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

RESOLUÇÃO CONSU/UFV Nº 12, DE 17 DE SETEMBRO DE 2024

Institui a Política de Segurança da Informação e da Comunicação (Posic) 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, considerando o que consta do Processo nº 23114.907438/2024-14 e o que foi deliberado em sua 493ª reunião, realizada em 13 de setembro de 2024,

RESOLVE:

CAPÍTULO I

DAS DIRETRIZES GERAIS

Art. 1º A Política de Segurança da Informação e da Comunicação (Posic) da Universidade Federal de Viçosa (UFV) fica disciplinada nos termos desta Resolução.

Art. 2º A Posic estabelece as diretrizes e critérios para o manuseio da informação, de forma eletrônica ou não, observando os requisitos mínimos de:

I - confidencialidade;

II - integridade;

III - disponibilidade;

IV - não repúdio;

V - autenticidade; e

VI - atendimento à legislação pertinente e às normas definidas pelos órgãos reguladores.

§ 1º A Posic é uma declaração formal da instituição acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores no que diz respeito a seus direitos e responsabilidades com os recursos computacionais da instituição e as informações neles armazenados.

§ 2º As diretrizes estabelecidas nesta política devem estar alinhadas ao Estatuto da UFV, ao Regimento, ao Planejamento Estratégico Institucional, ao Plano Diretor de Tecnologia da Informação e aos valores institucionais.

§ 3º Todas as unidades administrativas, servidores, estudantes, prestadores de serviço autorizados e usuários de serviços de Tecnologia da Informação e da Comunicação e dos sistemas de informação mantidos na UFV devem aplicar a Posic em suas atividades.

CAPÍTULO II

DA FINALIDADE

Art. 3º A Posic tem por finalidade orientar a UFV no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação e da Comunicação em conformidade com as disposições constitucionais, legais e regimentais vigentes; seu propósito é estabelecer as diretrizes a serem seguidas pela Instituição na adoção de procedimentos e mecanismos relacionados à segurança da informação.

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para os efeitos da Posic da UFV, considera-se:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Etir);

III - alta administração: pessoa ou grupo de pessoas que dirige e controla uma organização no mais alto nível;

IV - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

V - análise/avaliação de riscos: processo completo de uso sistemático de informações para identificar fontes de risco e estimar riscos e de uso de critérios para determinar sua importância/impacto;

VI - artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

VII - ataque: tentativa de se destruir, expor, alterar, desabilitar, roubar, ganhar acesso não autorizado ou ainda realizar uso não autorizado de um ativo;

VIII - atividades críticas: atividades que devem ser executadas visando garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

IX - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

X - auditoria: processo sistemático, independente e documentado utilizado para se obter

evidências de conformidade ou uma avaliação objetiva que visa determinar em qual grau, ou extensão, os critérios normativos foram atendidos;

XI - autenticação: provisão de garantia de que uma característica declarada de uma dada entidade é correta;

XII - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por determinada pessoa física, ou por determinado sistema, órgão ou entidade;

XIII - bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;

XIV - clareza: as regras que se fundam nesta Posic devem ser claras, objetivas e concisas, a fim de viabilizar sua fácil compreensão;

XV - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

XVI - Comitê de Segurança da Informação e da Comunicação (CSIC): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e da comunicação no âmbito do órgão ou entidade da Administração Pública Federal (APF);

XVII - comunidade ou público-alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Etir;

XVIII - comprometimento: perda de segurança resultante do acesso não autorizado;

XIX - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

XX - confiabilidade: propriedade de prover resultados esperados e consistentes;

XXI - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

XXII - conformidade: atendimento (ou preenchimento) de um requisito;

XXIII - contas de serviço: contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso;

XXIV - continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

XXV - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XXVI - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso, ressalvando que a credencial pode ser física, como crachá, cartão e selo, ou lógica, como identificação de usuário e senha;

XXVII - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

XXVIII - dispositivos móveis: equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento;

XXIX - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

XXX - evento de segurança da informação: ocorrência identificada de um sistema, serviço ou estado da rede indicando uma possível brecha na Posic ou falha dos controles, ou ainda uma situação previamente desconhecida que pode ser relevante para a segurança da informação;

