RESOLUÇÃO Nº 458, DE 20 DE DEZEMBRO DE 2017.

Regulamenta o uso de sistemas informatizados para registro e guarda de informações por regulados da ANAC.

A DIRETORIA DA AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL - ANAC, no exercício da competência que lhe foi outorgada pelo art. 11, inciso V, da Lei nº 11.182, de 27 de setembro de 2005, tendo em vista o disposto no art. 8º, incisos X e XLVI, e § 1º, da mencionada Lei, e considerando o que consta do processo nº 00058.519658/2017-81, deliberado e aprovado na 1ª Reunião Extraordinária Deliberativa da Diretoria, realizada em 19 de dezembro de 2017,

RESOLVE:

Art. 1º Regulamentar, nos termos desta Resolução, o uso de sistemas informatizados para registro e guarda de informações por regulados da Agência Nacional de Aviação Civil - ANAC, em substituição aos registros em papel.

Parágrafo único. O cumprimento dos preceitos desta Resolução é facultativo, exceto se, por atos normativos específicos, for determinado compulsório para algum caso.

CAPITULO I
DAS DEFINIÇÕES

Art. 2º Para os fins desta Resolução, considera-se:

I - autenticação: meios pelo qual um sistema valida a identidade de um usuário autorizado para executá-lo. Várias formas de autenticação podem ser combinadas para aumentar a confiança na identificação do usuário do sistema;

II - Sistema de Registro de Logs: sistema que registra eventos relevantes num sistema computacional. O sistema deve manter registros de entrada, manutenção, arquivamento, retiradas e outras operações que envolvem a manipulação de dados relevantes. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em um sistema;

III - *backup* de dados: uso de um método reconhecido para prover uma opção secundária de armazenamento digital dos dados, separadamente da opção original ou primária. O *backup* pode ser usado para recuperação de dados e informações em casos de perda, falha no sistema ou danos a opção original ou primária de armazenamento do sistema;

IV - verificação dos dados/informação: processo que assegura a fidedignidade da informação armazenada ao comparar, de forma sistemática ou aleatória, registros eletrônicos com registros manuais de entrada de dados, informações ou documentos;

V - assinatura digital: método de autenticação da informação digital que identifica quem assinou o documento, com data e hora. A assinatura digital deve ter como propriedades a autenticidade, integridade e irretratabilidade, ou não-repúdio;

Publicado no Diário Oficial da União de 22 de dezembro de 2017, Seção 1, página 385 e 386.

VI - chave pública: classe de protocolos de criptografia. A chave pública é utilizada, por exemplo, para encriptar ou verificar uma assinatura digital;

VII - chave privada: classe de protocolos de criptografia. A chave privada é utilizada, por exemplo, para decriptar uma informação ou criar uma assinatura digital;

VIII - assinatura eletrônica: funcionalidade equivalente a assinatura manuscrita. O termo assinatura eletrônica abrange processos eletrônicos anexados ou logicamente associados a um documento ou outro registro e executado ou adotado por uma pessoa com a intenção de assinar o registro;

IIX - *hashing*: formação de sequência reduzida de bits por algoritmo de dispersão que permita a identificação de uma informação de maneira única; e

IX - criptografia digital assimétrica: protocolo de criptografia baseado em algoritmos que requerem 2 (duas) chaves, uma pública e uma privada.

CAPÍTULO II
ACEITAÇÃO DE USO DE SISTEMAS PARA REGISTRO E GUARDA DE INFORMAÇÕES

Art. 3º Um sistema de informação poderá ser utilizado para registro, guarda ou acesso a informações de registro obrigatório, desde que:

I - tenha seu escopo de utilização explicitamente autorizado pela ANAC;

II - tenha sido avaliado e acreditado por entidades competentes, demonstrado por meio de relatórios de conformidade (ex: empresas certificadoras segundo ISO/IES 27000); e

III - esteja disponível a qualquer momento para auditoria.

§ 1º Um sistema já avaliado e aceito não necessita de novo processo de aceitação para o mesmo escopo, mesmo se utilizado por outra entidade.

§ 2º No caso de eventual atualização de um sistema que implique na mudança do método de cumprimento dos requisitos previstos nessa resolução, um novo processo de aceitação deverá ser proposto pelo interessado.

