DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN
DIGITO FINANCIAL TECHNOLOGY GROUP, LLC.

***OID**: 1.3.6.1.4.1.64999.6.1*

CONTROL DE VERSIONES

Versión	Fecha	Descripción de los cambios	Motivo
1.0	19 de diciembre de 2024	Creación inicial del documento.	Legislación
2.0	28 de abril de 2025	Modificación de la Sección 1.5.1, Sección 7.1	Solicitud del órgano regulador de República Dominicana
3.0	16 de marzo de 2026		Cambio de PKI
3.1	05 de mayo de 2026	Actualización integral de los Secciones	Alineación y cumplimiento estricto de los requisitos obligatorios de las normas ETSI
4.0	24 de junio de 2026	Actualización de PKI	Implementación de mejores prácticas
5.0	30 de junio de 2026	Actualización de PKI	Incorporación de nueva Issuing
6.0	31 de agosto de 2026	Incorporación de los procedimientos de registro, validación y revocación asociados al Certificado Cualificado de Firma Electrónica para Persona Física con Responsabilidad Institucional. Modificación de Formato y nueva información siguiendo el estándar RFC 3647	Incorporación de nuevo tipo de certificado

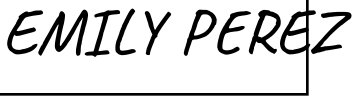
6.1	27 de octubre de 2026	Datos de activación con segundo factor de autenticación (§6.2.8 y §6.4); plazo de aceptación (§4.9.1, literal i); disponibilidad y mantenimiento programado (§4.10.2); terminación del acuerdo de vinculación (§4.11, literal c); medio de aviso de las modificaciones (§9.12.2); remisiones a la Normativa Vigente; definición de Suscriptor conforme a la Normativa Vigente y figura de la Organización Vinculada (§1.3, §1.3.3 y §1.6.1); pérdida y compromiso de los datos de activación (§4.9.1, literal c; §4.12.1).	Alineación con el funcionamiento de la plataforma y con la Normativa Vigente. Modificación no sustancial (§9.12.1)

APROBACION

La Autoridad de Políticas declara que el presente documento, versión 6.1, satisface los requisitos de las Políticas de Certificación aplicables, que cada requisito tiene una práctica que le da cumplimiento y que no existen contradicciones entre la Declaración y las Políticas.

Nombre	**Cargo**	**Rol**	**Firma**
Gregori Polanco	Administrador de la PKI	Autoridad de Políticas	

El órgano de dirección de **DIGITO FINANCIAL TECHNOLOGY GROUP, LLC** aprueba el presente documento, versión 6.1, con autoridad final conforme al requisito REQ-6.1-06 de la norma ETSI EN 319 401.

Nombre	**Cargo**	**Rol**	**Firma**
Gabriella Gomez	Directora Ejecutiva	Órgano de Dirección	
Emily Perez	Directora Legal, de Regulación y Cumplimiento	Órgano de Dirección	

1. Introduccion

La presente Política de Certificación tiene por objeto establecer las normas que regirán la emisión, gestión y revocación de certificados digitales por parte **DIGITO FINANCIAL TECHNOLOGY GROUP, LLC** (en lo adelante **DIGITO**) como Entidad de Certificación (EC) en República Dominicana, así como los derechos y obligaciones de las partes involucradas en el proceso de certificación.

1.1. Presentación general

La presente Declaración de Prácticas de Certificación establece las prácticas que **DIGITO** aplica en la prestación de sus servicios electrónicos de confianza, en su condición de Prestador Cualificado de Servicios de Confianza autorizado por el Instituto Dominicano de las Telecomunicaciones (INDOTEL)

El presente documento describe cómo **DIGITO** presta sus servicios. Las Políticas de Certificación y la Política de Sellado de Tiempo enumeradas en el §1.2 establecen qué se exige en cada clase de certificado o servicio. La correspondencia entre ambos se dictamina conforme al §1.5.3.

DIGITO mantiene una única Declaración de Prácticas de Certificación, común a la totalidad de las políticas que soporta, por corresponder a una única operación.

Esta Política está basada en la **Normativa Vigente** en la materia y en las mejores prácticas internacionales.

1.2. Nombre del documento e identificación

El presente documento se denomina Declaración de Prácticas de Certificación de Digito Financial Technology Group, LLC y se identifica mediante el identificador de objeto 1.3.6.1.4.1.64999.6.1, asignado conforme a la Taxonomía de OID de **DIGITO**.

La presente Declaración soporta las políticas siguientes:

Política	OID	Se fundamenta en
Política de Certificación de Persona Física	1.3.6.1.4.1.64999.1.3.1	QCP-n-qscd — ETSI EN 319 411-2
Política de Certificación de Persona Física con Responsabilidad Institucional	1.3.6.1.4.1.64999.1.3.4	QCP-n-qscd — ETSI EN 319 411-2
Política de Sellado de Tiempo Cualificado	1.3.6.1.4.1.64999.1.3.2	Baseline Time-Stamp Policy — ETSI EN 319 421
Root CA Policy	1.3.6.1.4.1.64999.1.0.1	—
Issuing CA Policy	1.3.6.1.4.1.64999.1.0.2	—

DIGITO identifica sus políticas mediante identificadores propios en lugar de los definidos por ETSI, por tratarse de un Prestador Cualificado sujeto a la legislación de la República Dominicana y no al Reglamento (UE) núm. 910/2014, conforme al requisito OVR-7.1-02 de la norma ETSI EN 319 411-1.

La versión, la fecha de aprobación y el historial de revisiones constan en el control de versiones. Las modificaciones se rigen por el §9.12.

El presente identificador designa el documento y no se incorpora a certificado ni sello alguno. Los identificadores que sí se incorporan son los de las políticas enumeradas.

1.3 Participantes de la ICP

La jerarquía comprende la Autoridad de Certificación Raíz (Root) de Digito y la Autoridad de Certificación Subordinada (Issuing), que emite certificados a entidades finales.

En todas las clases de certificado el Suscriptor coincide con el Titular, conforme a la Normativa Vigente. En las clases que incorporan atributos organizacionales interviene además una Organización Vinculada, persona jurídica distinta del Titular, conforme a la Política aplicable.

1.3.1 Autoridades de certificación

La Autoridad de Certificación Raíz (AC Raiz o *Digito Root CA,* por sus siglas en inglés) es una entidad dentro de una jerarquía que otorga certificados a otras Autoridades de Certificación (AC). El certificado de clave pública de la Autoridad de Certificación Raíz está firmado por sí misma (es decir, autofirmado) y su tarea principal es firmar los certificados de otras ACs que forman parte de la jerarquía de certificación. **DIGITO** es la Autoridad de Certificación Raíz, que a su vez, emite el certificado de la Autoridad de Certificación Subordinada (AC Subordinada).

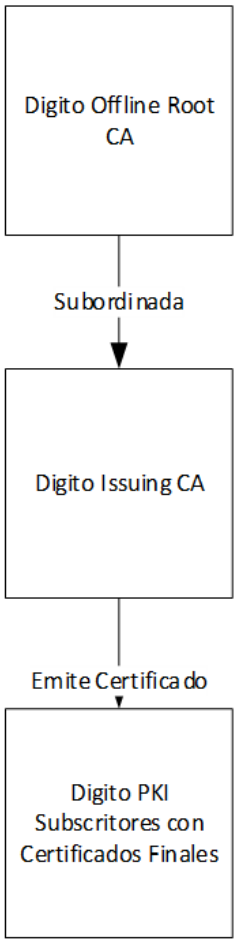
CN: DIGITO ROOT CA
Hash SHA256:
A855459DCCB649DB801D52B5FDF63988E98AD3970F7C6C345116223A688896BB
Válido desde el 22 de junio de 2026 hasta el 17 de junio de 2046
Longitud de Clave RSA 4096 – SHA256

De igual forma, **DIGITO** cuenta con una Autoridad de Certificación Subordinada (AC subordinada o *DIGITO Issuing CA,* por sus siglas en inglés) que tiene un único certificado en vigencia. Este certificado se ha generado utilizando el algoritmo SHA-256, y su capacidad de emisión está limitada mediante la extensión *basicConstraints* con *pathLenConstraint* igual a cero (0), de modo que no puede emitir certificados a otras Autoridades de Certificación.

CN: DIGITO ISSUING CA DO 02
Hash
SHA256:8CEA4726AFAE80F7B292BABDA0A003B5F991B68324BA3CD09CC575B6DA585CF2
Válido desde el 30 de junio de 2026 hasta el 27 de junio de 2036
Tipo de clave: RSA 4096 bits – SHA256

La Autoridad de Certificación Subordinada es aquella que emite certificados para aplicaciones específicas dentro de **DIGITO,** como parte de la infraestructura de clave pública (PKI) de **DIGITO**. De igual forma, la AC Subordinada puede emitir certificados para usuarios finales, dispositivos u otras entidades, y generalmente está sujeta a las políticas y procedimientos establecidos por la AC raíz. El certificado de clave pública de estas entidades está digitalmente firmado por la Autoridad de Certificación Raíz.

En ese sentido, la AC Subordinada también emite el certificado de la Autoridad de Sellado de Tiempo (TSA) de **DIGITO.** También, emite los certificados de las Autoridades de Registro (*Registration Authorities - RAs*) y las Autoridades de Registro Locales (*Local Registration Authorities - LRAs*).



1.3.2. Autoridades de registro (RAs)

Las Autoridades de Registro (o *Registration Authorities - RAs,* por sus siglas en inglés) son las responsables de verificar la identidad de los solicitantes de certificados, aprobar sus solicitudes y agregarlos a la Autoridad de Certificación, utilizando el Servicio de Gestión de Usuarios (*User Management Service - UMS,* por sus siglas en inglés). La función principal de un RA es facilitar el proceso de emisión de certificados asegurando la autenticidad y la identidad de los solicitantes.

Por su parte, las Autoridades de Registro Locales *(Local Registration Authorities - LRAs,* por sus siglas en inglés) son responsables de verificar la identidad de los solicitantes de certificados dentro de una organización o entidad específica, en este caso **DIGITO**. La función de un LRA es aprobar y gestionar las solicitudes de certificados, verificar la identidad de los solicitantes y garantizar que cumplan con los requisitos de seguridad establecidos antes de emitir los certificados correspondientes.

La diferencia entre RA y LRA radica en que el RA es responsable de la identificación de solicitantes de certificados y la emisión de códigos de activación y tokens criptográficos, mientras que el LRA actúa a nivel local y emite certificados de forma limitada, con acceso restringido a ciertas funciones como la solicitud y aprobación de certificados.

DIGITO podrá delegar funciones de registro en Autoridades de Registro Locales. La delegación no transfiere la responsabilidad: **DIGITO** responde de la correcta ejecución de las funciones delegadas y las audita conforme al §8.4.

Las funciones de registro ejercidas directamente por **DIGITO** se practican por su personal en roles de confianza conforme al §5.2.1: el Operador de Registro, respecto de la identidad de las personas físicas, y el Verificador de Organizaciones, respecto de los atributos organizacionales y de la facultad del Solicitante Autorizado. Ninguno de ellos constituye una Autoridad de Registro ni una Autoridad de Registro Local en el sentido de la presente sección.

1.3.3 Suscriptores / Titulares

Es Titular la persona física identificada en el certificado. Es Suscriptor, conforme a la Normativa Vigente, la persona que contrata con DIGITO la expedición del certificado para ser identificada en él, por lo que coincide con el Titular. En las clases que incorporan atributos organizacionales interviene además la Organización Vinculada, persona jurídica a la que se refieren dichos atributos, según lo previsto en la Política de Certificación aplicable. A efectos de la norma ETSI EN 319 411-1, la Organización Vinculada actúa como «subscriber» y el Titular como «subject».

Cuando intervenga una Organización Vinculada, el acuerdo se formaliza en dos instrumentos conforme al §4.1.2, en cumplimiento del requisito REG-6.3.4-09 de la norma ETSI EN 319 411-1.

1.3.4 Terceros que confían

Para los fines de este documento, un tercero que confía es una persona o entidad que acepta la validez del certificado digital emitido por una Autoridad de Certificación (AC), debido a que puede verificar la identidad del Titular del Certificado y confía en la seguridad del proceso de certificación.

1.3.4.1. RESPONSABILIDADES DE LOS TERCEROS QUE CONFÍAN

Los terceros que confían están obligados, sin que esto sea limitativo, a:

- Realizar la verificación del certificado. Esto implica, sin que sea limitativo, confirmar que fue emitido por una Autoridad de

Certificación (AC) de confianza, validar la información contenida en el certificado y consultar la lista de revocación de certificados (CRL);
- Notificar cualquier incidencia relacionada con el certificado a la Entidad de Certificación;
- Cumplir con la Normativa Vigente;
- Mantenerse actualizados de los cambios en la presente política de certificación y de las CRL.
- Usar el certificado de acuerdo con los términos y condiciones establecidos por **DIGITO**.
- Tomar medidas razonables para proteger el certificado contra el acceso no autorizado, la pérdida o el robo.

Los terceros que confían reconocen que son los únicos responsables del cumplimiento de estas obligaciones y que pueden incurrir en responsabilidad civil en caso de no llevarlas a cabo.

1.3.5 Otros participantes

Intervienen en la prestación los proveedores externos identificados en el §5.3.7, en particular el Prestador de Sistemas de Pruebas de Identidad, el operador del centro de datos, el proveedor de infraestructura en nube y el proveedor de distribución de contenido.

1.4. Uso de los certificados

1.4.1. Usos Apropiados De Los Certificados Digitales Emitidos Por Digito

DIGITO emite las clases de certificado siguientes:

Clase	OID de política	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
Certificado TLS / SSL	1.3.6.1.4.1.64999.1.2.1	Autenticación de servidor

Certificado TLS de servidor de firma remota	1.3.6.1.4.1.64999.1.2.2	Autenticación del servicio de firma remota
Certificado de Autoridad de Registro Local / SCO	1.3.6.1.4.1.64999.1.2.3	Operación de registro sobre certificados de nivel medio y básico
Certificado TLS de servidor de sellado de tiempo	1.3.6.1.4.1.64999.1.2.4	Autenticación del servicio de sellado de tiempo
Certificado de Autoridad de Registro operacional	1.3.6.1.4.1.64999.1.3.3	Acceso operacional de Autoridades de Registro

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.El servicio de sellado de tiempo no emite certificados. Emite sellos de tiempo conforme al IETF RFC 3161, en cuyo campo policy se consigna el identificador de la Política aplicable. El certificado del servidor de sellado se identifica mediante 1.3.6.1.4.1.64999.1.2.4 y se enumera en el cuadro anterior.

El certificado de la Autoridad de Certificación Subordinada incorpora en su extensión *certificatePolicies* el identificador 1.3.6.1.4.1.64999.1.0.2.

El certificado de la Autoridad de Certificación Raíz, por su condición de certificado autofirmado, no incorpora dicha extensión. El identificador 1.3.6.1.4.1.64999.1.0.1 designa el régimen aplicable a dicha Autoridad con finalidad documental y de auditoría.

Los certificados de ambas Autoridades se destinan exclusivamente a la firma de certificados y de listas de revocación dentro de la jerarquía de **DIGITO,** conforme al perfil establecido en el §7.1.

Los usos apropiados de cada clase se establecen en la Política de Certificación correspondiente. En caso de discrepancia entre la presente Declaración y una Política, prevalecerá esta última respecto de los certificados emitidos bajo su amparo.

DIGITO no emite clases de certificado distintas de las enumeradas. La incorporación de una clase nueva exige la aprobación de la Política correspondiente conforme al §1.5.4 y la asignación de un identificador conforme a la Taxonomía de OID.

1.4.2. Usos No Autorizados De Los Certificados Digitales Emitidos Por Digito

Los certificados digitales emitidos por **DIGITO** no están autorizados para realizar actos ilícitos, fraudulentos o que vayan en contra de la integridad y seguridad de terceros. Cualquier uso indebido del certificado digital, incluyendo la falsificación de firmas, suplantación de identidad, manipulación de información confidencial o cualquier actividad fraudulenta, será considerado una violación grave de esta Política de Certificación, que podrá resultar en la revocación inmediata del certificado y en el incurrimiento de las responsabilidades legales correspondientes.

1.5. Administración De Políticas

La Administración de Políticas se encuentra a cargo de la Autoridad de Política, la cual es responsable de:

- Definir todas las políticas;
- Asegurar que las funciones realizadas por el personal estén alineadas con la Política de Certificación y la Declaración de Prácticas de Certificación, además de las otras políticas y procedimientos internos establecidos en la Entidad de Certificación;
- Identificar y autorizar el punto de contacto primario (PCP) y los RA.

1.5.1. Autoridad De Políticas (AP)

DIGITO FINANCIAL TECHNOLOGY GROUP, LLC.

1.5.2. Contacto De La Autoridad De Políticas.

DIGITO FINANCIAL TECHNOLOGY GROUP, LLC.

Dirección: Av. Gustavo Mejía Ricart, No. 102, Edificio Corporativo 20/10, Piso 13, Local 1302.
Telefono: +1 809 920 8267.
Correo electrónico: pki@digito.do

1.5.3. Persona que determina la idoneidad de la DPC

Corresponde a la Autoridad de Políticas determinar si la presente Declaración satisface los requisitos de cada una de las Políticas enumeradas en el §1.2.

