Reglamento para Establecer el Procedimiento para el Uso y Manejo de Firmas Digitales, Firmas Electrónicas y Transacciones Electrónicas del Departamento de Estado del Gobierno de Puerto Rico

Tabla de Contenido

Reglamento para Establecer el Procedimiento para el Uso y Manejo de Firmas Digitales, Firmas Electrónicas y Transacciones Electrónicas del Departamento de Estado del Gobierno de Puerto Rico

Artículo 1: Título

Este Reglamento se conocerá y será citado como el "Reglamento para Establecer el Procedimiento para el Uso y Manejo de Firmas Digitales, Firmas Electrónicas y Transacciones Electrónicas del Departamento de Estado del Gobierno de Puerto Rico".

Artículo 2: Base Legal

Este Reglamento se promulga conforme a las facultades inherentes del Secretario de Estado para reglamentar los asuntos del Departamento de Estado, según dispuesto en el Código Político de Puerto Rico de 1902, 3 L.P.R.A. §§51-66j.

Además, se promulga en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", 3 L.P.R.A. §§ 991-998, la cual establece como política pública del Gobierno de Puerto Rico la incorporación de las tecnologías de información a los procedimientos gubernamentales, a la prestación de servicios y a la difusión de información, e impone a las agencias gubernamentales el deber desarrollar las actividades y gestiones necesarias dirigidas a incorporar activamente el uso de tecnologías de información y telecomunicaciones en el funcionamiento gubernamental, con especial atención a las siguientes áreas: servicios a los ciudadanos, compras y subastas, orientación y divulgación sobre temas de interés social, cultural y económico para los ciudadanos a través del portal del Gobierno.

Igualmente, este Reglamento se fundamenta en la Ley Núm. 148-2006, según enmendada, conocida como "Ley de Transacciones Electrónicas", 10 L.P.R.A. §§ 4081-4096, la cual en su Artículo 17 impone a la "Puerto Rico Innovation and Technology Service" (PRITS) la responsabilidad de aprobar la reglamentación necesaria para evaluar la capacidad de las agencias y sus funciones para participar de transacciones de forma electrónica, organizar y coordinar con las agencias el acceso de los ciudadanos a los servicios que ofrece el Gobierno mediante transacciones electrónicas, así como el uso de firmas electrónicas, garantizando la seguridad de las transacciones. En su Artículo 20, la Ley Núm. 148-2006, supra, PRITS deberá establecer los estándares para el uso de expedientes electrónicos o firmas electrónicas por parte de las agencias.

En cumplimiento con esta responsabilidad, PRITS publicó las "Guías para la Implementación de Firmas Electrónicas en las Agencias", las cuales proveen a las Agencias un marco para que puedan emplear el uso de firmas electrónicas en el curso de sus operaciones tanto internas como externas, mediante procesos electrónicos confiables,

minimizando la posibilidad de falsificación de la firma electrónica y el fraude en las transacciones electrónicas y asegurando que se lleve a cabo la supervisión y administración adecuada para las transacciones electrónicas realizadas por la Agencia.

Además, se adopta en cumplimiento con los requisitos exigidos por la "Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico", Ley Núm. 38-2017, 3 LPRA §9611-9630.

Artículo 3: Propósito, Resumen Ejecutivo y Análisis de Costo-Beneficio

Este Reglamento se aprueba con el propósito de establecer las normas y estándares que regirán el uso de las firmas digitales y electrónicas en el curso de las operaciones, tanto internas como externas, del Departamento de Estado del Gobierno de Puerto Rico. Mediante la aprobación de este Reglamento, se procura además minimizar la posibilidad de falsificación de las firmas electrónicas, así como el fraude en las transacciones electrónicas que se lleven a cabo en la Agencia.

Para lograr este propósito, en este Reglamento se establecen los parámetros necesarios para el uso adecuado de las firmas digitales, conforme a las disposiciones de las leyes y reglamentos vigentes.

Aprobado este Reglamento, el Departamento de Estado acepta y reconoce la validez de las firmas digitales y electrónicas en las transacciones y documentos que se generan en el curso ordinario de las labores en el mismo.

