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

Índice

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, Firmas y Transacciones 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, según enmendada, conocida como la “Ley de Gobierno Electrónico”, que establece como política pública la incorporación de tecnologías de información en la administración gubernamental.
    b) Ley Núm. 148-2006, según enmendada, conocida como la “Ley de Transacciones Electrónicas”, la cual delega en la 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, conocida como la "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, conocido como la "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.

e) Ley Núm. 40-2024, conocida como la 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.

2. Mediante la aprobación de este Reglamento, se pretende:

   a) Minimizar el riesgo de falsificación y fraude en firmas electrónicas.

   b) Garantizar la validez jurídica y seguridad de las transacciones electrónicas realizadas por la ASG.

   c) Proveer directrices claras sobre el uso adecuado de firmas digitales y electrónicas conforme a las leyes y regulaciones aplicables.

   d) Agilizar procesos administrativos mediante la digitalización de documentos y procedimientos internos.

   e) Adoptar como fines esenciales la confidencialidad, integridad y disponibilidad de la información.

   f) Reconocer la importancia de establecer el acceso a la red la ASG sobre una base de arquitectura de confianza cero.

3. Con la entrada en vigor de este Reglamento, la ASG acepta y 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. Este Reglamento será vinculante para todos los funcionarios y empleados de la ASG, quienes deberán cumplir rigurosamente con sus disposiciones.
3. En todo momento se deberán observar los Estándares y Principios Mínimos de Seguridad establecidos por la PRITS.

Artículo 1.5: Definiciones

a. Administración: Administración de Servicios Generales.
b. Administrador: Administrador de la Administración de Servicios Generales.
c. Agencia Certificadora (“Certification Agency” o “CA”): Organización que emite firmas digitales mediante certificados digitales y garantiza la autenticidad y seguridad de las transacciones electrónicas.
d. Arquitectura de confianza cero: Significa que se asume que ninguna conexión, usuario o activo es confiable hasta que esté verificado.
e. Autenticación: Proceso de verificación de la identidad de una persona.

f. Autenticación multifactorial: Proceso de autenticación de usuarios que requiere más de un mecanismo dentro del triángulo de autenticación (*¿Qué sé?, ¿Qué tengo?, ¿Quién soy?*). Se basa en al menos dos de los siguientes factores:

    i. Algo que el usuario sabe (contraseña o PIN).

    ii. Algo que el usuario tiene (tarjeta de acceso o dispositivo móvil).

    iii. Algo que el usuario es (biometría como huella dactilar o reconocimiento facial).

g. 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.

h. 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.

i. 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.

j. Certificación de Fondos: Documento emitido por el área de presupuesto que valida la disponibilidad de recursos económicos para sufragar los costos del contrato.

k. 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.

l. 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*).

m. Confidencialidad: Significará la prevención de daños a, protección y restauración de computadoras, sistemas y/o servicios de comunicación electrónica, incluyendo la

información contenida en ellos para garantizar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio.

n. 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.

o. Documento: Información inscrita en un medio tangible o almacenada en un medio electrónico, susceptible de ser recuperada de manera perceptible.

p. Documento electrónico: Archivo creado, generado, enviado, comunicado, recibido o almacenado por medios electrónicos.

q. Electrónico: Tecnología que utiliza capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas o similares.

r. Empleado: Persona que presta servicios a la Administración mediante nombramiento con estatus probatorio, regular en el servicio de carrera, de confianza, transitorio o irregular.

s. 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.

   Una firma digital permite verificar si:

   i. La conversión se realizó utilizando la llave privada correspondiente a la llave pública del firmante.

   ii. El mensaje o comunicación ha sido alterado desde la conversión.

t. 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.

u. 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:

    i. Una firma manuscrita digitalizada.
    ii. 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.

v. Firmante: Individuo que firma un documento manual, digital o electrónicamente en representación propia o de una entidad que le haya conferido autoridad.

w. Funcionario: Persona investida de autoridad estatal o que ocupa un cargo en la Administración, interviniendo en la formulación o implementación de políticas institucionales.

x. Gestión de incidentes: Significa todos los procedimientos administrativos, físicos y técnicos aplicados para la investigación y mitigación ante la sospecha o el reporte de un Incidente. Incluyendo las notificaciones de violación o brechas a las partes o individuos impactados por el Incidente, según aplicables por las regulaciones federales y locales.

