ato do Reitor.

§ 2º Os membros da Etir podem ser lotados em diferentes setores técnicos, como TI, segurança da informação, redes e desenvolvimento de sistemas, conforme a necessidade, mas atuarão de forma integrada, sob orientação do agente responsável pela Etir.

§ 3º Poderão ser convidados a colaborar com a Etir, em caráter de apoio técnico ou consultivo, outros servidores da UFV ou colaboradores externos com *expertise* específica, a critério do agente responsável pela Etir e mediante ciência do Gestor de Segurança da Informação e da Comunicação, desde que tais colaboradores observem os deveres de confidencialidade e sigilo previstos nesta Resolução.

Art. 8º A coordenação da Etir será exercida pelo agente responsável pela Etir, indicado pelo Diretor de Tecnologia da Informação e designado em ato do Reitor, dentre seus membros.

Parágrafo único. O agente responsável pela Etir deverá possuir comprovada capacidade técnica na área de segurança da informação.

Art. 9º A Etir será vinculada à Diretoria de Tecnologia da Informação e estará subordinada, para fins de supervisão estratégica e funcional, ao Gestor de Segurança da Informação e da Comunicação da UFV.

§ 1º O Gestor de Segurança da Informação e da Comunicação deverá zelar pelo alinhamento das atividades da Etir com a Posic e com as normas institucionais de segurança da informação.

§ 2º A Etir deverá reportar-se periodicamente ao Gestor de Segurança da Informação e da Comunicação, mantendo-o informado sobre suas operações, seus planos e incidentes relevantes.

CAPÍTULO IV

DAS ATRIBUIÇÕES

Art. 10. Ao agente responsável pela Etir incumbe:

I - planejar, coordenar e supervisionar as atividades da equipe, assegurando o cumprimento das competências estabelecidas nesta Resolução e o atendimento ágil e adequado aos incidentes de segurança que surgirem;

II - coordenar a implantação, o desenvolvimento e a manutenção da infraestrutura, das ferramentas e dos procedimentos necessários ao pleno funcionamento da Etir, como plataformas de

gerenciamento de incidentes, sistemas de monitoramento e laboratórios para análise forense, garantindo que a equipe disponha dos meios técnicos apropriados para exercer suas funções;

III - garantir que os eventos e os incidentes de segurança nas redes, nos sistemas e nos serviços da UFV sejam monitorados continuamente, definindo mecanismos eficazes de detecção e acompanhamento e assegurando que haja pessoal de prontidão para resposta quando necessário;

IV - estabelecer e implementar procedimentos de comunicação e *feedback* para assegurar que os usuários ou as unidades que reportarem incidentes de segurança sejam devidamente informados das ações adotadas e do desfecho de suas solicitações;

V - representar a Etir perante os fóruns internos e externos pertinentes, incluindo reuniões de comitês internos da UFV, como aqueles de segurança da informação ou governança de dados ou governança digital, e junto a entidades externas, por exemplo em interações com o CTIR Gov, participação na Rede de Incidentes Cibernéticos ou colaboração com equipes de outras instituições;

VI - apoiar e promover programas de capacitação e treinamento em segurança da informação no âmbito da UFV, fornecendo subsídios técnicos, estudos de caso e lições aprendidas a partir de incidentes reais, resguardados os aspectos sigilosos, para aperfeiçoar a preparação dos usuários e colaboradores da UFV no enfrentamento de ameaças; e

VII - zelar pela correta aplicação do disposto nesta Resolução, dirimindo dúvidas operacionais junto aos membros da Etir e orientando-os quanto às práticas e aos procedimentos esperados, bem como propondo ao Gestor de Segurança da Informação e da Comunicação eventuais revisões necessárias nas normas e nos processos relacionados à Equipe.

Art. 11. Ao Gestor de Segurança da Informação e da Comunicação da UFV incumbe, em relação à Etir:

I - articular junto às instâncias superiores para que a Etir disponha de recursos humanos, financeiros e tecnológicos necessários ao cumprimento de sua missão, providenciando ou propondo os meios adequados para a estruturação da Equipe, tais como alocação de servidores e contratação de soluções tecnológicas específicas;

II - prover o apoio institucional e gerencial às ações da Etir, garantindo que as recomendações e necessidades identificadas pela Equipe, como aplicação de correções emergenciais, aquisições de ferramentas de segurança e alterações em normas internas, sejam apreciadas pelas instâncias competentes da UFV e recebam o encaminhamento apropriado;

