DIGITO FINANCIAL TECHNOLOGY GROUP, LLC

DECLARACIÓN DE PRÁCTICAS DE PKI

PKI Disclosure Statement (PDS)

Campo	Detalle
Documento	Declaración de Divulgación de Prácticas de Digito Financial Technology Group, LLC
Identificador (OID)	1.3.6.1.4.1.64999.6.2
Versión	1.1
Fecha	27/10/2026
Localización (español)	https://digito.do/pds-es
Localización (inglés)	https://digito.do/pds-en
Idiomas disponibles	Español · Inglés

El presente documento resume, en forma accesible, las condiciones aplicables a los servicios electrónicos de confianza prestados por **Digito Financial Technology Group, LLC**. Se estructura conforme al Anexo A de la norma ETSI EN 319 411-1 y se pone a disposición en cumplimiento del requisito REQ-6.2-03 de la norma ETSI EN 319 401. Se dirige a los Titulares, que son los Suscriptores de sus certificados, a las Organizaciones Vinculadas y a las partes que confían, a quienes se pone a disposición con anterioridad a la aceptación del servicio.

Su localización se consigna en la declaración *QcPDS* (OID 0.4.0.1862.1.5) de los certificados cualificados emitidos por **DIGITO**, conforme a la norma ETSI EN 319 412-5.

No sustituye a las Políticas de Certificación de DIGITO ni a la Declaración de Prácticas de Certificación, que constituyen los documentos de referencia y prevalecen en caso de discrepancia. Todos ellos se encuentran publicados en el repositorio de DIGITO. Entre ellos, la Política de Certificación aplicable prevalece sobre la Declaración de Prácticas de Certificación.

GGT

EMILY PEREZ

1. Prestador del servicio de confianza y datos de contacto

Campo	Detalle
Razón social	Digito Financial Technology Group, LLC
Registro Nacional de Contribuyentes (RNC)	1-32-46998-4
Domicilio social	Av. Gustavo Mejía Ricart No. 102, esq. Abraham Lincoln, Torre Corporativo 2010, Piso 13, Local 1302, Piantini, Santo Domingo
Sitio web	https://digito.do
Correo electrónico de contacto	soporte@digito.do
Teléfono	+1 809 920 8267
Autoridad de Políticas	pki@digito.do
Centro de Atención al Consumidor y al Usuario	Los indicados en los campos anteriores
Solicitud de revocación (24 horas, 7 días)	Plataforma de DIGITO, previa autenticación (canal principal; en los certificados con responsabilidad institucional, también el Solicitante Autorizado desde el panel de la organización), o correo electrónico a soporte@digito.do. Véase la sección 4.
Autoridad de supervisión	Instituto Dominicano de las Telecomunicaciones (INDOTEL)
Número de autorización	115-2025

DIGITO presta sus servicios en calidad de Prestador Cualificado de Servicios de Confianza autorizado por el Instituto Dominicano de las Telecomunicaciones, conforme a la Ley núm. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales y a la Resolución núm. 067-2025 del Consejo Directivo del INDOTEL.

Las consultas, solicitudes de información, reclamaciones y solicitudes de soporte técnico se atienden a través del Centro de Atención al Consumidor y al Usuario, conforme a la sección 8 del presente documento.

2. Tipo de certificado, procedimiento de validación y usos

DIGITO emite las clases de certificado siguientes:

Clase de certificado	Identificador	Uso previsto
Certificado cualificado de firma electrónica de persona física	1.3.6.1.4.1.64999.1.3.1	Firma electrónica cualificada por personas físicas actuando en nombre propio
Certificado cualificado de firma electrónica de persona física con responsabilidad institucional	1.3.6.1.4.1.64999.1.3.4	Firma electrónica cualificada por personas físicas vinculadas a una persona jurídica

DIGITO presta asimismo el servicio de sellado de tiempo cualificado, conforme a la política identificada por el OID 1.3.6.1.4.1.64999.1.3.2. Dicha política se fundamenta en la Best Practices Time-Stamp Policy de la norma ETSI EN 319 421 (OID 0.4.0.2023.1.1). Con anterioridad a confiar en un sello de tiempo, la parte que confía debe verificar que está correctamente firmado y que la clave de la unidad de sellado no estaba comprometida en el momento de la verificación.

