

Administración de Servicios Generales
Gobierno de Puerto Rico

Número: 9686

Fecha: 18 de agosto de 2025


Aprobado: Rosachely Rivera Santana
Secretaria de Estado
Departamento de Estado

Reglamento para Establecer el Procedimiento para el Uso y Manejo de Firmas Digitales y
Electrónicas de la Administración de Servicios Generales del Gobierno de Puerto Rico



Índice

Capítulo I: Disposiciones Generales.....	1
Artículo 1.1: Título.....	1
Artículo 1.2: Base Legal	1
Artículo 1.3: Propósito y Resumen Ejecutivo.....	2
Artículo 1.4: Aplicabilidad.....	2
Artículo 1.5: Definiciones	3
Capítulo II: Regulación y Uso de Firmas Electrónicas y Digitales	6
Artículo 2.1: Guías de uso.....	6
Artículo 2.2: Disposiciones Generales.....	6
Artículo 2.3: Implementación de Firmas Digitales y Electrónicas	7
Capítulo III: Procedimientos de Firma y Seguridad.....	8
Artículo 3.1: Procedimiento para el Uso de Firmas Digitales.....	8
Artículo 3.2: Cláusula de Exclusión Voluntaria.....	8
Artículo 3.3: Copias Firmadas y Retención de Documentos	8
Capítulo IV: Cumplimiento, Supervisión y Sanciones	8
Artículo 4.1: Oficina de Informática	8
Artículo 4.2: Violaciones y Sanciones	9
Capítulo V: Disposiciones Finales.....	11
Artículo 5.1: Interpretación del Reglamento ante Enmiendas a la Ley.....	11
Artículo 5.2: Cláusula de Separabilidad.....	11
Artículo 5.3: Vigencia.....	11

Capítulo I: Disposiciones Generales

Artículo 1.1: Título

Este Reglamento se denominará "Reglamento para Establecer el Procedimiento para el Uso y Manejo de Firmas Digitales y Electrónicas de la Administración de Servicios Generales del Gobierno de Puerto Rico".

Artículo 1.2: Base Legal

1. Este Reglamento se promulga en virtud de la Ley de la Administración de Servicios Generales para la Centralización de las Compras del Gobierno de Puerto Rico, Ley Núm. 73-2019.
2. En su Artículo 5, esta Ley establece la Administración de Servicios Generales (en adelante, ASG) como la agencia de la Rama Ejecutiva encargada de:
 - a) Establecer la política pública de Puerto Rico en asuntos relacionados con compras de bienes, obras y servicios para entidades gubernamentales.
 - b) Implementar la centralización de las compras dentro del Gobierno.
3. Además, el Artículo 11, inciso (j) de la Ley faculta al Administrador de la ASG para:
 - a) Adoptar, enmendar y derogar reglamentos que permitan el cumplimiento de esta Ley y otras leyes aplicables.
4. Este Reglamento también se promulga en virtud de las siguientes leyes:
 - a) Ley Núm. 151-2004, Ley de Gobierno Electrónico, que establece como política pública la incorporación de tecnologías de información en la administración gubernamental.
 - b) Ley Núm. 148-2006, Ley de Transacciones Electrónicas, la cual delega en el *Puerto Rico Innovation and Technology Service* (PRITS) la responsabilidad de establecer estándares y reglamentaciones sobre transacciones electrónicas y uso de firmas digitales.
 - c) Ley Núm. 38-2017, Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico, que establece las normas para la aprobación, enmienda y publicación de reglamentos administrativos.

- d) Ley Núm. 75-2019, Ley de la Puerto Rico Innovation and Technology Service, que establece la política pública del Gobierno de Puerto Rico de que las tecnologías de información y comunicación sean administradas con niveles óptimos de eficiencia. Incluye además las cartas circulares, guías y otras normas que promulgue PRITS.
- e) Ley Núm. 40-2024, Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico, que establece que toda agencia, en colaboración con la PRITS, será responsable de desarrollar, documentar e implementar programas de ciberseguridad.

