DEPARTAMENTO DE

SALUD

GOBIERNO DE PUERTO RICO

# GUÍAS PARA LA IMPLEMENTACIÓN DE FIRMAS ELECTRÓNICAS EN EL DEPARTAMENTO DE SALUD

**2026**

## Tabla de Contenido


I. Título ..... 1
II. Base Legal ..... 1
III. Propósito ..... 1
IV. Aplicabilidad ..... 1
V. Interpretación ..... 2
VI. Definiciones ..... 2
VII. Requisitos Mínimos de Uso exigidos en la Agencia ..... 7
VIII. Implementación de la Forma Digital o Electrónica ..... 8
IX. Aplicación de la Política de Firmas Digitales y Electrónicas ..... 9
X. Cláusula de Exclusión Voluntaria ..... 10
XI. Copias Firmadas ..... 10
XII. Retención de Documentos ..... 10
XIII. Actualización de Políticas y Procedimientos ..... 10
XIV. No Aplicabilidad de esta Política ..... 10
XV. Responsabilidad de la Oficina de Informática y Avances Tecnológicos (OIAT) ..... 11
XVI. Violaciones y Sanciones ..... 11
XVII. Cláusula de Separabilidad ..... 12
XVIII. Derogación ..... 12
XIX. Vigencia ..... 12

## I. Título

Este documento se conocerá como la "Guías para la Implementación de Firmas Electrónicas en el Departamento de Salud".

## II. Base Legal

Estas "Guías" se establecen en virtud de la facultad conferida al Secretario de Salud por la:

- Ley Núm. 81 de 14 de marzo de 1912, según enmendada, conocida como la "Ley Orgánica de Departamento de Salud" (**Ley Núm. 81**);

- Ley Núm. 148-2006, según enmendada,conocida como la "Ley de Transacciones Electrónicas" (LTE) (**Ley Núm. 148**);

- Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico" (LGE)(**Ley Núm. 151**);

- Ley Núm. 75-2019, conocida como la "Ley de la Puerto Rico Innovation and Technology Service" (PRITS) (**Ley Núm. 75**), y

- el inciso núm. 8 de las "Guías para la Implementación de Firmas Electrónicas en las Agencias" PRITS-002 (12-09-2020) emitidas por PRITS, el cual dispone que cada Agencia tiene la responsabilidad de desarrollar las políticas, guías, regalamentación o procesos internos para viabilizar el uso de las firmas electrónicas y/o digitales, a tenor con la Carta Circular, sus guías y la Ley Núm. 148, *supra*.

## III. Propósito

Estas Guías tienen el propósito de establecer las normas que regirán los procedimientos relacionados con la implementación, monitoreo y uso de las firmas digitales y electrónicas en el curso de las operaciones y/o transacciones del Departamento de Salud del Gobierno de Puerto Rico.

Su implantación definirá los estándares técnicos y operacionales internos y externos necesarios, para minimizar la posibilidad de fraude o falsificación de firmas o fraude en las transacciones electrónicas efectuadas en la Agencia.

## IV. Aplicabilidad

Las Guías seran de aplicación a todas las dependencias, secretarías, oficinas, funcionarios y empleados del Departamento de Salud del Gobierno de Puerto Rico.

En la aplicación o implementación de estas Guías se prohíbe el discrimen por razón de raza, color, nacionalidad, origen, condición social, edad, ideas políticas, creencias o no religiosas, género, identidad de género, orientación sexual, 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 Estado Unidos de América o tener discapacidad física o mental.

## V. Interpretación

Las palabras o frases usadas en estas Guías se interpretarán según el contexto y significado aceptado por el uso común y corriente.

Los términos o palabras usadas en el tiempo presente, incluyen también el futuro; las usadas en singular, incluyen también el plural; las usadas en el género masculino, incluyen el femenino y el neutro; salvo los casos en que tal interpretación resulte ilógica, absurda o incompatible.

Si el lenguaje empleado es susceptible de dos (2) o más interpretaciones, se interpretará para adelantar los propositos de la Guía y del inciso, artículo o acápite particular objeto de interpretación.