Los certificados de persona física tienen un período de validez de treinta y seis (36) meses, y los certificados con responsabilidad institucional, de doce (12) meses, con re-verificación obligatoria del vínculo y del cargo al sexto mes. Ambas clases se emiten al público conforme a la política QCP-n-qscd de la norma ETSI EN 319 411-2 y tienen la consideración de Certificados Cualificados de Firma Electrónica conforme al artículo 38 de la Resolución núm. 067-2025. La clave privada reside en un dispositivo cualificado de creación de firma (QSCD) gestionado por **DIGITO**, bajo control exclusivo del titular.

Verificación de la identidad

Con anterioridad a la emisión de cualquier certificado, **DIGITO** verifica la identidad del titular mediante alguna de las modalidades siguientes:

a) Automática. Proceso desatendido en el que se verifica la autenticidad del documento de identidad, se practica una prueba de vida y se compara el rostro del solicitante con la fotografía del documento y con la conservada en los registros de la Junta Central Electoral. Cuando la identidad se acredite mediante pasaporte, no procede el cotejo con los registros de la Junta Central Electoral; la verificación comprende la autenticidad del documento, incluida la lectura de su chip cuando lo incorpore, la prueba de vida y el cotejo facial contra la fotografía del documento.

b) Asistida. Videoconferencia, previa cita, con un operador autorizado de **DIGITO**, en la que el solicitante exhibe su documento y responde a preguntas de control.

c) Presencial. Acreditación ante un operador autorizado de **DIGITO**, con exhibición física del documento.

Documentos de identidad admitidos: cédula de identidad y electoral emitida por la Junta Central Electoral de la República Dominicana, o pasaporte nacional o extranjero.

En los certificados con responsabilidad institucional se verifica adicionalmente la existencia y vigencia de la persona jurídica, mediante el Registro Nacional de Contribuyentes y el Registro Mercantil o el documento constitutivo que corresponda según el tipo de entidad, así como el vínculo institucional del titular, el cargo que se consignará en el certificado y la facultad del Solicitante Autorizado. Solo se admiten personas jurídicas registradas en la República Dominicana.

Alcance de los certificados con responsabilidad institucional

El certificado acredita la identidad del titular y la existencia, verificada al momento de la emisión, de un vínculo institucional con la persona jurídica consignada.

El certificado NO acredita el alcance de las facultades de representación del titular, ni su capacidad para obligar jurídicamente a la persona jurídica frente a terceros, ni la subsistencia del vínculo o del cargo con posterioridad a la emisión. La calidad en que el titular suscribe un documento determinado se deriva de la declaración incorporada al propio acto de firma y del régimen de representación aplicable. El atributo title tiene valor meramente informativo del cargo verificado al momento de la emisión.

Usos no autorizados

Los certificados emitidos por **DIGITO** no se destinan al cifrado de información, al establecimiento de claves de sesión, ni a la firma de código. No podrán utilizarse con posterioridad a su expiración o revocación, ni para fines distintos de los previstos en la Política de Certificación aplicable. Tampoco podrán emplearse para actos ilícitos o fraudulentos. En particular:

- Los certificados de persona física no acreditan la representación de una persona jurídica ni la pertenencia del titular a una organización.
- Los certificados con responsabilidad institucional no podrán utilizarse con posterioridad al cese del vínculo institucional del titular con la persona jurídica consignada, ni tras la modificación del cargo o función que figura en el certificado.

3. Límites de confianza

Los certificados emitidos conforme a las Políticas de Certificación de **DIGITO** se destinan exclusivamente a la creación de firmas electrónicas cualificadas (usos de clave digitalSignature y nonRepudiation), con los efectos previstos en los artículos 9 y 10 de la Ley núm. 126-02.

Límites aplicables:

- El certificado únicamente puede utilizarse durante su período de validez, indicado en el propio certificado.
- El uso del certificado para fines distintos de los previstos, o excediendo los límites establecidos, exonera a **DIGITO** de responsabilidad.
- **DIGITO** no verifica ni garantiza el contenido, la veracidad ni los efectos jurídicos de los documentos suscritos por el titular.
- **DIGITO** no verifica ni garantiza la capacidad o legitimación del titular para el acto que suscribe. En los certificados con responsabilidad institucional, tampoco verifica el alcance de las facultades conferidas al titular por la persona jurídica.
- La información de registro y los registros de eventos se conservan durante los períodos indicados en la sección 7, y pueden aportarse como evidencia.

