JUNTA DE GOBIERNO
UNIVERSIDAD DE PUERTO RICO

CERTIFICACIÓN NÚMERO 10
2021-2022

Yo, Mayda Velasco Bonilla, secretaria *pro tempore* de la Junta de Gobierno de la Universidad de Puerto Rico, CERTIFICO QUE:

La Junta de Gobierno, considerando las recomendaciones de su Comité de Apelaciones, Ley y Reglamento, acordó:

POR CUANTO: El 28 de junio de 2021, mediante la Certificación Núm. 118 (2020-2021), la Junta de Gobierno propuso la aprobación de una *Política Institucional sobre Firmas Digitales, Firmas Electrónicas y Transacciones Electrónicas de la Universidad de Puerto Rico*, con el propósito de aceptar y validar las firmas digitales y electrónicas en los documentos generados en la Universidad; permitir que se lleven a cabo ciertas transacciones a través de dispositivos electrónicos, internet, correos electrónicos u otro medio digital; reconocer la validez de las aprobaciones electrónicas en las distintas plataformas institucionales, que utilizan formularios electrónicos y pantallas transaccionales; entre otros asuntos.

POR CUANTO: En dicha Certificación Núm. 118 (2020-2021), se dispuso que: "De no recibirse ningún comentario o solicitud de vista en el referido periodo, se dará por aprobado definitivamente el reglamento propuesto y se autoriza al Secretario del cuerpo a emitir la certificación correspondiente a esos efectos para presentarlo al Departamento de Estado para su radicación conforme a la LPAU."

POR CUANTO: De conformidad con la Ley de Procedimiento Administrativo Uniforme del Estado Libre Asociado de Puerto Rico, Ley Núm. 38-2017, según enmendada, la Junta publicó el 2 de julio de 2021 un aviso en Internet y en un periódico de circulación general de Puerto Rico sobre la acción propuesta. Se dio oportunidad por un término de treinta (30) días, contados a partir de la fecha de publicación del anuncio, para someter comentarios por escrito o solicitud fundamentada de vista pública;

POR CUANTO: La Junta de Gobierno, dentro de dicho término y antes de hacer una determinación definitiva sobre la adopción de la

PO BOX 23326 SAN JUAN, PUERTO RICO 00931-3326
TEL. (787) 758-3350, FAX (787) 758-7196

referida Política, no recibió ningún comentario o solicitud de vista pública para la acción propuesta;

POR TANTO: En virtud de lo expresado anteriormente, la Junta de Gobierno resolvió:

1. Aprobar la nueva *Política Institucional sobre Firmas Digitales, Firmas Electrónicas y Transacciones Electrónicas de la Universidad de Puerto Rico*, con el propósito de aceptar y validar las firmas digitales y electrónicas en los documentos generados en la Universidad; permitir que se lleven a cabo ciertas transacciones a través de dispositivos electrónicos, internet, correos electrónicos u otro medio digital; reconocer la validez de las aprobaciones electrónicas en las distintas plataformas institucionales, que utilizan formularios electrónicos y pantallas transaccionales; entre otros asuntos.

2. Derogar todo reglamento interno o norma anterior con respecto a dicho asunto.

3. Determinar que la nueva *Política Institucional sobre Firmas Digitales, Firmas Electrónicas y Transacciones Electrónicas de la Universidad de Puerto Rico* se presente para su radicación en el Departamento de Estado del Gobierno de Puerto Rico, de conformidad con la referida Ley de Procedimiento Administrativo Uniforme;

4. Disponer que este nuevo reglamento entrará en vigor treinta (30) días después de su radicación en el Departamento de Estado.

Y PARA QUE ASÍ CONSTE, expido la presente Certificación, en San Juan, Puerto Rico, hoy 9 de agosto de 2021.

Mayda Velasco Bonilla
Secretaria Pro Tempore

UNIVERSIDAD DE PUERTO RICO

POLÍTICA INSTITUCIONAL SOBRE FIRMAS DIGITALES, FIRMAS ELECTRÓNICAS Y TRANSACCIONES ELECTRÓNICAS DE LA UNIVERSIDAD DE PUERTO RICO

Número: 9299

Fecha: 13 de agosto de 2021

Aprobado: **Omar J. Marrero Díaz**
Secretario de Estado

Gobierno de Puerto Rico
Departamento de Estado

CERTIFICACIÓN NÚM. 10 (2021-2022)

Contenido

Todo término utilizado para referirse a una persona o puesto
se refiere a ambos géneros: femenino y masculino)

ARTÍCULO I – TÍTULO

Este documento se conocerá como "Política Institucional sobre Firmas Digitales, Firmas Electrónicas y Transacciones Electrónicas de la Universidad de Puerto Rico".

