Puerto Rico Innovation and Technology Service

prITs

PRITS-002

GUIAS PARA LA IMPLEMENTACION DE FIRMAS ELECTRONICAS EN LAS AGENCIAS

Revisado: 12-09-2020

TABLA DE CONTENIDO

1 Introducción

El propósito, tanto de la Ley 148-2006, conocida como Ley de Transacciones Electrónicas (LTE), como de la Ley 151-2004, conocida como la Ley de Gobierno Electrónico (LGE), es facilitar las transacciones en el Gobierno de Puerto Rico mediante el uso de firmas electrónicas, y que dichas gestiones electrónicas tengan la misma validez legal que cualquier firma a mano o expediente físico. Sin embargo, no obligan a entes privados o Agencias a usar o aceptar firmas electrónicas, a menos que alguna otra ley así lo disponga. Entiéndase que el uso y aceptación de esos medios electrónicos es completamente voluntario en la mayoría de los casos. Por consiguiente, la Agencia no podrá compeler a un ciudadano o ente jurídico al uso de una firma electrónica.

Por su parte, la Resolución Conjunta 76-2020 también hace énfasis en el establecimiento de las guías para que las agencias del Gobierno de Puerto Rico acepten la presentación de facturas por bienes y servicios y los contratos electrónicos. Más aún, indica que una vez el PRITS "adopte y publique las guías, ninguna agencia, corporación o instrumentalidad pública del Gobierno de Puerto Rico podrá rechazar un contrato o factura por haber sido generado por la vía electrónica conforme a las guías".

Las Agencias que utilicen y acepten firmas electrónicas, deberán garantizar su autenticidad, integridad, seguridad y, cuando sea apropiado o requerido por ley o reglamento, su confidencialidad.

2 Propósito

El propósito de estas guías es proveer un marco para que las Agencias puedan emplear el uso de firmas electrónicas en el curso de sus operaciones tanto internas como externas, mediante procesos electrónicos confiables, así como también minimizar la posibilidad de falsificación de la firma electrónica y el fraude en las transacciones electrónicas y asegurar que se lleve a cabo la supervisión y administración adecuada para las transacciones electrónicas realizadas por la Agencia.

3 Base Legal

Estas Guías se promulgan en virtud del inciso (a) del Artículo 6 de la Ley 75-2019. El PRITS está facultada para implantar, desarrollar y coordinar la política pública del Gobierno sobre la innovación, información y tecnología. Por su parte, el inciso (w) del mismo artículo dispone que establecerá e implementará los planes estratégicos,

las políticas, estándares y la arquitectura integrada de las tecnologías de información y telecomunicación del Gobierno. Además, el Artículo 7, inciso (3) faculta al PRITS a emitir órdenes administrativas, opiniones y/o cartas circulares.

Por otra parte, la Ley 151-2004, faculta al PRITS a establecer las guías o directrices necesarias para implantar las normas y los procedimientos relativos al uso de las tecnologías de información a nivel gubernamental.

La Ley 148-2006, Ley de Transacciones Electrónicas, según enmendada, dispone que PRITS establecerá los estándares para el uso de expedientes electrónicos o firmas electrónicas por parte de las agencias.

4 Definiciones

1. **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?) .

2. **Bridge Letter** - Carta firmada por un auditor o entidad que realiza auditorías que demuestra que la empresa u organización que ofrece firmas electrónicas está en proceso de evaluación de auditoría.

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

4. **Carta de Controles** – Es una carta emitida por un Auditor de Sistemas Información (CISA) o Contador Público Autorizado (CPA) que certifica los controles básicos de información establecido en una organización.

5. **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.

6. **Firma digital** — Según la Ley Núm. 148-2006, Ley de Transacciones Electrónicas, 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**, así como el vínculo entre el titular de la firma digital y el mensaje de datos remitido.

a. **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).

b. **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).

7. **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.

8. **Firma Electrónica** — Según la Ley Núm. 148-2006, Ley de Transacciones Electrónicas, 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).

9. **ISO 27001** Information Security Management – es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

10. **Personal Identification Verification Compatible (PIV-C) –** Credencial de identidad con las mismas especificaciones técnicas que el PIV-I, con la diferencia que las firmas digitales en la credencial no están certificadas por el programa del gobierno federal (FBPKI). Este tipo de tecnología se utiliza para casos de organizaciones que deseen la capacidad tecnológica pero no las garantías de identidad provistas por el gobierno federal, por regla general son para uso interno en una organización.