De conformidad a la Ley 38, supra, se certifica que la adopción, aprobación y puesta en vigor de este Reglamento no tiene ningún impacto económico adicional para el Gobierno de Puerto Rico, el Departamento de Estado o la ciudadanía en general. El análisis de los beneficios que genera este reglamento supera sus costos, por los ahorros que conlleva las transacciones mediante documentos físicos, recursos utilizados y aspectos de seguridad para el Estado.

Artículo 4: Aplicabilidad

Este Reglamento será de aplicación a todas las dependencias, oficinas, funcionarios y empleados del Departamento de Estado del Gobierno de Puerto Rico.

Artículo 5: Interpretación

Las palabras y frases utilizadas en este Reglamento se interpretarán según el contexto y significado sancionado por el uso común y corriente.

Los términos utilizados en este Reglamento en el tiempo futuro incluyen también el tiempo presente; los usados en el género masculino incluyen el femenino y el neutro; el número singular incluye el plural y el plural incluye el singular, salvo los casos en que tal interpretación resulte absurda o incompatible.

Si el lenguaje empleado es susceptible de dos o más interpretaciones, se interpretará para adelantar los propósitos de este Reglamento y del artículo o inciso particular objeto de interpretación.

Artículo 6: Definiciones

Los siguientes términos o frases, según se utilizan en este Reglamento, tendrán los significados que se indican a continuación:

a) **Agencia Certificadora ("Certification Agency" o "CA") –** Organización que emite firmas digitales mediante certificados digitales.

b) **Autenticación –** Establecimiento de un medio de verificación de la identidad de la persona.

c) **Autenticación Multifactorial –** Proceso para autenticar usuarios que requiere más de un mecanismo de autenticación dentro del triángulo de autenticación (¿Qué sé?, ¿Qué tengo?, ¿Quién soy?).

d) **Autoridad para Firmar –** Permiso dado o delegado por el Secretario para firmar contratos, recibos o cualquier otro tipo de documentos en representación del Departamento de Estado o cualquiera de sus dependencias.

e) **Certificado Digital** - Es un archivo que certifica la identidad del usuario que contiene su llave pública y se puede utilizar para distintos tipos de transacciones. Por ejemplo, apoyar comunicaciones codificadas y firmar mensajes de correo electrónico. El propósito de un certificado digital es validar que el usuario tiene el derecho de utilizar su llave pública y privada otorgada por una Agencia Certificadora.

f) **Código de Verificación** - es un resultado de la técnica asimétrica que confirma que la información codificada mantuvo su integridad. Éste es asegurado por un código único codificado de un tamaño fijo (cantidad de bits).

g) **Departamento** - Departamento de Estado del Gobierno de Puerto Rico.

h) **Documento** - Significa aquella información inscrita en un medio tangible o almacenada en un medio electrónico, susceptible de ser recuperada de manera perceptible.

i) **Documento Electrónico** - Significa el archivo creado, generado, enviado, comunicado, recibido o almacenado por cualquier medio electrónico.

j) **Electrónico** - Significa cualquier tecnología con capacidad eléctrica, digital, magnética, inalámbrica, óptica, electromagnética, o de funcionamiento similar.

k) **Empleado –** Persona que rinde servicios al Departamento mediante nombramiento con estatus o regular en el servicio de carrera, de confianza, transitorio o irregular.

l) **Firma Digital** - es un tipo de firma electrónica que se representa como un conjunto de datos, sonidos, símbolos o procesos en forma electrónica, creados por una llave privada que utiliza una técnica asimétrica para asegurar la integridad del mensaje de datos a través de un código de verificación, así́ como el vínculo entre el titular de la firma digital y el mensaje de datos remitido. En la conversión de un mensaje con firma digital, la persona que tiene el mensaje o comunicación inicial y la llave pública del signatario puede determinar con exactitud si:
    1) La conversión se realizó utilizando la llave privada que corresponde a la llave pública del signatario;
    2) El mensaje o comunicación ha sido alterado desde que realizó la conversión.

m) **Firma Digital Federal o "Federal Bridge PKI" (FBPKI)** - Programa Federal que cualifica a las Agencias Certificadoras que emiten firmas, certificados y credenciales avaladas por del gobierno federal, según aplicable.