y. Incidente de seguridad de la información: – Significa un suceso que (i) pone en riesgo real o inminente, sin autoridad, la integridad, confidencialidad o disponibilidad de la información, sistema o proceso o un Recurso de información; o (ii) representa un uso indebido de un Recurso de información o una violación o amenaza inminente de violación de la ley, políticas de seguridad, procedimientos de seguridad, políticas de uso aceptable o prácticas estándar de seguridad informática.

z. 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.

aa. Key Usage de No Repudio: Parámetro en los certificados digitales que impide que un firmante niegue la autoría de una firma electrónica, garantizando la autenticidad y validez legal de la transacción firmada digitalmente.

bb. Pago por rescate: Significa la transferencia de dinero u otra propiedad o activo, incluyendo monedas virtuales, o cualquier fracción de estas, que se haya realizado en conexión a un ataque de Ransomware, excluyendo el pago legítimo de servicios por respuesta a un incidente.

cc. 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.

dd. 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.

ee. 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.

ff. Riesgo: significa toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y Recursos de información.

gg. 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.

hh. 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.

ii. 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.

jj. Técnica asimétrica: Algoritmo matemático basado en la estructura de llave pública/privada, utilizado para firmar digitalmente o codificar mensajes.

kk. Transacción electrónica: Interacción entre personas, sistemas o entidades gubernamentales realizada a través de medios electrónicos, incluyendo la generación, transmisión y almacenamiento de documentos electrónicos.

ll. 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: Requisitos Mínimos 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.

A. Firmas Electrónicas

1. Requisitos de Certificación
    a) Contar con una Bridge Letter del Informe de SSAE18 SOC2/SOC3; o
    b) Poseer informes de SSAE18 SOC2/SOC3, ISO27001 o equivalentes.
2. Contratación de Servicios
    a) La Administración podrá contratar, por un (1) año, una empresa proveedora de servicios de firma electrónica que cumpla con lo siguiente:
        i. Disponer de una carta de controles emitida por un Certified Information Systems Auditor (CISA) o un Certified Public Accountant (CPA) que certifique los controles de información implementados.

ii. Para renovar el contrato después del primer año, la empresa deberá cumplir con cualquiera de los requisitos establecidos en los puntos anteriores.

3. Desarrollo Interno
    a. Si la Administración decide desarrollar su propia firma electrónica, esta deberá cumplir con los controles de información establecidos en el SSAE18, SOC2 y/o SOC3 y con las guías de PRITS.

4. Requisitos adicionales
    a. Será imprescindible que cualquier herramienta a utilizarse permita el cifrado de datos en transito y en reposo, la autenticación multifactorial y los controles en capas.

B. Firmas Digitales

1. Requisitos de Emisión

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 y el programa FBPKI/PIVI.

2. Uso Interno

a) Si la Administración implementa firmas digitales para uso interno, estas deberán cumplir con los controles estipulados en SSAE18, SOC3 o PIV-C.

3. Transacciones Federales

a) Para transacciones con el Gobierno Federal, deberá utilizarse la firma digital federal.

4. Seguridad Máxima

a) Las firmas digitales certificadas bajo el programa FBPKI/PIV-I se consideran de máxima seguridad, ya que cuentan con:

i. Autenticación multifactorial.

ii. Key Usage de No Repudio.

Artículo 2.2: Disposiciones Generales

1. Aplicabilidad

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. Responsabilidad en la Implementación

El Director de la División de Sistemas de Información de la ASG, en conjunto con el Administrador, 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) Salvo acuerdo en contrario, 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.

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, siempre que se cumplan los siguientes requisitos:

2. Intención de firmar

Al igual que con una firma manuscrita, la parte firmante debe demostrar una intención clara de firmar el documento de manera electrónica. Esta intención puede manifestarse a través de:

a) El uso de un cursor o "pad" para dibujar la firma.

b) Escribir el nombre con el teclado.

c) Pulsar un botón de “aceptar” o seleccionar la opción debidamente identificada.

3. Consentimiento para realizar transacciones electrónicas

   a) 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."