11. **Personal Identification Verification Interoperability (PIV-I)** – Esta es una credencial de identidad regulado por el Gobierno Federal otorgado a entidades no federales con el propósito de crear una identidad digital confiable e interoperable, entiéndase por interoperable como la capacidad de poder ser utilizada en múltiples entidades y transacciones. La misma contiene firmas digitales federales que solamente son expedidas por Agencias Certificadoras aprobadas bajo el gobierno federal.

12. **SSAE 18 SOC 2** - Informe de Auditoría desarrollado por el Instituto Americano de Contadores Públicos Autorizados (AICPA) que evalúa los controles de información en una organización basándose en los Criterios y Principios de los Servicios de Confianza de AICPA: seguridad, integridad, disponibilidad, confidencialidad y privacidad.

13. **SSAE 18 SOC 3** – Versión abreviada del informe de auditoría SOC 2 Tipo 2, para usuarios que desean tener la seguridad sobre los controles de una organización, pero no necesitan todo el detalle que incluye el reporte SOC 2.

14. **Uso de Llaves (Key Usage)** - Campo descriptivo dentro de un certificado digital cual especifica los usos autorizados para las llaves del certificado.

    a. 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.

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

5 Aplicabilidad

Estas guías serán aplicables a todas las Agencias, según definidas en la Ley 75-2019. Quedan exceptuadas las transacciones consignadas en el Artículo 3(b) de la Ley 148-2006, y cualquier otra que, mediante ley debidamente aprobada, se excluya.

6 Requisitos Mínimos de Uso

Las Agencias del Gobierno de Puerto Rico cumplirán con los siguientes requisitos mínimos para el uso de firmas electrónicas o digitales.

1. **Firma Electrónicas**

    a. Bridge Letter de Informe de SSAE18 SOC2/SOC3; o

    b. Informes de SSAE18 SOC2/SOC3, ISO27001 o equivalentes

    c. Una agencia 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 “a” o “b” mencionados anteriormente.

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

2. **Firma Digital**

    a. 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.

    b. En caso de que la Agencia decida implementar firmas digitales para su uso interno, tendrá que cumplir con los controles estipulados en SSAE18 SOC3 o PIV-C.

    c. Para transacciones con el gobierno federal, se utilizará la firma digital federal.

d. 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.

7 Implementación

Para que una firma electrónica o digital sea legalmente vinculante bajo las leyes estatales y federales, es necesario que el proceso de manejo y almacenamiento de dichas firmas cumpla con los siguientes requisitos.

1. **Definir el tipo de la firma**: Determinar el tipo de firma a utilizar: firma digital o firma electrónica, Artículos 2(12) y 2(13) de la LTE, respectivamente.

2. **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. Tiene 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.

3. **Consentimiento para hacer negocios electrónicamente** – Es necesario que se obtenga el consentimiento previo. Las leyes de firma electrónica requieren consentimiento para hacer negocios electrónicamente. Un mecanismo ampliamente admitido es el de aceptar una cláusula de consentimiento estándar o que proporcionan una opción para personalizar una cláusula de consentimiento. Por ejemplo:

   > *"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 fuera suscrita a puño y letra para efectos de validez, obligatoriedad, consentimiento aplicabilidad y admisibilidad."*

4. **Identificación y autenticación del usuario** – La Agencia 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.

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

6. **Copias firmadas** - Todos los firmantes deben recibir una copia del documento firmado al completarse la transacción. Este requisito puede satisfacerse a través de la descarga una copia del documento preferiblemente en formato PDF o cualquier otro formato electrónico que garantice la integridad del documento.

7. **Retención de documentos** - Los requisitos de retención de registros electrónicos se detallan en el Artículo 11 de la Ley de Transacciones Electrónicas, que legitima la validez de los registros siempre que reflejen con precisión el documento y puedan reproducirse según sea necesario. La Agencia deberá establecer la frecuencia con la que realizará los resguardos de los documentos firmados digitalmente con la misma o mayor diligencia que si fuera un documento en papel.

   De no existir un periodo de retención que haya sido establecida por ley o reglamento, el documento será retenido por el tiempo necesario para evitar exponer a la Agencia o al Gobierno de Puerto Rico a reclamación alguna. En el ámbito penal, deberá conservarse hasta que transcurra el periodo de prescripción de cualquier delito que pueda quedar evidenciado por dicho documento. El documento final debe ser retenido en repositorios de documentos manejados por el Gobierno de Puerto Rico. Por ejemplo, Microsoft SharePoint o Microsoft OneDrive, que pueden ser protegidos por el Data Loss Prevention de Office 365 (DLP Policies).