El dictamen se emite con carácter previo a la aprobación de cualquier versión nueva de la Declaración o de cualquier Política, y se documenta

mediante la firma de la Autoridad de Políticas en la sección de aprobación del propio documento. Con su firma, la Autoridad de Políticas declara haber verificado que cada requisito de la Política tiene una práctica que le da cumplimiento y que no existen contradicciones entre ambos documentos.

1.5.4. Procedimiento de Aprobación del DPC

La aprobación sigue el procedimiento siguiente: elaboración de la propuesta con identificación de los cambios; revisión y dictamen de la Autoridad de Políticas conforme al §1.5.3; aprobación por el órgano de dirección con autoridad final conforme al requisito REQ-6.1-06 de la norma ETSI EN 319 401, que se documenta mediante su firma en la sección de aprobación del documento, con posterioridad a la firma de la Autoridad de Políticas; comunicación previa conforme al §9.12.2 cuando el cambio pueda afectar la aceptación del servicio; y publicación en el repositorio conforme al §2.2.

Las firmas se realizan con firma electrónica cualificada sobre la versión definitiva del documento. La aprobación requiere la firma de la mayoria de los miembros del órgano de dirección. La versión firmada es la que se publica y se conserva conforme al §5.5.2.

La Declaración se revisa como mínimo con periodicidad anual, con independencia de que existan cambios que introducir.

1.6. DEFINICIONES Y SIGLAS.

1.6.1. Definiciones.

Las siguientes definiciones son utilizadas por **DIGITO** para la interpretación de la presente Política de Certificación, sin que las mismas contradigan la Normativa Vigente en la materia:

- **Aplicativo Cliente**: Se refiere a una interfaz utilizada para que el solicitante, usuario o titular del certificado interactúe con la entidad de certificación. Este aplicativo proporciona la plataforma para que el solicitante, usuario o titular del certificado envíe solicitudes de certificados, haga uso de su firma digital cualificada y reciba notificaciones sobre el estado de sus certificados digitales.

- **Autenticación de la identidad:** Se refiere al proceso de verificar y confirmar la identidad de una persona física en la plataforma de **DIGITO** o a través del Aplicativo Cliente, asegurando que cada usuario sea identificado con su

cédula de identidad y electoral para evitar duplicidades y garantizar la integridad de los procesos de emisión y validación de certificados.

- **Certificado para persona física**: Es el documento digital emitido y firmado digitalmente por **DIGITO**, que identifica unívocamente a una persona durante el periodo de vigencia del mismo, y que se constituye en prueba de que dicho suscriptor es fuente u originador del contenido de un documento digital o mensaje de datos que incorpore su certificado asociado.

- **Certificado para Representantes**: Certificado digital utilizado por individuos para firmar en nombre de una entidad pública o privada.

- **Entidad de Certificación**: Organización responsable de emitir, gestionar y revocar certificados digitales, autorizada por el Instituto Dominicano de las Telecomunicaciones (INDOTEL).

- **Emisión del Certificado**: Se refiere al proceso en el cual una Autoridad de Certificación (AC) o una Autoridad de Registro (RA) verifica la identidad del solicitante, valida la información proporcionada y emite el certificado digital una vez cumplidos los requisitos necesarios para obtenerlo.

- **Firma Digital**: Proceso criptográfico que asegura la autenticidad e integridad de un documento electrónico.

- **Solicitante**: Persona que solicita los servicios de Autenticación de Identidad o emisión de un certificado digital.

- **Titular** del Certificado: Persona que es propietario y utiliza un certificado digital.

- **Usuario**: Persona que solicita los servicios de Autenticación de Identidad de **DIGITO**. Además puede utilizar los servicios de validación de **DIGITO**.

- Revocación de Certificado: Proceso de invalidar un certificado digital antes de su fecha de vencimiento.

  Normativa Vigente: A los efectos de este documento, se entenderá por 'Normativa Vigente' la Ley núm. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, su Reglamento de Aplicación, la Resolución núm. 067-2025 emitida por el Consejo Directivo del INDOTEL, las normas técnicas ETSI aplicables, así como cualquier ley, decreto, regulación o resolución que las modifique, complemente o sustituya en el futuro.

- **PKI (Infraestructura de Clave Pública)**: Conjunto de tecnologías, normas y procedimientos para administrar certificados digitales y claves públicas.

- **Listas de Revocación de Certificados (CRL)**: Lista que contiene los certificados digitales revocados por una entidad de certificación.

- **Repositorio**: Es un sistema de información para el almacenamiento y recuperación de certificados u otro tipo de información relevante para la expedición y validación de los mismos.

- **Suscriptor: persona que contrata con DIGITO la expedición de un certificado para ser nombrada o identificada en él, y que mantiene bajo su estricto y exclusivo control el procedimiento para generar su firma electrónica. Conforme a la Normativa Vigente, coincide con el Titular**
- **Organización Vinculada: persona jurídica a la que está vinculado el Titular y a la que se refieren los atributos organizacionales consignados en el certificado, en las clases cuya Política lo prevea. Contrata con DIGITO en un instrumento propio, actúa por medio de su Solicitante Autorizado y no es Suscriptor ni Titular del certificado**

- **Marco Normativo**: Conjunto de leyes y regulaciones que rigen las actividades de las entidades de certificación en la República Dominicana.

- **Operador de Registro**: persona en rol de confianza que verifica la identidad de las personas físicas conforme al §3.2.3 y aprueba o rechaza las solicitudes de emisión.
- **Verificador de Organizaciones**: persona en rol de confianza que verifica la existencia y vigencia de las personas jurídicas, sus atributos organizacionales, el vínculo institucional y el cargo del Titular, y la facultad del Solicitante Autorizado, conforme a los §3.2.2 y §3.2.5. No aprueba solicitudes de emisión.
- **Solicitante Autorizado**: persona física facultada por la Organización Vinculada para solicitar certificados en su nombre, conforme al §3.2.5.

2. Publicación y Responsabilidades del Repositorio

2.1. Repositorios.

Los repositorios son las bases de datos donde se almacena información de los certificados. Los mismos están referenciados por las siguientes URL.

Los repositorios comprenden:

a) El punto de distribución de listas de revocación, cuya localización se consigna en la extensión *cRLDistributionPoints* de cada certificado emitido.

b) El servicio de consulta del estado mediante el protocolo OCSP, cuya localización se consigna en la extensión *authorityInformationAccess*, conforme al §4.10.

c) El punto de publicación de los certificados de las Autoridades de Certificación, cuya localización se consigna en la extensión *authorityInformationAccess*, a lo establecido en la Normativa Vigente.

Certificado CA Raíz de DIGITO - http://pki.digito.do/CAs/DigitoRootCA.crt
Certificado CA Subordinada de DIGITO -
http://pki.digito.do/CAs/DigitoIssuingCADO02.crt
Lista de Certificados Revocados (CRL) CA Raíz de DIGITO -
http://crl.digito.do/CRLs/DigitoRootCA.crl
Lista de Certificados Revocados (CRL) CA Subordinada de Digito-
http://crl.digito.do/CRLs/DigitoIssuingCADO02.crl

DIGITO es responsable de la integridad y de la disponibilidad del repositorio. Los componentes que operan sobre infraestructura de terceros quedan sujetos al §5.3.7.

Los repositorios de **DIGITO** son accesibles a cualquier persona que desee consultarlos. La información en las URL estará disponible en línea las **veinticuatro (24) horas** del día, los **siete (7) días** de la semana. La integridad y disponibilidad de la información publicada es responsabilidad de **DIGITO**.

Las direcciones IP correspondientes a cada URL podrán ser múltiples y dinámicas, pudiendo ser modificadas sin previo aviso.

2.2. Publicación de la Información.

DIGITO publica en su repositorio, con acceso libre y gratuito:

a) La presente Declaración de Prácticas de Certificación y las Políticas de Certificación enumeradas en el §1.2, en su versión vigente.

b) Las versiones anteriores de dichos documentos, con indicación de su período de vigencia, conforme al §5.5.1.

c) Los términos y condiciones aplicables a los Titulares.

d) Los certificados de las Autoridades de Certificación y sus valores resumen, conforme al §6.1.4.

e) Las listas de revocación vigentes.

f) La constancia vigente de conformidad, conforme al §8.6.

g) La política de privacidad, conforme al §9.4.1.

h) Las tarifas vigentes y el procedimiento de reclamación, conforme al §9.1 y al §9.13.

Los certificados de entidad final no se publican en repositorio alguno de acceso público. Su distribución corresponde al Titular, quien lo remite a las partes con las que interactúa.

Lo anterior se entiende sin perjuicio de la publicación de la información de estado de revocación, que es pública conforme al §4.10.

2.3. Momento o frecuencia de publicación

a) Documentos. La Declaración y las Políticas se publican de forma inmediata tras su aprobación conforme al §1.5.4. Las modificaciones que puedan afectar la aceptación del servicio se comunican con la antelación del §9.12.2.

b) Listas de revocación. El régimen de emisión difiere según la Autoridad de Certificación emisora:

b.1) Autoridad de Certificación Subordinada. Emite y publica listas de revocación con una periodicidad de **seis (6) horas**, con independencia de que se hayan practicado o no revocaciones en el período. Cada lista se emite con un campo *nextUpdate* cuyo valor no excede de **tres (3) días**, y con una antelación no inferior a **diez (10) minutos** respecto de la expiración de la lista precedente.

b.2) Autoridad de Certificación Raíz. Por permanecer permanentemente fuera de línea conforme al §6.7, emite listas de revocación en el marco de una ceremonia documentada conforme al §5.2.2. Cada lista se emite con un campo *nextUpdate* cuyo valor no excede de **un (1) año**, y la lista siguiente se emite con una antelación no inferior a **treinta (30) días** respecto de la expiración de la precedente.

DIGITO emitirá adicionalmente una lista de revocación de la Autoridad de Certificación Raíz, con carácter extraordinario y en ceremonia convocada al

efecto, cuando se practique la revocación del certificado de una Autoridad de Certificación Subordinada o cuando concurra alguna de las circunstancias del §5.7.3.

El régimen completo se establece en el §4.9.7.

c) Información de estado en línea. Las respuestas OCSP se generan en el momento de la consulta y reflejan el estado sin retardo alguno derivado de almacenamiento en caché, conforme al §4.10.1.

d) Certificados de las Autoridades de Certificación. Se publican con anterioridad a la emisión del primer certificado bajo su amparo, y se mantienen publicados con posterioridad a su expiración a fin de permitir la verificación de las firmas generadas durante su vigencia.

e) Constancia de conformidad. Se publica tras su obtención y se actualiza en cada ciclo de evaluación.

2.4. Control de Acceso a los Repositorios.

El acceso de lectura al repositorio es libre y gratuito, y no requiere registro ni autenticación previa. **DIGITO** no establece restricción alguna que condicione la consulta de la información publicada, ni percibe tarifa por ella, conforme al §9.1.2 y al §9.1.3.

Lo anterior se entiende sin perjuicio de las medidas técnicas necesarias para preservar la disponibilidad del servicio frente a usos abusivos, que en ningún caso impedirán la consulta legítima del estado de un certificado.

La modificación del contenido del repositorio está restringida al personal en roles de confianza expresamente autorizado, conforme al §5.2.1. Toda modificación queda registrada conforme al §5.4.1.

DIGITO adopta las medidas necesarias para garantizar la integridad de la información publicada y para detectar cualquier alteración no autorizada.

3. Identificación y Autenticación.

3.1. Uso de Nombres

Los nombres consignados en los certificados emitidos por **DIGITO** se construyen conforme a los apartados siguientes y al perfil establecido en la Política de Certificación aplicable a cada clase.

3.1.1. Tipos de Nombres

Los certificados incorporan un Nombre Distintivo conforme a la Recomendación UIT-T X.501, codificado según el IETF RFC 5280.

La composición concreta del Nombre Distintivo se establece en el §7.1.4 de la Política de Certificación aplicable. Con carácter general:

a) Los certificados de persona física incorporan los atributos *countryName*, *surname*, *givenName*, serialNumber y *commonName*.

b) Los certificados que incorporen atributos organizacionales, en las clases cuya Política así lo prevea, incorporan además *organizationName*, *organizationIdentifier* y, cuando proceda, *title*.

c) Los certificados de componentes de la infraestructura incorporan los atributos propios de su función, conforme al §7.1 de la presente Declaración.

Los siguientes nombres distintivos son los Nombres Distintivos de la AC de **DIGITO**:

- AC Raiz: CN = Digito Root CA OU = Certification Authorities, O = Digito Group, C = DO
- AC Subordinada: CN = Digito Issuing <Issuing Name>, OU = Certification Authorities, O = Digito Group C = DO

Los siguientes son Nombres Distintivos de ejemplo para suscriptores de **DIGITO**:

- Servidores TSA: CN=TSA-Server-<unique name>, ou=Applications, O=Digito Group, c=DO
- RAs, LRAs y SCOs: CN= <First-Name Last-Name>, ou=Administrators, O=Digito Group, c=DO
- Clientes con una identidad de firma remota: CN=<givenName+surname>, serialNumber=<Regulator prefix> + (-) + <Customer ID Number> C=<Country>

3.1.2. Necesidad de que los nombres sean significativos

Los Nombres Distintivos son significativos: identifican de forma comprensible a la persona física o jurídica Titular, empleando su nombre real según consta en el documento de identidad o en el registro oficial correspondiente, y su identificador oficial.

DIGITO no emite certificados con nombres arbitrarios, alfanuméricos sin significado, ni denominaciones que puedan inducir a error sobre la identidad del Titular.

3.1.3. Empleo de Seudónimos

No se emplean seudónimos en los certificados emitidos por **DIGITO**, conforme a la Normativa Vigente.

3.1.4. Reglas de Interpretación de formatos de nombres

Los Nombres Distintivos se construyen conforme a la Recomendación UIT-T X.501 y se codifican conforme al IETF RFC 5280.

La semántica del atributo *serialNumber* de persona física se ajusta a la cláusula 5.1.3 de la norma ETSI EN 319 412-1: prefijo de tres caracteres correspondiente al tipo de documento (IDC para cédula de identidad y electoral, **PAS** para pasaporte), seguido del código de país del documento conforme a la norma ISO 3166, un guión y el número de documento.

La semántica del atributo *organizationIdentifier*, en las clases que lo incorporen, se ajusta a la cláusula 5.1.4 de la misma norma: prefijo **NTR** seguido del código de país, un guión y el número perteneciente al Registro Nacional de Contribuyentes.

Cuando la identidad se acredite mediante Pasaporte, el *countryName* y el código de país se corresponderá con el país emisor del documento, que podrá no ser la República Dominicana.

Los atributos se consignan en mayúsculas, sin acentos ni caracteres especiales, salvo cuando la fuente oficial de la que proceden los incluya.

3.1.5. Unicidad de los Nombres

DIGITO garantiza la unicidad de la asociación entre el Nombre Distintivo y el Titular al que corresponde. Un Nombre Distintivo empleado en un certificado no será

reasignado a un Titular distinto durante toda la vida operativa de la Autoridad de Certificación correspondiente.

La exigencia de unicidad recae sobre dicha asociación y no sobre el número de certificados emitidos a un mismo Titular. Los certificados se distinguen entre sí por el código de identidad del certificado, único para DIGITO conforme a la **Normativa Vigente**.

Un mismo Titular podrá ostentar simultáneamente más de un certificado vigente.

El atributo *serialNumber* del Nombre Distintivo identifica a la persona mediante su documento de identidad y es común a todos sus certificados. No debe confundirse con el campo Serial Number del certificado.

3.1.6. Pluralidad de certificados por Titular

No se establece límite al número de certificados vigentes que un mismo Titular pueda ostentar, sin perjuicio de lo que establezca la Política de Certificación aplicable a cada clase.

Cada emisión exige una validación de identidad propia conforme al §3.2.7, con el máximo de certificados por validación allí establecido, en cumplimiento del requisito REG-6.3.1-00E de la norma ETSI EN 319 411-1.

Cada certificado se asocia en todo caso a un par de claves propio y exclusivo, y a datos de activación independientes.

Todos los certificados emitidos a un mismo Titular quedan vinculados a un único expediente de registro.

3.2. Validación de identidad inicial

DIGITO practica la validación de identidad con anterioridad a la emisión de todo certificado, conforme a los requisitos de la Política aplicable y a la norma ETSI TS 119 461, incorporada por la Normativa Vigente.

3.2.1 Método de prueba de posesión de la clave privada

En los certificados cuyo par de claves se genera en el dispositivo cualificado de creación de firma gestionado por **DIGITO**, la posesión de la clave privada por el

Titular queda acreditada por el propio procedimiento de generación: la clave se genera dentro del módulo criptográfico, se asocia de forma exclusiva al Titular identificado y no es extraíble.

En los supuestos en que el par de claves sea generado fuera de la infraestructura de **DIGITO**, la posesión de la clave privada se acredita mediante la firma de la solicitud de certificado en formato PKCS#10, cuya verificación con la clave pública contenida en la propia solicitud constituye prueba de posesión.