ARTÍCULO II – RESUMEN EJECUTIVO

Esta Política tiene como objetivo establecer las normas y estándares para la aceptación de firmas digitales y electrónicas en los documentos que se generen en la Universidad de Puerto Rico (Universidad). La misma establece los parámetros necesarios para la aceptación, legalidad y uso adecuado de las firmas digitales y electrónicas en el sistema universitario. También atiende la aprobación de transacciones electrónicas utilizando flujos de trabajo computadorizado en los cuales el usuario autorizado descarga su función oprimiendo botones en pantallas a las que tiene acceso luego de autenticarse con su usuario institucional.

ARTÍCULO III – BASE LEGAL

Esta Política institucional se adopta y promulga en virtud de las facultades conferidas por la Ley Núm. 1 de 20 de enero de 1966, según enmendada, mejor conocida como la *Ley de la Universidad de Puerto Rico*; la Ley Núm. 148-2006, según enmendada, mejor conocida como la *Ley de Transacciones Electrónicas*, la Ley Núm. 151-2004, según enmendada, mejor conocida como la *Ley de Gobierno Electrónico;* la *Ley Federal de Firmas Electrónicas en el Comercio Global y Nacional*, mejor conocida por su nombre en inglés "*Electronic Signatures in Global and National Commerce Act (E-Sign)*" P.L. No. 106-229 promulgada el 30 de junio de 2000; y las Guías para la implementación de firmas electrónicas en las agencias, promulgada por la Puerto Rico Innovation and Technology Service (PRITS).

ARTÍCULO IV – PROPÓSITO Y APLICABILIDAD

A. Esta Política tiene el propósito de aceptar y validar las firmas digitales y electrónicas en los documentos generados en la Universidad y que, a su vez, se reconozca que las mismas ostentan el mismo efecto legal y valor que las firmas ológrafas o manuscritas tienen en nuestro ordenamiento jurídico. Con su aprobación se busca transformar la operación universitaria en una más ágil y eficiente, permitiendo que, de manera confiable y segura, se puedan llevar a cabo ciertas transacciones a través de dispositivos electrónicos, internet, correos electrónicos u otro medio digital.

B. Además, mediante la misma se reconoce la validez de las aprobaciones electrónicas utilizadas en el proceso de tramitación de los documentos digitales que se llevan a cabo a través de las plataformas institucionales, en los cuales se utilizan formularios electrónicos y pantallas

transaccionales que incluyen pasos de aprobación ejecutados por usuarios autenticados en la plataforma sin requerirles la inclusión de firmas digitales o electrónicas.

C. Esta Política aplicará a todos los miembros de la comunidad universitaria, incluyendo estudiantes, empleados docentes y no docentes, profesionales, voluntarios activos, contratistas, licitadores, entidades gubernamentales, suplidores y afiliados. Aplicará a todos los usos potenciales de la firma digital o electrónica o procesos automatizados para conducir acciones oficiales de la Universidad.

ARTÍCULO V – OBJETIVOS

Esta Política cumple los siguientes objetivos:

A. Adoptar la tecnología de firmas digitales y electrónicas para que su aplicación garantice que su uso en los documentos oficiales de la Universidad sea considerado legalmente válido y exigible.

B. Establecer los parámetros para la autorización, en la Universidad, del uso de la firma digital o electrónica o de aprobaciones mediante autenticación de identidad en plataforma para las aprobaciones electrónicas realizadas en plataformas institucionales con el objetivo de simplificar y agilizar el proceso de firma de documentos.

C. Fomentar una cultura de cero papel y digitalización en la Universidad para contribuir al medioambiente y a la reducción de costos.

D. Maximizar la eficiencia del flujo de trabajo automatizado en los procesos administrativos.

E. Agilizar los procesos de trámite, la aprobación de transacciones y los trámites administrativos relacionados a la contratación.