Además, si con posterioridad a la aprobación de estas Guías cualquier ley citada como base legal fuese enmendada, las disposiciones del mismo serán interpretadas conforme al estado de derecho vigente. En tal caso, se considerará derogada u obsoleta cualquer disposición que resulte contraria a la ley vigente.

## VI. Definiciones

1. **Agencia** - Se refiere a cualquier Junta, Cuerpo, Tribunal Examinador, Corporación Pública, Comisión, Oficina Independiente, División, Administración, Negociado, Departamento, Autoridad, Funcionario, Persona, Entidad o cualquier Instrumentalidad del Gobierno de Puerto Rico, incluyendo los Municipios.

2. **Autenticación** - Establecimiento de un medio de verificacion de la identidad de la persona.

3. **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?) .

4. **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 Salud o cualquiera de sus dependencias en virtud de la Ley Núm. 81 y leyes aplicables.

5. **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.

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

7. **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.

8. **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.

9. **Código de Verificación** - es un resultado de la técnica asimétrica que confirma que la información codificada matuvo su integridad. Es asegurado por un código único codificado de un tamaño fijo (cantidad de bits).
10. **Departamento de Salud** - Se refiere al Departamento de Salud del Gobierno de Puerto Rico.

11. **Documento** - Aquella información inscrita en un medio tangible o almacenada en un medio electrónico, susceptible de ser recuperada de manera perceptible.

12. **Documento Público** - Se refiere a todo documento que se origine, conserve o reciba en el Departamento de Salud o en cualquier dependencia del Gobierno de Puerto Rico, de acuerdo con la ley o en relación con el manejo de los asuntos públicos y se requiera conservar permanente o temporalmente como prueba de las transacciones o por su utilidad administrativa, valor legal, fiscal, cultural o histórico, según sea el caso y un ejemplar de todas las publicaciones de los organismos gubernamentales.

    Incluye aquellos producidos de forma electrónica que cumplan con los requisitos establecidos por las leyes y reglamentos. Se refiere a todo documento que se origine, conserve o reciba en el Departamento de Salud o en cualquier dependencia del Gobierno de Puerto Rico de acuerdo con la ley o en relación con el manejo de los asuntos públicos y se requiera conservar permanente o temporalmente como prueba de las transacciones o por su utilidad administrativa, valor legal, fiscal, cultural o histórico, según sea el caso y un ejemplar de todas las publicaciones de los organismos gubernamentales. Incluye aquellos producidos de forma electrónica que cumplan con los requisitos establecidos por las leyes y reglamentos.

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

14. **Empleado** - Persona que rinde servicios en el Departamento de Salud mediante nombramiento con estatus regular con el servicio de carrera, transitorio, confianza o irregular.

15. **Firma Digital** - Según la Ley Núm. 148-2006, según enmendada, 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).

16. **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 técnica asimétrica para asegurar la integridad del mensaje de datos a través de un código de verifiación, así como el vínculo entre el titular de la firma digital y el mensaje de datos remitido. En la conversación 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:

    a. La conversación se realizó utilizando la llave privada que corresponde a la llave pública del signatario;

    b. El mensaje o comunicación ha sido alterado desde que realizó la conversación.

17. **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.

18. **Firma Electrónica** - Según la Ley Núm. 148-2006, según enmendada, 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).

19. **Firmante** - Individuo que firme un documento manual. Digital o electrónicamente en representación propia de alguna entidad que le haya conferido la autoridad para ello.

20. **Funcionario** - Persona que está investida de parte de la soberanía del Estado o que ocupa un cargo o puesto en el Departamento de Salud e interviene en la formulación de la política pública.

21. **Función Pública** - actividad inherente realizada en el ejercicio o en el desempeño de cualquier cargo, empleo, puesto o posición en el servicio público, ya sea en forma retribuida o gratuita, permanente o temporera, en virtud de cualquier tipo de nombramiento, contrato o designación para la Rama Legislativa, Ejecutiva o Judicial del Gobierno de Puerto Rico, así como cualquiera de sus agencias, departamentos, subdivisiones, instrumentalidades, corporaciones públicas o municipios.