3.2.2 Autenticación de la identidad de una organización

En las clases de certificado cuya Política de Certificación prevea la incorporación de atributos organizacionales, **DIGITO** verifica:

> **a)** La existencia y vigencia de la persona jurídica, mediante el Registro Nacional de Contribuyentes y el Registro Mercantil vigente.Se exigen ambos documentos porque acreditan extremos distintos y ninguno sustituye al otro. El RNC acredita la existencia fiscal ante la DGII; el Registro Mercantil acredita la constitución vigente y la identificación de los órganos con facultad de representación, dato imprescindible para la verificación del Solicitante Autorizado del §3.2.5
>
> **b)** La correspondencia entre la razón social consignada y la que consta en el registro oficial.
>
> **c)** La existencia del vínculo institucional entre el Titular y la persona jurídica, y del cargo o función que se consignará.
>
> **d)** La facultad del Solicitante Autorizado, conforme al §3.2.5.

Las verificaciones de la presente sección las practica el Verificador de Organizaciones conforme al §5.2.1, literal d bis), con independencia de la verificación de la identidad del Titular del §3.2.3. El Registro Nacional de Contribuyentes se verifica contra la fuente oficial. **DIGITO** registra en el expediente, como evidencia, la fuente consultada, la fecha y hora de la consulta, el resultado obtenido y la identificación del Verificador de Organizaciones que la practicó.

La documentación admisible por tipo de entidad, los criterios de revisión y los supuestos de rechazo se detallan en Anexo.

3.2.3. Autenticación de la identidad de Persona Física

DIGITO verifica la identidad de la persona física con el nivel de aseguramiento exigido por la Política aplicable, mediante alguna de las modalidades siguientes:

a) Automática. Proceso desatendido en el que el sistema verifica la autenticidad del documento, coteja los datos extraídos con los declarados, practica la prueba de vida y compara el rostro capturado con la fotografía del documento y con la conservada en los registros de la Junta Central Electoral, conforme a la Normativa Vigente.

Cuando la identidad se acredite mediante pasaporte, la comparación contra los registros de la Junta Central Electoral prevista en la Normativa Vigente no resulta aplicable, por no existir dicho registro respecto de titulares de documentos extranjeros. En tal supuesto la acreditación comprende la verificación de la autenticidad del documento, incluida la lectura de su chip cuando el documento lo incorpore, la prueba de vida y el cotejo facial contra la fotografía del documento, practicados por el prestador identificado en el §3.2.6 dentro del alcance de su evaluación de conformidad con la norma ETSI TS 119 461, conforme a la Normativa Vigente.

b) Asistida. Proceso a distancia mediante videoconferencia con un Operador de Registro autorizado, previa cita, en el que el solicitante exhibe su documento a la cámara y responde a preguntas de control. El Operador verifica la correspondencia entre el solicitante y el documento exhibido Esta modalidad se practica cuando el proceso automatizado no arroje resultado concluyente, cuando el documento presentado no permita su verificación automatizada, cuando el requirente lo desee o cuando **DIGITO** lo estime necesario en atención al riesgo.

c) Presencial. Acreditación ante un Operador de Registro autorizado, con exhibición física del documento.

Cuando la identidad se acredite mediante cédula de identidad y electoral, únicamente se admitirá la emitida por la Junta Central Electoral de la República Dominicana.

En las tres modalidades se conservan las evidencias obtenidas, con valor probatorio, por el plazo del §5.5.2. En las modalidades asistida y presencial se registra la identidad del Operador que intervino.

DIGITO rechazará la solicitud cuando no se completen satisfactoriamente las verificaciones, cuando la documentación resulte ilegible, incompleta o vencida, cuando exista discrepancia con la fuente oficial, o cuando concurran indicios razonables de inautenticidad.

Todo usuario en **DIGITO**, necesita identificarse en el sistema de User Digito ID. El cual contiene la información, permisos y roles necesarios para la interacción con el ecosistema de **DIGITO**.

La forma de autenticación en el ecosistema de **DIGITO**, se basa en un algoritmo de identificación utilizando el estándar RS 256, que contiene información básica del usuario como:

- Identificador del sistema
- Nombre completo,
- Número telefónico,
- Identificación única del sistema,
- Verificación de fecha de expiración,
- Estado de la verificación
- Identificación de la autenticación.

3.2.4. Información del solicitante no verificada

DIGITO mantiene un estricto compromiso con la veracidad y la calidad de la información incluida en los certificados. Por tanto, ningún dato no verificado se incluirá o aceptará en nuestros procesos de certificación. Cada certificado emitido es el resultado de una exhaustiva verificación de los datos presentados, asegurando la precisión y la autenticidad de la información consignada en el mismo.

3.2.5. Validación de autoridad

En las clases de certificado cuya Política de Certificación prevea la intervención de un Solicitante Autorizado, únicamente podrán solicitar la emisión el representante legal de la persona jurídica, acreditado mediante acta de asamblea o nombramiento inscrito, y la persona designada expresamente por aquel.

El Solicitante Autorizado deberá estar identificado en la plataforma de **DIGITO** con el mismo nivel de aseguramiento exigido a un Titular, y su facultad verificada documentalmente.

La designación se registra a nombre de la cuenta de la organización y no de una dirección de correo electrónico individual. La baja de la persona designada no extingue la facultad, que será reasignada por el representante legal.

El primer alta de cada organización requiere doble control conforme al §5.2.2, literal e): verificación de la facultad por el Verificador de Organizaciones y aprobación por un Operador de Registro distinto de aquel. Ningún Solicitante Autorizado podrá aprobar su propia designación.

En las solicitudes posteriores, la vigencia de la facultad se comprueba de forma automatizada contra la verificación registrada, dentro de la ventana del §3.2.7, sin requerir nueva intervención del Verificador de Organizaciones mientras dicha ventana no haya expirado.

3.2.6. Criterios de interoperación

Para la validación de identidad, **DIGITO** ha establecido los medios técnicos y operacionales que garantizan la interoperabilidad con los servicios siguientes:

> **a)** Validación en línea del número de cédula de identidad y electoral a través de los servicios de la Junta Central Electoral de la República Dominicana, conforme a la Normativa Vigente. Aplicables únicamente a titulares de cédula dominicana.
>
> **b)** Verificación de la autenticidad de documentos de identidad y de viaje, extracción y cotejo de datos, prueba de vida y reconocimiento facial, a través de Sum and Substance Ltd, 30 St. Mary Axe, Londres, Inglaterra, en su condición de Prestador de Sistemas de Pruebas de Identidad conforme a la Normativa Vigente.
>
> Dicho prestador cuenta con evaluación de conformidad con las normas ETSI EN 319 401 y ETSI TS 119 461, exigidas por la Normativa Vigente, emitida por SRC Security Research & Consulting GmbH con el alcance que consta en el expediente de gestión de proveedores. Estos servicios resultan aplicables tanto a cédulas como a pasaportes, nacionales y extranjeros.

DIGITO conserva la responsabilidad sobre el proceso de identificación electrónica en su conjunto, que forma parte integral del servicio de confianza prestado, y verifica con periodicidad anual la vigencia y el alcance de las evaluaciones de conformidad de sus proveedores conforme al §5.3.7.

3.2.7. Vigencia y reutilización de la evidencia de verificación

La evidencia obtenida podrá reutilizarse en solicitudes posteriores conforme a los plazos siguientes:

Objeto	Ventana
Identidad de la persona física	**Veinticuatro (24) horas**
Existencia y vigencia de la persona jurídica	**398 días naturales**
Vínculo institucional y cargo	**180 días naturales**
Cargo o función consignada	Sujeta a la atestación de la política correspondiente
Facultad del Solicitante Autorizado	**398 días naturales**

Excedida la ventana aplicable, **DIGITO** practicará un nuevo proceso completo de validación en tiempo real, sin que resulte admisible el consumo de validaciones preexistentes. La renovación de las verificaciones relativas a la persona jurídica, al vínculo institucional, al cargo y a la facultad del Solicitante Autorizado corresponde al Verificador de Organizaciones. La renovación de la verificación de identidad de la persona física corresponde al Operador de Registro o a los procedimientos automatizados del §3.2.3.

Dentro de la ventana de identidad podrá emitirse un máximo de un (1) certificado sobre una misma validación, en cumplimiento del requisito REG-6.3.1-00E de la norma ETSI EN 319 411-1.

La reutilización quedará documentada en el expediente con referencia a la verificación original.

3.3. Identificación y Autenticación para solicitudes de Renovación de certificados

DIGITO no practica la renovación de certificados ni la renovación de claves como procedimientos del ciclo de vida, conforme a los §4.6 y §4.7.

Toda emisión de un certificado a un Titular que ya lo tuviere, sea por expiración del anterior, por su revocación o por cualquier otra causa, constituye una nueva emisión y se sujeta íntegramente a la identificación y autenticación del §3.2.

3.3.1. Identificación y autenticación para la renovación de claves rutinaria

DIGITO no practica la renovación de claves rutinaria conforme al §4.7.

3.3.2. Identificación y autenticación para la renovación de claves tras revocación

No estipulado como procedimiento diferenciado. La obtención de un certificado nuevo por un Titular cuyo certificado anterior hubiere sido revocado o hubiere caducado exige la repetición íntegra del procedimiento del §3.2, con independencia de la causa y de la antigüedad de la evidencia previamente obtenida.

No resulta admisible en estos supuestos el consumo de validaciones de identidad preexistentes, aun cuando se encontraran dentro de la ventana del §3.2.7.

3.4. Identificación y Autorización para solicitudes de Revocación de certificado

Toda solicitud de revocación se autentica con anterioridad a practicarla, comprobando que procede de fuente legitimada conforme al §4.9.2 y con el nivel de aseguramiento correspondiente a cada una:

a) Titular. Se autentica mediante sus credenciales de acceso a la plataforma de Digito, o mediante el procedimiento de identificación del §3.2.3 cuando no disponga de ninguno de los anteriores.

b) Tercero en nombre y representación legal del Titular, conforme a la Normativa Vigente. Se exige la acreditación documental de la representación y la identificación del solicitante conforme al §3.2.3, en modalidad asistida o presencial.

c) Solicitante Autorizado, en las clases de certificado cuya Política así lo prevea. Se autentica mediante sus credenciales, y DIGITO comprueba adicionalmente que su facultad se encuentre vigente conforme al §3.2.5 y dentro de la ventana del §3.2.7. La solicitud debe acompañarse de la justificación documental de la causal invocada, en particular del cese del vínculo institucional o de la modificación del cargo.

d) DIGITO, de oficio. No requiere autenticación de solicitante. La decisión se adopta por personal en rol de confianza, queda registrada conforme al §5.4.1 con identificación de quien la practicó y del fundamento invocado.

e) INDOTEL o autoridad judicial o administrativa competente. Se verifica la autenticidad de la resolución recibida y la competencia del órgano emisor por los cauces oficiales.

La solicitud puede presentarse por los canales habilitados por DIGITO, disponibles de forma ininterrumpida conforme al §4.9.5.

Cuando concurran indicios razonables de compromiso de la clave privada y no resulte posible completar la autenticación del solicitante, **DIGITO** practicará la revocación de forma preventiva, notificándolo al Titular. Prevalece la protección frente al uso indebido sobre la certeza acerca del origen de la solicitud.

La revocación es irreversible conforme al §4.9.13. **DIGITO** extremará la verificación de la legitimación con anterioridad a practicarla, salvo en el supuesto del párrafo anterior.

4. Ciclo de Vida de los Certificados Digitales y Requisitos Operacionales.

4.1. Solicitud de Certificado

El procedimiento de solicitud de certificado se practica a través de la plataforma de **DIGITO** y comprende la identificación del solicitante, la verificación de su identidad conforme al capítulo 3, la aceptación de los términos y condiciones aplicables y la obtención del consentimiento del Titular.

4.1.1. Quién puede presentar una solicitud

Podrán presentar una solicitud de certificado:

a) La persona física que vaya a ser Titular del certificado, actuando en nombre propio.

b) El Solicitante Autorizado de una persona jurídica, en las clases de certificado cuya Política de Certificación así lo prevea, conforme al §3.2.5. En este supuesto se requiere en todo caso el consentimiento del Titular en los términos del §4.1.2.

c) El personal de **DIGITO** en rol de confianza, respecto de los certificados de componentes de la infraestructura.

No se admiten solicitudes presentadas por sujetos distintos de los enumerados, ni por canales distintos de los habilitados por **DIGITO.**

4.1.2. Proceso de Inscripción y Responsabilidades

El proceso de inscripción comprende:

a) El registro del solicitante en la plataforma de **DIGITO** y la verificación del control del canal de comunicación declarado.

b) La verificación de la identidad del Titular conforme al §3.2.3, y de los atributos organizacionales conforme al §3.2.2 cuando la Política aplicable los prevea.

c) La puesta a disposición del solicitante de los términos y condiciones aplicables, con anterioridad a su aceptación, conforme al requisito REQ-6.2-03 de la norma ETSI EN 319 401 y al requisito REG-6.3.4-02 de la norma ETSI EN 319 411-1.

d) La aceptación expresa de dichos términos y condiciones.

e) La obtención del consentimiento del Titular en los términos del §9.4.5, incluido el relativo al tratamiento de sus datos biométricos y a la incorporación al certificado de los datos del §9.4.3.

f) El establecimiento por el Titular de sus datos de activación conforme al §6.4.1.

Cuando intervenga una Organización Vinculada, el acuerdo se formalizará en dos instrumentos, en cumplimiento del requisito REG-6.3.4-09 de la norma ETSI EN 319 411-1: el contrato celebrado con la Organización Vinculada, y los términos y condiciones aceptados por el Titular.

Cada Titular suscribe individualmente su propio acuerdo de servicios, con independencia del contrato celebrado con la persona jurídica. La aceptación del

Titular no se entiende implícita en dicha contratación, ni puede ser prestada por la Organización Vinculada ni por su Solicitante Autorizado en su nombre.

En las clases en que no intervenga una Organización Vinculada, la aceptación de los términos y el consentimiento se otorgan en un único acto.

DIGITO conserva la evidencia del consentimiento y de la aceptación por el plazo del §5.5.2, e informa al solicitante de las obligaciones que asume conforme al §9.6.3, en cumplimiento del requisito REQ-6.2-03 de la norma ETSI EN 319 401.

4.2. Procesamiento de la solicitud de certificado

Recibida la solicitud, **DIGITO** ejecuta las funciones de identificación y autenticación del capítulo 3 y resuelve su aprobación o rechazo conforme a los apartados siguientes.

4.2.1. Ejecución de las funciones de identificación y autenticación

DIGITO ejecuta las funciones aplicables del capítulo 3 con carácter previo a la aprobación. Ningún certificado se emite antes de haberse completado satisfactoriamente todas las funciones aplicables.

Según la clase de certificado solicitada se ejecutan: la verificación de la identidad del Titular conforme al §3.2.3; la prueba de posesión de la clave privada conforme al §3.2.1; la verificación de los atributos organizacionales conforme al §3.2.2, cuando la Política aplicable los prevea; y la verificación de la facultad del Solicitante Autorizado conforme al §3.2.5.

La verificación de la identidad del Titular y del Solicitante Autorizado se ejecuta por los Operadores de Registro o por los procedimientos automatizados de identificación conforme a la norma ETSI TS 119 461. La verificación de los atributos organizacionales y de la facultad del Solicitante Autorizado se ejecuta por el Verificador de Organizaciones. Ambos actúan en el desempeño de un rol de confianza conforme al §5.2.1.

DIGITO puede delegar su ejecución en Autoridades de Registro o Autoridades de Registro Locales conforme al §1.3.2. La delegación no transfiere la responsabilidad: **DIGITO** responde de la correcta ejecución de las funciones delegadas y audita periódicamente su desempeño conforme al §8.4.

De cada función ejecutada se conserva en el expediente: la identificación del Operador o del sistema que la practicó, la fecha y hora, la evidencia obtenida, la

fuente consultada y el resultado. Esta información constituye la evidencia del cumplimiento del capítulo 3 y se conserva conforme al §5.5.2.

4.2.2. Aprobación o rechazo de solicitudes

DIGITO aprobará la solicitud cuando se hayan completado satisfactoriamente todas las verificaciones exigidas y el solicitante haya aceptado los términos y condiciones aplicables.

DIGITO rechazará la solicitud, sin que ello genere derecho a indemnización, cuando concurra alguno de los supuestos siguientes:

a) Imposibilidad de verificar la identidad del Titular, o resultado no satisfactorio de alguno de los controles del §3.2.3.

b) Documentación ilegible, incompleta, vencida o carente de la legalización o apostilla exigible.

c) Discrepancia entre los datos aportados y los que constan en la fuente oficial.

d) Imposibilidad de verificar contra la fuente oficial, cuando dicha verificación resulte exigible.

e) Indicios razonables de inautenticidad de la documentación aportada.

f) Falta de acreditación de la facultad del Solicitante Autorizado, cuando resulte aplicable.

g) Ausencia del consentimiento del Titular en los términos del §4.1.2.

h) Existencia de prohibición legal o de medida cautelar que lo impida.

i) Registro Mercantil vencido, o discrepancia en la razón social, en las clases que incorporen atributos organizacionales.

Si el defecto fuere subsanable, el solicitante dispone de siete (7) días calendario para subsanarlo, transcurridos los cuales **DIGITO** evalúa nuevamente la solicitud. Transcurrido dicho plazo sin subsanación, la solicitud se tiene por desistida.

El rechazo se comunica al solicitante con indicación del motivo y, cuando proceda, del plazo de subsanación, salvo que la comunicación del motivo esté legalmente restringida.