n) **Firma Electrónica** - es la totalidad de datos en forma electrónica consignados en un mensaje, documento o transacción electrónica, o adjuntados o lógicamente asociados a dicho mensaje, documento o transacción, que puedan ser utilizados para identificar al signatario e indicar que éste aprueba la información recogida en el mensaje, documento o transacción. La firma electrónica puede ser una representación visual de una firma manuscrita digitalizada, como también puede ser un gesto de aceptación de condiciones. La firma electrónica demuestra la intención de firmar un documento por parte de un firmante. No obstante, no garantiza su identidad. Si el firmante utiliza una firma digital a su nombre como complemento en la implementación de su firma electrónica, entonces podrá estar garantizada su identidad, dependiendo de la clasificación de uso de llaves (Key Usage) de su firma digital y quién le otorga su firma digital (Agencia Certificadora).

o) **Firmante** - Individuo que firma un documento manual, digital o electrónicamente en representación propia o de alguna entidad que le haya conferido la autoridad para ello.

p) **Funcionario** - Persona que está investida de parte de la soberanía del Estado o que ocupa un cargo o puesto en el Departamento que interviene en la formulación o implementación de la política institucional.

q) **Secretario –** Secretario del Departamento de Estado del Gobierno de Puerto Rico.

r) **Técnica asimétrica –** Es un algoritmo matemático que utiliza la estructura de llave pública/privada. Esta técnica puede ser utilizada ya sea para firmar digitalmente un mensaje electrónico o codificar un mensaje. Lo que determina esta función es el orden en el cual se utilicen las llaves. Por ejemplo, a los fines de firmar un documento electrónico, con el propósito de asegurar la integridad y la identidad del firmante, se utiliza la llave privada para codificar un mensaje el cual produce un código (algoritmo matemático) único; el destinatario del mensaje codificado utilizará la llave pública para corroborar la integridad del mensaje. En caso de que la intención sea proteger la información y su confidencialidad, el emisor del mensaje utiliza la llave pública del destinatario para que solamente el destinario tenga acceso a la información a través de su llave privada (la cual se utiliza para decodificar el mensaje que tiene la información).

s) **Uso de Llaves ("Key Usage") -** Campo descriptivo dentro de un certificado digital el cual especifica los usos autorizados para las llaves del certificado.
    1) No Repudio - Es una característica de una firma digital que permite al autor, o "firmante", de un mensaje demostrar su identidad. Asegura que el origen de una información no puede rechazar su transmisión o su contenido, y/o que el receptor de una información no puede negar su recepción o su contenido.

t) **"WebTrust for Certification Authorities" –** Programa de auditorías para Agencias Certificadoras que emiten firmas y certificados digitales.

Artículo 7: Requisitos Mínimos de Uso

De conformidad a las Guías de "Puerto Rico Innovation and Technology Services" (PRITS), El Departamento cumplirá con los siguientes requisitos mínimos para el uso de firmas electrónicas o digitales.

a. Firmas electrónicas:
    1. Bridge Letter de Informe de SSAE18 SOC2/SOC3; o
    2. Informes de SSAE18 SOC2/SOC3, ISO27001 o equivalentes.
    3. El Departamento podrá contratar, por un (1) año, una empresa que ofrece firma electrónica que contenga una carta de controles emitida por un CISA o un CPA que certifica los controles implementados de información. Para continuar el contrato después del año, tendrá que cumplir con cualquiera de los requisitos "1" o "2" mencionados anteriormente.

4. En caso de que El Departamento cree su propia firma electrónica, cumplirá con los controles de información conforme al SSAE18 SOC2/SOC3 y las guías establecidas.

b. Firma digital:
    1. La misma debe ser emitida por una Agencia Certificadora que:
        i. posea el Informe de Auditoría WebTrust for Certification Authorities; o
        ii. provenga de los suplidores autorizados bajo el Gobierno Federal y el programa de FBPKI/PIV-I.
    2. En caso de que el Departamento decida implementar firmas digitales para su uso interno, tendrá que cumplir con los controles estipulados en SSAE18 SOC3 o PIV-C.
    3. Para transacciones con el gobierno federal, se utilizará la firma digital federal.
    4. Se considera como firma digital de máxima seguridad las firmas digitales FBPKI/PIV-I, las cuales cuentan con autenticación multifactorial y Key Usage de No Repudio.

Artículo 8: Aplicación de la Política de Firmas Digitales y Electrónicas

La política instituida en este Reglamento será de aplicación a las transacciones y procedimientos administrativos, internos y externos, entre el Departamento de Estado y cualquier agencia o dependencia gubernamental, entidad privada o persona.