CAPÍTULO III
DA SEGURANÇA DO SISTEMA OU SOLUÇÃO UTILIZADA

Art. 4º O sistema ou solução a ser utilizado pelos interessados deverá seguir minimamente os seguintes aspectos:

I - no tocante aos requisitos de segurança, a solução planejada deverá implementar minimamente:

a) criptografia digital assimétrica;

b) assinatura digital e eletrônica;

c) *hashing*;

d) chave pública;

Publicado no Diário Oficial da União de 22 de dezembro de 2017, Seção 1, página 385 e 386.

e) chave privada; e

f) certificado digital disponibilizado por uma entidade autorizada - ICP Brasil ou equivalente;

II - o processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:

a) singularidade: uma assinatura eletrônica só é válida se for exclusiva ao signatário individual. Deve identificar um indivíduo específico e deve dificultar sua duplicação;

b) controle: uma assinatura eletrônica válida deve estar sob o exclusivo controle do signatário e exigir que o signatário use um nome de usuário e uma senha únicos para acessar o sistema e afixar a assinatura;

c) notificação: o sistema deve notificar o signatário de que a assinatura foi afixada;

d) intenção de assinatura: o signatário deve ser solicitado antes que sua assinatura seja afixada. Deve haver uma palavra ou declaração de intenção que transmite definitivamente a intenção do signatário de afixar sua assinatura;

e) deliberação: um indivíduo que usa uma assinatura eletrônica deve tomar ações deliberadas e reconhecíveis para afixar sua assinatura, deve restar claro o que está sendo assinado, inclusive permitindo revisar ou modificar o conteúdo a ser assinado;

f) associação da assinatura: uma assinatura deve ser anexada, ou logicamente associada, ao registro ou documento que está sendo assinado, caso contrário, tal registro ou documento não será considerado legalmente válido;

g) rastreável e recuperável: o usuário deve ser capaz de identificar e recuperar os documentos aos quais sua assinatura eletrônica foi aplicada. Uma assinatura eletrônica deve fornecer rastreabilidade positiva ao indivíduo que assinou um registro, ou qualquer outro documento;

h) protocolos de segurança e prevenção de acesso e modificação não autorizados: um processo de assinatura eletrônica deve ser seguro e deve impedir o acesso não autorizado ao sistema que afixa a assinatura aos documentos ou registros pretendidos. O processo deve garantir que somente o signatário pretendido pode afixar sua assinatura e deve impedir que pessoas não autorizadas modifiquem o conteúdo assinado ou documentos anexos. O processo deve impedir modificações em informações / dados ou entradas adicionais em registros ou documentos sem requerer uma nova assinatura. Além disso, o processo deve conter restrições e procedimentos para proibir o uso da assinatura eletrônica de um indivíduo quando o indivíduo sair ou encerrar o emprego;

i) permanente e inalterável: uma assinatura eletrônica válida deve ser uma parte permanente do registro ou documento ao qual foi afixada. As informações contidas no registro ou documento devem ser inalteráveis sem uma nova assinatura para validar a alteração;

j) identificação e autenticação: o software de assinatura eletrônica deve ter capacidades de autenticação que podem identificar uma assinatura como pertencente apenas a um determinado signatário. Um indivíduo que use uma assinatura eletrônica deve ser obrigado a usar um método de autenticação que identifique positivamente o indivíduo dentro do sistema de assinatura eletrônica;

k) corrigível: um processo de assinatura eletrônica deve incluir um meio para que um detentor de certificado corrija registros ou documentos que foram assinados eletronicamente por erro, bem como os documentos em que uma assinatura está corretamente adotada, mas as informações ou dados estão em erro. Uma assinatura eletrônica deve ser invalidada sempre que uma entrada substitutiva for feita para corrigir o registro ou documento. As informações ou assinaturas que estão sendo corrigidas devem ser anuladas, mas permanecerem no lugar. A nova informação e / ou assinatura devem ser facilmente identificáveis;

l) arquivável: deve haver um meio para que os documentos assinados eletronicamente sejam arquivados de forma segura; e

m) não repúdio: uma assinatura eletrônica válida é aquela que não pode ser negada (repudiada) pelo responsável pela assinatura. Um processo de assinatura eletrônica deve conter procedimentos e controles que assegurem a autenticidade da assinatura e impeça que o responsável pela assinatura negue ter afixado sua assinatura a um registro, documento ou dado específico.