Artículo 1.3: Propósito y Resumen Ejecutivo

- 1. El propósito de este Reglamento es establecer normas y estándares que regulen el uso de firmas digitales y electrónicas en todas las operaciones, tanto internas como externas, de la ASG, en tanto las herramientas necesarias para ello hayan sido adoptadas.
- 2. Mediante la aprobación de este Reglamento, se pretende:
 - a) Proveer directrices claras sobre el uso adecuado de firmas digitales y electrónicas conforme a las leyes y regulaciones aplicables.
 - b) Agilizar procesos administrativos mediante la digitalización de documentos y procedimientos internos.
- 3. Con la entrada en vigor de este Reglamento, la ASG reconoce la validez de las firmas digitales y electrónicas en todas sus transacciones y documentos oficiales.
- 4. Conforme a lo establecido en la Ley Núm. 38-2017, *supra*, se certifica que la adopción, aprobación y puesta en vigor de este Reglamento no tendrá impacto económico adicional para la ASG ni para la ciudadanía en general.

Artículo 1.4: Aplicabilidad

- 1. Las disposiciones de este Reglamento serán de aplicación a:
 - a) Todas las dependencias, oficinas y funcionarios de la ASG.
 - b) Toda transacción o procedimiento administrativo en el cual la ASG utilice firmas digitales o electrónicas.

- c) Cualquier interacción entre la ASG y entidades gubernamentales, contratistas, proveedores o ciudadanos, cuando se requiera el uso de firmas electrónicas.
2. En todo momento se deberán observar los Estándares y Principios Mínimos de Seguridad establecidos por la PRITS.

Artículo 1.5: Definiciones

1. Administración: Administración de Servicios Generales.
2. Administrador: Administrador de la Administración de Servicios Generales.
3. Agencia Certificadora (“Certification Agency” o “CA”): Organización que emite firmas digitales mediante certificados digitales y garantiza la autenticidad y seguridad de las transacciones electrónicas.
4. Autenticación: Proceso de verificación de la identidad de una persona.
5. Autenticación multifactorial: Proceso de autenticación de usuarios que requiere más de un mecanismo dentro del triángulo de autenticación (*¿Qué sé?, ¿Qué tengo?, ¿Quién soy?*).
6. Autoridad para firmar: Permiso otorgado o delegado por el Administrador para firmar contratos, recibos u otros documentos en representación de la ASG o cualquiera de sus dependencias.
7. Bridge Letter: Documento emitido por un auditor que confirma que una organización sigue cumpliendo con los estándares de auditoría mientras se espera la finalización de un informe formal.
8. CISA (Certified Information Systems Auditor): Certificación global otorgada por la Information Systems Audit and Control Association (ISACA), que valida la competencia de un profesional en auditoría, control y seguridad de sistemas de información.
9. Certificación de Fondos: Documento emitido por el área de presupuesto que valida la disponibilidad de recursos económicos para sufragar los costos del contrato.
10. Certificado digital: Archivo que certifica la identidad del usuario y contiene su llave pública. Se utiliza en diversas transacciones, como apoyar comunicaciones codificadas y firmar mensajes de correo electrónico. Su propósito es validar que el usuario tiene derecho a utilizar la llave pública y privada otorgada por una Agencia Certificadora.

- 
11. Código de verificación: Resultado de una técnica asimétrica que confirma la integridad de la información codificada mediante un código único de tamaño fijo (*cantidad de bits*).
 12. CPA (Certified Public Accountant): Título profesional otorgado a contadores públicos certificados que cumplen con los requisitos de educación, experiencia y examen en contabilidad y auditoría financiera.
 13. Documento: Información inscrita en un medio tangible o almacenada en un medio electrónico, susceptible de ser recuperada de manera perceptible.
 14. Documento electrónico: Archivo creado, generado, enviado, comunicado, recibido o almacenado por medios electrónicos.
 15. Electrónico: Tecnología que utiliza capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas o similares.
 16. Empleado: Persona que presta servicios a la Administración mediante nombramiento con estatus probatorio, regular en el servicio de carrera, de confianza, transitorio o irregular.
 17. Firma digital: Tipo de firma electrónica representada como un conjunto de datos, sonidos, símbolos o procesos en forma electrónica, creada por una llave privada que utiliza una técnica asimétrica para garantizar la integridad del mensaje de datos y vincular al titular de la firma con el mensaje remitido.
 18. Firma Digital Federal o “Federal Bridge PKI” (FBPKI): Programa del Gobierno Federal de los EE. UU. que establece una infraestructura de clave pública (PKI) para permitir la interoperabilidad entre diferentes entidades gubernamentales y certificadores digitales.
 19. Firma electrónica: Conjunto de datos en forma electrónica consignados en un mensaje, documento o transacción, o asociados lógicamente a ellos, que identifican al firmante e indican su aprobación.