22. **Gobierno** - Se refiere al gobierno de Puerto Rico, incluyendo todos y cada uno de los organismos que componen las tres ramas del Gobierno, sus subdivisiones políticas y la Oficina del Contralor.

23. **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.

24. **OIAT** - significa la Oficina de Informática y Avances Tecnológicos del Departamento de Salud.

25. **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.

26. **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.

27. **PRITS** - Se refiere al Puerto Rico Innovation and Technology Service establecido en la Ley Núm. 75-2019.

28. **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.

29. **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.

30. **Secretario** - Se refiere al Secretario de Salud de Puerto Rico.

31. **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.

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

## VII. Requisitos Mínimos de Uso exigidos en la Agencia

El Departamento de Salud y sus dependencias cumplirá con los siguientes requisitos mínimos para el uso de firmas electrónicas o digitales de conformidad con las "Guías para la Implementación de Firmas Electrónicas en las Agencias" PRITS-002 (12-09-2020) emitidas por PRITS:

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.

## VIII. Implementación de la Forma Digital o Electrónica

Para que una firma electrónica o digital requerida por la Agencia, sea aceptada como equivalente de la firma ológrafa o manuscrita, 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 legítima 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 período 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 período 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.

## IX. Aplicación de la Política de Firmas Digitales y Electrónicas

La política instituida en esta Guía será de aplicación a las transacciones y procedimientos administrativos internos y externos entre el Departamento de Salud y cualquier agencia o dependencia gubernamental, entidad pública, entidad privada, persona natural o persona jurídica.

El Director de la Oficina de Informática y Avances Tecnológicos (OIAT) del Departamento será el encargado de seleccionar, autorizar y validar los métodos específicos de firma digital y/ o electrónica, así como la autenticación de identidad requerido para los diferentes tipos de procesos.

## X. Cláusula de Exclusión Voluntaria

Si un firmante decide no utilizar una firma electrónica, el Departamento proveerá instrucciones accesibles sobre como 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 formante puede optar por no firmar electrónicamente ningún otro documento.

## XI. 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.

## XII. Retención de Documentos

La retención de los documentos electrónicos se realizará conforme a los dispuesto en el Artículo 1 de la Ley Núm. 148-2006, *supra*.

## XIII. 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.

## XIV. No Aplicabilidad de esta Política

La política sobre firmas electrónicas y digitales del Departamento de Salud 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 forma 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, cualquier otra ley o reglamento aplicable que sea incompatible con la firma digital o electrónica.

## XV. Responsabilidad de la Oficina de Informática y Avances Tecnológicos (OIAT)

La Oficina de Informática y Avances Tecnológicos (OIAT) respecto a la política e implementación de uso de firmas digitales y electrónicas del Departamento de Salud sera responsable de:

a. Mantener un sistema que permita la creación de las firmas digitales o electrónicas, así como el maneo y la conservación de los documentos firmados;

b. 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;

c. Gestionar la contratación de los servicios de la Agencia Certificadora de firmas digitales comforme a las leyes aplicables;

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

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

## XVI. Violaciones y Sanciones

Constituye una violación a estas Guías, las actuaciones de todo empleado o funcionario que utilice la firma digital o electrónica de otra persona con o sin su consentimiento. Esta actuación conllevará la sanción de destitución en su primera infracción, modalidad mínima y máxima.

Cualquier empleado o funcionario con autoridad de firmar es responsable del manejo y ejecución adecuado de los documentos que firme en nombre o en representación del Departamento de Salud, ya sea que firme de forma ológrafa, digital o electrónica.

Cualquier empleado o funcionario que reconozca de propio y personal de conocimiento o sospeche de alguna acción fraudulente con relación a las firmas digitales o electrónicas, tiene el deber de reportarlo inmediatamenre a su supervisor inmediato y/o a la OIAT.

