MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE LAVRAS
REITORIA

PORTARIA Nº 1.327, DE 13 DE NOVEMBRO DE 2019.

Dispõe sobre a Política de Segurança da Informação e Comunicações da Universidade Federal de Lavras.

O REITOR DA UNIVERSIDADE FEDERAL DE LAVRAS, no uso de suas atribuições legais e regimentais, e,

CONSIDERANDO a Portaria/Reitoria N°187, de 19 de fevereiro de 2019,

CONSIDERANDO o Plano Diretor de Tecnologia da Informação e Comunicações da Universidade Federal de Lavras - triênio - 2017-2020,

CONSIDERANDO Resolução do CUNI 054 de julho de 2011,

CONSIDERANDO o disposto no artigo 5º, incisos IV e VI, da Instrução Normativa GSI nº 1, de 13/6/2008, do Gabinete de Segurança Institucional da Presidência da República, publicada na seção 1 do D.O.U. nº 115, de 18/6/2008,

CONSIDERANDO o disposto na Lei 12.527 de 18 de novembro de 2011, Lei de Acesso da Informação,

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação - PNSI, no âmbito da administração pública federal,

CONSIDERANDO as Boas Práticas em Segurança da Informação do Tribunal de Contas da União - 4ª Edição.

RESOLVE:

Art. 1º Atualizar a Política de Segurança da Informação e Comunicações (POSIC) da Universidade Federal de Lavras - UFLA, conforme anexo desta Portaria.

Art. 2º Esta portaria entra em vigor na data de sua assinatura, revogadas as disposições em contrário.

JOSÉ ROBERTO SOARES SCOLFORO
Reitor

ANEXO - PORTARIA Nº 1.326, DE 13 DE NOVEMBRO DE 2019

Política de Segurança da Informação e Comunicações (POSIC)

Universidade Federal de Lavras (UFLA)

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Seção I
Da Finalidade

Art. 1º A Política de Segurança da Informação e Comunicações (POSIC) da UFLA é uma declaração formal da Instituição acerca do seu compromisso com a proteção dos Ativos de informação, de hardware, de software e intangíveis de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos que tenham acesso esporádico ou permanente a quaisquer desses ativos.

Art. 2º O objetivo desta POSIC é estabelecer diretrizes e responsabilidades no que diz respeito ao manuseio, tratamento, controle e proteção dos ativos mencionados, servindo de apoio à direção executiva, além de representar seu compromisso formal na implementação da gestão de segurança da informação e comunicações na UFLA, buscando assegurar os princípios estabelecidos no capítulo II, art 5°, desta política.

Art. 3º A finalidade da POSIC da UFLA é servir de diretriz genérica e ampla, e como base de referência para elaboração dos demais documentos normativos de segurança da informação, no qual as ações de segurança da informação serão desenvolvidas na UFLA.

Seção II
Do Escopo

Art. 4º O escopo da POSIC da UFLA é determinar ações e diretrizes com foco em segurança da informação, com o intuito de estabelecer regras para o controle, manutenção e proteção dos ativos de informação, Hardware, Software e Intangíveisda UFLA.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 5º A POSIC da UFLA é guiada pelos princípios básicos da administração pública. Para o contexto dos serviços, recursos e informações gerenciadas na infraestrutura de tecnologia da informação e comunicações da UFLA, considera-se ainda os preceitos básicos da segurança da informação: a confidencialidade, a integridade, a autenticidade, o não-repúdio, a conformidade, o controle de acesso, a auditabilidade, a legalidade e a disponibilidade.

CAPÍTULO III
CONCEITOS E DEFINIÇÕES
Seção I
Da Terminologia

Art. 6º São termos e definições utilizados nesta POSIC:

I – Ameaça: causa potencial de um incidente, que pode resultar em dano para um sistema ou para a Instituição;

II – Ativo: qualquer bem, tangível ou intangível, que tenha valor para a Instituição;

III – Ativos de informação: banco de dados e arquivos, imagens, vídeos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, documentos do acervo acadêmico digital, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;

VI – Ativos de software: aplicativos, sistemas e ferramentas de desenvolvimento e utilitários;

V – Ativos de hardware: envolve toda infraestrutura de equipamentos computacionais, redes de telecomunicações, mídias removíveis e outros equipamentos;

VI – Ativos intangíveis: a reputação e a imagem da organização;

VII – Auditoria: consiste na avaliação dos registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna e à internet;

VIII – Comunicação: no contexto da POSIC, comunicação se refere a transmissão de dados;

IX–Sistema de Informação: Um conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização.