Los rechazos se registran conforme al §5.4.1, con identificación del fundamento invocado.

4.2.3. Plazo de procesamiento de las solicitudes

En los procedimientos de identificación automática, el procesamiento es inmediato una vez superadas satisfactoriamente las comprobaciones automatizadas.

En las modalidades asistida y presencial, **DIGITO** procesará las solicitudes en un plazo no superior a cinco (5) días hábiles desde la recepción de la documentación completa y la celebración de la sesión de acreditación.

El plazo se suspende durante el período de subsanación del §4.2.2.

Estos plazos se entienden sin perjuicio de los que resulten de los acuerdos de nivel de servicio suscritos con determinados Suscriptores o Organizaciones Vinculadas, que en ningún caso podrán ser inferiores a los exigidos por la normativa aplicable.

4.3. Emisión de Certificado

Aprobada la solicitud conforme al §4.2.2, **DIGITO** procede a la emisión del certificado conforme a los apartados siguientes y al perfil establecido en el capítulo 7 de la Política de Certificación aplicable.

4.3.1. Actuaciones de la AC durante la emisión

DIGITO practica las actuaciones siguientes:

a) Genera el par de claves del Titular en el dispositivo cualificado de creación de firma, conforme al §6.1.1. La clave privada se genera de modo que no resulte extraíble.

b) Construye el certificado conforme al perfil de la clase solicitada, con el Nombre Distintivo del §3.1 y las extensiones del capítulo 7.

c) Asigna el código de identidad del certificado mediante un generador de números aleatorios criptográficamente seguro, con entropía no inferior a sesenta y cuatro (64) bits, único para DIGITO conforme a la **Normativa Vigente**.

d) Firma el certificado con la clave privada de la Autoridad de Certificación Subordinada correspondiente.

e) Registra el evento de emisión conforme al §5.4.1, con identificación del expediente de registro que lo fundamenta.

f) Pone el certificado a disposición del Titular para su aceptación conforme al §4.4.

El certificado no se considera emitido a los efectos de su utilización hasta que el Titular lo haya aceptado conforme al §4.4.1 y establecido sus datos de activación conforme al §6.4.1.

4.3.2. Notificación de la emisión al suscriptor

DIGITO notifica al Titular el resultado de la solicitud por el canal de comunicación registrado en su expediente.

Aprobada la solicitud, la notificación indica el código de identidad del certificado, su período de validez y las actuaciones necesarias para su aceptación.

Rechazada la solicitud, la notificación se practica en los términos del §4.2.2.

Cuando intervenga una Organización Vinculada, **DIGITO** notifica asimismo a su Solicitante Autorizado la emisión practicada, sin que ello comporte el traslado de información distinta de la contenida en el propio certificado.

4.4. Aceptación del certificado

La aceptación del certificado por el Titular determina el momento a partir del cual éste asume las obligaciones y garantías del §9.6.3.

4.4.1. Conducta que constituye aceptación

La aceptación del certificado requiere un acto explícito, voluntario e inequívoco del Titular.

En los certificados emitidos a personas físicas para uso individual, la aceptación podrá manifestarse mediante cualquiera de los actos siguientes:

a) La firma del Acuerdo de Uso de Certificados Digitales.

b) La aceptación electrónica expresa de los términos y condiciones aplicables en el portal de registro.

c) El uso voluntario del certificado una vez aceptadas expresamente las condiciones de emisión y uso correspondientes.

En los certificados que incorporen atributos organizacionales, en las clases cuya Política así lo prevea, la aceptación exige la ratificación de dos sujetos con carácter acumulativo: la de la Organización Vinculada, mediante su Solicitante Autorizado, y la del Titular. La emisión queda condicionada a la validación de ambas ratificaciones.

El Titular manifiesta su aprobación del contenido del certificado mediante la remisión de éste a una o más personas, o mediante la solicitud de su publicación.

No se admite la aceptación tácita. El silencio, el transcurso del tiempo, la ausencia de objeción o la falta de respuesta del Titular no constituyen en ningún caso aceptación del certificado ni de las condiciones asociadas.

Con la aceptación, el Titular asume las garantías del §9.6.3.

4.4.2. Publicación del certificado por la AC

El presente apartado regula la publicación del contenido de los certificados emitidos. La publicación de la información de estado de revocación se rige por el §4.9.7 y el §4.10.

Los certificados de las Autoridades de Certificación se publican conforme al §2.2, y su localización se consigna en la extensión *authorityInformationAccess*, en cumplimiento de la Normativa Vigente.

Los certificados de entidad final no se publican en repositorio de acceso público, por corresponder su distribución al Titular, quien los remite a las partes con las que interactúa. Ello obedece a la protección de los datos personales del Titular conforme al §9.4.

Lo anterior se entiende sin perjuicio de la publicación de la información de estado de revocación, que es pública conforme al §4.10.

4.4.3. Notificación a otras entidades

DIGITO no notifica la emisión ni la renovación de certificados a otras Entidades de Certificación ni a terceras entidades.

Lo anterior se entiende sin perjuicio de las obligaciones de publicación e información frente al INDOTEL previstas en la Normativa Vigente, que se rigen por el capítulo 2.

4.5. Uso del par de claves y del certificado

El uso del par de claves y del certificado queda limitado al período de validez del certificado y a los usos autorizados conforme al §1.4.1 y a la Política de Certificación aplicable.

4.5.1. Uso de la clave privada por el suscriptor

- Si lo aplicare, el Titular debe mantener el control del acceso a su clave privada y preservarla del conocimiento de terceras personas.
- El Titular debe utilizar el certificado únicamente para los fines previstos en el §1.4.1 y conforme a las leyes y regulaciones aplicables. El uso para fines distintos, o excediendo los límites establecidos, exonera a **DIGITO** de responsabilidad conforme al §9.8.
- La clave privada y el certificado únicamente pueden utilizarse durante el período de validez del certificado. Concluido dicho período, o revocado el certificado, cesa toda posibilidad de uso legítimo.
- El uso de la clave privada requiere su activación previa mediante los datos de activación del §6.4, bajo control exclusivo del Titular. Cada operación de firma exige una autorización específica del Titular, conforme al §6.2.8.

4.5.2. Uso de la clave pública por terceros 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 o la lista de revocación, conforme al §4.9.6 y al §4.9.10.

c) Verificar que el certificado se encontraba vigente en la fecha de la firma, mediante sello de tiempo cualificado cuando la verificación sea posterior a su expiración.

d) Comprobar que el uso del certificado se corresponde con el previsto en el §1.4.1 y con los límites establecidos en la Política de Certificación aplicable.

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

La parte que confía debe notificar a **DIGITO** cualquier incidencia que detecte en relación con un certificado emitido, conforme al §4.9.2.

Estas comprobaciones son responsabilidad exclusiva de la parte que confía. Su omisión excluye la condición de tercero de buena fe exento de culpa a los efectos de la Normativa Vigente y de las limitaciones de responsabilidad del §9.8.

La parte que confía queda sujeta a la Política de Certificación y a la presente Declaración en la versión publicada en el repositorio al momento de practicar la verificación.

4.6. Renovación del certificado

DIGITO no practica la renovación de certificados en ninguna de sus modalidades.

A los efectos de la presente Declaración, se entiende por renovación la emisión de un certificado nuevo al mismo Titular conservando el par de claves del certificado anterior, conforme a la cláusula 6.3.6 de la norma ETSI EN 319 411-1.

La obtención de un certificado nuevo por un Titular que ya lo tuviere, sea por expiración del anterior, por su revocación o por cualquier otra causa, se sujeta íntegramente al procedimiento de solicitud y registro del §4.1, con verificación completa de la identidad conforme al §3.2.3 y generación de un par de claves nuevo conforme al §6.1.1.

El certificado anterior, de encontrarse vigente, no resulta afectado por la emisión del nuevo, y conservará su validez hasta la expiración de su período o hasta su revocación conforme al §4.9.

4.7. Renovación de claves del certificado (re-key)

DIGITO no practica la renovación de claves como procedimiento del ciclo de vida del certificado.

A los efectos de la presente Declaración, se entiende por renovación de claves la emisión de un certificado nuevo al mismo Titular con un par de claves nuevo, conforme a la cláusula 6.3.7 de la norma ETSI EN 319 411-1. En el modelo operativo de **DIGITO** dicha operación no constituye un procedimiento diferenciado, sino una nueva emisión sujeta al §4.1.

Todo certificado emitido por **DIGITO** comporta la generación de un par de claves nuevo y exclusivo. En ningún caso se emite un certificado conservando el par de claves de otro anterior, ni se reutiliza un par de claves entre certificados.

Lo anterior se entiende sin perjuicio del cambio de claves de las Autoridades de Certificación, que se rige por el §5.6 y no constituye renovación de claves de entidad final.

4.8. Modificación del certificado

Un certificado emitido no admite modificación de su contenido.

La naturaleza del certificado como objeto firmado criptográficamente determina que toda alteración de los datos en él consignados invalide la firma de la Autoridad de Certificación emisora. En consecuencia, **DIGITO** no practica la modificación de certificados.

Toda alteración de los datos consignados en un certificado exige su revocación conforme al §4.9 y la emisión de un certificado nuevo, sujeta al procedimiento de registro del §4.1.

4.9. Revocación de certificados

La revocación es el proceso de invalidar un certificado con anterioridad a la fecha de su expiración. Practicada, es definitiva e irreversible.

DIGITO no practica la suspensión de certificados conforme al §4.9.13.

4.9.1. Circunstancias para la revocación

DIGITO revocará un certificado cuando concurra alguna de las circunstancias siguientes:

a) A solicitud del Titular, en cualquier momento y sin necesidad de justificación.

b) Uso indebido del certificado, entendido como su utilización incorrecta, ilegal o fraudulenta, incluida la falsificación de identidad y la realización de transacciones no autorizadas.

c) Vulneración, sospecha de vulneración o exposición de la clave privada o de los datos de activación del §6.4, o pérdida de control de la clave privada. La sola pérdida de los datos de activación, sin indicio de vulneración, se rige por el §6.4.2.

d) Modificación de los datos consignados en el certificado, de forma que dejen de ser exactos, conforme al §4.8.1.

e) Confirmación de que alguna información o hecho contenido en el certificado es falso, conforme a la **Normativa Vigente**.

f) Incumplimiento por el Titular de las políticas, términos y condiciones establecidos por **DIGITO**.

g) Fallecimiento del Titular, o declaración judicial de su incapacidad o de la restricción de su capacidad.

h) Pérdida de cumplimiento normativo o técnico del certificado o de la Autoridad de Certificación emisora, incluida la degradación de los algoritmos o longitudes de clave empleados.

i) Falta de aceptación del certificado por el Titular dentro del plazo que indique la plataforma.

j) Cese de actividades de **DIGITO** conforme al §5.8, o terminación del acuerdo de vinculación conforme al §4.11.

k) Resolución del INDOTEL o de autoridad judicial o administrativa competente.

l) Falta de atestación periódica del §4.9.14, en las clases cuya Política la prevea, transcurrido el plazo de subsanación

En las clases de certificado cuya Política de Certificación prevea atributos organizacionales, constituyen asimismo causal de revocación: el cese del vínculo institucional del Titular; la modificación del cargo o función consignada; la modificación de la razón social o del identificador de la persona jurídica; su extinción, disolución o liquidación; y la constatación de inautenticidad de la documentación organizacional aportada.

Las causales operan con independencia del procedimiento en cuyo curso **DIGITO** haya tomado conocimiento de ellas.

El deber de revocar de **DIGITO** se activa por el conocimiento de la causal, con independencia de la fuente de la que provenga y de la existencia o no de culpa de **DIGITO** o del Titular, y no es susceptible de limitación ni exclusión por acuerdo entre las partes.

4.9.2. Quién puede solicitar la revocación

Están legitimados para solicitar la revocación:

a) El Titular del certificado, en cualquier momento y sin necesidad de justificación, así como un tercero que actúe en su nombre y representación legal, conforme a la **Normativa Vigente**.

b) El Solicitante Autorizado de la persona jurídica, en las clases cuya Política así lo prevea, aportando justificación documental de la causal invocada.

c) DIGITO, de oficio, al tomar conocimiento de la concurrencia de cualquiera de las causales del §4.9.1. En este supuesto la revocación no requiere solicitud ni consentimiento del Titular, y se practica con independencia de su voluntad.

d) El INDOTEL, así como la autoridad judicial o administrativa competente, mediante resolución que así lo ordene.

Toda solicitud se autentica conforme al §3.4 y se tramita conforme al §4.9.3.

4.9.3. Procedimiento de solicitud de revocación

El procedimiento se encuentra disponible de forma ininterrumpida, veinticuatro horas al día los siete días de la semana.

Recibida la solicitud, **DIGITO** comprueba que procede de fuente legitimada conforme al §4.9.2 y la auténtica conforme al §3.4, con anterioridad a practicar la revocación.

Verificada la legitimación, **DIGITO** practica la revocación, pública el estado dentro del plazo del §4.9.5 y notifica al Titular, salvo imposibilidad material.

Cuando concurran indicios razonables de compromiso de la clave privada y no resulte posible completar la autenticación del solicitante, **DIGITO** practicará la revocación de forma preventiva conforme al §3.4.

Toda solicitud, sea estimada o desestimada, se registra conforme al §5.4.1 con identificación del solicitante, de la causal invocada y de la resolución adoptada.

La solicitud de revocación puede presentarse por los canales siguientes:

a) Plataforma de DIGITO. Es el canal principal para el Titular, previa autenticación conforme al §3.4, y permite la revocación inmediata.

b) Correo electrónico a soporte@digito.do. Para el Titular que no disponga de acceso a la plataforma, para el reporte de compromiso de clave o de uso

indebido por parte de terceros, y para el INDOTEL y las autoridades competentes.

Ambos canales se encuentran disponibles de forma ininterrumpida. Las comunicaciones recibidas por correo electrónico generan alerta inmediata al personal en rol de confianza, y el plazo del §4.9.5 se computa desde su recepción.

El procedimiento operativo detallado se publica en el repositorio conforme al §2.2.

4.9.4. Período de gracia de la solicitud

No se establece período de gracia. El Titular debe solicitar la revocación de forma inmediata desde que tenga conocimiento de la concurrencia de cualquiera de las causales del §4.9.1, y en todo caso dentro de las **veinticuatro (24) horas** siguientes.

El incumplimiento genera la responsabilidad prevista en la Normativa Vigente frente a los terceros de buena fe exentos de culpa que hubieren confiado en el contenido del certificado.

Este plazo obliga al Titular y no condiciona ni retrasa el deber de revocar de **DIGITO**, que se rige por el §4.9.5.

4.9.5. Plazo de procesamiento por la AC

DIGITO procesa las solicitudes al momento de su recepción, y publica el estado de revocación en un plazo máximo de **veinticuatro (24) horas** contadas desde la recepción, conforme a la **Normativa Vigente.** La revocación es efectiva inmediatamente después de su publicación.

El plazo corre desde la recepción de la solicitud o desde que **DIGITO** toma conocimiento de la causal por cualquier medio, y no se suspende ni se interrumpe por la tramitación de ningún otro procedimiento relativo al mismo certificado, ni por plazo de subsanación alguno.

El servicio de recepción y procesamiento de solicitudes de revocación se encuentra disponible de forma ininterrumpida, veinticuatro horas al día los siete días de la semana.

La revocación es irreversible. Practicada, no cabe su reversión ni la reactivación del certificado, dado que Digito no ofrece suspensión conforme al §4.9.13.

4.9.6. Obligación de comprobación por terceros que confían

Las partes que confían deben comprobar el estado de revocación con anterioridad a otorgar efectos a un certificado, mediante el servicio OCSP indicado en la extensión *authorityInformationAccess* o mediante la lista de revocación indicada en *cRLDistributionPoints*.

La respuesta OCSP es la fuente preferente, por reflejar el estado sin retardo derivado de almacenamiento en caché.

La verificación comprende, además del estado de revocación, la validación de la cadena de certificación hasta el certificado raíz de **DIGITO**, la vigencia del certificado en la fecha de la firma y la adecuación del uso al previsto en el §1.4.1.

La omisión de estas verificaciones excluye la condición de tercero de buena fe exento de culpa a los efectos de la Normativa Vigente y de las limitaciones de responsabilidad del §9.8.

4.9.7. Frecuencia de emisión de la CRL

El régimen difiere según la Autoridad de Certificación emisora:

> **a) Autoridad de Certificación Subordinada**. Emite y publica listas de revocación con una periodicidad de **seis (6) horas**, con independencia de que se hayan practicado o no revocaciones en el período. Cada lista se emite con un campo *nextUpdate* cuyo valor no exceda de **tres (3) días**, y con una antelación no inferior a **diez (10) minutos** respecto de la expiración de la lista precedente.
>
> **b) Autoridad de Certificación Raíz**. Por permanecer permanentemente fuera de línea conforme al §6.7, emite listas de revocación en el marco de una ceremonia documentada conforme al §5.2.2. Cada lista se emite con un campo *nextUpdate* cuyo valor no exceda de **un (1) año**, y la lista siguiente se emite con una antelación no inferior a **treinta (30) días** respecto de la expiración de la precedente.

DIGITO emitirá adicionalmente una lista de revocación de la Autoridad de Certificación Raíz, con carácter extraordinario y en ceremonia convocada al efecto, cuando se practique la revocación del certificado de una Autoridad de Certificación Subordinada o cuando concurra alguna de las circunstancias del §5.7.3.