El Director de la División de Sistemas de Información del Departamento, en conjunto con el Secretario, será el encargado de seleccionar, autorizar y validar los métodos específicos de firma digital y/o electrónica, así como la autenticación de usuarios, asegurándose de cumplir con el nivel de certeza de autenticación de identidad requerido para los diferentes tipos de procesos.

Artículo 9: Implementación de la Firma Digital o Electrónica

Cuando una firma digital o electrónica sea requerida por el Departamento, ésta será aceptada como equivalente de la firma ológrafa o manuscrita, y será legalmente vinculante, siempre y cuando se cumplan los siguientes requisitos:

a) Intención de firmar - De la misma manera que con una firma manuscrita, la parte firmante debe mostrar intención clara de firmar el documento de manera electrónica. Por ejemplo, el firmante puede demostrar la intención usando el cursor o "pad" para dibujar su firma, escribir su nombre con el teclado, pulsando sobre un botón de "aceptar" o seleccionando la opción de "aceptar", debidamente

identificada. Esto con el propósito de minimizar el riesgo de que el firmante pueda reclamar que utilizó una firma electrónica por error o sin tener pleno conocimiento que se estaba obligando legalmente o haciendo representaciones que puedan tener consecuencias legales, sean civiles y/o penales.

b) Consentimiento para hacer negocios electrónicamente – El Departamento validará el consentimiento del firmante incluyendo en los documentos a ser firmados electrónicamente una cláusula que indique lo siguiente:

> *"Las partes acuerdan que este documento puede ser firmado electrónicamente. Las partes acuerdan que las firmas electrónicas que aparecen en este documento son tan válidas como si fuesen suscritas a puño y letra para efectos de validez, obligatoriedad, consentimiento, aplicabilidad y admisibilidad".*

c) Identificación y autenticación del usuario – El Departamento debe asegurarse que la solución tecnológica que seleccione permita identificar al firmante, validar el consentimiento y corroborar la firma. Es importante que pueda correlacionar el documento con la firma electrónica con el propósito de asegurarse que el documento y la firma electrónica queden relacionados y/o unidos.

Artículo 10: Cláusula de Exclusión Voluntaria

Si un firmante decide no utilizar una firma electrónica, el Departamento le debe hacer fácilmente accesibles las instrucciones sobre cómo firmar el documento manualmente. El uso de una firma electrónica en una ocasión no vincula al firmante a utilizar ese mismo método para firmar cualquier otro documento. En cualquier momento, el firmante puede optar por no firmar electrónicamente ningún otro documento.

Artículo 11: Copias Firmadas

El Departamento se asegurará que todos los firmantes reciban una copia del documento firmado al completarse la transacción. Este requisito puede satisfacerse a través de la descarga de una copia del documento, preferiblemente en formato PDF o cualquier otro formato electrónico que garantice la integridad del documento.

Artículo 12: Retención de Documentos

La retención de los documentos electrónicos se realizará conforme a lo dispuesto en el Artículo 11 de la Ley Núm. 148-2006, *supra*.

Artículo 13: Actualización de Políticas y Procedimientos

El Departamento actualizará sus políticas y procedimientos internos de forma que se facilite que las transacciones se puedan realizar de forma electrónica, salvo que se demuestre que esta alternativa no es factible para la agencia.

Artículo 14: Publicidad de la Política de Firmas Digitales y Electrónicas

El Departamento publicará anuncios tanto en la Agencia como en su página de Internet sobre la política de firmas digitales y electrónicas aprobada.

Artículo 15: No Aplicabilidad de esta Política

La política sobre firmas electrónicas y digitales del Departamento de Estado no será aplicable en las siguientes transacciones o documentos:

a) Transacciones que estén legisladas o reglamentadas por la Ley Notarial o su reglamentación aplicable, en las cuales se requiere la presencia frente a un notario público para la firma; o cualquier otro documento que, por su naturaleza, requiere de la firma ológrafa o manual;

b) Cualquier transacción o documento que no puede ser firmado de forma digital o electrónica por haber sido excluido por alguna ley especial o un reglamento aprobado en virtud de éstas;

c) Cualquier transacción o acto que contenga un requisito de forma, conforme al Código Civil de Puerto Rico y cualquier otra ley o reglamento externo aplicable, que sea incompatible con la firma digital o electrónica.