III - fomentar a capacitação contínua dos membros da Etir, viabilizando a participação em cursos, treinamentos, certificações e eventos de aperfeiçoamento em segurança da informação, de modo a manter a Equipe atualizada frente às evoluções tecnológicas e às novas ameaças;

IV - zelar para que as atividades e os procedimentos da Etir permaneçam alinhados às políticas e às diretrizes institucionais de segurança da informação e de proteção de dados, orientando a integração da equipe aos modelos de governança existentes, como comitês de TI, segurança da informação e o Comitê Permanente de Governança de Dados, e promovendo a sinergia entre a resposta a incidentes e as demais iniciativas de segurança da UFV; e

V - autorizar, quando cabível e mediante avaliação técnica, em conjunto com o Diretor de Tecnologia da Informação, a utilização de serviços públicos especializados de segurança da informação, como Centros de Operações de Segurança (*SOC as a Service*) ou Equipes de Tratamento e Resposta a Incidentes Cibernéticos (*ETIR as a Service*) providos por órgãos da Administração Pública federal, como meio complementar às ações da Etir, observados os princípios de confidencialidade, integridade e disponibilidade das informações institucionais.

CAPÍTULO V

DA ATUAÇÃO EM PRIVACIDADE E DA PROTEÇÃO DE DADOS PESSOAIS

Art. 12. No exercício de suas atividades, a Etir deverá observar rigorosamente os aspectos relativos à privacidade e à proteção de dados pessoais previstos na Lei nº 13.709, de 14 de agosto de 2018, e nos normativos internos da UFV.

Parágrafo único. Incidentes de segurança que envolvam ou possam vir a envolver dados pessoais, como vazamento de informações pessoais, acessos não autorizados a bases de dados contendo dados de pessoas ou perda de mídias com dados pessoais, serão tratados como prioritários e de acordo com as exigências legais específicas.

Art. 13. Em caso de incidente de segurança envolvendo dados pessoais, a Etir deverá acionar imediatamente o Comitê Permanente de Governança de Dados e comunicar o fato ao Encarregado pelo Tratamento de Dados Pessoais designado pela UFV.

Parágrafo único. A Etir fornecerá ao Comitê Permanente de Governança de Dados todas as informações técnicas disponíveis sobre o incidente, como natureza dos dados comprometidos, número de titulares afetados e medidas de contenção adotadas, de forma a viabilizar a avaliação do risco e a definição célere de ações conjuntas de resposta.

Art. 14. As ações de resposta a incidentes que envolvam dados pessoais serão conduzidas pela Etir em cooperação direta com o Encarregado pelo Tratamento de Dados Pessoais e o Comitê Permanente de Governança de Dados, observando-se as diretrizes desse Comitê para a proteção de dados e garantindo-se a integração entre segurança da informação e governança de dados.

§ 1º Caso um incidente de segurança possa acarretar risco ou dano relevante aos titulares dos dados pessoais envolvidos, a UFV deverá comunicar o ocorrido à Autoridade Nacional de Proteção de Dados e aos próprios titulares afetados.

§ 2º Caberá à Etir assessorar o Comitê Permanente de Governança de Dados e a alta administração da UFV na comunicação a que se refere o § 1º, fornecendo as informações e evidências técnicas necessárias para dar pleno cumprimento às exigências legais, incluindo a descrição do incidente, dos dados afetados, dos impactos e das medidas de mitigação adotadas ou planejadas.

Art. 15. Todas as atividades da Etir relativas a dados pessoais deverão ser realizadas com observância estrita dos princípios da necessidade, minimização e sigilo previstos na Lei nº 13.709, de 14 de agosto de 2018, assegurando-se que apenas os membros autorizados da Equipe tenham acesso às informações pessoais estritamente indispensáveis à contenção e à análise do incidente.

§ 1º Devem ser aplicadas medidas de segurança adicionais, quando cabíveis, para proteger os dados pessoais durante o processo de resposta, como criptografia de relatórios e controle de acesso às evidências.

§ 2º Eventuais orientações específicas expedidas pelo Comitê Permanente de Governança de Dados referentes à gestão de incidentes de privacidade deverão ser incorporadas aos procedimentos operacionais da Etir.

CAPÍTULO VI

DA AUTONOMIA OPERACIONAL E DAS RELAÇÕES INSTITUCIONAIS

Art. 16. A Etir possui autonomia técnica e operacional para adotar, no curso do tratamento de incidentes de segurança, as medidas que julgar necessárias à imediata contenção de ameaças e à mitigação de danos, inclusive de forma emergencial e preemptiva em situações de grave risco à infraestrutura de TI, aos sistemas ou aos dados da UFV.