X – Incidente de segurança: qualquer evento adverso relacionado à segurança de sistemas de informação levando ao comprometimento de um ou mais princípios básicos de Segurança da Informação;

XI– Gestor de Ativo: Indivíduo que recebeu responsabilidade de segurança da informação sobre algum ativo, podendo delegar tarefas de segurança da informação para outros, porém permanecendo responsável pelo ativo e pela verificação de que quaisquer tarefas delegadas tenham sido corretamente executadas.

XII – Usuário da Informação: todos os usuários internos e externos à

UFLA que tenham acesso esporádico ou permanente a quaisquer ativos de informação, incluindo, mas não se limitando a servidores, discentes e terceiros.

Seção II
Das Instâncias Administrativas

Art. 7º Para os efeitos desta Política e das normas dela originadas, entende-se por:

I – Reitoria: é o órgão executivo superior, ao qual compete dirigir, administrar, planejar, coordenar, estabelecer parcerias e fiscalizar as atividades da universidade;

II – Comitê Interno de Governança (CIGOV): Art 1° da portaria 1.499 de 2018 da Reitoria.Comitê responsável por elaborar e revisar periodicamente a POSICe normas relacionadas, submetendo à aprovação da Reitoria, entre outras competências; tem entre suas atribuições principais: participar e orientar o planejamento dos investimentos em Tecnologia da Informação e Comunicações de acordo com as diretrizes do Plano de Desenvolvimento Institucional (PDI) em execução; estabelecer as políticas, diretrizes e prioridades na área de Tecnologia da Informação e Comunicações (TIC); promover e estimular o desenvolvimento da Tecnologia da Informação e Comunicações no âmbito da UFLA; elaborar, acompanhar e avaliar um Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) para a UFLA; elaborar, acompanhar e avaliar as Políticas de Segurança da Informação e Comunicações para a UFLA;

III – Diretoria de Gestão de Tecnologia da Informação (DGTI): instância administrativa/executiva responsável pelo desenvolvimento, implantação e manutenção dos ativos de sistemas de informação;

IV – Coordenadoria de Segurança da Informação: responsável por monitorar e analisar o cumprimento das políticas, normas e procedimentos de segurança dos sistemas de informação e comunicações, além de elaborar estratégias para comunicação, publicação e divulgação das políticas, normas e procedimentos de segurança dos sistemas de informação e comunicações;

V – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): portaria da reitoria nº 275, 15 de março de 2019. Equipe mantida pela Diretoria de Tecnologia da Informação (DGTI) que possui a missão de realizar o tratamento de vulnerabilidades e incidentes de segurança, emissão de alertas e advertências relativos à rede computacional da UFLA;

VI – Unidade organizacional: qualquer instância administrativa da UFLA a exemplo dos campi, unidades ligadas aos campi, núcleos de pesquisa e centros com funcionalidades específicas.

CAPÍTULO IV
COMPETÊNCIAS E RESPONSABILIDADES

Art. 8º. Compete à Coordenadoria de Segurança da Informação:

I – elaborar estratégias para comunicação, publicação e divulgação das políticas, normas e procedimentos de segurança dos sistemas de informação e comunicações;

II – propor, avaliar e revisar normas complementares alinhadas à POSIC em conformidade com as legislações vigentes;

III – apoiar o CIGOV nas ações de segurança da informação e comunicações;

IV – elaborar em conjunto com a DGTI proposta anual de alocação de recursos orçamentários necessários às ações de segurança da informação e comunicações;

V – realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicações;

VI – propor programas destinados à conscientização e à capacitação de recursos humanos em segurança da informação e comunicações.