ARTÍCULO VI – DEFINICIONES

Para propósitos de esta Política, los siguientes términos tendrán el significado que se expresa a continuación:

A. **Acuerdo** – convenio entre las partes, surja éste de lenguaje contractual expreso, o que pueda inferirse de las circunstancias de la transacción particular y de las reglas, reglamentos, legislación o procesos aplicables a dicha transacción que tenga efecto vinculante sobre las partes

B. **Agencia Certificadora** – organización que emite firmas digitales mediante certificados digitales

C. **Análisis de Transformación Digital** – estudio de como la integración de las nuevas tecnologías en áreas de una empresa pueden optimizar los procesos, mejorar su competitividad y ofrecer un nuevo valor añadido a sus clientes

D. **Autenticación** – establecimiento de un medio de verificación de la identidad de la persona

E. **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?)

F. **Autoridad de aprobación de la unidad** – director de la oficina, que aprueba el uso de firma electrónica o autenticación para procesos específicos según su sensibilidad o requisitos de cumplimiento

G. **Autoridad para Firmar** – permiso dado o delegado para firmar contratos, recibos o cualquier tipo de documento en representación de la Universidad o algunas de sus dependencias

H. **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

I. **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)

J. **Contrato** – pacto o convenio firmado entre las partes que se obligan sobre una materia o una cosa determinada y a cuyo cumplimiento pueden ser compelidas

K. **Contratista** – toda persona natural o jurídica que labore o preste servicios mediante acuerdo o contrato para la Universidad

L. **Documento** – información administrativa, fiscal, legal, histórica y esencial presentada en forma de manuscrito o impreso en papel u otro medio que pueda ser leído y cualquier otro material informativo, sin importar su forma o característica física. Incluye, además aquellos documentos o formularios generados de forma electrónica o automatizada, aunque nunca sean impresos en papel u otro medio distinto al creado originalmente, o que por ley o contrato se requiere su conservación

M. **Documento Electrónico** – documento, administrativo, fiscal, legal, activo e inactivo creado o contenido en un soporte electrónico

N. **Electrónico** – cualquier tecnología con capacidad eléctrica, digital, magnética, inalámbrica, óptica, electromagnética, o de funcionamiento similar

O. **Empleado o Funcionario** – toda persona que preste servicios a cambio de salario, sueldo, jornal o cualquier tipo de remuneración como empleado de carrera, de confianza, a tiempo parcial, temporero, por jornal o cualquier otro tipo de nombramiento dentro del esquema de Recursos Humanos de la Universidad

P. **Entidad Gubernamental** – la rama ejecutiva, legislativa y judicial y los municipios del Estado Libre Asociado de Puerto Rico, un Estado de los Estados Unidos o el gobierno federal o cualquier división, subdivisión, departamento, instrumentalidad, comisión, junta, corporación pública, agencia o autoridad adscrita a las mismas

Q. **Estudiante** – toda persona que esté tomando uno o más cursos de cualquier naturaleza o propósito en cualquiera de los recintos o unidades institucionales de la Universidad. Las personas que se dan de baja de la institución luego de alejadamente incurrir en conducta en contravención de las disposiciones de esta Política Institucional, o que no están matriculados oficialmente durante un periodo lectivo en particular, pero mantienen una relación de continuidad con la institución, o a quienes se les ha notificado que han sido admitidos a la Universidad, también serán considerados "estudiantes". Se consideran estudiantes, además, las personas que viven en las residencias estudiantiles de la Universidad, aunque no estén matriculadas

R. **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

S. **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

T. **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 utilizadospara 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)

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

V. **Firma Ológrafa** – firma manuscrita o la que se hace de puño y letra del firmante

W. **Flujos de trabajo electrónicos** – la secuencia de acciones, actividades o tareas utilizadas para la ejecución de un proceso automatizado, incluyendo el seguimiento del estado de cada una de sus etapas y la aportación de las herramientas necesarias para gestionarlo

X. **Llave** – información secreta que adapta el algoritmo de cifrado para cada usuario

Y. **Llave Privada** – clave utilizada para descifrar datos

Z. **Llave Pública** – clave utilizada para cifrar datos

AA. **OSI**- Oficina de Sistemas de Información

BB. **Persona** – un individuo, corporación, fideicomiso, sociedad, compañía de responsabilidad limitada, asociación, entidad gubernamental, corporación pública o cualquier otra entidad legal o comercial

CC. **Política** – Política Institucional sobre Firmas Digitales, Firmas Electrónicas y Transacciones Electrónicas de la Universidad de Puerto Rico