§ 1º Em casos excepcionais, em que ações emergenciais sejam tomadas sem prévia consulta superior, a Etir deverá comunicá-las ao Gestor de Segurança da Informação e da Comunicação e às demais instâncias competentes logo que possível, justificando as medidas empregadas e relatando os resultados obtidos.

§ 2º A autonomia operacional visa garantir rapidez na resposta a incidentes críticos, sem prejuízo do posterior controle administrativo e da responsabilização, se for o caso, pelos atos praticados.

Art. 17. A Etir deverá manter estreita cooperação e interlocução com órgãos e entidades externos e internos pertinentes à sua área de atuação.

§ 1º A Etir integrará a Rede Federal de Gestão de Incidentes Cibernéticos, instituída pelo Decreto nº 10.748, de 16 de julho de 2021, participando dos esforços coordenados de prevenção, tratamento e resposta a incidentes no âmbito da Administração Pública federal.

§ 2º A Etir observará os procedimentos e os formatos de troca de informações estabelecidos pelo CTIR Gov para notificação de incidentes e intercâmbio de dados técnicos com as demais equipes integrantes da Rede Federal de Gestão de Incidentes Cibernéticos, além de articular ações com o Centro de Atendimento de Incidentes de Segurança da Rede Nacional de Pesquisa.

§ 3º A Etir poderá compartilhar indicadores de comprometimento, alertas de vulnerabilidades ou outras informações relevantes com equipes de tratamento de incidentes de outras instituições governamentais, observando os acordos de confidencialidade cabíveis e as orientações do órgão central competente.

Art. 18. No âmbito interno, a Etir atuará de forma integrada às demais instâncias institucionais de governança em TI, segurança da informação e proteção de dados da UFV.

§ 1º Deverá haver articulação permanente com os comitês e os grupos de trabalho existentes na UFV relacionados a essas matérias, como o Comitê de Segurança da Informação e da Comunicação e o Comitê Permanente de Governança de Dados, de modo a garantir coerência e alinhamento entre as ações de tratamento de incidentes e as políticas, os planos e as decisões estratégicas adotadas pela UFV.

§ 2º A Etir fornecerá às instâncias a que se refere o *caput* informações, relatórios e pareceres técnicos que auxiliem na tomada de decisão e na melhoria contínua da segurança cibernética e da governança de dados institucionais.

Art. 19. A Etir poderá estabelecer parcerias e canais de comunicação com entidades externas especializadas, redes acadêmicas ou órgãos de apoio, com vistas ao aprimoramento de suas capacidades operacionais.

§ 1º A Etir poderá participar de fóruns de Grupos de Resposta a Incidentes de Segurança em Computadores acadêmicos ou governamentais, realizar intercâmbio de conhecimento com equipes de resposta a incidentes de outras Instituições Federais de Ensino Superior e cooperar com órgãos de fiscalização ou investigação quando um incidente assim o exigir, observados os trâmites legais para compartilhamento de evidências e informações.

§ 2º As relações institucionais de que trata este artigo deverão respeitar as normas superiores e contar com a anuência do Gestor de Segurança da Informação e da Comunicação quando envolverem compromissos formais.

CAPÍTULO VII

DOS PROCEDIMENTOS E DAS OPERAÇÕES TÉCNICAS

Art. 20. A Etir deverá elaborar e manter atualizados os seus Procedimentos Operacionais Padrão – POPs ou planos formais de resposta a incidentes, detalhando as etapas, os métodos, os fluxos de comunicação e as responsabilidades em cada fase do tratamento de incidentes.

§ 1º Os POPs devem contemplar, no mínimo:

I - a detecção/identificação do incidente;

II - a notificação interna das partes envolvidas;

III - a contenção;

IV - a erradicação/solução do problema;

V - a recuperação dos sistemas afetados; e

VI - a etapa de lições aprendidas, incluindo a incorporação de melhorias após o incidente.

§ 2º Os POPs da Etir deverão estar alinhados com referências consagradas, como as normas ABNT NBR ISO/IEC, NIST ou CIS Controls, e com os guias e manuais expedidos pelos órgãos centrais governamentais em segurança da informação, de forma a adotar as melhores práticas disponíveis.

Art. 21. Todos os incidentes de segurança tratados pela Etir deverão ser registrados em sistema ou repositório apropriado.

§ 1º Cada registro de incidente deve incluir informações como:

I - data e hora da detecção ou do reporte;

II - descrição sumária do incidente;

III - categoria ou tipo do incidente;

IV - unidades ou sistemas afetados;

V - nomes dos responsáveis pelo atendimento;

VI - medidas adotadas e cronologia das ações;

VII - tempo de resolução;

VIII - impactos observados; e

IX - *status* final (resolvido, em andamento, etc.).