Artículo 16: Responsabilidad de la División de Sistemas de Información

Con relación a la política de uso de firmas digitales y electrónicas, la División de Sistemas de Información del Departamento de Estado será responsable de:

a) Gestionar la contratación de los servicios de la Agencia Certificadora de firmas digitales;

b) Mantener un sistema que permita la creación de las firmas digitales o electrónicas, así como el manejo y la conservación de los documentos firmados de tal manera;

c) Mantener las medidas de seguridad necesarias para proteger las firmas digitalizadas que puedan estar grabadas en la base de datos del Departamento contra el acceso por personas no autorizadas.

d) Adoptar estándares de autenticación de identidad razonables y apropiados conforme al nivel de responsabilidad y control de riesgo aplicable a cada tipo de transacción, proceso o formulario electrónico en el cual se utilizarán firmas digitales, electrónicas, o aprobación mediante botones en formularios electrónicos; y

e) Proveer apoyo consultivo y asesoría técnica a las distintas divisiones del Departamento en el proceso de implementación de la política de firmas digitales y electrónicas.

Artículo 17: Violaciones y Sanciones

a) Cualquier empleado o funcionario con autoridad de firmar es responsable del manejo y ejecución adecuada de los documentos que firme en nombre de o en representación del Departamento de Estado, ya sea que firme de forma ológrafa (manuscrito), digital o electrónica. De incumplir con cualquiera de las disposiciones establecidas en este Reglamento podrá estar sujeto a la imposición de acciones disciplinarias.

b) Constituye una violación a este Reglamento, y podría estar sujeto a la imposición de acciones disciplinarias, el que un empleado o funcionario utilice la firma digital o electrónica de otra persona con o sin su consentimiento.

c) Cualquier empleado o funcionario que conozca de propio y personal conocimiento o sospeche de alguna acción fraudulenta con relación a las firmas digitales o electrónicas, tiene el deber de reportarlo inmediatamente a su supervisor inmediato y/o la División de Sistemas de Información.

d) Empleados o funcionarios que falsifiquen firmas digitales o electrónicas estarán violando este Reglamento y estarán sujetos a acciones disciplinarias, incluyendo la posible destitución de empleo y radicación de cargos bajo las leyes estatales y federales.

Artículo 18: Interpretación de este Reglamento ante Enmiendas a la Ley

Si con posterioridad a la aprobación y puesta en vigor de este Reglamento cualquiera de las leyes citadas como su base legal fuese enmendada, las disposiciones del Reglamento serán interpretadas conforme al estado de derecho vigente. En tal caso, se considerará derogada cualquier disposición que resulte contraria a la ley vigente.

Artículo 19: Prohibición de Discrimen

En la implementación y aplicación de este Reglamento se prohíbe el discrimen por razón de raza, color, nacionalidad, origen, condición social, edad, ideas políticas, creencias o no religiosas, género, orientación sexual, identidad de género, información genética, ser víctima o ser percibida como víctima de violencia de género, agresión sexual o acecho, ser militar, veterano, servir o haber servido en las fuerzas armadas de los Estados Unidos de América, o tener incapacidad física o mental.

Artículo 20: Separabilidad

Si cualquier cláusula, párrafo, subpárrafo, oración, palabra, letra, artículo, disposición, sección, subsección, título, capítulo, subcapítulo, acápite o parte de este Reglamento fuera anulada o declarada inconstitucional, la resolución, dictamen o sentencia a tal efecto dictada no afectará, perjudicará, ni invalidará las restantes disposiciones del mismo, sino que su efecto se limitará a la palabra, oración, inciso, artículo, sección o parte específica declarada inconstitucional o nula en esa controversia.

Artículo 21: Derogación

Este Reglamento deroga cualquier otro reglamento anterior, así como cualquier otro reglamento, regla, orden administrativa, carta circular, memorando, comunicación escrita o instrucción anterior que esté en contravención con el presente Reglamento.

Artículo 22: Vigencia

Este Reglamento entrará en vigor a los treinta (30) días de haberse presentado en el Departamento de Estado, conforme con las disposiciones de la Ley Núm. 38-2017, según enmendada, conocida como Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico.

En San Juan, Puerto Rico, hoy ___ de _____ de 2024.