Límites operativos de la plataforma de firma

- No se admiten documentos en formato PDF que superen los cien (100) MB para el proceso de firma.
- Certificados de persona física: el documento firmado permanece disponible para su descarga durante siete (7) días calendario. Transcurrido dicho plazo se elimina de la plataforma y no puede recuperarse. Corresponde al titular conservar copia del documento firmado.
- Certificados con responsabilidad institucional: el documento firmado permanece disponible en la plataforma mientras esté vigente el contrato entre DIGITO y la Organización Vinculada, y durante los treinta (30) días calendario siguientes a su terminación. Transcurrido dicho plazo se elimina de la plataforma y no puede recuperarse.

DIGITO no establece límite económico por certificado. Los certificados emitidos no incorporan la declaración QcLimitValue.

4. Obligaciones del titular (suscriptor) y de la Organización Vinculada

Aceptación del certificado

La aceptación requiere un acto explícito, voluntario e inequívoco del titular: la firma del Acuerdo de Uso de Certificados Digitales, la aceptación electrónica expresa de los términos y condiciones en el portal de registro, o el uso voluntario del certificado una vez aceptadas expresamente dichas condiciones. No se admite la aceptación tácita. En los certificados con responsabilidad institucional se requiere, además, la ratificación de la Organización Vinculada por conducto de su Solicitante Autorizado.

Garantías y obligaciones del titular

Al aceptar el certificado, el titular garantiza que:

a) La firma electrónica generada mediante el certificado estará bajo su control exclusivo.

b) Ninguna persona tendrá acceso al procedimiento de generación de su firma.

c) La información contenida en el certificado es verdadera y corresponde a la suministrada a **DIGITO**.

Son asimismo obligaciones del titular:

- Suministrar información completa, precisa y verídica, y mantenerla actualizada.
- Custodiar sus datos de activación y no divulgarlos a terceros. **DIGITO** no puede recuperarlos ni restablecerlos sin una nueva verificación de identidad.
- Utilizar el certificado únicamente para los fines previstos y durante su período de validez.
- Solicitar la revocación de forma inmediata, y en todo caso dentro de las veinticuatro (24) horas, desde que tenga conocimiento de cualquier circunstancia que la motive, en particular el compromiso o la sospecha de compromiso de sus datos de activación.
- Mantener la confidencialidad de sus credenciales de acceso a la plataforma y responder de la actividad que ocurra en su cuenta.
- No permitir el uso de su clave privada por terceros. Queda prohibido todo uso no autorizado de la clave.
- Notificar sin demora a **DIGITO** cualquier inexactitud o modificación de la información contenida en el certificado.

- Cesar de forma definitiva en el uso de la clave privada tras su compromiso o sospecha de compromiso, o cuando sea informado de la revocación del certificado o del compromiso de la Autoridad de Certificación emisora.
- Mantener actualizados sus datos de contacto en la plataforma y consultar en ella el estado de vigencia de sus certificados. **DIGITO** no notifica individualmente la proximidad de la expiración.
- En los certificados con responsabilidad institucional, notificar de forma inmediata a **DIGITO** o a la Organización Vinculada toda modificación de su cargo o función y el cese de su vínculo institucional.

En los certificados con responsabilidad institucional, la Organización Vinculada responde de la autenticidad de la documentación aportada y de la vigencia del vínculo institucional y del cargo consignado. Debe comunicar a DIGITO, dentro de las veinticuatro (24) horas, toda modificación que les afecte; practicar con periodicidad semestral la atestación de sus titulares, vínculos y cargos, cuya falta, transcurridos quince (15) días desde el requerimiento, es causal de revocación; y no exigir al titular sus datos de activación. Responde de los daños derivados de la omisión o el retraso en dichas notificaciones.

El incumplimiento de la obligación de solicitar la revocación genera responsabilidad frente a los terceros de buena fe que hubieren confiado en el certificado, conforme al artículo 49 de la Ley núm. 126-02.