Todo empleado o funcionario que falsifiquen firmas digitales o electrónicas estarán en violación a la Guía. Esta actuación conllevará la sanción de destitución en su primera infracción, modalidad mínima y máxima. También estarán sujetos a los referidos correspondientes a las Agencias estatales y federales conforme a las leyes aplicables.

## XVII. Cláusula de Separabilidad

Si cualquier artículo, parte, párrafo, subpárrafo, oración, palabra, letra o inciso de esta Guía fuera anulada o declarada inconstitucional, inválido o nulo por un tribunal competente, tal resolución, dictamen o sentencia no afectará, perjudicará, ni invalidará las demás disposiciones y continuarán vigentes.

## XVIII. Derogación

Estas Guías dejan sin efecto cualquier otra disposición administrativa, carta, memorando, protocolo, regla o comunicación escrita o instrucción anterior que este en contravención con la misma.

## XIX. Vigencia

Estas Guías entrarán en vigor inmediatamente luego de la aprobación del Puerto Rico Innovation and Technology Service (PRITS).

En San Juan, Puerto Rico, Hoy 9 de marzo de 2026.

**VÍCTOR M. RAMOS OTERO, MD, MBA**
**SECRETARIO DE SALUD**

**Subject:** FW: [EXTERNAL]El Boleto: ##RE-149515## Solicitado por usted ha sido cerrado.

**From:** servicedesk@prits.pr.gov <servicedesk@prits.pr.gov>
**Sent:** Thursday, March 26, 2026 6:05 PM
**To:** Virna Silvestriz Alejandro <silvestriz.virna@salud.pr.gov>
**Subject:** [EXTERNAL]El Boleto: ##RE-149515## Solicitado por usted ha sido cerrado.

Saludos Virna Silvestriz Alejandro,

La Petición de Servicio solicitada por usted ha sido completada. Su solicitud : **"DEPARTAMENTO DE SALUD OFICINA DEL SECRETARIO - APROBACION DE GUIAS PARA LA FIRMA DIGITALIZADA - CyberSecurity"**

Agencia o Municipio: **Departamento de Salud**

**Boleto 149515**

Resolución :

**Evaluada la propuesta con la documentación presentada, Recomendamos Favorable.**

**La aprobación aquí provista se limita únicamente a los parámetros establecidos en la Ley 75-2019 y no es extensiva a ningún otro asunto o propósito fuera de los delineados en la Ley 75-2019. Aparte de la Ley 75-2019, la consideración de PRITS de la Solicitud no abarca una revisión o aprobación legal bajo las leyes, reglamentos, cartas normativas u otras análogas aplicables, sean federales o estatales. En particular se aclara que la presente aprobación no excluye cualquier trámite que el Solicitante tenga que llevar a cabo ante cualquier ente estatal o federal.**

Ningún software, desarrollo, aplicación móvil, portal o web puede ser publicado sin la expresa autorización por PRITS, una vez completado el desarrollo el mismo se presentará a PRITS para certificar el cumplimiento con las guías o normativa establecidas por PRITS y con la Ley 229 -2003 conocida como la Ley de Accesibilidad, según enmendada u otra ley aplicable. Lo desarrollado no podrá ser publicado sin la expresa autorización de PRITS.

**Este documento tiene una vigencia de 60 días.**

**Comité Evaluador de Compras y Servicios Tecnológicos PRITS.**

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

PRITS

GOBIERNO DE PUERTO RICO

**Nota: Recuerde que Prits emitió una guía para la implementación de firmas digitales. Favor hacer referencia.**

**Enlace: https://docs.pr.gov/files/prits/Guias/PRITS-002%20-%20Gu%C3%ADas%20de%20Firmas%20Electr%C3%B3nicas%20(Carta%20Circular%202020-04).pdf**

**Siempre a la orden, Support | Prits**

Si aun no está satisfecho(a) con el servicio brindado, nos puede contactar al número abajo indicado. También nos puede escribir a: support@prits.pr.gov

Estamos para servirle.

**Service Desk PRITS**
(939) 910-9100 | (939) 293-2361 | (939) 910-9092