VII –fornecer apoio ao CIGOV-UFLA e à DGTI sobre a elaboração e monitoramento do plano de gestão de riscos de TI;

Art. 9º. Compete à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): receber, analisar e responder aos incidentes de segurança envolvendo computadores conectados à rede institucional de dados da UFLA.

Art. 10 Compete aos gestores de ativos e ocupantes de cargo de chefia:

I – adotar medidas administrativas cabíveis em caso de violação das regras estabelecidas de acordo com as leis específicas, normas e procedimentos de segurança da informação;

II – atualizar-se, periodicamente quanto às políticas, normas e procedimentos de
segurança da informação vigentes na UFLA;

III – manter o devido registro e controle ao autorizar e fornecer acesso aos ativos sob sua responsabilidade a qualquer usuário da informação;

IV – gerenciar o cumprimento da POSIC, por parte de seus subordinados, se houver;

V – proteger, em nível físico e lógico, os ativos de informação da UFLA relacionados com sua área de atuação;

VI – garantir que o pessoal sob sua supervisão compreenda e colabore para com a proteção dos ativos de informação da UFLA;

VII – solicitar à DGTI a concessão de acesso privilegiado a usuários sob sua supervisão que podem acessar as informações da unidade administrativa sob sua responsabilidade.

Art. 11. Compete aos usuários da informação:

I – conhecer e cumprir os princípios, diretrizes e responsabilidades desta POSIC, bem como suas demais normas e resoluções complementares;

II – zelar pela segurança da informação e comunicações;

III – comunicar os incidentes de segurança, por eles conhecidos;

IV – propor melhorias à segurança da informação e comunicações no âmbito da UFLA;

V – preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de tecnologia da informação (TI);

VI – responder por todo e qualquer acesso aos recursos de TI da UFLA, bem como pelos efeitos desses acessos efetivados através do seu código de identificação ou outro atributo empregado para esse fim;

VII – abster-se de utilizar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação à legislação de propriedade intelectual pertinente.

CAPÍTULO V
DIRETRIZES GERAIS

Art. 12 São diretrizes gerais da POSIC da UFLA:

I – dispor sobre os objetivos estratégicos, processos, requisitos legais e estrutura da UFLA, bem como o PDTIC da UFLA;

II – estabelecer medidas e procedimentos para assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio, a conformidade, o controle de acesso, a auditabilidade, a legalidade e a disponibilidade;

III – observar as boas práticas e procedimentos de Segurança da Informação e Comunicações recomendados por órgãos e entidades responsáveis pelo estabelecimento de padrões.

Art. 13 As Diretrizes de Segurança da Informação definidas neste documento são aplicadas aos ativos de informação, de hardware, de software e intangíveis, fornecendo orientações para práticas de gestão de segurança da informação.

Art. 14 É dever de todos os usuários da informação zelar pela Segurança da Informação e Comunicações.

Seção I
Das Diretrizes para o Tratamento de Ativos

Art. 15 Os ativos deverão ser inventariados, classificados, documentados e sua documentação mantida atualizada, devendo ser revista sempre que ocorrerem fatos que justifiquem sua atualização.

§1º A documentação dos ativos deverá fornecer subsídios para a sua recuperação após um incidente de segurança.

§2º As regras de documentação dos ativos serão definidas em normas específicas.

Art. 16 Os ativos de um setor deverão ser de responsabilidade do seu gestor, ou de alguém por ele designado, que ficará encarregado pela sua manutenção e documentação, bem como pela notificação de qualquer evento que aconteça a ele.

Art. 17 A instituição deverá adotar as medidas necessárias para que os responsáveis pelos ativos possam geri-los adequadamente, cabendo ao gestor do ativo solicitar os recursos necessários para tal.

Seção II
Dos Ativos de Informação

Art. 18 As informações existentes no âmbito da UFLA apresentam diferentes níveis de confidencialidade e devem ser classificadas de acordo com a legislação vigente.

Art. 19 Normas complementares estabelecerão procedimentos que visem garantir a integridade, a confidencialidade e a disponibilidade das informações, incluindo procedimentos para a criação, manutenção e verificação dos ativos de informação e de suas cópias de segurança.