§ 2º Os registros de que trata este artigo serão utilizados para compor estatísticas internas e possibilitar a análise de tendências, servindo de base para relatórios gerenciais e para o aprimoramento dos controles de segurança.

Art. 22. A Etir deverá adotar procedimentos para a devida preservação de evidências digitais durante o tratamento dos incidentes.

§ 1º Sempre que possível e aplicável, ao responder a um incidente, a Etir irá coletar e resguardar *logs*, arquivos, imagens de disco, tráfego de rede ou quaisquer outros artefatos relevantes, de maneira a permitir investigações posteriores mais aprofundadas ou auditorias.

§ 2º As evidências coletadas devem ser armazenadas de forma segura, com controle de integridade e acesso restrito, respeitando-se as cadeias de custódia necessárias quando houver possibilidade de uso em processos administrativos ou judiciais.

Art. 23. Periodicamente, a Etir deverá conduzir testes e exercícios simulados de seus planos de resposta a incidentes, bem como avaliações técnicas proativas, incluindo simulações de ataques cibernéticos (*table-top exercises* ou simulações controladas), testes de invasão autorizados (*pentests*) em infraestruturas críticas e novas varreduras de vulnerabilidade abrangentes, com o objetivo de avaliar a eficácia dos procedimentos, identificar eventuais lacunas ou pontos de melhoria na postura de segurança da UFV e treinar os membros da equipe para resposta rápida.

Parágrafo único. Os resultados de cada exercício ou teste deverão ser documentados e discutidos internamente, gerando, se for o caso, planos de ação para aprimoramento dos processos e da capacitação da equipe.

Art. 24. A Etir deverá produzir e encaminhar relatórios trimestrais de suas atividades ao Gestor de Segurança da Informação e da Comunicação, contendo:

I - o número de incidentes registrados no período e sua classificação;

II - as principais causas e tendências observadas;

III - o tempo médio de resposta;

IV - as ações de prevenção implementadas;

V - as dificuldades encontradas; e

VI - recomendações para o próximo período.

Parágrafo único. Os relatórios de que trata o *caput* servirão para prestar contas da atuação da Etir e para embasar decisões orçamentárias e administrativas referentes à segurança da informação e à proteção de dados.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 25. Os membros da Etir, inclusive eventuais colaboradores autorizados, devem manter sigilo sobre todas as informações confidenciais ou sensíveis às quais tiverem acesso no exercício de suas funções.

§ 1º Detalhes técnicos de vulnerabilidades não corrigidas, informações sobre a segurança dos sistemas da UFV e dados pessoais de titulares envolvidos em incidentes não poderão ser divulgados a terceiros não autorizados, sob pena de responsabilização disciplinar, civil e penal, na forma das normas aplicáveis.

§ 2º O compromisso de confidencialidade dos membros da Etir permanece válido mesmo após o eventual desligamento destes da Equipe.

Art. 26. Os casos omissos e as situações não previstas nesta Resolução serão dirimidos pelo Gestor de Segurança da Informação e da Comunicação da UFV, em conjunto com as demais instâncias competentes da Universidade.

§ 1º Quando a questão omissa envolver políticas de proteção de dados pessoais ou tiver reflexos sobre a governança de dados, o Gestor de Segurança da Informação e da Comunicação deverá consultar o Comitê Permanente de Governança de Dados antes de propor soluções, a fim de assegurar consonância com as diretrizes desse Comitê.

§ 2º As decisões tomadas para suprir omissões desta Resolução devem ser registradas por escrito e, se necessário, submetidas à apreciação da autoridade superior competente.

Art. 27. Esta Resolução entra em vigor na data de sua publicação.

DEMETRIUS DAVID DA SILVA

Presidente

Documento assinado eletronicamente por **DEMETRIUS DAVID DA SILVA**, **Presidente do Conselho Universitário (CONSU)**, em 18/08/2025, às 14:19, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.dti.ufv.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1717732** e o código CRC **B51DA45A**.

Referência: Processo nº 23114.906951/2025-79 SEI nº 1717732

Campus Viçosa
Av. Peter Henry Rolfs, s/nº, *Campus* Universitário
36570-900 Viçosa/MG

Campus Florestal
Rodovia LMG-818, km 6
35690-000 Florestal/MG

Campus Rio Paranaíba
Rodovia MG-230, Km 7, Zona Rural, Rodoviário
38810-000 Rio Paranaíba/MG