DD. **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

EE. **Tercero** – un individuo, corporación, fideicomiso, sociedad, compañía de responsabilidad limitada, asociación, entidad gubernamental, corporación pública o cualquier otra entidad legal o comercial, que no es parte de la Universidad, y que comparece para la firma de un documento ya sea de manera electrónica y/o digital

FF. **Transacción** – el acto o conjunto de actos entre dos o más personas, con relación a asuntos gubernamentales, comerciales o de negocios

GG. **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

HH. **Unidad Institucional** – Cada uno de los recintos o unidades administrativas y académicas autónomas del sistema universitario, incluyendo aquellas otras unidades que estén bajo la supervisión directa del presidente de la Universidad de Puerto Rico.

II. **Universidad** – la Universidad de Puerto Rico que incluye sus recintos, unidades institucionales y sus dependencias

JJ. **Uso de Llaves (*Key Usage*)** – campo descriptivo dentro de un certificado digital el 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 origende 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

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

ARTÍCULO VII – REQUISITOS MÍNIMOS PARA EL USO

A. De conformidad a las Guías de PRITS, la Universidad como una corporación pública del Gobierno de Puerto Rico cumplirá 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. La Universidad podrá contratar, por un (1) año, una empresa que ofrezca firma electrónica que contenga una carta de controles emitida por un Auditor de Sistemas Información (CISA) o un Contador Público Autorizado (CPA) que certifica los controles implementados de información. Para continuar el contrato después del año, tendrá que cumplir con cualquiera de los incisos “a” o “b” mencionados anteriormente.

d. En caso de que la Universidad 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:

1) posea el Informe de Auditoría *WebTrust for Certification authorities*; o

2) provenga de los suplidores autorizados bajo el gobierno federal y el Programa de FBPKI/PIV-I.

b. En caso de que la Universidad 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.

ARTÍCULO VIII – DISPOSICIONES GENERALES

A. Esta Política aplica a las transacciones y procesos administrativos internos entre la Universidad y cualquier persona o entidad. La misma se regirá conforme a lo siguiente:

1. El director de la Oficina de Sistemas de Información (OSI) de la Administración Central seleccionará, autorizará y validará los métodos específicos de firma digital, electrónica, y de autenticación de usuarios, asegurándose de establecer los criterios de adopción de cada método conforme al nivel de certeza de autenticación de identidad requerido para los diferentes tipos de procesos. En ninguna circunstancia se pondrá en riesgo información confidencial o sensitiva de la Universidad.

2. Cuando una firma digital, aprobación o autorización sea solicitada o requerida para una transacción en la Universidad, ya sea por ley, reglamento, política, certificación o por práctica, una firma digital, aprobación o autorización electrónica será aceptada como equivalente de la firma ológrafa (manuscrita) y será legalmente vinculante siempre y cuando cumpla con los siguientes requisitos:

a. **Intención de firmar** – De la misma manera que ocurre 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 utilizando 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", debidamenteidentificada. Esto 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 de que ese estaba

obligando legalmente o haciendo representaciones que puedan tener consecuencias legales, sean civiles y/o penales.

b. **Consentimiento para hacer negocios electrónicamente** – Para validar el consentimiento del firmante se deberá incluir en los documentos a ser firmados electrónicamente una cláusula que lea de la siguiente manera:

"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."

c. **Autorización previa** – La autoridad de aprobación de la unidad ha autorizado el uso de la firma digital, electrónica o aprobación mediante usuario autenticado para dicha transacción.

d. **Ejemplos de firma digital** – Pueden ser la certificación insertada en un formulario electrónico emitida por una Agencia Certificadora luego de autenticar al firmante; ejemplos de firma electrónica pueden ser: la imagen digitalizada de una firma ológrafa (manuscrita) o realizada con un dedo o implemento digital; algunos ejemplos de las aprobaciones mediante autenticación de usuario incluyen: presionar en un teclado o cursor "*mouse*" opciones como: "Yo acepto", "Yo apruebo", "Yo autorizo", "Yo no acepto", "Yo no apruebo", "Yo no autorizo" luego de autenticar al usuario con su nombre de usuario y contraseña para acceder al formulario electrónico y el método de firma digital aprobado por el Tribunal Supremo de Puerto Rico para la presentación de los escritos judiciales por parte de los abogados: "*f.* Lcdo/a.".