Puede presentarse en diferentes formas:

- a. Una firma manuscrita digitalizada.
- b. Un gesto de aceptación dentro de una plataforma electrónica.

Si se complementa con una firma digital, puede garantizar la identidad del firmante dependiendo del uso de llaves y la entidad certificadora que la emite.

20. ISO 27001 (International Organization for Standardization 27001): Norma internacional para la gestión de la seguridad de la información, que establece las mejores prácticas para proteger datos sensibles y garantizar la integridad y confidencialidad de la información.
21. PIV-I (Personal Identity Verification – Interoperable): Estándar de credenciales digitales adoptado por el Gobierno Federal de los EE. UU. para garantizar autenticación segura en sistemas electrónicos.
22. PIV-C (Personal Identity Verification – Compatible): Variante del PIV-I que ofrece compatibilidad con el estándar federal sin ser necesariamente emitido por una entidad gubernamental. Se usa para asegurar autenticación digital segura en sistemas gubernamentales.
23. PRITS (Puerto Rico Innovation and Technology Service): Agencia del Gobierno de Puerto Rico responsable de establecer estándares y regulaciones para la implementación de tecnologías de información y seguridad digital en las agencias gubernamentales.
24. SSAE18 (Statement on Standards for Attestation Engagements No. 18): Estándar de auditoría emitido por el American Institute of Certified Public Accountants (AICPA) que establece requisitos de control sobre informes de certificación y cumplimiento en la gestión de datos y sistemas de información de terceros.
25. SOC2 (Service Organization Control 2): Informe de cumplimiento basado en el SSAE18, enfocado en la seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad de los sistemas de información de una organización.
26. SOC3 (Service Organization Control 3): Variante del informe SOC2, diseñado para su divulgación pública. Certifica que una empresa cumple con los controles de seguridad requeridos, sin revelar detalles internos del informe.
27. Técnica asimétrica: Algoritmo matemático basado en la estructura de llave pública/privada, utilizado para firmar digitalmente o codificar mensajes.
28. Transacción electrónica: Interacción entre personas, sistemas o entidades gubernamentales realizada a través de medios electrónicos, incluyendo la generación, transmisión y almacenamiento de documentos electrónicos.

29. WebTrust for Certification Authorities: Programa de auditorías para Agencias Certificadoras que emiten firmas y certificados digitales.

Capítulo II: Regulación y Uso de Firmas Electrónicas y Digitales

Artículo 2.1: Guías de uso

De conformidad con las guías del PRITS, la Administración de Servicios Generales cumplirá con los siguientes requisitos mínimos para el uso de firmas electrónicas y digitales. En todo momento, se sujetan estos requisitos mínimos a los contemplados en la Ley Núm. 40-2024 o cualquier otro estatuto que en el futuro la sustituya.

1. Firmas Electrónicas

- 
- a. Contar con una Bridge Letter del Informe de SSAE18 SOC2/SOC3; o
 - b. Poseer informes de SSAE18 SOC2/SOC3, ISO27001 o equivalentes.
 - c. La Administración podrá contratar con una empresa proveedora de servicios de firma electrónica que cumpla disponga de una carta de controles que certifique los controles de información implementados.

2. Firmas Digitales

- a. Las firmas digitales deberán ser emitidas por una Agencia Certificadora que:
 - i. Posea el Informe de Auditoría WebTrust for Certification Authorities; o
 - ii. Sea un proveedor autorizado bajo el Gobierno Federal.
- b. Para transacciones con el Gobierno Federal, deberá utilizarse la firma digital federal.
- c. Las firmas digitales certificadas bajo el programa FBPKI/PIV-I se consideran de máxima seguridad.