Revocación del certificado

La revocación puede solicitarse en cualquier momento (24 horas, 7 días) a través de la plataforma de **DIGITO** o por correo electrónico a soporte@digito.do: por el titular, sin necesidad de justificación; en los certificados con responsabilidad institucional, por la Organización Vinculada por conducto de su Solicitante Autorizado; por **DIGITO**, de oficio; o por el INDOTEL o la autoridad competente. **DIGITO** publica la revocación en un plazo máximo de veinticuatro (24) horas. La revocación es irreversible; **DIGITO** no practica la suspensión ni la renovación de certificados, y un certificado nuevo exige una verificación de identidad completa. En los certificados con responsabilidad institucional son causales de revocación el cese del vínculo, la modificación del cargo o de los datos de la persona jurídica, la falta de re-verificación o de atestación y la terminación del contrato con la Organización Vinculada (§4.9 de la Política de Certificación aplicable).

5. Obligaciones de verificación de las partes que confían

Con anterioridad a otorgar efectos a un certificado emitido por **DIGITO**, la parte que confía debe:

a) Verificar que el certificado ha sido emitido por una Autoridad de Certificación de **DIGITO**, validando la cadena de certificación hasta el certificado raíz.

b) Comprobar el estado de revocación del certificado, mediante el servicio de consulta en línea (OCSP) o la lista de revocación, cuyas localizaciones constan en el propio certificado. La respuesta OCSP es la fuente preferente. No debe otorgarse efecto a un certificado respecto del cual el servicio devuelva el estado «unknown».

c) Verificar que el certificado se encontraba vigente en la fecha de la firma. Cuando la verificación sea posterior a su expiración, se requiere un sello de tiempo cualificado que acredite el momento de la firma.

d) Comprobar que el uso del certificado se corresponde con el previsto en la Política de Certificación aplicable. En los certificados con responsabilidad institucional, verificar por los medios procedentes la capacidad del titular para el acto concreto que suscribe.

e) Verificar la firma de la respuesta del servicio de consulta del estado y la validez del certificado del respondedor.

f) Adoptar las demás precauciones previstas en la Política de Certificación, en la Declaración de Prácticas de Certificación y en los acuerdos aplicables.

g) Notificar a **DIGITO** cualquier incidencia que detecte en relación con un certificado emitido.

El acceso a la información de estado de revocación es gratuito y no requiere registro ni autenticación previa. El servicio se encuentra disponible de forma ininterrumpida, veinticuatro (24) horas al día los siete (7) días de la semana, con una tasa de continuidad del noventa y nueve coma siete por ciento (99,7 %) en términos anuales, del noventa y nueve coma cinco por ciento (99,5 %) mensual durante los días hábiles entre las 8:00 y las 20:00 horas y del noventa y nueve coma dos por ciento (99,2 %) en otros horarios, conforme al artículo 48, literal c), de la Resolución núm. 067-2025. Las interrupciones por mantenimiento programado se anuncian en la sección «Mantenimientos» del sitio web de DIGITO con una antelación mínima de cinco (5) días hábiles y se realizan preferentemente en horarios de menor actividad.

Los certificados de las Autoridades de Certificación y las listas de revocación se publican en el repositorio de **DIGITO** (Declaración de Prácticas de Certificación, §2.1).

La omisión de estas comprobaciones excluye la condición de tercero de buena fe exento de culpa a los efectos del artículo 49 de la Ley núm. 126-02 y de las limitaciones de responsabilidad de DIGITO.

6. Garantías, exención de garantías y limitación de responsabilidad

DIGITO garantiza que presta sus servicios conforme a las Políticas de Certificación, a la Declaración de Prácticas de Certificación y a la normativa aplicable; que la información consignada en el certificado se corresponde con la verificada al momento de la emisión; y que revoca los certificados y mantiene disponible la información de estado en los términos de este documento. No otorga otras garantías; en particular, no garantiza el contenido ni los efectos jurídicos de los documentos suscritos, la capacidad o las facultades del titular para el acto que suscribe, ni el comportamiento de aplicaciones de terceros.