4.9.8. Latencia máxima de la CRL

El intervalo máximo entre la práctica de una revocación y su reflejo en la lista publicada no excede de **seis (6) horas** en la Autoridad de Certificación Subordinada, sin perjuicio del plazo de **veinticuatro (24) horas** del §4.9.5.

En la Autoridad de Certificación Raíz, la revocación del certificado de una Autoridad de Certificación Subordinada da lugar a la emisión extraordinaria del §4.9.7, literal b), dentro del plazo del §4.9.5.

La información de estado de revocación se mantiene disponible más allá del período de validez del certificado, conforme al requisito CSS-6.3.10-02 de la norma ETSI EN 319 411-2. A tal efecto, los certificados revocados no se retiran de la lista una vez expirados, y la lista incorpora la extensión *ExpiredCertsOnCRL* prevista en la Recomendación UIT-T X.509, con fecha coincidente con el inicio de validez del certificado de la Autoridad de Certificación emisora. La conservación abarca la totalidad de los certificados emitidos desde el inicio de la operación.

4.9.9. Disponibilidad de comprobación en línea (OCSP)

DIGITO opera un servicio de consulta del estado mediante el protocolo OCSP, conforme al IETF RFC 6960, cuya localización se consigna en la extensión *authorityInformationAccess* de cada certificado emitido, en cumplimiento de la Normativa Vigente.

El servicio se presta respecto de los certificados emitidos por las Autoridades de Certificación Subordinadas. El estado de los certificados emitidos por la Autoridad de Certificación Raíz se consulta exclusivamente mediante la lista de revocación del §4.9.7, literal b), dada su condición permanentemente fuera de línea.

Las características operativas y la disponibilidad se establecen en el §4.10.

4.9.10. Requisitos de comprobación en línea

La parte que confía debe verificar la firma de la respuesta OCSP y la validez del certificado del respondedor, cuya cadena se incorpora en la propia respuesta.

La comprobación se practica mediante el servicio OCSP indicado en la extensión *authorityInformationAccess* del certificado, o mediante la lista de revocación publicada en el punto indicado en la extensión *cRLDistributionPoints*. La respuesta OCSP es la fuente preferente, por reflejar el estado sin retardo.

Las partes que confían no otorgarán efectos a un certificado respecto del cual el servicio devuelva el estado '*unknown*'. Dicho estado no equivale a la ausencia de revocación y no permite tener por válido el certificado.

Tratándose de firmas cuya validez deba acreditarse con posterioridad al período de validez del certificado, la parte que confía debe conservar la información de estado obtenida al momento de la verificación, o disponer de un sello de tiempo cualificado que acredite que la firma fue generada durante la vigencia.

4.9.11. Otras formas de divulgación de la revocación

DIGITO notifica al Titular la revocación de su certificado conforme al §4.9.2, sin que dicha notificación constituya mecanismo de divulgación frente a terceros ni sustituya la comprobación exigida por el §4.9.10.

No se estipulan formas de divulgación del estado de revocación distintas del servicio OCSP del §4.9.9 y de las listas de revocación del §4.9.7.

4.9.12. Requisitos especiales por compromiso de clave

En los casos que aplique, el compromiso, la sospecha de compromiso o la pérdida de control de la clave privada del Titular constituye causal de revocación conforme al §4.9.1, literal c), y debe ser comunicada a **DIGITO** de forma inmediata conforme al §4.9.4.

El compromiso de la clave privada de una Autoridad de Certificación, así como la constatación de que los algoritmos o longitudes de clave empleados han dejado de garantizar la vinculación entre el Titular y su clave pública, determinan la revocación de la totalidad de los certificados afectados y la activación del procedimiento del §5.7.3.

En tal supuesto Digito notificará de forma inmediata al INDOTEL, a los Titulares afectados y, mediante publicación en su repositorio, a las partes que confían, indicando el alcance de los certificados afectados, la fecha desde la cual las firmas generadas no pueden considerarse fiables y las medidas adoptadas.

El procedimiento operativo, incluidos los plazos de activación y la generación de la última lista de revocación, se establece en el §5.7.3.

4.9.13. Circunstancias para la suspensión

DIGITO no practica la suspensión de certificados. No se estipulan circunstancias que den lugar a la suspensión.

La revocación practicada conforme al §4.9 es definitiva e irreversible, y no admite reactivación del certificado. La obtención de un certificado nuevo tras una revocación se sujeta al procedimiento de registro completo conforme al §3.3.2.

4.9.14. Atestación periódica de la Organización Vinculada

Con periodicidad semestral, para los tipos de certificados aplicables, la Organización Vinculada confirmará, por conducto de su Solicitante Autorizado y a través de la plataforma de **DIGITO**, la exactitud del listado de Titulares vinculados a la organización, de sus vínculos institucionales vigentes y de los cargos consignados en sus certificados.

La atestación constituye declaración expresa de la Organización Vinculada sobre la exactitud de la información consignada. Su otorgamiento renueva la ventana de reutilización de la evidencia del vínculo y del cargo conforme al §3.2.7.

La falta de atestación, transcurrido el requerimiento y el plazo de subsanación de **quince (15) días** naturales, constituye causal de revocación de los certificados afectados conforme al §4.9.1, literal l). **DIGITO** notificará a la Organización Vinculada y a los Titulares afectados con anterioridad a la revocación.

La atestación no exonera a la Organización Vinculada de su obligación de notificar de forma inmediata cualquier modificación, conforme al §9.6.3, ni desplaza el deber de revocar de **DIGITO** conforme al §4.9.2.

La revisión de la atestación y de la documentación justificativa de las modificaciones relativas a la persona jurídica, al vínculo institucional o al cargo corresponde al Verificador de Organizaciones. La tramitación de la revocación que de ello resulte corresponde al Operador de Registro conforme al §4.9.3.

4.10. Servicios de estado del certificado

DIGITO pone a disposición de las partes que confían dos mecanismos de consulta del estado de los certificados: el servicio OCSP y las listas de revocación.

4.10.1. Características operativas

El servicio OCSP opera conforme al protocolo definido en el IETF RFC 6960. Las respuestas se generan en el momento de la consulta y son firmadas por un respondedor cuyo certificado es emitido por la Autoridad de Certificación emisora de los certificados sobre los que informa.

El servicio de consulta en línea del estado mediante el protocolo OCSP se presta respecto de los certificados emitidos por las Autoridades de Certificación Subordinadas de **DIGITO**.

El estado de los certificados emitidos por la Autoridad de Certificación Raíz —esto es, los certificados de las Autoridades de Certificación Subordinadas— se consulta exclusivamente mediante la lista de revocación publicada conforme al §2.3, literal b.2). Dicha limitación obedece a la condición permanentemente fuera de línea de la Autoridad de Certificación Raíz.

Las respuestas incorporan el certificado del respondedor y su cadena de certificación, a fin de que las partes que confían puedan verificarlas sin necesidad de obtener información adicional.

Las respuestas no incorporan el campo *nextUpdate*, indicando así que la información de estado se encuentra disponible de forma continua y que no procede su almacenamiento en caché. En consecuencia, la revocación es efectiva frente a las consultas en línea desde el momento de su publicación conforme al §4.9.5.

El respondedor devuelve el estado unknown respecto de los números de serie que no consten en su base de información. **DIGITO** no emite en ningún caso respuestas de estado good respecto de números de serie no emitidos por sus Autoridades de Certificación.

Las listas de revocación se emiten y publican conforme al §4.9.7, y conservan las entradas de los certificados revocados con posterioridad a su expiración conforme al §4.9.8.

El perfil técnico de las respuestas OCSP se establece en el §7.3, y el de las listas de revocación en el §7.2.

4.10.2. Disponibilidad del servicio

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 %) medida 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 a la Normativa Vigente, sujeta al calendario de mantenimiento programado del párrafo siguiente.

Los mantenimientos que afecten a los servicios de certificación (emisión, revocación, repositorio, servicio de consulta del estado, listas de revocación y sellado de tiempo), aunque afecten también a otros servicios de la plataforma, se anuncian en la sección «Mantenimientos» del sitio web de DIGITO con una antelación mínima de cinco (5) días hábiles. Se realizan preferentemente en horarios de menor actividad, con una duración máxima de cuatro (4) horas por ventana y de ocho (8) horas acumuladas por mes. Cada aviso indica la fecha y la hora de inicio y fin con su zona horaria, los servicios afectados y no afectados, el motivo, el estado (programado, en curso o completado) y el contacto de soporte, y se actualiza si la ventana se extiende o se cancela. Cada mantenimiento queda registrado con su aviso, sus horas reales de inicio y fin y su resultado. DIGITO informa al INDOTEL de las interrupciones que excedan los límites anteriores o comprometan la prestación del servicio. Las interrupciones programadas anunciadas conforme a este párrafo no constituyen incidente de seguridad significativo, conforme al requisito REQ-7.9.3-08 de la norma ETSI EN 319 401. Los mantenimientos que solo afecten a los demás servicios de la plataforma se rigen por los Términos de uso de la plataforma.

El acceso es gratuito y no requiere registro ni autenticación previa de la parte que confía, conforme al §9.1.3.

El frontal del servicio opera sobre infraestructura de un proveedor de distribución de contenido, sujeto al §5.3.7. **DIGITO** mantiene configurada dicha infraestructura de modo que no se almacene en caché ninguna respuesta del servicio de consulta del estado, a fin de preservar lo establecido en el §4.10.1.

La información de estado se mantiene disponible durante toda la vida operativa de la Autoridad de Certificación emisora, y con posterioridad al cese de actividades de **DIGITO** en los términos del §5.8.

4.10.3. Funciones opcionales

No se estipulan funciones opcionales del servicio de consulta del estado.

DIGITO no emplea la extensión *ArchiveCutOff* prevista en el IETF RFC 6960, por cuanto la disponibilidad de la información de estado con posterioridad a la expiración del certificado se provee mediante la conservación de las entradas en las listas de revocación conforme al §4.9.8.

4.11. Fin de la Suscripción

La suscripción concluye por cualquiera de las causas siguientes:

a) Expiración del certificado por transcurso de su período de validez.

b) Revocación del certificado conforme al §4.9.

c) Terminación del acuerdo de vinculación. El Suscriptor, que es el propio Titular, la Organización Vinculada cuando intervenga y DIGITO podrán terminarlo con el preaviso que establezca la Normativa Vigente o, en su caso, el pactado entre las partes. Vencido el preaviso, DIGITO revocará los certificados que se encuentren pendientes de expiración.

d) Cese de actividades de **DIGITO** conforme al §5.8.

En el supuesto del literal a), el certificado caduca por el solo transcurso del plazo, sin que proceda ni sea necesaria su revocación y sin que Digito deba practicar acto alguno. La expiración no se refleja en las listas de revocación ni en las respuestas del servicio de estado, por no constituir revocación.

Concluida la suscripción, la obtención de un certificado nuevo se sujeta al procedimiento de registro completo del §4.1. No cabe la renovación de un certificado caducado ni revocado, conforme a los §4.6 y §4.7.

La conclusión de la suscripción no extingue las obligaciones de conservación de **DIGITO** conforme al §5.5.2, ni la disponibilidad de la información de estado conforme al §4.10.2, ni las responsabilidades del Titular respecto de los actos realizados durante la vigencia del certificado.

4.12. Custodia y recuperación de claves

DIGITO no ofrece servicios de custodia ni de recuperación de claves.

4.12.1. Política y prácticas de custodia y recuperación de claves

DIGITO no deposita en custodia ni recupera claves privadas de firma de entidades finales.

Las claves privadas asociadas a los certificados emitidos se generan en un dispositivo cualificado de creación de firma, no son extraíbles y se mantienen bajo control exclusivo del Titular conforme al §6.2.8. En consecuencia, **DIGITO** no dispone de mecanismo alguno que le permita acceder a dichas claves, reproducirlas o recuperarlas, ni siquiera a instancia del propio Titular o por requerimiento de autoridad.

La pérdida de los datos de activación por el Titular determina la imposibilidad de utilizar la clave privada asociada mientras no se establezcan datos de activación nuevos conforme al §6.4.2. Cuando concurra vulneración, sospecha de vulneración o exposición, constituye causal de revocación conforme al §4.9.1,

literal c), y la obtención de un certificado nuevo se sujeta al procedimiento de registro del §4.1.

Lo anterior se entiende sin perjuicio del respaldo de las claves privadas de las Autoridades de Certificación conforme al §6.2.4, que no constituye custodia de claves de entidad final.

4.12.2. Política y prácticas de encapsulación y recuperación de claves de sesión

Los certificados emitidos por **DIGITO** se destinan a la firma electrónica conforme al §1.4.1, y no se emplean para el cifrado de información ni para el establecimiento de claves de sesión.

5. CONTROLES DE INSTALACIONES, GESTIÓN Y OPERATIVOS

5.1. Controles Fisicos

Los servicios de certificación de **DIGITO** se soportan sobre una infraestructura mixta. Los dispositivos criptográficos que albergan las claves privadas de las Autoridades de Certificación, así como el sistema de gestión de la activación de las claves de los Titulares, se alojan en un centro de datos situado en la República Dominicana y operado por un tercero. Los restantes componentes aplicativos se alojan en infraestructura de nube.

Los controles de seguridad física del emplazamiento son ejecutados por el operador del centro de datos conforme a sus propios procedimientos y certificaciones. Los controles de acceso a las jaulas en que se ubican los dispositivos criptográficos son ejecutados por **DIGITO,** conforme al §5.1.2.

DIGITO verifica el cumplimiento de los controles a cargo de terceros mediante la revisión de sus certificaciones e informes de auditoría independiente, en los términos del §5.3.7, y conserva la responsabilidad sobre la seguridad física de la infraestructura que soporta sus servicios.

5.1.1. Ubicación y construcción del emplazamiento

Los sistemas que soportan los servicios de certificación de **DIGITO** se alojan en instalaciones que cumplen los requisitos siguientes:

a) Se sitúa en ubicación sin riesgos significativos derivados de amenazas naturales o del entorno, y su construcción resiste las amenazas ambientales previsibles.

b) Dispone de perímetro de seguridad física definido, con barreras que impiden el acceso no autorizado.

c) Establece áreas de seguridad diferenciadas mediante jaulas de acceso independiente. Los dispositivos criptográficos de la Autoridad de Certificación Raíz se ubican en una jaula distinta y físicamente separada de aquella en que se ubican los de las Autoridades de Certificación Subordinadas, de modo que el acceso a una no habilita el acceso a la otra.

d) El operador garantiza suministro eléctrico redundante, control ambiental y sistemas de detección y extinción de incendios, conforme a los §5.1.3 a §5.1.5.

Cuando **DIGITO** recurra a instalaciones operadas por terceros, éstas quedarán sujetas a los mismos requisitos y a las obligaciones del §5.3.7.

La ubicación concreta de las instalaciones no se divulga, por constituir información cuya reserva es necesaria para su propia protección.

5.1.2. Acceso físico

a) El acceso al recinto del centro de datos se rige por los procedimientos de control de acceso de su operador, que registra la identidad de toda persona que accede, así como la fecha y hora de entrada y salida.

b) El acceso a las jaulas de **DIGITO** requiere, adicionalmente, autorización expresa de **DIGITO** conforme a la lista de personal autorizado que ésta mantiene y comunica al operador del centro de datos.

c) El acceso a las jaulas de **DIGITO** por parte del personal del operador del centro de datos, en ejercicio de sus funciones de mantenimiento de la infraestructura, requiere notificación previa a **DIGITO,** queda registrado por el operador y se comunica a **DIGITO** con indicación de la fecha, hora y motivo. **DIGITO** verifica la integridad de los precintos de seguridad con posterioridad a todo acceso de esta naturaleza.

d) Los racks en que se alojan los dispositivos criptográficos se mantienen cerrados mediante cerradura de doble llave y precintados con precintos de seguridad numerados, cuyo registro mantiene **DIGITO.** El personal del operador del centro de datos no dispone de las llaves de dichos racks ni de acceso alguno a los dispositivos criptográficos.

e) El uso de la clave privada de una Autoridad de Certificación requiere, en todo caso, la concurrencia de los componentes de activación previstos en el §6.2.2, que se custodian fuera del centro de datos conforme al §5.1.6 y se

encuentran bajo control exclusivo de **DIGITO**. En consecuencia, el acceso físico a la jaula o al recinto no habilita el acceso a las claves privadas ni su utilización.

f) No se admite la prestación de servicios de asistencia técnica remota por personal del operador del centro de datos sobre los racks en que se alojan los dispositivos criptográficos. Dichos servicios podrán prestarse respecto de los restantes equipos de **DIGITO** alojados en el centro de datos.

g) El acceso a la jaula en que se ubica el dispositivo de la Autoridad de Certificación Raíz y Emisora requiere la presencia simultánea de al menos dos personas en roles de confianza, conforme al §5.2.2, y se practica únicamente en el marco de una ceremonia documentada.

h) Todo acceso a las jaulas de **DIGITO** se registra en el sistema del operador del centro de datos y en el registro propio de **DIGITO**. Ambos registros se conservan conforme al §5.5.2.

i) Los visitantes y el personal externo acceden únicamente previa autorización de **DIGITO**, quedan identificados y permanecen acompañados durante toda su estancia.

j) La lista de personal autorizado se revisa periódicamente y las autorizaciones se revocan de forma inmediata al cesar el motivo que las justificó, comunicándolo al operador del centro de datos sin dilación.