XXXI - gestão de riscos de segurança da informação e comunicação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXXII - gestão de segurança da informação e comunicação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicação;

XXXIII - Gestor de Segurança da Informação e da Comunicação (GSIC): é responsável pelas ações de segurança da informação e da comunicação no âmbito do órgão ou entidade da APF;

XXXIV - incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXXV - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXXVI - informação classificada: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor, a qual, em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, é classificada como ultrassecreta, secreta ou reservada;

XXXVII - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

XXXVIII - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXXIX - legalidade: ações de segurança da informação e comunicação, que levarão em consideração as leis, as políticas, as normas e os procedimentos organizacionais, administrativos, técnicos e operacionais da UFV, formalmente estabelecidos;

XL - não-repudiação: habilidade de se provar a ocorrência de um evento requisitado (ou ação) e as entidades que o originaram;

XLI - plano de continuidade de negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

XLII - plano de gerenciamento de incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente, que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

XLIII - política: intenções e direção de uma organização formalmente expressa pela alta administração;

XLIV - Posic: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicação;

XLV - publicidade: transparência no trato da informação, observados os critérios legais;

XLVI - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicação;

XLVII - redução de risco: forma de tratamento de risco em que a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

XLVIII - responsabilidade: toda comunidade de usuários da UFV é responsável pelo cumprimento das normas de segurança da informação e comunicação;

XLIX - risco de segurança da informação e comunicação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

L - segurança da informação e comunicação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade, o não repúdio e a autenticidade das informações;

LI - sistema de informação: aplicações, serviços, ativos de tecnologia da informação ou outros componentes de gerenciamento de informações;

LII - terceirização: arranjo em que uma organização externa desempenha parte da função ou processo de outra organização; e

LIII - termo de responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade, o não repúdio e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

CAPÍTULO IV

DOS PRINCÍPIOS E DIRETRIZES

Art. 5º As ações relacionadas à Posic da UFV são norteadas pelos seguintes princípios:

I - autenticidade;

II - confidencialidade;

III - clareza;

IV - disponibilidade;

V - integridade;

VI - legalidade;

VII - não repúdio;

VIII - publicidade; e

IX - responsabilidade.

Art. 6º A Posic e suas normas complementares são regidas pelas seguintes diretrizes, que orientam a definição de normas e procedimentos específicos relacionados à segurança da informação e da comunicação no âmbito da UFV:

I - garantir a segurança das informações institucionais transportadas na rede acadêmica da UFV, inclusive no uso de dispositivos móveis;

II - assegurar que todos os usuários estejam conscientes e cumpram as suas responsabilidades pela segurança da informação na UFV;

III - identificar os ativos de informação da UFV e as responsabilidades apropriadas definidas para a proteção deles;

IV - assegurar que a informação receba um nível adequado de proteção, de acordo com a legislação vigente;

V - limitar o acesso lógico e físico à informação e aos recursos de processamento da informação da UFV, assegurando-se o acesso apenas às pessoas devidamente autorizadas;

VI - garantir a operação segura e correta dos recursos de processamento da informação da UFV, visando, principalmente, a proteção contra perda de dados;

VII - assegurar que os ativos de informação estejam protegidos contra códigos maliciosos;

VIII - registrar eventos e gerar evidências nas operações envolvendo ativos de informação dentro da UFV;

XIX - garantir a integridade e atualizar periodicamente os sistemas computacionais utilizados dentro da rede acadêmica da UFV;

X - garantir que a segurança da informação esteja projetada e implementada durante todas as fases do ciclo de vida dos sistemas de informação desenvolvidos dentro da UFV;

XI - manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores;

XII - garantir um enfoque consistente e efetivo para se gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação;

XIII - assegurar a disponibilidade dos ativos de informação críticos através da implementação de mecanismos de redundância e de uma política de continuidade de negócios; e

XIV - evitar a violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança da informação, dentro da UFV.