3. El recinto, unidad institucional o dependencia de la Universidad deberá actualizar sus políticas y procesos internos para facilitar que sus transacciones puedan realizarse de forma electrónica, salvo que se demuestren que no es factible luego de un análisis de sus riesgos y beneficios.

4. El director de la OSI de la Administración Central emitirá una guía para realizar el "Análisis de Transformación Digital de Procesos, Documentos y Formularios" que será utilizada por cada unidad para identificar y analizar sus prácticas y realizar su análisis de transformación digital para determinar la viabilidad, tecnología y método de autenticación aplicable acorde a los estándares institucionales establecidos. Además, proveerá los apoyos consultivos y de asesoría técnica a las unidades. La autoridad de aprobación de la unidad asignará la coordinación de este análisis a una oficina o persona específica para lograr que cada facultad, departamento y oficina de su unidad realice el estudio en el tiempo dispuesto y proveerá el apoyo consultivo y de asesoría técnica necesario. De igual manera, tendrá a su cargo la evaluación de los análisis emitidos en su unidad y pasará juicio para aprobar, enmendar o rechazar sus recomendaciones.

5. El recinto, unidad o dependencia de la Universidad utilizará un método y un protocolo de autenticación aprobado por el Director de la OSI el cual sea apropiado para garantizar que el nivel de seguridad es el adecuado para el tipo de transacción.

6. Los directores de las oficinas de sistemas de información de los recintos, unidades o dependencias de la Universidad serán responsables de orientar a la comunidad de los procedimientos y de colaborar en la implementación de los métodos aprobados por el director de la OSI.

B. La firma digital debe ser atribuible a una persona que tiene la intención y la autoridad de firmar el documento con el uso de unas medidas adecuadas de seguridad y de autenticación. Una vez se reciba el documento, el receptor de la transacción deberá estar habilitado para permanentemente retener y guardar el documento electrónico de la transacción.

C. La firma digital, así como las credenciales de identidad utilizadas para acceder a flujos de trabajo electrónicos, debe ser personal e intransferible, por lo que, queda prohibido compartir, prestar, traspasar y/o cualquier otro acto que implique dar o autorizar para su uso. En caso de incumplimiento con esta prohibición, el documento será nulo en todos sus aspectos.

D. La conservación y disposición de documentos generados conforme a esta Política, se regirá por el Reglamento para la Administración, Conservación y Disposición de Documentos de la Universidad de Puerto Rico.

ARTÍCULO IX – DISPOSICIONES NO APLICABLES A ESTA POLÍTICA

A. Esta Política no aplicará a las siguientes transacciones:

1. 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 se determine requiera de la firma ológrafa o manual en los documentos;

2. Cualquier otra transacción que se declare excluida por leyes especiales o reglamentos aprobados en virtud de estas;

3. Cualquier otra transacción o acto que contenga un requisito de forma conforme al Código Civil de Puerto Rico y cualquier otra ley y reglamento externo aplicable.

ARTÍCULO X – ACEPTACIÓN DE FIRMAS ELECTRÓNICAS O DIGITALES DE TERCEROS

A. Los términos del acuerdo, contrato o transacción entre la Universidad y el tercero deben evidenciar el uso y la aceptación de las firmas digitales.

B. En los contratos o acuerdos a ser otorgados por la Universidad, en los que se utilizará la firma digital, se deberá incluir el siguiente lenguaje:

> *"Las partes acuerdan y consienten el uso de firmas digitales con el único fin de ejecutar el Acuerdo o cualquier documento transaccional relacionado. Las partes acuerdan que las firmas digitales que aparecen en este documento son tan válidas como si fuera suscrito a puño y letra para efectos de validez, obligatoriedad, consentimiento, aplicabilidad y admisibilidad. Dicha firma electrónica se considerará que tiene el mismo efecto legal y vinculante que una firma ológrafa (manuscrita)."*

C. Por medio de esta Política se garantiza el derecho de cualquier miembro de la comunidad universitaria que opte por no utilizar firmas digitales ("*opt-out*"). En caso de que decida no utilizar las firmas digitales, se le debe orientar sobre las instrucciones de cómo firmar el documento manualmente. El uso de una firma electrónica en una ocasión no obliga al firmante a utilizar ese mismo método para firmar cualquier otro documento.

D. Todos los firmantes deben recibir una copia del documento firmado al completarse la transacción. `Esto esta un poco dificil....`

E. La OSI determinará el tipo de firma particular requerida a terceros (i.e., digital, electrónica o *clic* en formulario) acorde al nivel de validación de identidad que amerite la transacción.