5.1.3. Energía y aire acondicionado

El operador garantiza suministro eléctrico redundante, con sistemas de alimentación ininterrumpida capaces de sostener la operación durante el tiempo necesario para el cierre ordenado o la conmutación a la fuente alternativa.

Los sistemas de control ambiental mantienen temperatura y humedad dentro de los márgenes de operación de los equipos, con monitorización continua y generación de alertas.

5.1.4. Exposición al agua

Las instalaciones se sitúan y construyen de modo que se minimice el riesgo de daño por agua, y cuentan con mecanismos de detección de presencia de agua con generación de alerta.

5.1.5. Prevención y protección contra incendios

Las instalaciones cuentan con sistemas de detección temprana y con medios de extinción adecuados a los equipos protegidos, que no comprometen su integridad ni la de los soportes de información. Los sistemas se someten a revisión y mantenimiento periódicos.

5.1.6. Almacenamiento de soportes

Los soportes que contengan respaldos de claves privadas de Autoridades de Certificación, componentes de activación de los dispositivos criptográficos, llaves de las cerraduras de los racks y documentación de las ceremonias de claves se almacenan en contenedores de seguridad bajo control directo de **DIGITO**, en ubicación distinta de aquella en que se encuentran los dispositivos criptográficos.

Los soportes se inventarían, se etiquetan conforme a la clasificación de información aplicable y su acceso queda registrado, restringido a los roles de confianza que lo requieran.

Los soportes que contengan información sensible se protegen frente a acceso, daño y degradación durante todo el período en que deban conservarse conforme al §5.5.2.

Los soportes que contengan respaldos de claves privadas de Autoridades de Certificación, componentes de activación de los dispositivos criptográficos y documentación de las ceremonias de claves se almacenan en contenedores de seguridad bajo control directo de **DIGITO**, en ubicación distinta de aquella en que se encuentran los dispositivos criptográficos.

5.1.7. Eliminación de residuos

Los dispositivos criptográficos que hubieren contenido claves privadas de Autoridades de Certificación se someten al procedimiento de cambio de estado previsto en el §6.2.10 con anterioridad a su retirada, y su destrucción se documenta en acta suscrita por dos personas en roles de confianza.

5.1.8. Respaldo externo

DIGITO mantiene copias de respaldo de la información necesaria para la continuidad del servicio en ubicación distinta de la principal, con separación geográfica suficiente para que un mismo evento no afecte a ambas.

Las copias se protegen con los mismos controles de seguridad física y lógica aplicables a la ubicación principal, y su integridad y capacidad de restauración se verifican periódicamente conforme al §5.7.4.

El procedimiento de respaldo, su periodicidad y las pruebas de restauración se establecen en el §5.1.8 y en el §5.7.4.

5.2. Controles Procedimentales

Los controles procedimentales de **DIGITO** tienen por objeto asegurar que las operaciones críticas de los servicios de certificación se ejecutan por personal expresamente designado, en roles con responsabilidades definidas, y con la concurrencia de más de una persona cuando la naturaleza de la operación lo requiera.

5.2.1 Roles de confianza

Son roles de confianza aquellos cuyas funciones pueden afectar de forma significativa a la seguridad, la integridad o la fiabilidad de los servicios de certificación prestados por **DIGITO**, y en particular a la generación, custodia y uso de las claves privadas de las Autoridades de Certificación, a la verificación de la identidad de los solicitantes, a la emisión y revocación de certificados, y a la gestión de los registros de auditoría.

DIGITO ha establecido los roles siguientes:

a) Autoridad de Políticas. Aprueba la presente Política y la Declaración de Prácticas de Certificación, y dictamina sobre su idoneidad conforme al §1.5.3.

b) Oficial de Seguridad de la Información. Responsable de la implantación y supervisión de las políticas de seguridad, y de la gestión de incidentes.

c) Responsable de Tecnología. Responsable de la operación, configuración y mantenimiento de los sistemas que soportan los servicios de certificación.

d) Operador de Registro. Practica la verificación de la identidad de los Titulares y de los Solicitantes Autorizados conforme al §3.2.3; aprueba o rechaza las solicitudes de emisión, comprobando que constan completas en el expediente todas las verificaciones aplicables; y tramita las solicitudes de revocación.

d bis) Verificador de Organizaciones. Práctica la verificación de la existencia y vigencia de la persona jurídica, de la razón social, del vínculo

institucional y del cargo del Titular, y de la facultad del Solicitante Autorizado, conforme a los §3.2.2 y §3.2.5, y revisa la documentación justificativa de las causales de revocación de naturaleza organizacional. No aprueba solicitudes de emisión ni ejecuta operaciones de emisión o revocación.

e) Operador de la Autoridad de Certificación. Ejecuta las operaciones sobre los dispositivos criptográficos y sobre los sistemas de emisión, incluidas las ceremonias de claves.

f) Auditor Interno. Revisa los registros de auditoría y verifica la conformidad de las operaciones con la presente Política y con la Declaración de Prácticas de Certificación.

La designación requiere la verificación previa de antecedentes conforme al §5.3.2 y la formación del §5.3.3, y queda documentada de forma expresa.

La designación nominal de las personas que desempeñan cada rol consta en el registro interno de designaciones de **DIGITO** y no forma parte de la presente Declaración.

5.2.2. Número de personas requeridas por tarea

Requieren la participación simultánea de más de una persona en roles de confianza:

a) La generación, activación, respaldo, restauración y destrucción de las claves privadas de las Autoridades de Certificación, que requiere la concurrencia de un quorum de portadores de componentes de activación, conforme al §6.2.2.

b) El acceso físico a la jaula de la Autoridad de Certificación Raíz, conforme al §5.1.2, literal e).

c) La emisión de listas de revocación de la Autoridad de Certificación Raíz, ordinaria y extraordinaria, conforme al §4.9.7, literal b).

d) La modificación de los perfiles de certificado y de la configuración de las Autoridades de Certificación.

e) La primera designación de un Solicitante Autorizado de una organización, en las clases cuya Política así lo prevea, que requiere la verificación por el Verificador de Organizaciones y la aprobación por un Operador de Registro distinto, conforme al §3.2.5

Las ceremonias se documentan en acta suscrita por todos los intervinientes, con indicación de las operaciones practicadas, que se conserva conforme al §5.5.2.

5.2.3. Identificación y autenticación para cada rol

El personal en roles de confianza se identifica y autentica con anterioridad al ejercicio de sus funciones, mediante credenciales individuales y no compartidas.

El acceso a los sistemas que soportan los servicios de certificación se somete a autenticación multifactor, y los privilegios se asignan conforme al principio de mínimo privilegio y en función del rol desempeñado.

El Verificador de Organizaciones dispone en el Servicio de Gestión de Usuarios exclusivamente de los privilegios necesarios para registrar el resultado y la evidencia de las verificaciones de los §3.2.2 y §3.2.5, sin privilegios de aprobación, emisión o revocación de certificados.

Toda operación queda registrada con identificación del individuo que la practicó, conforme al §5.4.1. No se admite el uso de cuentas genéricas o compartidas para funciones propias de roles de confianza.

El acceso a los dispositivos criptográficos requiere, adicionalmente, la autenticación mediante los componentes de activación previstos en el §6.2.8.

5.2.4. Roles que exigen separación de funciones

DIGITO establece la separación de funciones entre los roles siguientes, de modo que una misma persona no pueda desempeñarlos simultáneamente:

a) El Auditor Interno no desempeña ningún otro rol de confianza, ni participa en las operaciones que revisa.

b) El Operador de Registro que practica la verificación de identidad no aprueba su propia verificación cuando el procedimiento exija doble control.

c) El Responsable de Tecnología no desempeña simultáneamente funciones de Operador de Registro ni de Verificador de Organizaciones.

d) Quien administra los sistemas de registro de auditoría no dispone de privilegios para modificar o suprimir sus contenidos, conforme al §5.4.4.

e) El Verificador de Organizaciones no desempeña simultáneamente funciones de Operador de Registro.

f) Quien verifica la facultad de un Solicitante Autorizado en su primera designación no aprueba dicha designación.

Cuando por razones organizativas una misma persona deba desempeñar más de un rol de confianza, dicha acumulación se documenta expresamente, se somete a autorización de la Autoridad de Políticas y se compensa con controles adicionales de supervisión.

5.3 Controles de personal

DIGITO aplica a su personal controles orientados a asegurar que quienes intervienen en la prestación de sus servicios reúnen la cualificación necesaria, son dignos de confianza y conocen las obligaciones derivadas de sus funciones.

5.3.1. Cualificación, experiencia y habilitación

El personal en roles de confianza cuenta con la formación, conocimientos y experiencia necesarios para el ejercicio de sus funciones, evaluados con anterioridad a su designación.

DIGITO no asigna funciones propias de roles de confianza a personal que no haya superado la verificación del §5.3.2 y recibido la formación del §5.3.3.

Los criterios específicos de cualificación y experiencia por rol se documentan en el registro interno de designaciones. En particular, el Verificador de Organizaciones acredita formación jurídica o experiencia en la revisión de documentación societaria, registral y tributaria.

5.3.2. Verificación de antecedentes

Con anterioridad a la designación en un rol de confianza, **DIGITO** practica una verificación de antecedentes proporcionada a la responsabilidad del rol, que comprende la comprobación de la identidad, de la trayectoria profesional declarada y de la ausencia de antecedentes penales, dentro de los límites que permita la normativa aplicable.

La verificación se practica igualmente respecto del personal externo que deba desempeñar funciones propias de roles de confianza, conforme al §5.3.7.

La evidencia se conserva conforme al §5.5.2, con sujeción a la normativa de protección de datos personales.

5.3.3. Requisitos de formación

Todo el personal que intervenga en la prestación recibe formación con anterioridad al ejercicio de sus funciones, que comprende al menos:

a) La Política de Certificación aplicable y la presente Declaración, en lo relativo a las funciones del rol.

b) El marco normativo aplicable.

c) Las políticas y procedimientos de seguridad de la información de **DIGITO**

d) Los procedimientos operativos propios del rol, incluidos los de verificación de identidad, emisión y revocación.

e) El procedimiento de gestión de incidentes y el deber de notificación.

f) Las obligaciones en materia de protección de datos personales y de confidencialidad.

Los Operadores de Registro que intervengan en la modalidad asistida del §3.2.3 reciben formación específica sobre detección de documentos falsificados y sobre el procedimiento de acreditación a distancia.

El Verificador de Organizaciones recibe formación específica sobre la documentación admisible por tipo de entidad, la consulta de las fuentes oficiales del Registro Nacional de Contribuyentes y del Registro Mercantil, y la detección de documentación societaria alterada o carente de vigencia.

La formación se documenta y se conserva conforme al §5.5.2.

5.3.4. Frecuencia y requisitos de reciclaje formativo

El personal que desempeña roles de confianza recibe formación de actualización con periodicidad anual.

Se imparte además formación específica y sin sujeción a dicha periodicidad cuando se produzca una modificación sustancial de la presente Política, de la Declaración de Prácticas de Certificación, de los procedimientos operativos o de la

normativa aplicable, así como con ocasión de la incorporación de nuevos sistemas o de la designación en un rol distinto.

DIGITO conserva registro de la formación de actualización impartida.

5.3.5. Frecuencia y secuencia de rotación de puestos

Dada la dimensión de la organización y la especialización requerida por los roles de confianza, **DIGITO** no establece un régimen de rotación de puestos al momento de esta Política de Certificación pudiendo esto cambiar más adelante.

Los riesgos que dicha rotación pudiese mitigar se abordan mediante la separación de funciones del §5.2.4, el control multipersona del §5.2.2 y la revisión independiente del §5.4.

5.3.6. Sanciones por acciones no autorizadas

Las acciones no autorizadas del personal, así como el incumplimiento de las políticas y procedimientos de **DIGITO**, dan lugar a la aplicación del procedimiento disciplinario establecido, y a la suspensión inmediata de los privilegios de acceso cuando la naturaleza de la conducta lo requiera.

Constatada una conducta que pueda afectar a la seguridad o fiabilidad de los servicios, **DIGITO** adopta de forma inmediata las medidas de contención necesarias, incluida la revocación de las autorizaciones de acceso físico y lógico, y activa el procedimiento del §5.7.1.

Lo anterior se entiende sin perjuicio de las responsabilidades civiles y penales que pudieran derivarse.

5.3.7. Requisitos para contratistas independientes

DIGITO recurre a proveedores externos para la prestación de determinados componentes de sus servicios, sujetos a las obligaciones establecidas contractualmente conforme al requisito REQ-6.1-04 de la norma ETSI EN 319 401.

Proveedores que intervienen en la prestación del servicio:

Proveedor	Componente	Régimen aplicable

Operador del centro de datos	Alojamiento de los dispositivos criptográficos y del sistema de gestión de activación	Controles de seguridad física del §5.1
Proveedor de infraestructura en nube	Alojamiento de componentes aplicativos	Controles de seguridad física y lógica
Proveedor de distribución de contenido (CDN)	Frontal del servicio de consulta del estado	Disponibilidad del §4.10.2
Prestador de Sistemas de Pruebas de Identidad	Verificación documental, prueba de vida y reconocimiento facial	Normativa Vigente; ETSI EN 319 401 y ETSI TS 119 461

El personal externo que desempeñe funciones propias de roles de confianza queda sujeto a los mismos requisitos de verificación de antecedentes, formación y confidencialidad exigidos al personal propio, conforme a los §5.3.2 a §5.3.6. El personal externo no desempeña roles de confianza con acceso a las claves privadas de las Autoridades de Certificación.

DIGITO mantiene un registro de proveedores con indicación del componente prestado, de las obligaciones asumidas contractualmente y de las certificaciones y evaluaciones de conformidad aplicables, y verifica con periodicidad anual su vigencia y alcance.

Los contratos con los proveedores comprenden, al menos: obligaciones de confidencialidad, conservación de evidencias, notificación de incidentes de seguridad en plazo determinado, sujeción a las auditorías de **DIGITO** y de los Organismos de Evaluación de la Conformidad, y régimen aplicable a la terminación del contrato.

5.3.8. Documentación suministrada al personal

DIGITO pone a disposición de su personal la documentación necesaria para el ejercicio de sus funciones, que comprende al menos la presente Política, la Declaración de Prácticas de Certificación, las políticas de seguridad de la información, los procedimientos operativos del rol desempeñado y el procedimiento de gestión de incidentes.

El personal acusa recibo de dicha documentación y de sus actualizaciones, y la aceptación queda registrada.

Las condiciones de empleo y las obligaciones de confidencialidad se formalizan por escrito o digital (cuando se firma con firma electrónica cualificada) con anterioridad al inicio de las funciones.

5.4 Procedimientos de registro de auditoría

DIGITO registra los eventos relevantes para la seguridad y la trazabilidad de sus servicios, de modo que sea posible reconstruir con posterioridad las operaciones practicadas, identificar a quien las practicó y determinar el momento en que tuvieron lugar.

5.4.1 Tipos de eventos registrados

Se registran, al menos, los eventos siguientes:

a) El ciclo de vida de las claves de las Autoridades de Certificación: generación, activación, respaldo, restauración, cambio y destrucción, así como toda ceremonia de claves.

b) El ciclo de vida de los certificados: solicitud, verificación de identidad, aprobación o rechazo, emisión, aceptación, revocación y expiración.

c) Las operaciones de verificación de identidad y de atributos organizacionales practicadas, con indicación de la modalidad empleada, del resultado obtenido, de las fuentes consultadas y del Operador de Registro o Verificador de Organizaciones interviniente.

d) El acceso físico a las jaulas y racks en que se alojan los dispositivos criptográficos, así como la verificación de precintos practicada conforme al §5.1.2.

e) Los accesos lógicos a los sistemas que soportan los servicios, incluidos los intentos fallidos de autenticación, y las modificaciones de privilegios.

f) Las modificaciones de configuración de las Autoridades de Certificación, de los perfiles de certificado y de los sistemas de emisión y revocación.

g) La emisión y publicación de listas de revocación y la operación del servicio de consulta del estado.

h) Los incidentes de seguridad detectados y las medidas adoptadas.

i) Los arranques, paradas y fallos de los sistemas, y las operaciones de respaldo y restauración.

Cada registro comprende, al menos, la fecha y hora del evento, su naturaleza, la identidad del sujeto o sistema que lo originó y su resultado.

5.4.2. Frecuencia de procesamiento del registro

Los sistemas de **DIGITO** se someten a monitorización continua y automatizada, mediante mecanismos que procesan los registros de auditoría y generan alertas ante eventos que puedan indicar un incidente de seguridad, conforme a los requisitos REQ-7.9.1-01, REQ-7.9.1-05 y REQ-7.9.1-07 de la norma ETSI EN 319 401.

Las actividades anómalas que indiquen una posible violación de seguridad, incluida la intrusión en la red de **DIGITO**, se detectan y se reportan como alarmas conforme al requisito REQ-7.9.1-03. Los umbrales de alarma se establecen y revisan periódicamente.

Las alertas generadas se atienden conforme al §5.7.1.