4. Identificación y autenticación del usuario

   a) La Administración deberá garantizar que la solución tecnológica seleccionada permita:

      i. Identificar al firmante.

      ii. Validar el consentimiento del firmante.

      iii. Corroborar la relación entre el documento y la firma electrónica.

   b) Es imprescindible que la solución asegure que el documento y la firma electrónica estén correlacionados y/o unidos de manera indisoluble, preservando su integridad y autenticidad.

   c) Adicionalmente se deberán establecer requisitos de verificación criptográfica de integridad y trazabilidad de los documentos.

5. La ASG deberá realizar auditorías técnicas de las plataformas a ser utilizadas al menos una vez cada seis (6) meses.

Artículo 2.4: Uso Preferente de Firmas Electrónicas y Digitales

1. Las firmas electrónicas o digitales serán el mecanismo de firma preferente en todas las transacciones administrativas de la ASG.
2. Salvo acuerdo en contrario, toda documentación suscrita entre la ASG, agencias gubernamentales, entidades privadas o personas naturales deberá utilizar este método de firma.
3. La utilización de firmas digitales garantizará:
    a) Validez jurídica conforme a la legislación aplicable.
    b) Mayor eficiencia en los procesos administrativos.
    c) Reducción de costos asociados con la impresión y almacenamiento de documentos físicos.
    d) Mayor seguridad mediante el uso de mecanismos de autenticación multifactorial.
4. En los casos en los que no sea viable el uso de una firma digital o electrónica, se deberá justificar su exclusión en el expediente administrativo correspondiente.
5. En todo momento la solución adoptada deberá cumplir con los principios de seguridad por diseño, además de la arquitectura de confianza cero.

Capítulo III: Procedimientos de Firma y Seguridad

Artículo 3.1: Procedimiento para el Uso de Firmas Digitales

1. La ASG adoptará procedimientos para garantizar que las firmas digitales sean utilizadas de manera segura, eficiente y conforme a la normativa vigente.
2. Toda firma digital deberá cumplir con los estándares de seguridad y autenticación establecidos por el PRITS.
3. Se garantizará que cada usuario autorizado para utilizar una firma digital cuente con los accesos, permisos y certificaciones requeridos.
4. Se implementarán protocolos para el almacenamiento seguro de documentos firmados digitalmente, asegurando su integridad y trazabilidad.

5. Se verificará la autenticidad y validez de las firmas digitales antes de que sean aceptadas en cualquier transacción gubernamental.

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.
3. En caso de optar por la firma manual, se deberá garantizar que el documento sea procesado dentro de los mismos términos y condiciones aplicables a las firmas electrónicas.

Artículo 3.3: Copias Firmadas y Retención de Documentos

1. La Administración garantizará que todos los firmantes reciban una copia del documento firmado al completarse la transacción.
2. La copia del documento firmado podrá ser descargada en formato PDF o en cualquier otro formato electrónico que garantice la integridad del documento.
3. La retención de documentos electrónicos se llevará a cabo conforme a lo dispuesto en el Artículo 11 de la Ley Núm. 148-2006, conocida como la “Ley de Transacciones Electrónicas”.
4. Se implementarán medidas para la conservación, acceso y recuperación de documentos electrónicos en cumplimiento con las disposiciones legales aplicables.
5. Será necesario establecer un cifrado obligatorio para los documentos que sean firmados electrónicamente.
6. Deberán incluirse controles de acceso que eviten la manipulación o divulgación no autorizada.

Capítulo IV: Cumplimiento, Supervisión y Sanciones

Artículo 4.1: Responsabilidad de la División de Sistemas de Información

1. La División de Sistemas de Información será la unidad responsable de garantizar la correcta implementación y cumplimiento del presente Reglamento en lo referente al uso de firmas digitales y electrónicas en la ASG.
2. Las responsabilidades de la División incluyen, pero no se limitan a:
    a) Gestión de contratación: Gestionar la contratación de los servicios de una Agencia Certificadora para la emisión de firmas digitales y garantizar que estas cumplan con los requisitos normativos.
    b) Mantenimiento del sistema: Implementar y administrar los sistemas tecnológicos que permitan la creación, validación y almacenamiento seguro de firmas digitales y electrónicas.
    c) Seguridad de la información: Aplicar medidas de seguridad para proteger las firmas digitales almacenadas en los sistemas de la ASG, evitando accesos no autorizados o alteraciones indebidas.
    d) Cumplimiento normativo: Asegurar 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.
    e) 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.
    f) Monitoreo y auditoría interna: Supervisar el cumplimiento del Reglamento mediante auditorías y revisiones periódicas de los procesos de firma digital y electrónica.
3. La ASG tendrá la obligación de colaborar con la PRITS en toda gestión incidental a la seguridad de la solución adoptada.