ARTÍCULO XI – RESPONSABILIDAD DE LOS DIRECTORES DE LAS OFICINAS DE SISTEMAS DE INFORMACIÓN

Los directores de la Oficina de Sistemas de Información tendrán la responsabilidad de:

A. Contratar los servicios de una compañía que se dedique a emitir certificaciones digitales, cuando se opte por la alternativa de firmas digitales.

B. Procurar y mantener un sistema que permita crear firmas digitales o electrónicas para documentos electrónicos y que, además, permita manejarlos y preservarlos.

C. Tomar las medidas de seguridad necesarias para proteger las firmas digitalizadas que puedan estar grabadas en bases de datos contra el acceso por personas no autorizadas.

D. Adoptar y mantener continuamente la plataforma centralizada de manejo de identidad de los usuarios, y la configuración en esa plataforma de los grupos de seguridad, que determinarán el acceso a las plataformas electrónicas de la Universidad ya que este será el principal vehículo para administrar la automatización de procesos de la institución.

E. Adoptar estándares de autenticación de identidad razonables y apropiados para el nivel de responsabilidad y control de riesgo aplicable a cada tipo de transacción, proceso o formulario

electrónico en el cual se utilizarán firmas digitales, electrónicas, o aprobación mediante botones en formularios electrónicos.

F. Proveer apoyo consultivo y de asesoría técnica a las unidades para desarrollar sus Análisis de Transformación Digital y en sus gestiones de adopción y administración de firmas digitales, electrónicas, y aprobaciones en flujos de trabajo automatizados.

ARTÍCULO XII – VIOLACIÓN Y SANCIONES

A. El empleado o funcionario con autoridad de firmar es igualmente responsable de la ejecución adecuada de los documentos en nombre de la Universidad, ya sea que firme el documento de forma ológrafa (manuscrito), digital o electrónica. De no cumplir con cualquier de las disposiciones establecidas en esta Política podrá estar sujeto a la imposición de acciones disciplinarias.

B. Constituye una violación a esta Política el que una persona sin autorización utilice la firma digital o electrónica de otra persona con o sin su consentimiento.

C. Los empleados, funcionarios y estudiantes tienen el deber de reportar, inmediatamente al supervisor o encargado del departamento, facultad u oficina, cualquier acción o sospecha de actividades fraudulentas con relación a las firmas electrónicas que le consten de propio y personal conocimiento.

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

E. Estudiantes que falsifiquen firmas digitales o electrónicas estarán violando esta Política y estarán sujetos a acciones disciplinarias, y la radicación de cargos bajo las leyes estatales y federales.

ARTÍCULO XIII – INTERPRETACIÓN

Esta Política será interpretada a tenor con las disposiciones de las leyes y reglamentos que confieren autoridad en el Estado Libre Asociado de Puerto Rico. Cualquier controversia sobre su interpretación será resuelta por el presidente de la Universidad.

ARTÍCULO XIV – SEPARABILIDAD

Si cualquier artículo o segmento de esta Política Institucional fuese declarado inconstitucional, inválido o nulo por un tribunal de justicia o autoridad con jurisdicción para ello, tal determinación no afectará, menoscabará ni invalidará las restantes disposiciones y partes de esta Política, sino que su efecto se limitará al artículo o segmento así declarado inconstitucional o nulo.

ARTÍCULO XV – ENMIENDAS

Las disposiciones de esta Política podrán ser enmendadas por la Junta de Gobierno, previa recomendación del presidente o motu proprio, conforme a la reglamentación de la Universidad de Puerto Rico y a la Ley Núm. 38-2017, según enmendada, mejor conocida como "Ley de Procedimiento Administrativo Uniforme de la Universidad de Puerto Rico". Las enmiendas estarán sujetas a la aprobación de la Junta de Gobierno de la Universidad.3

ARTÍCULO XVI – VIGENCIA

Esta Política entrará en vigor transcurridos treinta (30) días a partir de su presentación ante el Departamento de Estado, de conformidad en lo establecido en la Ley Núm. 38-2017, según enmendada.

Aprobado por la Junta de Gobierno de la Universidad de Puerto Rico según surge de la Certificación 10 (2021-2022), la cual se acompaña.

Mayda Velasco

Mayda Velasco Bonilla
Secretaria *Pro Témpore*