INSTRUÇÃO NORMATIVA PROAGI Nº 03/2021

Dispõe sobre acesso, aquisição, fornecimento e utilização da certificação digital no âmbito da Universidade Federal da Integração Latino-Americana - UNILA.

O Pró-Reitor de Administração, Gestão e Infraestrutura, no uso das competências delegadas por meio da Portaria Nº 283/2020/GR, e tendo em vista o disposto no art. 5º, inciso LXXVIII, da Constituição da República Federativa do Brasil de 1988, no qual são assegurados a todos, no âmbito judicial e administrativo, a razoável duração do processo e os meios que garantam a celeridade de sua tramitação; o disposto Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal; a Medida Provisória no 2.200-2, de 24 de agosto de 2001, que institui a Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil, e transforma o Instituto Nacional de Tecnologia da Informação em autarquia; a Lei Nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; o Decreto nº 10.543, de 13 de novembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas na administração pública federal e regulamenta o art. 5º da Lei nº 14.063, de 23 de setembro de 2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público; a necessidade de estabelecer procedimentos para a devida utilização dos certificados digitais no âmbito da UNILA; a atual política da UNILA, a qual trata da redução da utilização de papel indo ao encontro dos norteadores da Agenda Ambiental da Administração Pública – A3P; e a busca por maior eficiência, eficácia e transparência do serviço público,

RESOLVE:

Art. 1° Fica regulamentado o acesso, aquisição, fornecimento e utilização de Certificação Digital no âmbito da Universidade Federal da Integração Latino-Americana- UNILA.

DAS DEFINIÇÕES

Art 2º. Para fins desta Instrução Normativa, considera-se:

I - assinatura eletrônica simples: tipo de assinatura eletrônica admitida para as hipóteses cujo conteúdo da interação não envolva informações protegidas por grau de sigilo e não ofereça risco direto de dano a bens, serviços e interesses do ente público, conforme inciso I, do art. 4º do Decreto nº 10.543/2020.

II - assinatura eletrônica avançada: tipo de assinatura eletrônica admitida para as hipóteses previstas no inciso I e nas hipóteses de interação com o ente público que, considerada a natureza da relação jurídica, exijam maior garantia quanto à autoria, conforme inciso II, do art. 4º do Decreto nº 10.543/2020.

III - assinatura eletrônica qualificada: tipo de assinatura eletrônica aceita em qualquer interação eletrônica com entes públicos e obrigatória para os atos de transferência e de registro de bens imóveis, ressalvados os atos realizados perante as juntas comerciais; os atos assinados pelo Presidente da República e pelos Ministros de Estado; e demais hipóteses previstas em lei; conforme inciso III, do art. 4º do Decreto 10.543/2020.

IV - Autoridade Certificadora - AC: entidade pública ou privada que emite, renova ou revoga certificados digitais de outras autoridades ou de titulares finais;

V - Autoridade de Registro – AR: é responsável pela interface entre o usuário e a Autoridade Certificadora – AC. Vinculada a uma AC, tem por objetivo o recebimento, a validação, o encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma pessoal, de seus solicitantes;

VI - Autoridade Certificadora Raiz: é a primeira autoridade da cadeia de certificação. Compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu;

VII - Certificação digital: Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora. O armazenamento do certificado digital pode ser feito em dispositivos do tipo *smart card*, *token*, na nuvem ou localmente no equipamento do usuário;

VIII - Equipamentos de Certificação Digital Padrão ICP-Brasil: Todo e qualquer aparelho, dispositivo ou elemento físico que compõe meio necessário ou suficiente à realização da certificação digital Padrão ICP-Brasil;

IX - S*mart card e Token*: São dispositivos portáteis que funcionam como mídias armazenadoras. Em seus chips são armazenadas as chaves privadas dos usuários. O acesso às informações neles contidas é feito por meio de uma senha pessoal, determinada pelo titular. O *smart card* assemelha-se a um cartão magnético, sendo necessário um aparelho leitor para seu funcionamento. Já o *token* é semelhante a um *pen drive*, permitindo a sua conexão a uma porta USB de um computador ou outro equipamento com uma entrada USB;

X - PIN (*Personal Identification Number*): sequência de números e/ou letras (senha) usadas para liberar o acesso à chave privada, ou outros dados armazenados na mídia, somente para pessoas autorizadas;

XI - PUK (*Personal Identification Number Unblocking Key*): chave para desbloqueio do número de identificação pessoal (PIN), o qual normalmente fica bloqueado após várias tentativas inválidas. Como o PIN, a senha PUK deve ser guardada de forma segura, pois ambas permitem, em dispositivos como *tokens* e *smart cards*, o acesso à chave privada de um titular de certificado;

XII - Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICP-Edu): serviço de certificação digital oferecido pela Rede Nacional de Ensino e Pesquisa, que provê a infraestrutura para a emissão de certificados digitais e chaves de segurança. Dispensa a utilização de *smartcard* e *token*.