8. **Registro de transacción** – La solución utilizada por la Agencia tiene que generar un archivo que contenga el detalle de las evidencias electrónicas sobre el proceso de firma por cada transacción. Por ejemplo: direcciones de correo del solicitante y firmante, información sobre el dispositivo desde el que se realiza la transacción, dirección IP, entre otros, dicho documento servirá como un registro acreditativo de la transacción, según sea aplicable.

9. **Transacciones de un firmante** – De utilizarse una firma digital para transacciones o documentos que son firmadas por una sola persona, se implementará un mecanismo mínimo de autenticación, el cual se recomienda que sea una autenticación multifactorial.

8 Políticas

Cada Agencia es responsable de desarrollar las políticas, guías, reglamentación o procesos internos para viabilizar el uso de las firmas electrónicas y/o digitales a tenor con la presente Carta Circular, sus guías y la Ley 148-2006.

Las políticas de firmas electrónicas y firmas digitales se deberán trabajar por separado en la Agencia debido a que requieren tecnologías, implementación, auditorías y marcos regulatorios diferentes. Toda política implantada por una Agencia tiene que incluir como mínimo:

1. Un procedimiento detallado donde se exponga la manera en la cual que se informarán sobre los procesos de uso y no-uso de firma electrónica y/o digital.

2. Las medidas de seguridad adecuadas que tomarán para el manejo y almacenamiento de información y documentos.

3. Los protocolos para evitar la falsificación de firma y el fraude electrónico. Por ejemplo: autenticación, controles de accesos físicos y lógicos a la información, registro de la transacción, etc.

4. Los estándares, limitaciones y procesos específicos, incluyendo, pero no limitado a:

    a. Opciones de tecnología que la Agencia posea.

    b. Las transacciones específicas en las cuales la Agencia utilizará firmas electrónicas o digitales en las siguientes instancias:

        i. servicios al ciudadano,
        ii. transacciones y comunicaciones internas de la agencia,
        iii. transacciones y comunicaciones interagenciales y municipales,
        iv. transacciones y comunicaciones con el sector privado y
        v. transacciones y comunicaciones federales.

5. Procesos y metodologías de la Agencia, tales como el proveer a los usuarios un documento imprimible o descargable como parte del proceso de firma electrónica.

6. Instrucciones al usuario.

7. Literatura para entrenamiento sobre el uso de firmas electrónica y digitales, sus diferencias y las instancias dentro de las Agencias que se utilizara una o la otra.

8. Las Agencias tendrá disponibles procedimientos para que los usuarios opten por no utilizar firmas electrónicas (“opt-out”).

9. Advertencia sobre las obligaciones de las personas que utilicen el sistema de firmas electrónicas.

10. Colocación de anuncios en la Agencia, y sus páginas de Internet, sobre la política de firmas electrónicas y digital.

11. Procedimientos para enmendar la política de firmas electrónicas y digitales.

12. Una advertencia contenida en el documento a ser firmado comunicando a los firmantes de que se hace bajo la LTE y que la firma electrónica es tan válida como si fuera suscrita a puño y letra. Véase sección 7(3).

13. Política de confidencialidad - La Agencia tiene la obligación de mantener la confidencialidad de los documentos que contengan información sensitiva o privilegiada independientemente del método que se utilice para firmar el mismo.

9 Responsabilidad y Autoridad de las Agencias y PRITS

1. Las Agencias enviarán a PRITS a través de support@prits.pr.gov las políticas que se aprueben sobre el uso de firmas electrónicas y digitales. Estas políticas entrarán en vigor una vez sean autorizadas por la autoridad nominadora de la Agencia y enviadas, con el acuse de recibido oficial a PRITS.

2. PRITS podría evaluar estas políticas según lo estipulado en la Ley 148-2006, por nuevas tecnologías de seguridad disponibles en la industria y/o nueva legislación y reglamentación federal y/o estatal.

3. Cada Agencia es responsable de seguir las disposiciones legales aplicables a los procesos de adquisiciones de bienes y servicios, tal y como si fuera una transacción en papel.

4. Cada Agencia es responsable de acatar toda regulación estatal y federal aplicable para el uso de firmas electrónicas y digitales.

10 Mantenimiento de las Guías

El Principal Ejecutivo de Innovación e Información del Gobierno de Puerto Rico es quien tiene la autoridad para llevar a cabo cualquier cambio a este documento. Las Guías se revisarán a medida que evolucionen los procedimientos y tecnologías relacionadas.