Adicionalmente, el Auditor Interno revisa los registros con periodicidad mensual, mediante muestreo de los eventos registrados y examen íntegro de los clasificados como críticos, a fin de identificar tendencias inusuales o no deseadas conforme al requisito REQ-7.9.1-10.

El resultado de cada revisión se documenta, con indicación de las anomalías detectadas y de las medidas adoptadas.

DIGITO mantiene un sistema que monitoriza la disponibilidad de los propios sistemas de monitorización y registro, independiente de los sistemas monitorizados, conforme al requisito REQ-7.9.1-17.

5.4.3. Período de conservación del registro

Los registros de auditoría se conservan en línea durante un período no inferior a **dos (2) meses** desde su generación, y se archivan con posterioridad conforme al §5.5.

El período total de conservación no será inferior al establecido en el §5.5.2, ni al que resulte exigible conforme a la Normativa Vigente al momento de la publicación de esta Declaración de Prácticas de Certificación.

5.4.4 Protección del registro de auditoría

Los registros de auditoría se protegen frente a modificación, supresión y acceso no autorizado, mediante mecanismos que permitan detectar cualquier alteración de su contenido.

El acceso a los registros se restringe al personal en roles de confianza que lo requiera, y toda consulta queda a su vez registrada.

Quien administra los sistemas que generan los registros no dispone de privilegios para modificarlos ni suprimirlos, conforme a la separación de funciones del §5.2.4, literal d).

Los registros se sellan temporalmente conforme al §5.5.5, a fin de acreditar el momento de su generación y su integridad posterior.

5.4.5 Procedimientos de respaldo del registro

Los registros de auditoría se respaldan con periodicidad diaria, y las copias se conservan en la ubicación externa prevista en el §5.1.8, con los mismos controles de protección aplicables a los originales.

La integridad de las copias y su capacidad de restauración se verifican periódicamente.

5.4.6. Sistema de recolección

Los registros de auditoría se recolectan mediante un sistema centralizado bajo control de **DIGITO**, que consolida los eventos generados por los distintos componentes de la infraestructura. La recolección es automática y continua, y no requiere intervención de los sujetos que originan los eventos.

Los registros generados por proveedores externos en la prestación de componentes del servicio, en particular los de acceso físico al centro de datos, se incorporan al sistema de **DIGITO** o se obtienen y conservan conforme a las obligaciones contractuales del §5.3.7.

5.4.7. Notificación al sujeto causante del evento

No estipulado. **DIGITO** no notifica a los sujetos que originan los eventos el hecho de su registro.

El personal y los Titulares son informados con carácter general de que sus operaciones quedan registradas, conforme al §5.3.8 y a los términos y condiciones aplicables, y en los términos previstos en el §9.4.

5.4.8. Evaluaciones de vulnerabilidad

DIGITO practica evaluaciones de vulnerabilidad sobre los sistemas que soportan sus servicios de certificación con periodicidad trimestral, y con ocasión de todo cambio significativo en la infraestructura.

Practica asimismo pruebas de penetración con periodicidad anual, ejecutadas por personal o entidad independiente de quien opera los sistemas evaluados.

Las vulnerabilidades detectadas se clasifican en función de su severidad y se remedian conforme a los plazos establecidos, priorizando aquellas que puedan comprometer las claves privadas de las Autoridades de Certificación o la integridad del proceso de emisión.

El resultado de las evaluaciones y las medidas adoptadas se documentan y se conservan conforme al §5.5.2.

5.5 Archivo de Registros

DIGITO archiva la información generada en la prestación de sus servicios de certificación durante los períodos establecidos en el §5.5.2, de modo que sea posible acreditar con posterioridad las circunstancias de la emisión, el uso y la revocación de los certificados, y sostener el valor probatorio de las firmas generadas con ellos.

5.5.1. Tipos de registros archivados

Se archivan, al menos:

a) Los expedientes de registro de los Titulares, incluida la evidencia de la verificación de identidad, las fuentes consultadas y sus resultados.

b) La evidencia del consentimiento del Titular y de la aceptación de los términos y condiciones, conforme al §4.1.2.

c) Los certificados emitidos, con su contenido íntegro, y las listas de revocación publicadas.

d) Las solicitudes de emisión y revocación, y la resolución recaída sobre cada una.

e) Los registros de auditoría del §5.4.1, una vez concluido su período de conservación en línea.

f) Las actas de las ceremonias de claves y la documentación de las operaciones sobre los dispositivos criptográficos.

g) Las versiones sucesivas de la presente Declaración de Prácticas de Certificación y de todas las Políticas de **DIGITO**, con indicación de su período de vigencia.

h) Los informes de evaluación de conformidad y la documentación de las auditorías practicadas.

i) La documentación relativa a los incidentes de seguridad y a las medidas adoptadas.

5.5.2. Período de conservación del archivo

La información archivada se conserva 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**, conforme a la Normativa Vigente
Expedientes de registro y evidencia de verificación de identidad	**Veinte (20) años**, conforme a la Normativa Vigente
Evidencia del consentimiento y aceptación de términos	**Veinte (20) años**
Solicitudes y resoluciones del ciclo de vida	**Veinte (20) años**
Registros de auditoría	**Diez (10) años**
Actas de ceremonias de claves	Vida operativa de la Autoridad de Certificación más **diez (10) años**
Versiones de la Política y de la Declaración de Prácticas	**Veinte (20) año**s desde el cese de su vigencia

Los períodos anteriores responden a dos obligaciones legales distintas. El registro de certificados emitidos se conserva durante **cuarenta (40) años**, conforme a la Normativa Vigente. Los datos proporcionados por los Titulares y la documentación de apoyo, incluida la evidencia de verificación de identidad, se conservan durante **veinte (20) años**, conforme a la Normativa Vigente.

La extensión `QcRetentionPeriod` de los certificados emitidos conforme a la presente practica de certificacion declara el período de **veinte (20) años**, correspondiente a la conservación de la información de identidad del Titular. Dicha declaración no reduce el período de **cuarenta (40) años** aplicable al registro de certificados emitidos.

DIGITO no conserva los datos personales del Titular por un período superior al exigido, en aplicación del principio de minimización previsto en la Normativa Vigente de protección de datos personales.

5.5.3. Protección del archivo

La información archivada se protege frente a modificación, supresión, acceso no autorizado y degradación durante todo el período de conservación.

El acceso se restringe al personal en roles de confianza que lo requiera y queda registrado. La información que contenga datos personales se conserva con sujeción al §9.4 y a la normativa aplicable.

DIGITO adopta las medidas necesarias para que la información permanezca legible y utilizable durante todo el período de conservación, incluida la migración a nuevos soportes o formatos cuando la obsolescencia tecnológica lo requiera, preservando en tal caso la integridad y el valor probatorio de la información migrada.

5.5.4. Procedimientos de respaldo del archivo

El archivo se respalda periódicamente y las copias se conservan en la ubicación externa prevista en el §5.1.8, con los mismos controles de protección aplicables a los originales.

La integridad de las copias y su capacidad de restauración se verifican con periodicidad anual, y el resultado de la verificación se documenta.

5.5.5. Requisitos de sellado de tiempo de los registros

Los registros archivados incorporan información fiable sobre el momento de su generación.

Los sistemas que soportan los servicios de certificación mantienen su reloj sincronizado con el Tiempo Universal Coordinado (UTC) al menos una vez cada veinticuatro (24) horas, conforme al requisito REQ-7.10-06 de la norma ETSI EN 319 401 y al requisito REV-6.2.4-07 de la norma ETSI EN 319 411-1.

La totalidad de los sistemas emplea fuentes de tiempo sincronizadas entre sí, a fin de permitir la correlación de los registros generados por componentes distintos, conforme al requisito REQ-7.9.1-15 de la norma ETSI EN 319 401.

Se registra el tiempo preciso de los eventos de sincronización de reloj, así como de los eventos significativos de entorno y de gestión de claves, conforme al requisito REQ-7.10-05 de la norma ETSI EN 319 401.

Los registros se protegen frente a supresión o destrucción conforme al §5.4.4, en cumplimiento del requisito REQ-7.10-08 de la norma ETSI EN 319 401.

5.5.6. Sistema de recolección del archivo

El archivo se constituye mediante sistemas bajo control de **DIGITO**, que incorporan la información procedente de los distintos componentes de la infraestructura una vez concluido su período de conservación en línea.

La información generada por proveedores externos que deban archivarse se obtiene y conserva conforme a las obligaciones contractuales del §5.3.7, con anterioridad a la terminación de la relación con dichos proveedores.

5.5.7. Procedimientos de obtención y verificación del archivo

DIGITO puede recuperar la información archivada y verificar su integridad durante todo el período de conservación.

La recuperación se practica a solicitud de persona legitimada, previa verificación de su legitimación, y queda registrada conforme al §5.4.1. Están legitimados el Titular respecto de su propio expediente, el INDOTEL, la autoridad judicial o administrativa competente, y los Organismos de Evaluación de la Conformidad en el ámbito de sus actuaciones.

La verificación de la integridad de la información archivada y de su capacidad de recuperación se practica con periodicidad anual, y el resultado se documenta.

El plazo máximo de atención de las solicitudes de recuperación es de **diez (10) días** hábiles desde la verificación de la legitimación del solicitante.

Dicho plazo no resulta aplicable cuando la normativa o la resolución de la autoridad competente establezcan uno distinto, en cuyo caso prevalecerá este último.

Cuando la recuperación requiera acceso a información conservada en soportes de archivo o la migración de formatos conforme al §5.5.3, el plazo podrá extenderse hasta **veinte (20) días** hábiles, comunicándolo al solicitante.

5.6. Cambio de claves

DIGITO practica el cambio del par de claves de una Autoridad de Certificación con anterioridad a que concluya su período de utilización, de modo que los certificados emitidos bajo la clave saliente no excedan en su período de validez al del propio certificado de la Autoridad.

Se practica asimismo cuando la longitud de clave o el algoritmo empleados dejen de garantizar la vinculación entre el Titular y su clave pública, o cuando concurra compromiso o sospecha conforme al §5.7.3.

La generación del nuevo par se practica en ceremonia documentada conforme al §6.1.1, con el control multipersona del §5.2.2.

Producido el cambio, **DIGITO** continúa publicando información de estado respecto de los certificados emitidos bajo la clave anterior durante el período del §4.10.2, y mantiene disponible el certificado de la Autoridad saliente para permitir la verificación de las firmas generadas durante su vigencia.

5.7 Compromiso y recuperación de desastres

DIGITO mantiene procedimientos que le permiten responder ante incidentes de seguridad, compromiso de claves, corrupción de sistemas o datos y situaciones de desastre, y restablecer la prestación dentro de los plazos comprometidos.

5.7.1. Procedimientos de gestión de incidentes y compromiso

DIGITO dispone de un procedimiento de gestión de incidentes que comprende su detección, clasificación por severidad, contención, erradicación, recuperación y análisis posterior.

Los incidentes que afecten a la seguridad de los servicios o a la integridad de los certificados emitidos se notifican al INDOTEL en los plazos y términos exigidos por la normativa aplicable, y a los Titulares y partes que confían cuando resulten afectados.

DIGITO evalúa, respecto de cada incidente, si concurre alguna de las causales del §4.9.1, y practica en su caso la revocación conforme al §4.9.5.

Los incidentes y las medidas adoptadas se registran conforme al §5.4.1 y se conservan conforme al §5.5.2.

5.7.2. Corrupción de recursos, software o datos

Detectada la corrupción o la alteración no autorizada de sistemas, software o datos, **DIGITO** suspende de forma inmediata las operaciones afectadas,

determina el alcance de la corrupción y restablece la operación a partir de las copias de respaldo previstas en los §5.4.5 y §5.5.4.

Con anterioridad a restablecer la emisión de certificados, **DIGITO** verifica la integridad de los sistemas y de la información restaurada, y comprueba que no se han emitido certificados de forma indebida durante el período afectado.

Los certificados que se constate haber sido emitidos de forma indebida se revocan conforme al §4.9.1.

5.7.3. Procedimientos por compromiso de clave privada

El compromiso o la sospecha de compromiso de la clave privada de una Autoridad de Certificación determina la activación inmediata del procedimiento de contingencia, que comprende:

a) La suspensión inmediata de la emisión de certificados bajo la Autoridad afectada.

b) La revocación de la totalidad de los certificados emitidos bajo dicha Autoridad, así como del certificado de la propia Autoridad de Certificación.

c) La emisión y publicación de una última lista de revocación conforme al §4.9.7.

d) La notificación inmediata al INDOTEL, a los Titulares afectados y, mediante publicación en el repositorio, a las partes que confían. La comunicación indicará el alcance de los certificados afectados, la fecha a partir de la cual las firmas generadas no pueden considerarse fiables y las medidas adoptadas.

e) La generación de un nuevo par de claves conforme al §5.6 y el restablecimiento del servicio, previa verificación de que las circunstancias que dieron lugar al compromiso han sido subsanadas.

Igual procedimiento se aplica cuando se constate que los algoritmos o las longitudes de clave empleados han dejado de garantizar la vinculación entre el Titular y su clave pública.

El compromiso de la clave privada de un Titular se rige por el §4.9.1, literal c).

5.7.4 Capacidad de continuidad tras un desastre

DIGITO mantiene un plan de continuidad del negocio que le permite restablecer la prestación de sus servicios tras una situación de desastre.

El servicio de consulta del estado de los certificados se restablece con carácter prioritario, a fin de sostener la disponibilidad comprometida en el §4.10.2. El período máximo de indisponibilidad de dicho servicio no excederá de **ocho (8) horas**.

El plan comprende la disponibilidad de la infraestructura alternativa, la recuperación de la información a partir de las copias del §5.1.8, y los criterios de restablecimiento progresivo de los servicios.

El plan se somete a prueba con periodicidad anual, y el resultado de las pruebas se documenta y da lugar a su revisión.

5.8. Terminación de la AC o la AR

El cese de actividades de **DIGITO** como Prestador Cualificado de Servicios de Confianza, sea voluntario o no voluntario, se sujeta al procedimiento siguiente:

a) DIGITO comunicará su intención de cesar al INDOTEL con una antelación no inferior a **noventa (90) días**, conforme a la **Normativa Vigente**, y a los Titulares y partes que confían mediante publicación en su repositorio.

b) Durante el preaviso cesará la emisión de certificados nuevos y mantendrá los servicios de revocación y de consulta del estado.

c) Revocará los certificados pendientes de expiración a la conclusión del preaviso, conforme al §4.11, literal c).

d) La información archivada conforme al §5.5 se transferirá a la entidad que el INDOTEL determine, o se conservará en los términos que éste disponga, preservándose los períodos del §5.5.2.

e) DIGITO adoptará las medidas necesarias para que la información de estado permanezca disponible con posterioridad al cese, conforme al §4.10.2 y al requisito CSS-6.3.10-12 de la norma ETSI EN 319 411-2.

e) DIGITO adoptará las medidas necesarias para que la información de estado permanezca disponible con posterioridad al cese, conforme al §4.10.2 y al requisito CSS-6.3.10-12 de la norma ETSI EN 319 411-2.

g) Cesará asimismo el servicio de sellado de tiempo, preservándose la información necesaria para la verificación de los sellos emitidos.

DIGITO mantiene provisiones suficientes para atender los costes derivados del cese, conforme al §9.2.

La ejecución del cese corresponde a los roles siguientes, conforme al plan de cese que Digito mantiene actualizado:

Actuación	Responsable	Plazo
Decisión de cese y comunicación al INDOTEL	Órgano de dirección	Día 0
Publicación del aviso en el repositorio	Autoridad de Políticas	Día 0 + 5 días
Comunicación individual a Titulares y Organizaciones Vinculadas	Autoridad de Políticas	Día 0 + 10 días
Cese de la emisión de certificados nuevos	Responsable de Tecnología	Día 0
Mantenimiento de los servicios de revocación y consulta del estado	Responsable de Tecnología	Hasta el día 90
Revocación de los certificados pendientes de expiración	Operador de la AC	Día 90
Emisión de la última lista de revocación	Operador de la AC + control multipersona (§5.2.2)	Día 90
Transferencia del archivo a la entidad que el INDOTEL determine	Oficial de Seguridad + Legal	Día 90 + 30 días
Aseguramiento de la disponibilidad de la información de estado posterior al cese	Responsable de Tecnología	Antes del día 90
Destrucción de las claves privadas de las Autoridades de Certificación	Operador de la AC + control multipersona	Tras la transferencia del archivo
Cese del servicio de sellado de tiempo	Responsable de Tecnología	Día 90
Acta de cierre y comunicación final al INDOTEL	Órgano de dirección	Día 90 + 45 días

Los plazos se cuentan desde la comunicación al INDOTEL prevista en el literal a). La destrucción de las claves privadas no se practica hasta haberse completado la transferencia del archivo y asegurado la disponibilidad de la información de estado, a fin

de no comprometer la verificación de las firmas generadas durante la vigencia de los certificados emitidos.

El plan de cese se revisa con periodicidad anual y con ocasión de toda modificación relevante de la estructura organizativa o de la infraestructura.

Los plazos consignados en la presente tabla, con excepción del preaviso de **noventa (90) días** exigido por la Normativa Vigente, son plazos propios establecidos por **DIGITO** y podrán ser modificados por instrucción del INDOTEL en ejercicio de la facultad que la Normativa Vigente le reconoce.

