SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

INSTRUÇÃO SUSEP N.º 79, DE 28 DE MARÇO DE 2016.

Dispõe sobre o uso do certificado digital no âmbito da Superintendência de Seguros Privados – Susep.

O SUPERINTENDENTE DA SUPERINTENDÊNCIA DE SEGUROS PRIVADOS – SUSEP, no uso das atribuições que lhe confere o inciso X do artigo 68 do Regimento Interno, de que trata a Resolução CNSP n.º 333, de 9 de dezembro de 2015, e considerando o que consta no processo n.º 15414.003187/2014-12,

RESOLVE:

Art. 1.º O uso de certificado digital no âmbito da Superintendência de Seguros Privados – Susep obedece ao disposto nesta Instrução, observada a legislação vigente.

Art. 2.º Para os efeitos desta Instrução, entende-se por:

I – usuário interno: servidor ativo efetivo ou em comissão da Susep que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas por esta Autarquia;

II – documento eletrônico: documento armazenado sob a forma de arquivo eletrônico, inclusive aquele resultante de digitalização;

III – assinatura eletrônica: registro realizado eletronicamente por usuário identificado de modo inequívoco com vistas a firmar determinado documento com sua assinatura;

IV – autoridade certificadora: entidade autorizada a emitir, suspender, renovar ou revogar certificados digitais; bem como a emitir listas de certificados revogados e manter registros de suas operações;

V – certificado digital: arquivo eletrônico que contém dados de uma pessoa ou instituição e um par de chaves criptográficas utilizados para comprovar identidade em ambiente computacional;

VI – certificado digital do tipo A3: certificado em que a geração e o armazenamento das chaves criptográficas são feitos em mídias do tipo cartão inteligente ou token, observando-se que as mídias devem ter capacidade de geração de chaves e ser protegidas por senha ou hardware criptográfico aprovado pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil); e

VII – mídia de armazenamento do certificado digital: dispositivos portáteis – como os *tokens* – que contêm o certificado digital e são inseridos no computador para efetivar a assinatura digital.

Art. 3.º Os documentos eletrônicos produzidos no âmbito de atuação da Susep terão garantia de autoria, autenticidade e integridade asseguradas nos termos da lei, mediante utilização de assinatura eletrônica nas seguintes modalidades:

I – assinatura digital baseada em certificado digital tipo A3, de uso pessoal e intransferível, emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil; ou

II – assinatura mediante uso de usuário (*login*) e senha.

§ 1.° O uso de certificado digital é obrigatório, ressalvado o disposto em normas que disciplinem procedimentos eletrônicos específicos no âmbito da Susep, para assinatura de documentos de conteúdo decisório com circulação externa, para atos regulamentares dos mercados supervisionados pela Susep e para outros procedimentos que necessitem de comprovação de autoria e integridade em ambiente externo à Autarquia.

§ 2.º Os documentos eletrônicos produzidos na Susep cuja modalidade de assinatura não se enquadre nas hipóteses tratadas no § 1º deste artigo poderão ser assinados mediante uso de usuário (*login*) e senha.

§ 3.º A utilização de assinatura eletrônica importa aceitação pelo usuário das normas sobre o assunto, inclusive no que se refere à responsabilidade por eventual uso indevido.

Art. 4.º A Susep proverá os usuários internos de certificado digital e respectiva mídia de armazenamento.

§ 1.º A distribuição de certificados digitais será realizada na medida da necessidade e da implantação das funcionalidades tecnológicas que exijam o seu uso.

§ 2.º A Susep promoverá a reemissão do certificado digital sempre que houver a expiração do respectivo prazo de validade.

Art. 5.º O detentor de certificado digital é responsável por sua utilização, guarda e conservação.

§ 1.° O certificado digital é de uso pessoal, intransferível e hábil a produzir efeitos legais em todos os atos nos quais vier a ser utilizado, dentro ou fora da Susep.

§ 2.° A utilização do certificado digital para qualquer operação implica não-repúdio, não podendo o detentor negar a autoria da operação nem alegar que tenha sido praticada por terceiro.

§ 3.° O não-repúdio de que trata o parágrafo anterior se aplica também às operações efetuadas entre o período de solicitação da revogação ou suspensão do certificado e respectiva inclusão na lista de certificados revogados publicada pela autoridade certificadora.

Art. 6.º Na hipótese de o certificado digital perder a validade, as assinaturas digitais anteriormente efetuadas permanecem válidas, podendo, também, ser verificadas a autoria e a integridade dos documentos já assinados.