DIGITO no responde de los vicios de la documentación aportada que no fueran detectables mediante los procedimientos de verificación previstos; de la omisión o el retraso del titular o de la Organización Vinculada en solicitar la revocación o en comunicar modificaciones; del uso del certificado excediendo sus límites; de los daños derivados de que la parte que confía omita las comprobaciones de la sección 5; ni, en los certificados con responsabilidad institucional, del alcance de las facultades de representación del titular. Estas limitaciones no afectan al deber de revocar de **DIGITO** ni a las responsabilidades que no puedan excluirse legalmente.

DIGITO mantiene vigente una póliza de seguro de responsabilidad civil con la cobertura mínima exigida por la normativa aplicable. El titular, la Organización Vinculada y las partes que confían mantendrán indemne a **DIGITO** frente a las reclamaciones de terceros derivadas del incumplimiento de sus respectivas obligaciones.

7. Período de conservación de la información

DIGITO conserva la información relativa a los certificados emitidos durante los períodos siguientes, contados desde la expiración o revocación del certificado, lo que ocurra primero:

Información	Período
Registro de certificados emitidos, certificados y listas de revocación	Cuarenta (40) años
Expedientes de registro y evidencia de verificación de identidad	Veinte (20) años
Evidencia del consentimiento y aceptación de términos	Veinte (20) años
Solicitudes y resoluciones del ciclo de vida	Veinte (20) años
Documentación de la organización, del vínculo institucional y del cargo; facultad del Solicitante Autorizado; atestaciones periódicas; y contrato con la Organización Vinculada (certificados con responsabilidad institucional)	Veinte (20) años
Registros de auditoría	Diez (10) años

El período de cuarenta (40) años responde al artículo 52 de la Ley núm. 126-02. El de veinte (20) años responde a los artículos 14 y 17, literal h), del Reglamento de Aplicación de dicha Ley.

La información de estado de revocación se mantiene disponible con posterioridad a la expiración de los certificados, a fin de permitir la verificación de las firmas generadas durante su vigencia.

8. Procedimiento de reclamación y resolución de conflictos

DIGITO dispone de un Centro de Atención al Consumidor y al Usuario que recibe y atiende las solicitudes de consulta y petición de información, las reclamaciones sobre los servicios prestados y las solicitudes de soporte técnico para la firma de documentos y el uso de los servicios de confianza. Las controversias derivadas de la prestación de los servicios se someten, en primer término, a este procedimiento.

Aspecto	Régimen
Plazo para presentar una reclamación	Treinta (30) días calendario desde el hecho que la origina (artículo 32 de la Resolución núm. 142-06)
Plazo de respuesta de **DIGITO**	Veinte (20) días calendario desde su presentación (artículo 37.1 de la Resolución núm. 142-06)
Forma de la respuesta	Notificación por escrito al reclamante
Canales	Correo electrónico a soporte@digito.do y demás canales publicados en el repositorio de DIGITO
Costo	Gratuito. No se condiciona a pago previo

El reclamante tiene derecho a conocer en cualquier momento el curso y estado de su reclamación, y a obtener copia de los documentos del expediente.

Las decisiones de **DIGITO** sobre las reclamaciones pueden recurrirse mediante Recurso de Queja ante la Dirección Ejecutiva del INDOTEL dentro de los veinte (20) días calendario siguientes a la notificación de la decisión o, si no se hubiere recibido respuesta, al vencimiento del plazo para emitirla (artículos 38 y 39 de la Resolución núm. 142-06), sin perjuicio de la facultad de acudir a los tribunales competentes.

El Centro de Atención se rige por el artículo 19 de la Resolución núm. 142-06 del Consejo Directivo del INDOTEL, en la redacción dada por el artículo 55.3 de la Resolución núm. 067-2025.

9. Ley aplicable y jurisdicción

Los servicios prestados por **DIGITO** se rigen por el derecho de la República Dominicana, y en particular por:

- La Ley núm. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales y su Reglamento de Aplicación (Decreto núm. 335-03).
- La Resolución núm. 067-2025 del Consejo Directivo del INDOTEL, sobre Servicios Electrónicos de Confianza.

- La Ley núm. 172-13 sobre Protección de Datos de Carácter Personal.
- La Resolución núm. 142-06 sobre Protección de los Derechos de los Consumidores y Usuarios.