Art. 20 Os ativos de informação armazenados nos equipamentos utilizados pelos usuários (computadores, dispositivos móveis, dispositivos de armazenamento externo, entre outros) são de sua responsabilidade, cabendo aos mesmos adotar as medidas necessárias para realizar as cópias de segurança desses ativos e proceder à sua recuperação em caso de perda.

Seção III
Dos Ativos de Software

Art. 21 A utilização de ativos de software em equipamentos da instituição deve ser previamente autorizada pelo seu responsável, conforme o art. 16 desta POSIC, cabendo ao mesmo providenciar os procedimentos necessários à sua utilização.

Art. 22 É vedada a utilização e/ou instalação de software que possa de qualquer forma ferir esta política de segurança, bem como direitos autorais, de propriedade intelectual ou quaisquer normas e legislações vigentes.

Seção IV
Dos Ativos de Hardware

Art. 23 Os ativos de hardware constituem ativos passíveis de inventário, documentação e auditoria, devendo estes procedimentos serem definidos através de normas específicas.

Art. 24 Cabe ao responsável pelo ativo a elaboração de procedimentos para o seu uso e controle, devendo ainda zelar pelo cumprimento destes procedimentos.

Seção V
Dos Ativos Intangíveis

Art. 25 A referenciação dos ativos intangíveis será disciplinada em norma específica.

CAPÍTULO VI
DIRETRIZES ESPECÍFICAS
Seção I
Do Tratamento de Incidentes de Segurança da Informação e Comunicações

Art. 26 A UFLA manterá permanentemente uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) com a responsabilidade de receber, analisar e responder aos incidentes de segurança envolvendo computadores conectados à rede institucional de dados da UFLA.

Seção II
Da Gestão de Risco

Art. 27 Um Plano de Gestão de Riscos deve ser elaborado e mantido pela UFLA, com base na legislação vigente, contendo necessariamente uma lista das ameaças mais prováveis e suas ocorrências, uma classificação dos riscos e alternativas para mitigá-los.

Seção III
Da Gestão de Continuidade

Art. 28 Faz-se necessária a adoção de um conjunto de procedimentos emergenciais, através da definição de um Sistema de Gestão de Continuidade de Negócios (SGCN), para a eventualidade da ocorrência de algum incidente de segurança da informação que possa causar interrupção na continuidade de processos organizacionais para a UFLA, decorrentes de desastres ou falhas em Ativos de Informação.

Seção IV
Da Auditoria

Art. 29 Todos os ativos de informação, de hardware, de software e

intangíveis no âmbito da UFLA são passíveis de auditoria técnica a cargo da DGTI, segundo plano a ser estabelecido em norma específica.

Parágrafo único. Cabe ao CIGOV propor o plano de Auditoria e Conformidade que deverá incluir métodos, técnicas, procedimentos, normas e responsabilidades para o efetivo cumprimento do estabelecido por esta POSIC no âmbito da UFLA.

Seção V
Dos Controles de Acesso

Art. 30 O objetivo do controle de acesso é limitar as ações que um usuário legítimo de um sistema pode efetuar, buscando prevenir a realização de atividades que venham ocasionar algum incidente de segurança.

Art. 31 Deve ser definido Plano de Controle de Acesso que estabeleça procedimentos para a identificação dos ativos de informação, de hardware, de software e intangíveis com acesso controlado, assim como dos usuários que devem ter privilégio de acesso, e as áreas físicas protegidas contra o acesso de pessoas não autorizadas.

Seção VI
Do Uso de Correio Eletrônico Institucional

Art. 32 O serviço de correio eletrônico institucional será usado para atividades acadêmicas e administrativas dos usuários da informação no âmbito da UFLA.

Art. 33 As responsabilidades, direitos e penalidades referentes ao uso de correio eletrônico institucional serão especificadas através de normas complementares específicas.

Seção VII
Do Acesso e Publicação de Informações na Internet

Art. 34 O acesso à Internet no âmbito da UFLA é fornecido para fins diretos e complementares às atividades da instituição, sendo, portanto, passível de registro e auditoria.