XIII - Gov.br: O gov.br é uma plataforma e projeto de unificação dos canais digitais do governo federal, que reúne, em um só lugar, serviços para o cidadão e informações sobre a atuação de todas as áreas do governo. Com o gov.br é possível assinar de forma eletrônica e gratuita documentos diversos, para substituir assinaturas físicas ou certificados pagos.

XIV - interação eletrônica - o ato praticado por particular ou por agente público, por meio de edição eletrônica de documentos ou de ações eletrônicas, com a finalidade de adquirir, resguardar, transferir, modificar, extinguir ou declarar direitos; impor obrigações; ou requerer, peticionar, solicitar, relatar, comunicar, informar, movimentar, consultar, analisar ou avaliar documentos, procedimentos, processos, expedientes, situações ou fatos.

DA CERTIFICAÇÃO DIGITAL

Art. 3° Os certificados digitais, a serem fornecidos por pessoa jurídica contratada, habilitada/credenciada pela Autoridade Certificadora Raiz (ITI) e em conformidade com as normas em vigor para prestação de serviços de certificação digital, destinam-se aos servidores públicos em exercício na Unila.

§1º Os serviços de certificação digital a serem prestados, credenciados ou contratados pela UNILA deverão, preferencialmente, ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, ou por Autoridade Certificadora validada pela UNILA.

§2º O recebimento de mídia ou token de certificado digital se dará mediante assinatura de Termo de Responsabilidade, conforme orientações da Seção de Protocolo e Arquivo (SEPRO-UNILA).

Art. 4° A utilização do Certificado Digital permite a segurança dos usuários em função das seguintes características:

I. Autenticidade: assegura a identificação do autor do documento eletrônico ou do autenticador do documento reproduzido em meio eletrônico, assinado digitalmente;

II. Confidencialidade: garantia de que somente as pessoas envolvidas no processo terão acesso às informações transmitidas de forma eletrônica pela rede;

III. Identidade: garantia de que o emissor de uma mensagem ou pessoa que executou determinada transação de forma eletrônica não poderá negar sua autoria, salvo em caso de fraude devidamente comprovada;

IV. Irretratabilidade: impossibilita ao usuário negar a autenticidade do documento após esse ter sido devidamente assinado digitalmente; e

V. Integridade: garantia de que a assinatura digital não mais corresponderá ao documento quando da realização de qualquer alteração/modificação no conteúdo deste.

Art. 5° Os certificados de assinatura digital são de uso pessoal e intransferível, sendo obrigatório ao titular zelar pelo dispositivo o qual contém as chaves pública e privada (*smart card* ou *token*), bem como certificar-se da não divulgação das senhas PIN e/ou PUK, sob pena de responsabilização administrativa, civil e penal, nos termos da legislação.

Art. 6° O certificado digital funcionará como uma identidade virtual, na qual será permitida a identificação segura e inequívoca do autor da realização de transações feitas em meios eletrônicos, bem como para a utilização nos softwares internos e de uso próprio da UNILA.

Art. 7° Será fornecido o certificado digital aos servidores cujo exercício de função pública demande assinatura eletrônica qualificada, mediante apresentação da respectiva justificativa e autorização pela Chefia da Macrounidade ou, na impossibilidade desta, por autoridade imediatamente superior.

Art. 8° O certificado digital e o respectivo suporte criptográfico (*smart card* ou *token*) serão concedidos gratuitamente aos servidores que demandem a utilização de assinatura digital em razão do cargo público ou da função gratificada para a qual forem nomeados/designados.

Art. 9° Nos sistemas utilizados na UNILA, a certificação digital confere aos documentos assinados digitalmente o mesmo valor administrativo e/ou jurídico dos documentos em papel assinados de próprio punho.

Art. 10 A validação de atos em documentos eletrônicos por usuários detentores de certificados digitais deverá se dar, obrigatoriamente, através de tal dispositivo, sendo vedada a utilização por terceiros.

§ 1° O portador é responsável administrativamente, civil e criminal pelos atos praticados.

§ 2° A utilização do certificado digital tanto dentro quanto fora dos sistemas da UNILA é de inteira responsabilidade do seu portador.