Las controversias se someten a los tribunales competentes de la República Dominicana, sin perjuicio de las competencias de supervisión del INDOTEL.

La remisión a normas técnicas de ETSI y a especificaciones del IETF se practica a los efectos técnicos previstos en el artículo 35 de la Resolución núm. 067-2025, sin que comporte sujeción al ordenamiento jurídico de la Unión Europea.

10. Autorización, evaluación de conformidad y auditoría

Aspecto	Detalle
Autoridad de supervisión	Instituto Dominicano de las Telecomunicaciones (INDOTEL)
Número de autorización	115-2025
Fecha de autorización	3 de noviembre de 2025
Organismo de Evaluación de la Conformidad	INDOTEL
Normas de referencia	ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 y ETSI EN 319 421
Esquema de evaluación	ETSI EN 319 403, conforme al artículo 35 de la Resolución núm. 067-2025, por un Organismo de Evaluación de la Conformidad acreditado y reconocido por el INDOTEL
Periodicidad de la evaluación	No superior a veinticuatro (24) meses, y con ocasión de toda modificación sustancial o de la incorporación de una nueva clase de certificado. Auditoría interna anual
Dispositivo cualificado de creación de firma	Entrust nShield Connect XC, con certificación Common Criteria EAL4+ conforme al Perfil de Protección EN 419 221-5 (certificado CSA_CC_21008, vigente hasta el 27/06/2027); sistema de activación conforme a EN 419 241-2 (certificado CCN-CC-26/2025)

DIGITO publica en su repositorio la constancia vigente de conformidad, con indicación del organismo emisor, del alcance de la evaluación y de su período de validez.

El Organismo de Evaluación de la Conformidad es independiente de **DIGITO**. **DIGITO** no contrata con dicho organismo servicios de consultoría sobre las materias objeto de evaluación.

11. Protección de datos personales

El tratamiento de datos personales por **DIGITO** se sujeta a la Ley núm. 172-13 sobre Protección de Datos de Carácter Personal. **DIGITO** mantiene una política de privacidad, publicada en su repositorio, que describe los datos tratados, las finalidades, los plazos de conservación y el modo de ejercer los derechos.

Información publicada en el certificado

Los datos que se incorporan al certificado quedan incrustados de forma permanente e inmutable en cada documento que el titular suscriba, y son accesibles a cualquier tercero que lo verifique. Comprenden:

- En los certificados de persona física: nombre, apellidos, dirección de correo electrónico y número de documento de identidad, con indicación del tipo de documento y de su país emisor.
- En los certificados con responsabilidad institucional, adicionalmente: razón social e identificador de la persona jurídica, cargo o función del titular y dirección de correo electrónico institucional.

Dicha información permanece accesible con posterioridad al cese del vínculo institucional, respecto de los documentos suscritos durante la vigencia del certificado.

Información no publicada

No se incorporan al certificado el domicilio ni el teléfono del titular, las imágenes, grabaciones y datos biométricos obtenidos en el proceso de acreditación, las copias de los documentos de identidad, ni los datos de activación. Dicha información se conserva en el expediente de registro con las medidas de protección aplicables. En los certificados con responsabilidad institucional tampoco se incorporan la documentación acreditativa de la organización, del vínculo y del cargo, los datos del Solicitante Autorizado ni el contenido de las atestaciones periódicas.

El titular presta su consentimiento expreso, que comprende el tratamiento de sus datos biométricos para la verificación de identidad y que, en los certificados con responsabilidad institucional, no pueden prestar en su nombre la Organización Vinculada ni su Solicitante Autorizado. La verificación de identidad se practica por cuenta de **DIGITO** a través de un Prestador de Sistemas de Pruebas de Identidad evaluado conforme a la norma ETSI TS 119 461.

Derechos del titular

El titular puede ejercer sus derechos de acceso, rectificación, supresión, oposición y limitación conforme a la Ley núm. 172-13, mediante el procedimiento publicado en el repositorio de **DIGITO**. El ejercicio del derecho de supresión no alcanza a la información cuya conservación resulte legalmente exigible conforme a la sección 7, ni al contenido de los certificados ya emitidos.