Artículo 2.2: Disposiciones Generales

1. Las disposiciones establecidas en este Reglamento serán de aplicación a todas las transacciones y procedimientos administrativos, tanto internos como externos, entre la ASG y cualquier:
 - a. Agencia o dependencia gubernamental,
 - b. Entidad privada, o

- c. Persona natural.
- 2. La Administración será responsable de:
 - a. Seleccionar, autorizar y validar los métodos específicos de firma digital y/o electrónica.
 - b. Determinar y gestionar los mecanismos de autenticación de usuarios.
 - c. Garantizar el cumplimiento con el nivel de certeza requerido para la autenticación de identidad en los diferentes tipos de procesos administrativos.
- 3. Uso Preferente de Firmas Electrónicas y Digitales
 - a. Tan pronto estén habilitadas las herramientas correspondientes, las firmas electrónicas o digitales serán el método preferencial de firma en toda transacción o documento suscrito entre la ASG, entidades o agencias gubernamentales, entidades privadas o personas naturales.
 - b. Todo pliego o solicitud de cotización deberá contener una advertencia a los efectos de informar a las personas interesadas de la preferencia por el uso de firmas digitales o electrónicas, la posibilidad de su uso y su derecho a solicitar el uso de firmas físicas.

Artículo 2.3: Implementación de Firmas Digitales y Electrónicas

1. Cuando una firma digital o electrónica sea requerida por la ASG, esta será aceptada como equivalente a la firma ológrafa o manuscrita y tendrá carácter legalmente vinculante.
2. Al igual que con una firma manuscrita, la parte firmante debe demostrar una intención clara de firmar el documento de manera electrónica.
3. La Administración validará el consentimiento del firmante incluyendo en los documentos que serán firmados electrónicamente una cláusula con el siguiente texto:

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

Capítulo III: Procedimientos de Firma y Seguridad

Artículo 3.1: Procedimiento para el Uso de Firmas Digitales

La ASG adoptará procedimientos para garantizar que las firmas digitales sean utilizadas de manera segura, eficiente y conforme a la normativa vigente.

Artículo 3.2: Cláusula de Exclusión Voluntaria

1. Si un firmante decide no utilizar una firma electrónica, la Administración deberá proporcionar instrucciones claras y accesibles sobre cómo firmar manualmente el documento.
2. La utilización de una firma electrónica en una transacción no obligará al firmante a emplear este método en transacciones futuras.

Artículo 3.3: Copias Firmadas y Retención de Documentos

La Administración garantizará que todos los firmantes reciban una copia digital del documento firmado al completarse la transacción.

Capítulo IV: Cumplimiento, Supervisión y Sanciones

Artículo 4.1: Oficina de Informática

1. La Oficina de Informática de la ASG fomentará la correcta implementación y cumplimiento del presente Reglamento en lo referente al uso de firmas digitales y electrónicas en la ASG.
2. Entre sus deberes están los siguientes:
 - a) Mantenimiento del sistema: Implementar y administrar los sistemas tecnológicos que permitan la creación, validación y almacenamiento seguro de firmas digitales y electrónicas.
 - b) Seguridad de la información: Aplicar medidas de seguridad para proteger las firmas digitales almacenadas en los sistemas de la ASG.
 - c) Cumplimiento normativo: En colaboración con la Oficina de Asuntos Legales procurar que los estándares de autenticación y validación de identidad cumplan

con las normativas aplicables, incluyendo la Ley de Gobierno Electrónico, la Ley de Transacciones Electrónicas y las guías de PRITS.

- d) Asesoría técnica y capacitación: Brindar orientación y apoyo técnico a todas las unidades administrativas de la ASG en relación con el uso correcto de firmas digitales y electrónicas.
3. La ASG colaborará con PRITS en toda gestión incidental a la seguridad de la solución adoptada.