III - o sistema a ser utilizado deverá possuir e seguir políticas e procedimentos para assegurar a segurança e integridade das informações nele registradas seguindo minimamente os seguintes requisitos:

a) processo de auditoria: políticas e procedimentos de assinatura eletrônica deverão incluir um processo de auditoria para garantir que todos os requisitos para assinaturas eletrônicas continuem a ser atendidos. O processo deve incluir o reconhecimento não autorizado de eventos, que inclui ações a serem tomadas pelo titular do certificado após a descoberta de uma tentativa de um indivíduo não autorizado de usar uma assinatura eletrônica;

b) alteração de processos: as políticas e os procedimentos do processo de assinatura eletrônica de um detentor de certificado devem abordar como o detentor do certificado enviará alterações ao processo de assinatura eletrônica para ANAC;

c) *backup* e preservação de Dados: a política e os procedimentos devem abordar como os dados de *backup* e preservação dos dados serão realizados; e

d) treinamento e usabilidade: as políticas e os procedimentos de um detentor de certificado devem incluir qualquer treinamento e instruções necessárias para garantir que usuários autorizados compreendam como acessar e aplicar corretamente o processo de assinatura eletrônica. Os procedimentos devem descrever como os usuários são notificados de mudanças no processo de assinatura eletrônica.

IV - visando a integridade e confiabilidade da informação, o sistema deverá, comprovadamente, demonstrar:

a) como o processo de assinatura eletrônica previne que pessoas não autorizadas assinem um documento ou registro;

b) como os processos aplicados no sistema previnem que alguém além do signatário pretendido consiga assinar o registro ou documento;

c) como as modificações em um documento assinado são evitadas sem uma nova assinatura; e

d) como a assinatura é afixada de forma permanente ao documento ou registro a ser assinado;

V - os sistemas de manutenção e registro eletrônico de logs e dados devem incluir os seguintes elementos:

a) da segurança:

1. o sistema deverá proteger informações confidenciais;

2. o sistema deverá garantir que a informação em um registro eletrônico não seja alterada de forma não autorizada; e

3. o sistema deverá providenciar acesso seguro e conter garantias contra acesso não autorizado;

b) dos procedimentos:

1. um detentor de sistema certificado deverá fornecer seus registros em um formato aceitável pela Agência. A ANAC poderá solicitar ao detentor de um sistema de registro eletrônico acesso direto ao sistema eletrônico com a finalidade de inspecionar registros regulatórios;

2. o sistema ou solução deverá ter procedimentos para auditoria periódica de forma a garantir a qualidade, integridade e precisão do sistema (um registro da auditoria deverá ser preenchido e mantido em arquivo.);

3. o sistema deverá incluir procedimentos para manutenção e suporte que incluem provisões para interrupções de sistema eletrônico (hardware, software, rede de aplicativos etc) e protegem contra a perda de dados de registro. O sistema também deverá incluir medidas de *backup* para manter e fornecer acesso aos registros em caso de falha do sistema. O sistema de *backup* poderá ser um sistema eletrônico separado, um servidor de *backup* ou uma unidade de *backup*. O *backup* também poderá incluir mídia como impressão ou CD-ROM, unidade externa ou outra mídia aceitável pela ANAC;

4. os procedimentos deverão garantir que os registros atendam aos requisitos regulamentares expedidos em atos específicos da ANAC;

5. os procedimentos do sistema deverão conter diretrizes para que os representantes autorizados do detentor do sistema usem registros eletrônicos e tenham acesso aos registros apropriados;

6. a autenticação eletrônica, assinatura, validação ou endosso deverão ser uma parte permanente de qualquer registro eletrônico. Qualquer forma eletrônica de validação deverá atender aos requisitos legais da assinatura eletrônica conforme descrito nesta resolução;