Art. 35 Perfis de redes sociais, sites e portais específicos, pertencentes a alguma das unidades organizacionais da UFLA, devem ser criados, atualizados e descontinuados sob a anuência do gestor responsável pela unidade, devendo, quando possível, estar registrado em um domínio da UFLA.

Art. 36 O conteúdo acessado ou publicado não pode possuir elementos que possam ser considerados ofensivos, destrutivos, difamatórios ou pejorativos, incluindo, mas não limitado a comentários ou imagens sexuais, calúnias raciais, ou outros comentários/imagens que possam ofender alguém por sua raça, classe social, nacionalidade, gênero, orientação sexual, crença religiosa, orientação política ou condição de deficiência.

Art. 37 Não é permitida a utilização de conteúdos de terceiros, sujeitos às leis de direito autoral ou classificados como segredo, sem autorização escrita, em

qualquer tipo de publicação on-line pertencente a alguma das unidades organizacionais da UFLA.

Art. 38 As responsabilidades, direitos e penalidades referentes ao uso, acesso e publicação na internet serão especificadas através de normas complementares específicas e a legislação vigente.

Seção VIII
Da Capacitação e Aperfeiçoamento

Art. 39 Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicações.

Seção IX
Da Utilização de Equipamentos Particulares/Privados

Art. 40 Equipamentos particulares e/ou privados, como computadores ou quaisquer dispositivos que possam armazenar dados, não devem ser usados para armazenar informações que sejam classificadas como sensíveis para a atividade da UFLA, sem prévia autorização expressa do custo diante dos dados ou da Direção da Unidade.

Seção X
Dos Cuidados com o Posto de Trabalho

Art. 41 Nenhuma informação sensível deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

Seção XI
Das Conversas em Locais Públicos, Redes Sociais e outros meios

Art. 42 Não se deve discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de qualquer tipo em qualquer meio que não garanta sigilo.

CAPÍTULO VII
VIOLAÇÕES, PENALIDADES E SANÇÕES

Art. 43 A desobediência ou violação das regras da POSIC da UFLA e suas normas complementares aprovadas pelo CIGOV implicará em sanções administrativas nos termos da lei, normas complementares, regimentos e resoluções internas, sem prejuízo de outras previstas nas esferas cível e penal.

Parágrafo Único: O procedimento para a aplicação das penalidades e/ou sanções seguirá o rito específico da legislação, norma, regimento ou resolução a que corresponder o caso concreto.

CAPÍTULO VIII
DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

Art. 44 A POSIC e suas normas complementares devem ser publicadas,

amplamente divulgadas e comunicadas a todos os usuários da informação da UFLA e dispostas de maneira que o seu conteúdo possa ser consultado a qualquer momento.

CAPÍTULO IX
FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

Art. 45 As referências legais e normativas utilizadas para a elaboração da POSIC da UFLA estão de acordo com:

I – o disposto no artigo 5º, incisos IV e VI, da Instrução Normativa nº 1, de 13/6/2008, do Gabinete de Segurança Institucional da Presidência da República, publicada na seção 1, do Diário Oficial da União nº 115, de 18/6/2008;

II – a Lei 12.527, de 18 de novembro de 2011, Lei de Acesso da Informação;

III – o Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação - PNSI, no âmbito da administração pública federal;

IV – a Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais;

V – a Lei 9.069, de 19 de fevereiro de 1998,Lei do Software;

VI– a Lei 12.965, de 23 de abril de 2014, Marco Civil da Internet;

VII– a Portaria 1.499, de 19 de novembro de 2018, da Reitoria da UFLA, Institui o Comitê Interno de Governança da Universidade Federal de Lavras (CIGOV-UFLA);

VIII– a Portaria 275, de 15 de março de 2019, da Reitoria da UFLA, Institui a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR - UFLA;

IX– as Boas Práticas em Segurança da Informação do Tribunal de Contas da União - 4ª Edição.

CAPÍTULO X
DISPOSIÇÕES FINAIS

Art. 46 Os casos omissos e as dúvidas surgidas na aplicação do disposto na POSIC da UFLA deverão ser analisados pela reitoria, com o parecer do CIGOV da UFLA.

Art. 47 A presente política passa a vigorar a partir da data de sua publicação, revogando-se as disposições em contrário.