4. A su vez, deberá adoptar la práctica de enviar informes periódicos de incidentes a la PRITS.

Artículo 4.2: Violaciones y Sanciones

A. Violaciones

1. 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.
2. Entre las conductas que se consideran violaciones se incluyen, pero no se limitan a:
    a) Uso indebido o fraudulento de firmas digitales o electrónicas.
    b) Emisión, creación o manipulación de firmas digitales sin cumplir con los requisitos legales y técnicos establecidos.
    c) Incumplimiento de los protocolos de seguridad en el almacenamiento y gestión de firmas digitales.
    d) Uso no autorizado de claves privadas, certificados digitales o credenciales emitidas para la Administración o sus dependencias.
    e) Alteración, modificación o manipulación de documentos firmados digital o electrónicamente.
    f) Implementación de soluciones tecnológicas sin cumplir con los estándares establecidos en este Reglamento y en las guías de PRITS.
    g) Falta de actualización o mantenimiento de los sistemas relacionados con firmas digitales y electrónicas.
    h) Acceso no autorizado a sistemas de firma digital o intento de suplantación de identidad en procesos de autenticación.

B. Sanciones

Las violaciones a este Reglamento estarán sujetas a sanciones, las cuales dependerán de la naturaleza y gravedad de la infracción.

1. Sanciones para empleados de la ASG

    a) 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.

    b) 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.

    c) Destitución: Para infracciones graves, tales como el uso fraudulento de firmas digitales o la manipulación dolosa de documentos electrónicos.

2. Sanciones para contratistas, proveedores o terceros

    a) Rescisión del contrato: En caso de que un proveedor incumpla con las disposiciones del Reglamento, la ASG podrá terminar el contrato de manera inmediata.

    b) 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.

    c) Reclamaciones legales: Si la violación causa perjuicio económico a la ASG, se podrán iniciar acciones legales para reclamar daños y perjuicios.

3. Sanciones adicionales

    a) 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.

    b) 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.

Capítulo V: Disposiciones Finales

Artículo 5.1: Interpretación del Reglamento ante Enmiendas a la Ley

1. Si, con posterioridad a la aprobación y entrada en vigor de este Reglamento, cualquiera de las leyes citadas como base legal es enmendada, sus disposiciones deberán ser interpretadas conforme al nuevo marco normativo vigente.
2. Se considerará automáticamente derogada cualquier disposición de este Reglamento que sea incompatible con la legislación actualizada, sin que ello afecte la validez del resto de sus disposiciones.
3. 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.
4. La ASG tendrá un deber continuo de revisar las normativas vinculantes con el fin de que este Reglamento conserve su máxima utilidad.
5. 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.
3. En caso de que una parte de este Reglamento sea declarada inconstitucional y se afecte su aplicabilidad, se podrán realizar enmiendas mediante los procesos administrativos correspondientes para garantizar el cumplimiento con la legislación vigente.

Artículo 5.3: Revisión Periódica

1. Este Reglamento será revisado cada tres (3) años, o antes si las circunstancias lo requieren, para garantizar su conformidad con cambios legales, tecnológicos y administrativos.
2. La revisión estará a cargo del Administrador de la Administración de Servicios Generales o de su Representante Autorizado.
3. Como parte del proceso de revisión, se podrá solicitar la opinión de expertos en tecnología, seguridad informática y asuntos legales para garantizar la actualización y efectividad del Reglamento.

Artículo 5.4: 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.
2. Se mantendrá su vigencia hasta que sea enmendado, derogado o sustituido por un nuevo reglamento debidamente aprobado.

En San Juan, Puerto Rico, a __ de _____ de 2025.

_____

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