7. cada sistema de manutenção de registros eletrônicos deverá conter treinamento e instruções de usuário para as pessoas responsáveis pela entrada, manutenção e recuperação de dados do sistema. O treinamento deverá incluir consciência de segurança e integridade do sistema, bem como procedimentos que são necessários para autorizar o acesso ao sistema de registro eletrônico;

8. avanços tecnológicos poderão tornar desejável ou necessário para um regulado que seu sistema de registro eletrônico seja atualizado ou que haja transferência dos dados para um novo sistema. O titular desse sistema deverá ter políticas e procedimentos que assegurem a integridade contínua dos dados de registro quando houver movimentação de dados e registros de um sistema para outro. Isso poderá implicar a execução de sistemas redundantes por um curto período de tempo;

9. o sistema deverá ter um método para garantir a continuidade dos dados durante a transição de um sistema de legado (cópia) para um novo sistema eletrônico;

10. os procedimentos deverão garantir a continuidade com os fornecedores de manutenção. Os detentores de sistemas deverão garantir a continuidade entre seus programas e respectivos fornecedores de manutenção. Isso será necessário para garantir a qualidade e integridade de cada registro que será mantido através do sistema de registro eletrônico.

c) equipe responsável: políticas e procedimentos deverão identificar a pessoa ou equipe que terá autoridade e responsabilidade geral pela integridade e segurança do sistema de registro eletrônico de logs e dados e que são responsáveis pelo controle de acesso ao sistema. Políticas e procedimentos também deverão identificar as pessoas com a autoridade e a responsabilidade de modificar o sistema de registro eletrônico, bem como aqueles que são responsáveis pela entrada de dados no sistema.

d) procedimentos de auditoria: o detentor do sistema deverá ter procedimentos de auditoria que assegurem a qualidade e integridade de cada registro mantido no sistema e que todos os requisitos do sistema de registro eletrônico continuem a ser cumpridos. Os procedimentos deverão incluir o reconhecimento de eventos não autorizados, que inclui as ações a serem tomadas pelo detentor do certificado após a descoberta de uma tentativa por parte de um indivíduo não autorizado de acessar e / ou fazer inscrições no sistema eletrônico de manutenção de registros.

CAPÍTULO IV
DA UTILIZAÇÃO DO SISTEMA

Art. 5º Um interessado apenas poderá registrar determinada informação em um único sistema de maneira oficial.

§ 1º O uso do registro em um sistema de informação implicará a não utilização de novos registros em papel.

§ 2º Uma informação pode estar replicada em mais de um banco de dados, contanto que apenas uma seja a fonte para uso oficial e as demais apenas referenciais.

§ 3º Estão excetuadas do caput deste artigo os *backups* dos dados, mesmo quando estejam sendo utilizados de maneira primária no caso de falha do sistema principal.

Art. 6º No caso de descontinuação de uso de um sistema as informações deverão ser preservadas até prazo previsto em normativo específico, ou repassadas de forma adequada para quem for de direito.

CAPÍTULO V
DA DISPONIBILIDADE PARA FISCALIZAÇÃO

Art. 7º Todas as informações armazenadas em sistemas informatizados deverão estar disponíveis para fins de fiscalização ou eventual transmissão de dados, na forma e periodicidade definida em normativo específico para cada escopo.

Art. 8º É responsabilidade do operador a guarda das informações.

Parágrafo único. Eventual perda de informações, independente do motivo, será considerada como se as informações nunca tivessem sido registradas.

CAPÍTULO VI
DISPOSIÇÕES FINAIS

Publicado no Diário Oficial da União de 22 de dezembro de 2017, Seção 1, página 385 e 386.

Art. 9º Caberá ao interessado o fornecimento de relatório que comprove o atendimento aos requisitos estabelecidos nesta Resolução.

Parágrafo único. Será de responsabilidade da Superintendência de Tecnologia da Informação - STI o recebimento e a conferência do relatório recebido quanto aos requisitos de segurança e integridade.

Art. 10. Esta Resolução entra em vigor na data de sua publicação.

JOSÉ RICARDO PATARO BOTELHO DE QUEIROZ
Diretor-Presidente

Publicado no Diário Oficial da União de 22 de dezembro de 2017, Seção 1, página 385 e 386.