11 Guía Básica

Para asistir a las Agencias en la preparación de su normativa sobre el uso de firmas electrónicas, se provee la siguiente Guía Básica, la cual contiene los asuntos medulares que cada Agencia debe atender en su normativa para el uso de firmas electrónicas:

I. Nombre de la agencia (información)

II. Propósito
   a. Servir de guía para implantar un procedimiento en el uso y manejo de firmas digitales que cumpla con la Ley 148-2006, Ley de Transacciones Electrónicas, según enmendada ("Ley 148" o "LTE") y la Ley Núm. 151-2004, Ley de Gobierno Electrónico, según enmendada ("Ley 151" o "LGE").

III. Alcance
   a. Esta guía aplica a toda transacción generada como parte de las actividades de esta agencia [enumerar]. No aplicará a las siguientes transacciones [enumerar]. Puede presentar en forma de tabla. Ejemplo:

Transacción	Descripción	Aplica (si/no)

IV. Trasfondo
   a. El Gobierno ha reconocido que la innovación es un pilar del desarrollo económico y que su estructura debe mantenerse a la par con la evolución de las tecnologías para así lograr eficiencias en las operaciones gubernamentales y con ello incrementar la rapidez y la

calidad del servicio. Por tanto, la inserción de métodos innovadores, para dar continuidad a las operaciones gubernamentales, requiere de estándares uniformes que sirvan de apoyo operacional y legal para la adquisición de los mismos.

b. El propósito de la LGE y la LTE es facilitar las transacciones en el Gobierno de Puerto Rico mediante el uso de firmas electrónicas, y que dichas gestiones electrónicas tengan la misma validez legal que cualquier firma a mano o expediente físico. La LGE y la LTE, no obligan a entes privados o Agencias a usar o aceptar firmas electrónicas, a menos que alguna otra ley disponga lo contrario. Entiéndase que el uso y aceptación de esos medios electrónicos es completamente voluntario en la mayoría de los casos. Ninguna Agencia podrá compeler a un ciudadano o ente jurídico al uso de una firma electrónica.

V. Definiciones

a. Para los propósitos de estas Guías, los términos aquí utilizados tendrán el significado que se le otorga tanto la Ley 75-2019 como en la Ley 148-2006, resaltando las siguientes:

i. “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 este aprueba la información recogida en el mensaje, documento o transacción

ii. “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, así 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.

VI. Política (incluir/detallar lo siguiente)

a. Identificar claramente los estándares, limitaciones y procesos específicos, incluyendo, pero no limitado a:

i. Opciones de tecnología que la Agencia ya posea.
ii. Las transacciones específicas en las cuales la Agencia utilizará firmas electrónicas.

Ejemplo:

Tipo de documento	Uso de firma electrónicas(sí/no)	Aplicación autorizada para firmas electrónicas
Memos internos	Sí	
Memos externos	Sí	

iii. Determinar, de ser aplicable, si el uso será para solicitudes iniciales, para renovaciones o para ambas.
iv. Procesos y metodologías para seguir por la Agencia, tales como el proveer a los usuarios un documento imprimible o descargable como parte del proceso de firma electrónica.
v. Instrucciones al usuario, literatura para entrenamiento.
vi. Las Agencias también deben considerar el tener disponibles procedimientos para que usuarios opten por no utilizar firmas electrónicas (“opt-out”).
vii. Advertencia sobre las obligaciones de las personas que utilicen el sistema de firmas electrónicas.
viii. Colocación de anuncios en la Agencia y sus páginas de internet sobre la política de firmas electrónicas.
ix. Procedimientos para enmendar la política propuesta.
x. La Agencia deberá someter a la PRITS la advertencia contenida en el documento a ser firmado advirtiendo a los firmantes de que se hace bajo la LTE y que la firma electrónica es tan válida como si fuera suscrita a puño y letra.

xi. Política de confidencialidad.

VII. Responsabilidades

a. Enumerar y presentar el rol del personal a cargo de gerenciar el proceso y/o cualquiera otra información relevante al proceso de administrar el proceso

Ejemplo:

Nombre	Departamento	Puesto	Rol en el proceso	Información de contacto	Comentarios

VIII. Procedimientos

a. Describir cualquier proceso asociado a la implantación del programa de firmas electrónicas.

IX. Apéndices

a. Adjuntar cualquier documentación particular y pertinente de la Agencia que tenga relevancia o estime debe acompañar este documento como parte del proceso de firmas electrónicas.

X. Referencias

a. Adjuntar cualquier referencia que estime necesario que tenga relevancia o estime debe acompañar este documento como parte del proceso de firmas electrónicas.

XI. Historia (del SOP)

Ejemplo:

Escrito/Revisado por:	Aprobado por:	Fecha de aprobación	Versión	Comentarios