Art. 11 Será realizada nova certificação do servidor quando:

I. Inviabilizar o certificado após exceder, sem sucesso de acesso à senha, por quinze tentativas de PIN e/ou por três tentativas de PUK, bem como por exceder o número de tentativas em decorrência do tipo de mídia relativa ao certificado;

II. Ocorrer perda do *smart card* ou *token* e do certificado digital;

III. Ocorrer dano irreparável do *smart card* ou *token* e do certificado digital;

IV. Ocorrer furto ou roubo do *smart card* ou *token* e do certificado digital;

V. Quando houver necessidade de renovação do certificado digital em decorrência do prazo de vencimento.

§ 1º Nos casos dos incisos I, II e III a UNILA fornecerá, gratuitamente, no máximo 1 certificação por ano de exercício, cabendo ao servidor providenciar certificação caso exceda essa necessidade, arcando com os custos decorrentes.

§ 2º Nos casos dos incisos II e IV, será necessário realizar o pedido de nova certificação mediante apresentação de Boletim de Ocorrência Policial e comprovante de revogação do certificado.

§3º No caso do inciso III, o *smart card* ou *token* danificado deverá ser entregue à Seção de Protocolo e Arquivo.

Art. 12 Em caso de desligamento do usuário dos quadros da UNILA, por qualquer motivo, e em casos de vencimento do certificado, no qual o servidor não necessitará mais utilizar o tipo de certificado, o portador deverá remeter o *token*, ou equivalente, à Seção de Protocolo e Arquivo para adoção das devidas providências.

Art. 13 A assinatura digital gerada a partir de um certificado digital pessoal vinculado à Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICP-Edu) é reconhecida para todos os fins na instituição e é aceita com presunção de legalidade, em consonância com o art. 10 § 2º, da MP 2.200-2/2001, para todos os efeitos legais intrainstitucionais.
Parágrafo único. Os certificados digitais pessoais são emitidos na ICP-Edu gratuitamente para todos os membros da comunidade universitária com vínculo comprovado pela Comunidade Acadêmica Federada (CAFe), possuem validade de um ano e devem ser gerados e revogados, quando necessário, pelo próprio usuário, no website do serviço https://pessoal.icpedu.rnp.br/.

Art. 14 A assinatura digital gerada a partir das credenciais do cidadão na plataforma gov.br, do governo federal, é reconhecida para todos os fins na instituição e admitida com presunção de legalidade.

DAS COMPETÊNCIAS

Art. 15 Compete à Seção de Protocolo e Arquivo- SEPRO, em especial:

I. Adotar as medidas cabíveis quanto à gestão dos certificados digitais, compreendida a emissão, renovação e distribuição de certificados digitais.

II. Registrar e controlar os certificados fornecidos pela UNILA.

Art. 16 Compete à Coordenadoria de Tecnologia da Informação - CTIC, em especial:

I. Adequar a infraestrutura de Tecnologia da Informação para uso dos certificados digitais;

II. Elaborar e divulgar padrões de compatibilidade dos certificados digitais e dos respectivos suportes criptográficos utilizados na UNILA;

III. Prover solução de Tecnologia da Informação para autorizar a troca de informações, por meio eletrônico, entre a UNILA e outros órgãos ou demais entidades, com a utilização de certificado digital;

IV. Fornecer suporte técnico aos usuários em relação à instalação e uso do certificado digital para acesso nos sistemas utilizados pela Instituição.

Art. 17 Compete à Seção de Almoxarifado:

I. Providenciar a aquisição de novas mídias Token ou de dispositivo compatível com a Certificação Digital.

Art. 18 O suporte, assistência e treinamento para o uso de sistemas específicos, que fazem uso do certificado digital, será de competência da própria unidade que coordena e/ou utiliza estes sistemas.

Art. 19 Compete ao próprio usuário do certificado a obrigação da revogação nos casos estabelecidos nos incisos II e IV do art. 11, e no caso de desligamento da UNILA.

DAS DISPOSIÇÕES FINAIS

Art. 20 No procedimento eletrônico observar-se-ão todas as regras processuais inerentes aos atos praticados.

Art. 21 Poderá o servidor certificado autorizar a Seção de Protocolo e Arquivo a realizar o cadastro da senha PUK de maneira a poder restaurar a senha PIN em caso de perda por excesso de tentativa.

Art. 22 Casos omissos serão tratados pela Pró-Reitoria de Administração, Gestão e Infraestrutura.

Art. 23 Esta Instrução Normativa entra em vigor em 1º de agosto de 2021, nos termos do Art. 4º do Decreto nº 10.139/2019, e será submetida à revisão na ocorrência de alteração legislativa ou por necessidade da Administração.