CAPÍTULO V

DAS PENALIDADES

Art. 7º Ações que violem a Posic ou quaisquer de suas diretrizes e normas ou que quebrem os controles de segurança da informação serão apuradas para responsabilização pelas instâncias competentes.

Parágrafo único. Eventuais ações corretivas para mitigação de riscos à segurança da informação estarão enunciadas em normas específicas, decorrentes das diretrizes gerais de segurança da informação enumeradas nesta Resolução.

CAPÍTULO VI

COMPETÊNCIAS E RESPONSABILIDADES

Art. 8º A estrutura para a gestão da segurança da informação e da comunicação na UFV é composta por:

I - CSIC;

II - GSIC;

III - Etir; e

IV - usuários das soluções de tecnologia da informação.

Seção I

Do Comitê de Segurança da Informação e da Comunicação (CSIC) da UFV

Art. 9º O CSIC da UFV, atuando sob a direção do Comitê de Governança Digital (CGD) e vinculado à Pró-Reitoria de Planejamento e Orçamento (PPO), tem o propósito principal de assessorar a implementação das ações de segurança da informação e comunicação, garantindo a conformidade com a Posic da UFV, as diretrizes estratégicas, de governança digital e as legislações pertinentes.

Art. 10. São responsabilidades do CSIC da UFV:

I - garantir a elaboração, supervisão e atualização constante da Posic da UFV, assegurando a proteção da integridade, confidencialidade e disponibilidade das informações;

II - formar comitês temáticos temporários para tratar de questões específicas de segurança da informação e comunicação, contribuindo para a gestão eficaz dos ativos de informação da UFV;

III - propor, revisar e aprovar normas e procedimentos internos em segurança da informação e comunicação, alinhando-se à Posic da UFV, às diretrizes de governança digital e às legislações aplicáveis;

IV - promover a conscientização e capacitação em segurança da informação e da comunicação para a comunidade universitária, visando fortalecer uma cultura de segurança na instituição;

V - coordenar a avaliação periódica da eficácia das políticas e procedimentos de segurança implementados, propondo melhorias e ajustes necessários;

VI - supervisionar a gestão de incidentes de segurança da informação, em colaboração com a Etir da UFV, para assegurar uma resposta eficiente e a minimização de danos; e

VII - assegurar a integração e o alinhamento das ações de segurança da informação com as políticas e diretrizes de governança digital da UFV.

Parágrafo único. A composição, funcionamento, atribuições específicas e procedimentos do CSIC da UFV estarão definidos em regimento próprio.

Seção II

Do Gestor de Segurança da Informação e da Comunicação da UFV (GSIC)

Art. 11. O GSIC será designado dentre os servidores públicos ocupantes de cargo efetivo da UFV, com formação ou capacitação técnica compatível às suas atribuições;

Art. 12. O GSIC da UFV tem as seguintes competências:

I - prestar contas das atividades de segurança da informação ao CSIC da UFV;

II - coordenar a elaboração da Posic e das normas internas de segurança da informação e da comunicação da UFV, observadas as normas afins exaradas pelas instâncias competentes do governo federal e as melhores práticas sobre o assunto;

III - assessorar a administração superior da Universidade Federal de Viçosa na implementação e atualização da Posic da UFV;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação e da comunicação na UFV;

V - promover a divulgação da política e das normas internas de segurança da informação e da comunicação da UFV a todos os servidores, usuários e prestadores de serviços;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação na UFV;

VII - propor recursos necessários às ações de segurança da informação e da comunicação na UFV;

VIII - acompanhar os trabalhos da Etir da UFV;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação e da comunicação na UFV;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação e da comunicação na UFV;

XI - prestar as informações necessárias para as ações da equipe de conformidade da UFV e avaliar o relatório de conformidade em segurança da informação e comunicação;

XII - manter contato direto com as instâncias competentes do governo federal em assuntos relativos à segurança da informação e comunicação;

XIII - designar os agentes responsáveis pela gestão de ativos de informação e mudanças em aspectos de segurança da informação e comunicação;

XIV - acessar aos ativos de informação;

XV - avaliar e monitorar riscos em segurança da informação e comunicação;