Art. 7.º É permitido ao usuário interno adquirir, por meios próprios, para uso na Susep, certificado digital e respectiva mídia de armazenamento, desde que ambos possuam características compatíveis com as especificações de certificação digital adotada pela Susep, não sendo cabível, em qualquer hipótese, o ressarcimento pela Autarquia dos custos havidos.

Art. 8.º O certificado digital será inutilizado nas seguintes situações:

I – digitação sucessiva de senha incorreta na tentativa de utilização do certificado;

II – dano ou formatação da mídia que armazena o certificado;

III – esquecimento da senha de utilização do certificado; ou

IV – perda ou extravio.

§ 1.º A inutilização pode ser efetuada automaticamente por solução de TI ou mediante solicitação de revogação à autoridade certificadora, e implica reemissão de novo certificado digital.

§ 2.º Em caso de perda ou extravio antes do final do prazo de validade do certificado digital e quando comprovada a falta de zelo pela conservação do patrimônio público, o servidor será responsabilizado, inclusive arcando com os custos para nova aquisição ou ressarcimento do *token* e do certificado digital.

Art. 9.º Incumbe à Coordenação-Geral de Tecnologia da Informação (CGETI):

I - manter o fornecimento de unidades de *token* e emissão de certificados em número suficiente ao atendimento da demanda;

II - autorizar emissão de certificado digital;

III - emitir certificado digital através de empresas certificadoras;

IV - orientar os servidores sobre a utilização de certificados digitais, por meio de campanhas institucionais;

V - manter compatibilidade dos certificados emitidos com os sistemas do Governo Federal;

VI - auxiliar servidores em eventual processo de revogação de certificados;

VII - promover, quando necessário e em quantidade suficiente, a emissão de certificado na sede e Regionais da Susep;

VIII – instalar programa para utilização de senha de desbloqueio do *token*, que ficará sob a guarda da Coordenação Geral de TI.

IX - prover solução de TI para permitir o cadastramento, no Portal da Susep, de certificados digitais de usuários supervisionados ou representantes de entidades supervisionadas;

X – prover aplicação para identificação da autoridade certificadora;

XI – prover aplicação para conferência de assinatura, por terceiro, em documentos eletrônicos produzidos no âmbito da Susep;

Parágrafo único. Em caso de bloqueio do *token*, o respectivo usuário deverá reportar-se à Coordenação Geral de TI para orientação sobre o procedimento de desbloqueio.

Art. 10. Compete ao usuário interno detentor de certificado digital:

I – solicitar imediatamente a revogação do certificado digital em caso de perda, roubo ou ocorrência de qualquer fato que comprometa a privacidade do certificado;

II – prestar informações no cadastro online, no sítio da prestadora ou autoridade credenciada, devendo comprová-las durante o processo de validação presencial;

III – assinar termo digital de recebimento do *token* e do certificado digital, garantindo o perfeito funcionamento do validador.

IV – apresentar tempestivamente, à autoridade certificadora, a documentação necessária à emissão do certificado digital conforme orientação da CGETI;

V – estar de posse do certificado digital para o desempenho de atividades profissionais que requeiram o uso deste;

VI – alterar imediatamente a senha de acesso ao certificado em caso de suspeita de seu conhecimento por terceiro;

VII – manter a mídia de armazenamento dos certificados digitais em local seguro e com proteção física contra acesso indevido, descargas eletromagnéticas, calor excessivo e outras condições ambientais que representem risco à integridade dessas mídias; e

VIII – solicitar o fornecimento de nova mídia ou certificado digital nos casos de inutilização do certificado;

§ 1.º A prática de atos assinados eletronicamente importará aceitação das normas regulamentares sobre o assunto e da responsabilidade pela utilização indevida da assinatura eletrônica.

§ 2.º A vacância do quadro de pessoal da Susep não implica recolhimento, pela Autarquia, do certificado digital – e da respectiva mídia de armazenamento – anteriormente distribuído ao usuário interno.

Art. 11. O uso inadequado do certificado digital fica sujeito à apuração de responsabilidade penal, civil e administrativa, na forma da legislação em vigor.

Art. 12. Aplica-se o disposto nesta Instrução aos certificados digitais distribuídos pela Susep anteriormente à vigência desta norma.

Art. 13. Fica o Comitê de Segurança da Informação e Comunicações – CSIC autorizado, no âmbito de suas respectivas competências, a editar os atos que se fizerem necessários para a operacionalização desta Instrução, assim como para dirimir os casos omissos.

Art. 14. Esta Instrução entra em vigor na data de sua publicação.

ROBERTO WESTENBERGER

Superintendente