DIGITO no accede a las claves privadas de los titulares ni dispone de mecanismo alguno para utilizarlas.

12. Política de reembolso

La tarifa se percibe una vez completadas satisfactoriamente las verificaciones exigidas y aprobada la solicitud de certificado.

DIGITO no percibe tarifa alguna por solicitudes rechazadas, con independencia de la causa del rechazo.

DIGITO reembolsará el importe percibido cuando el certificado no llegue a emitirse por causa imputable a **DIGITO**, o cuando deba revocarse por error en la emisión atribuible a **DIGITO**.

No procede reembolso cuando la revocación obedezca a causa imputable al titular o a la Organización Vinculada, ni por el compromiso o la exposición de los datos de activación conforme a la sección 4.

La revocación, el acceso a la información de estado y el acceso a los documentos indicados en esta declaración son gratuitos. Las reclamaciones relativas al reembolso se sustancian conforme a la sección 8.

Acuerdos aplicables y documentos de referencia

Documento	Identificador	Localización
Declaración de Prácticas de Certificación	1.3.6.1.4.1.64999.6.1	https://cps.digito.do/
Política de Certificación de Persona Física	1.3.6.1.4.1.64999.1.3.1	https://digito.do/politica-de-certificacion
Política de Certificación de Persona Física con Responsabilidad Institucional	1.3.6.1.4.1.64999.1.3.4	https://digito.do/politica-de-certificacion
Términos y condiciones de uso	1.3.6.1.4.1.64999.6.3	https://digito.do/terminos-y-condiciones

Contrato con la Organización Vinculada (certificados con responsabilidad institucional)	—	Se entrega a la Organización Vinculada con anterioridad a la contratación
Política de privacidad	—	https://digito.do/pol%C3%ADtica-de-privacidad

En caso de discrepancia entre el presente documento y la Política de Certificación o la Declaración de Prácticas de Certificación, prevalecerán estas últimas y, entre ellas, la Política de Certificación aplicable. Las modificaciones que puedan afectar a la aceptación del servicio se comunican con una antelación no inferior a treinta (30) días naturales.

Control de versiones

Versión	Fecha	Descripción
1.0	12/10/2026	Versión inicial. Alineada con la Declaración de Prácticas de Certificación v6.0, la Política de Certificación de Persona Física v7.0 y la Política de Certificación de Persona Física con Responsabilidad Institucional v1.0
1.1	27/10/2026	Distinción del plazo de disponibilidad de los documentos firmados según la clase de certificado (sección 3). Tasa de continuidad del servicio de estado conforme al artículo 48, literal c), de la Resolución núm. 067-2025 y aviso de mantenimiento programado (sección 5). Causales de revocación de los certificados con responsabilidad institucional (sección 4) y corrección de erratas (domicilio, RNC y fecha de autorización). Alineada con la Declaración de Prácticas de Certificación v6.1, la Política de Certificación de Persona Física v7.1 y la Política de Certificación de Persona Física con Responsabilidad Institucional v1.1.

Las firmas electrónicas a continuación cuentan con el respaldo de Digito Group, Entidad de Certificación y Proveedora de Servicios Electrónicos de Confianza autorizada por el INDOTEL mediante la Resolución Núm. 115-2025.

Esta lista solo incluye las firmas realizadas con Digito. Este documento puede contener firmas realizadas por otros medios o proveedores.

Documento firmado por 3/3 personas

Gregori Alejandro Polanco Capellan

Firma electrónica cualificada
Digito Group - Autoridad de certificación

Fecha de firma
27 de Octubre, 2026

Hora
13:15:42 GMT-4

Imagen de firma

Emily Altagracia Perez Trinidad

Firma electrónica cualificada
Digito Group - Autoridad de certificación

Fecha de firma
27 de Octubre, 2026

Hora
13:18:59 GMT-4

Imagen de firma

Gabriella Gisela Gomez Tolari

Firma electrónica cualificada
Digito Group - Autoridad de certificación

Fecha de firma
27 de Octubre, 2026

Hora
13:27:18 GMT-4

Imagen de firma

El documento ha sido protegido criptográficamente. Puedes verificar la integridad de sus firmas y contenido en el validador de Digito.

Escanea o visita
valida.digito.do