XVI - avaliar, monitorar e tratar incidentes e vulnerabilidades nos ativos de informação;

XVII - avaliar e monitorar a continuidade de negócios em segurança da informação e comunicação;

XVIII - proporcionar a interação constante entre as equipes de gestão de mudanças em aspectos de segurança da informação, de gestão de riscos de segurança da informação e de gestão de continuidade de negócios em segurança da informação e da comunicação na UFV; e

XIX - coordenar os seguintes processos de realização obrigatória pelos órgãos e pelas entidades da administração pública federal:

a) mapeamento de ativos de informação;

b) gestão de mudanças nos aspectos de segurança da informação e comunicação;

c) gestão de acesso aos ativos de informação;

d) gestão de riscos de segurança da informação e comunicação;

e) gestão de incidentes e vulnerabilidades nos ativos de informação; e

f) gestão de continuidade de negócios em segurança da informação e comunicação.

§ 1º Quanto à gestão de riscos, o GSIC deverá aprovar:

I - o plano de gestão de riscos de segurança da informação e comunicação;

II - o relatório de identificação, análise e avaliação dos riscos de segurança da informação e comunicação; e

III - o relatório de tratamento de riscos de segurança da informação e comunicação.

§ 2º Quanto à gestão de mudanças, o GSIC deverá:

I - analisar o documento de avaliação; e

II - aprovar as mudanças para apreciação e aprovação da administração superior da UFV.

§ 3º Nos casos de violação da segurança da informação e comunicação, o GSIC deverá:

I - acompanhar a aplicação de ações corretivas e administrativas cabíveis; e

II - acompanhar os trabalhos da Etir da UFV.

§ 4º Quanto à avaliação de conformidade nos aspectos de segurança da informação, o GSIC deverá:

I - fornecer ao(s) agente(s) responsável(is) pela avaliação de conformidade todas as informações necessárias ao processo de gestão de conformidade nos aspectos de segurança da informação;

II - emitir parecer técnico sobre o relatório de avaliação de conformidade;

III - apresentar o parecer técnico e o relatório de avaliação de conformidade ao CSIC da UFV; e

IV - adotar as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade aprovado pela administração superior da UFV.

Seção III

Da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da UFV (Etir)

Art. 13. A Etir tem como missão prioritária identificar, proteger, detectar e responder a

incidentes de segurança cibernética e de sistemas empregados na ambiência da instituição, bem como cooperar com outras equipes e participar em fóruns e seminários de redes nacionais e internacionais relacionados às ações de segurança da informação.

Art. 14. A composição, funcionamento, atribuições específicas e procedimentos da Etir estarão definidos em regimento próprio.

Seção IV

Dos Usuários das Soluções de Tecnologia da Informação

Art. 15. Compete aos usuários das soluções de tecnologia da informação oferecidas pela UFV:

I - conhecer e cumprir os princípios, diretrizes e responsabilidades contidos nesta Posic, suas normas e resoluções complementares; e

II - zelar pela segurança da informação e comunicação; comunicar os incidentes de segurança, por eles conhecidos e propor melhorias à segurança da informação e da comunicação no âmbito da UFV.

CAPÍTULO VII

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 16. A Posic da UFV está alinhada ao Plano de Desenvolvimento Institucional e ao Plano Diretor de Tecnologia da Informação da UFV, como também está em consonância com os atos normativos que regem a segurança da informação e comunicação, assim como as boas práticas de governança neste tema.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 17. A Posic será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta política.

Art. 18. As propostas de alteração ou criação de normas internas sobre segurança da informação e da comunicação deverão ser encaminhadas ao CSIC da UFV.

Art. 19. Após sua publicação, o CSIC da UFV deverá dar ampla divulgação da Posic a todos os agentes públicos.

Art. 20. Os casos omissos e as dúvidas surgidas na aplicação desta Resolução serão dirimidos pelo CSIC da UFV.

Art. 21. Fica revogada a Resolução Consu nº 16, de 11 de dezembro de 2019.

Art. 22. 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 17/09/2024, às 18:00, 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 **1436070** e o código CRC **4718D6D4**.

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