Artículo 4.2: Violaciones y Sanciones

1. Violaciones

- a. Se considerará una violación al presente Reglamento cualquier acción u omisión que incumpla con las normas establecidas para el uso, manejo y gestión de firmas digitales y electrónicas en la ASG.
- b. Entre las conductas que se consideran violaciones se incluyen, pero no se limitan a:
 - i. Uso indebido o fraudulento de firmas digitales o electrónicas.
 - ii. Emisión, creación o manipulación de firmas digitales sin cumplir con los requisitos legales y técnicos establecidos.
 - iii. Incumplimiento de los protocolos de seguridad en el almacenamiento y gestión de firmas digitales.
 - iv. Alteración, modificación o manipulación de documentos firmados digital o electrónicamente.
 - v. Falta de actualización o mantenimiento de los sistemas relacionados con firmas digitales y electrónicas.
 - vi. Acceso no autorizado a sistemas de firma digital o intento de suplantación de identidad en procesos de autenticación.

2. Sanciones

- a. Las violaciones a este Reglamento estarán sujetas a sanciones, conforme a las normativas que vinculen a las respectivas personas.

- b. Sanciones para empleados de la ASG
 - i. Amonestación escrita: Para infracciones menores o no intencionales que no representen un riesgo grave a la seguridad de los sistemas o la integridad de los documentos.
 - ii. Suspensión laboral: Por un período determinado, en casos de incumplimiento de medidas de seguridad, uso negligente de firmas digitales o reiteradas violaciones a las normas establecidas.
 - iii. Destitución: Para infracciones graves, tales como el uso fraudulento de firmas digitales o la manipulación dolosa de documentos electrónicos.
- c. Sanciones para contratistas, proveedores o terceros
 - i. Rescisión del contrato: En caso de que un proveedor incumpla con las disposiciones del Reglamento, la ASG podrá terminar el contrato de manera inmediata.
 - ii. Inhabilitación: Se podrá prohibir temporal o permanentemente la participación del contratista en futuros contratos con la ASG mediante su exclusión de los Registros Únicos de Licitadores y/o de Proveedores de Servicios Profesionales.
 - iii. Reclamaciones legales: Si la violación causa perjuicio económico a la ASG, se podrán iniciar acciones legales para reclamar daños y perjuicios.
- d. Sanciones adicionales
 - i. Sanciones civiles: Los daños y perjuicios que resulten de un incumplimiento con las disposiciones de este Reglamento podrán dar lugar una acción civil ante el Tribunal de Primera Instancia.
 - ii. Sanciones penales: Si la conducta constituye un delito, los responsables estarán sujetos a las sanciones previstas en las leyes penales aplicables, incluyendo el Código Anticorrupción de Puerto Rico y la Ley de Ética Gubernamental. Para ello la ASG emitirá el referido correspondiente a las autoridades del orden público.
 - iii. Sanciones administrativas: La ASG se reserva la facultad de imponer, conforme a los reglamentos correspondientes, aquellas multas y sanciones para las cuales tiene autoridad conforme a la Ley Núm. 73-2019.

Capítulo V: Disposiciones Finales

Artículo 5.1: Interpretación del Reglamento ante Enmiendas a la Ley

1. En caso de duda sobre la interpretación de este Reglamento, se aplicarán las disposiciones legales y reglamentarias vigentes que rijan el uso de firmas electrónicas y digitales en la ASG.
2. La ASG tendrá un deber continuo de revisar las normativas vinculantes con el fin de que este Reglamento conserve su máxima utilidad.
3. Toda revisión futura deberá contemplar aquellos nuevos desarrollos, tanto en oportunidades como en riesgos, que surjan con la evolución tecnológica.

Artículo 5.2: Cláusula de Separabilidad

1. Si cualquier artículo, inciso, párrafo, oración, palabra o disposición de este Reglamento fuese declarado inconstitucional, nulo o inválido por un tribunal con jurisdicción, dicha resolución no afectará, perjudicará ni invalidará las restantes disposiciones.
2. El efecto de la declaración judicial se limitará exclusivamente a la parte específica que haya sido declarada inconstitucional o nula en la controversia judicial.

Artículo 5.3: Vigencia

1. Este Reglamento entrará en vigor treinta (30) días después de su presentación ante el Departamento de Estado de Puerto Rico, conforme a lo dispuesto en la Ley Núm. 38-2017, conocida como la “Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico”, según enmendada.

En San Juan, Puerto Rico, a 1 de agosto de 2025.



Lcda. Karla G. Mercado Rivera
Administradora y Principal Oficial de Compras