6. CONTROLES DE SEGURIDAD TÉCNICA

Los pares de claves se generan e instalan con sujeción a los apartados siguientes, según correspondan a Autoridades de Certificación, a componentes de la infraestructura o a Titulares.

6.1.1. Generación del par de claves

a) Autoridad de Certificación Raíz. El par de claves se genera en ceremonia documentada, dentro de un módulo criptográfico de hardware conforme al §6.2.1, con el control multipersona del §5.2.2. La ceremonia se practica en la jaula del §5.1.1, literal c), y se levanta acta suscrita por todos los intervinientes.

b) Autoridad de Certificación Subordinada. Igual procedimiento. La solicitud de certificación se remite a la Autoridad de Certificación Raíz en el marco de la ceremonia.

c) Componentes de la infraestructura. Los pares de claves de los servidores y componentes que requieran certificado propio se generan en el propio componente o en módulo criptográfico, según su función.

d) Titulares. El par de claves se genera dentro del dispositivo cualificado de creación de firma gestionado por **DIGITO**, en el momento de la emisión y de forma exclusiva para el certificado que se emite.

d) Titulares. El par de claves se genera dentro del dispositivo cualificado de creación de firma gestionado por **DIGITO**, en el momento de la emisión y de forma exclusiva para el certificado que se emite.

6.1.2. Entrega de la clave privada al suscriptor

No procede la entrega de la clave privada al Titular. La clave se genera dentro del dispositivo cualificado de creación de firma, permanece en él durante todo su ciclo de vida y no es extraíble.

El Titular ejerce el control exclusivo sobre su clave privada mediante los datos de activación del §6.4, sin que ello comporte su posesión material.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública se transfiere internamente al servicio de generación de certificados por canales protegidos dentro de la infraestructura de **DIGITO**, sin transitar por redes públicas.

La integridad de la clave pública y su correspondencia con la clave privada generada se verifican con anterioridad a la emisión.

6.1.4. Entrega de la clave pública de la AC a las partes que confían

Los certificados de las Autoridades de Certificación de **DIGITO** se publican en el repositorio conforme al §2.2, y su localización se consigna en la extensión *authorityInformationAccess* de los certificados emitidos, en cumplimiento de la Normativa Vigente.

DIGITO publica asimismo los valores resumen (*hash*) de los certificados de sus Autoridades de Certificación, a fin de permitir su verificación por medios independientes.

6.1.5. Tamaños de clave

a) Autoridades de Certificación. Algoritmo RSA con longitud de clave de 4096 bits y algoritmo de resumen SHA-256.

b) Titulares. Algoritmo RSA con longitud de clave no inferior a 2048 bits y algoritmo de resumen SHA-256, conforme al perfil de la Política aplicable.

c) Componentes de la infraestructura. Conforme al perfil del capítulo 7.

DIGITO revisa periódicamente la adecuación de los algoritmos y longitudes empleados a la evolución del estado de la técnica, y practica su sustitución

conforme al §5.6 cuando dejen de garantizar la vinculación entre el Titular y su clave pública.

6.1.6. Generación y calidad de los parámetros de clave pública

Los parámetros se generan conforme a las especificaciones del algoritmo empleado, dentro del dispositivo criptográfico y mediante su generador de números aleatorios, cuya calidad se encuentra acreditada por la certificación del propio dispositivo conforme al §6.2.1.

DIGITO verifica que las claves públicas presentadas para certificación satisfacen los criterios de calidad aplicables.

6.1.7. Propósitos de uso de la clave

Los propósitos de uso se establecen mediante la extensión keyUsage, conforme al perfil del capítulo 7 y de la Política aplicable.

Los certificados de firma electrónica cualificada incorporan keyUsage marcada como crítica con los valores *digitalSignature* y *nonRepudiation*, y no incorporan *extendedKeyUsage*.

Los certificados de las Autoridades de Certificación incorporan *keyCertSign* y *cRLSign*, y basicConstraints.

El uso de la clave para fines distintos de los previstos en el §1.4.1 excede los límites de la Política aplicable y se rige por el §9.8.

6.2. Protección de la clave privada y controles del módulo criptográfico

Las claves privadas se generan, almacenan y utilizan dentro de dispositivos criptográficos conforme al §6.2.1, y se protegen frente a acceso, uso, divulgación, modificación y destrucción no autorizados.

6.2.1. Estándares y controles del módulo criptográfico

a) Las claves privadas de los Titulares se generan, almacenan y utilizan en un dispositivo cualificado de creación de firma electrónica (QSCD) que satisface los requisitos de la Normativa Vigente y de la norma ETSI EN 319 411-2 para la política QCP-n-qscd.

El dispositivo empleado es Entrust nShield Connect XC 12.16.15, que cuenta con certificación Common Criteria EAL4+ conforme al Perfil de Protección CEN EN 419 221-5, certificado núm. CSA_CC_21008, emitido por la Cyber

Security Agency of Singapore (CSA) y vigente hasta el 2027-06-27, cuyo alcance comprende la configuración efectivamente empleada por **DIGITO**, conforme a la Normativa Vigente.

b) Claves de las Autoridades de Certificación. Se generan, almacenan y utilizan en módulos criptográficos de hardware conforme al §6.2.11, alojados en el centro de datos descrito en el §5.1.

c) Sistema de gestión de activación. La gestión de la activación de las claves de los Titulares se practica mediante el sistema de gestión de activación (SAM) de **DIGITO, que** cuenta con certificación conforme a CEN EN 419 241-2, certificado núm. CCN-CC-26/2025, alojado en las mismas instalaciones, que asegura que cada operación de firma requiere la autorización específica del Titular conforme al §6.4.

6.2.2. Control multipersona de la clave privada

El uso de la clave privada de una Autoridad de Certificación requiere la concurrencia de al menos un quorum definido por N de M componentes de activación, custodiados por personas distintas en roles de confianza.

Los portadores son designados expresamente, y su designación y toda sustitución se documentan en acta. Los componentes se custodian conforme al §5.1.6, en ubicación distinta de aquella en que se encuentran los dispositivos criptográficos.

Ninguna persona dispone por sí sola de componentes suficientes para activar una clave privada de Autoridad de Certificación.

El uso de la clave privada de un Titular no requiere control multipersona, por corresponder su control de forma exclusiva al propio Titular conforme al §6.4.

6.2.3 Custodia de la clave privada

DIGITO no deposita en custodia claves privadas de firma, conforme al §4.12.1.

6.2.4. Respaldo de la clave privada

Las claves privadas de las Autoridades de Certificación se respaldan en forma cifrada, dentro de dispositivos criptográficos, con el mismo control multipersona del §6.2.2. Las copias se custodian conforme al §5.1.6, con los mismos controles aplicables a los originales.

Las claves privadas de los Titulares no se respaldan. La pérdida de la capacidad de uso determina la revocación del certificado conforme al §4.9.1 y la emisión de uno nuevo, sin que resulte posible su recuperación.

6.2.5. Archivo de la clave privada

DIGITO no archiva claves privadas de firma de entidades finales, conforme al §4.12.1.

Las claves privadas de las Autoridades de Certificación se destruyen conforme al §6.2.10 al concluir su ciclo de vida, sin que se conserven con posterioridad.

6.2.6. Transferencia de la clave privada a o desde el módulo criptográfico

Las claves privadas de los Titulares no se transfieren fuera del dispositivo en que fueron generadas, en forma alguna, ni cifrada ni en claro.

Las claves privadas de las Autoridades de Certificación se transfieren únicamente entre dispositivos criptográficos, en forma cifrada, en el marco de las operaciones de respaldo y restauración del §6.2.4, con el control multipersona del §6.2.2 y en ceremonia documentada.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas permanecen almacenadas dentro del dispositivo criptográfico durante todo su ciclo de vida, protegidas por los mecanismos propios del dispositivo conforme a su certificación.

Los dispositivos son resistentes a la manipulación y responden a los intentos de acceso físico no autorizado mediante la destrucción del material criptográfico que albergan.

6.2.8. Método de activación de la clave privada

La clave privada del Titular únicamente puede utilizarse previa activación mediante los datos de activación descritos en el §6.4, que se encuentran bajo control exclusivo del Titular.

Cada operación de firma requiere una autorización específica del Titular, vinculada criptográficamente a los datos que van a ser firmados y a la clave concreta que va a utilizarse. La autorización no es reutilizable para operaciones posteriores ni resulta aplicable a datos distintos de aquellos para los que fue otorgada.

La autorización se otorga dentro de una sesión en la que el Titular se ha autenticado con su contraseña y su segundo factor conforme al §6.4, mediante la confirmación expresa de cada firma. La plataforma de DIGITO transmite al módulo de activación de firma, certificado conforme a la norma

EN 419 241-2, una autorización protegida en su integridad y vinculada al Titular, a la clave y a los datos que van a firmarse, que el módulo verifica antes de activar la clave. Los componentes de la plataforma que intervienen en esta verificación forman parte del ámbito de la evaluación de conformidad.

DIGITO no dispone de mecanismo alguno que le permita activar o utilizar la clave privada de un Titular sin la concurrencia de los datos de activación de éste.

Las claves privadas de las Autoridades de Certificación se activan mediante los componentes del §6.2.2, y su activación se practica únicamente en el marco de las operaciones autorizadas.

6.2.9. Método de desactivación de la clave privada

La autorización de uso de la clave privada del Titular se desactiva automáticamente al completarse la operación de firma para la que fue otorgada y en todo caso al revocarse el certificado asociado.

Las claves privadas de las Autoridades de Certificación se desactivan al concluir la operación autorizada. El dispositivo que alberga la clave de la Autoridad de Certificación Raíz se mantiene fuera de línea de forma permanente, conforme al §6.7.

6.2.10. Método de destrucción de la clave privada

Concluido el ciclo de vida de una clave privada de Autoridad de Certificación, ésta se destruye mediante los mecanismos previstos por el dispositivo criptográfico, junto con la totalidad de sus copias de respaldo, de modo que resulte imposible su recuperación.

La destrucción se practica en ceremonia documentada, con el control multipersona del §6.2.2, y se levanta acta suscrita por los intervinientes que se conserva conforme al §5.5.2.

Las claves privadas de los Titulares se destruyen al revocarse o expirar el certificado asociado, conforme a los procedimientos del dispositivo cualificado de creación de firma.

Los dispositivos criptográficos que se retiren del servicio se someten a este procedimiento con anterioridad a su salida de las instalaciones, conforme al §5.1.7.

6.2.11. Calificación del módulo criptográfico

Los módulos criptográficos que albergan las claves privadas de las Autoridades de Certificación cuentan con certificación FIPS 140-2 Nivel 3 y Common Criteria EAL 4+.

El dispositivo cualificado de creación de firma empleado para las claves de los Titulares cuenta con la certificación indicada en el §6.2.1.

DIGITO verifica la vigencia de dichas certificaciones y su adecuación a la configuración efectivamente empleada.

6.3. Otros aspectos de la gestión del par de claves

Los aspectos de la gestión del par de claves distintos de los regulados en los §6.1 y §6.2 se rigen por los apartados siguientes.

6.3.1. Archivo de la clave pública

Las claves públicas quedan archivadas como parte del certificado que las contiene, conforme al régimen de conservación del §5.5.2.

El archivo permite la verificación de las firmas generadas durante el período de validez del certificado con posterioridad a su expiración o revocación, en concordancia con la disponibilidad de la información de estado prevista en el §4.9.8.

6.3.2. Períodos operativos del certificado y del par de claves

El período de validez de los certificados de entidad final es el establecido en la Política de Certificación aplicable a cada clase.

El período de utilización de la clave privada coincide con el período de validez del certificado. Concluido éste, la clave privada no puede utilizarse para generar firmas, conforme al §4.5.1.

La clave pública permanece utilizable para la verificación de las firmas generadas durante el período de validez con posterioridad a su conclusión, sin que ello comporte la posibilidad de generar firmas nuevas.

El período de validez de los certificados de las Autoridades de Certificación es el que consta en los propios certificados. **DIGITO** no emite certificados cuyo período de validez exceda al del certificado de la Autoridad emisora, y practica el cambio de claves conforme al §5.6 con la antelación necesaria.

Los períodos de validez podrán reducirse cuando la evolución del estado de la técnica lo requiera conforme al §6.1.5.

6.4 Datos de activación

Se entiende por datos de activación la información, distinta de la clave privada, necesaria para autorizar su utilización.

En el servicio de firma electrónica remota prestado por **DIGITO**, los datos de activación del Titular están constituidos por el segundo factor de autenticación configurado por él, de entre los medios que admita la plataforma, que se le exige en cada inicio de sesión junto con su contraseña, y por la confirmación expresa de cada firma dentro de una sesión así autenticada. Los datos de activación son distintos de la clave privada, que permanece en el dispositivo cualificado de creación de firma, y constituyen el mecanismo mediante el cual el Titular ejerce el control exclusivo sobre ella, en cumplimiento de la Normativa Vigente y de los requisitos aplicables a la política QCP-n-qscd de la norma ETSI EN 319 411-2.

Constituyen asimismo datos de activación los componentes de activación de los dispositivos criptográficos que albergan las claves privadas de las Autoridades de Certificación, regulados en el §6.2.2.

6.4.1. Generación e instalación de los datos de activación

El Titular establece sus datos de activación registrando su segundo factor de autenticación durante el proceso de registro, con posterioridad a la verificación de su identidad conforme al §3.2.3 y con anterioridad a la primera utilización del certificado.

DIGITO no almacena en claro la contraseña del Titular ni los secretos asociados a su segundo factor, ni los transmite en claro.

DIGITO impone requisitos mínimos de complejidad a la contraseña de acceso y verifica que no coincida con valores triviales ni con credenciales comprometidas conocidas.

La contraseña de acceso no constituye por sí sola dato de activación ni permite el uso de la clave privada: el inicio de sesión exige además el segundo factor, y cada firma, su confirmación expresa dentro de una sesión así autenticada. La sesión tiene la duración máxima que determine la plataforma, sin exceder de treinta (30) minutos.

Los componentes de activación de los dispositivos criptográficos de las Autoridades de Certificación se generan en el marco de la ceremonia de generación de claves, se distribuyen a los portadores designados conforme al §6.2.2 y se custodian conforme al §5.1.6.

6.4.2. Protección de los datos de activación

Los datos de activación se protegen frente a divulgación y uso no autorizado. No se almacenan en claro en ningún componente de la infraestructura de **DIGITO**, ni se transmiten en claro.

Ningún miembro del personal de **DIGITO**, con independencia del rol que desempeñe, dispone de mecanismo alguno que le permita establecer o sustituir los datos de activación de un Titular ni utilizar su clave privada.

La sustitución del segundo factor sin disponer del vigente, por pérdida, sustracción o compromiso, exige un procedimiento de identificación del Titular con el mismo nivel de aseguramiento exigido en el registro inicial conforme al §3.2.3. No podrá practicarse mediante la contraseña de acceso ni por intervención del personal de **DIGITO. El cambio del correo electrónico que figura en el certificado conlleva su revocación conforme al §4.9.1, y la obtención de un certificado nuevo se sujeta al procedimiento de registro del §4.1.**

Practicada la re-identificación, el Titular podrá establecer datos de activación nuevos, con un segundo factor nuevo, para el mismo certificado, sin que ello altere la clave privada, cuando se trate de la sola pérdida de los datos de activación, por olvido, cambio o extravío del dispositivo, sin indicio de uso por persona distinta del Titular. Concurriendo vulneración, sospecha de vulneración o exposición de la clave privada o de los datos de activación, incluida la sustracción del segundo factor, procede la revocación conforme al §4.9.1, literal c), y la emisión de un certificado nuevo.

La contraseña de acceso a la plataforma podrá ser restablecida por el propio Titular mediante el canal de comunicación registrado, sin intervención del personal de **DIGITO**. Su restablecimiento no modifica los datos de activación ni habilita por sí solo el uso de la clave privada.

El Titular es responsable de la custodia de sus datos de activación, incluido su segundo factor, y de su contraseña, y de no entregarlos ni divulgarlos a terceros, conforme al §9.6.3. Debe solicitar la revocación en caso de compromiso o sospecha de compromiso de la clave privada o de los datos de activación, conforme al §4.9.1, literal c), y al §4.9.4.

6.4.3. Otros aspectos de los datos de activación

Los datos de activación se establecen de forma individual para cada Titular y no se comparten entre Titulares. Un mismo Titular emplea sus datos de activación para autorizar el uso de la clave privada de cada uno de sus certificados.

El Titular puede registrar factores adicionales o sustituir el existente a través de la plataforma, autenticándose con su contraseña y con el factor vigente. La sustitución sin el factor vigente se rige por el §6.4.2. Ninguna de estas operaciones altera la clave privada ni el certificado emitido.

6.5. Controles de seguridad informática

Los sistemas que soportan los servicios se someten a controles de seguridad proporcionados al riesgo.

6.5.1. Requisitos técnicos específicos

Los sistemas implantan al menos:

a) Control de acceso basado en roles, con privilegios conforme al principio de mínimo privilegio y revisión periódica de las autorizaciones.

b) Autenticación multifactor para el acceso administrativo.

c) Identificación individual de los usuarios, sin cuentas genéricas ni compartidas para funciones propias de roles de confianza, conforme al §5.2.3.

d) Registro de las operaciones conforme al §5.4.1.

e) Protección frente a código malicioso y mecanismos de detección de intrusiones.

f) Gestión de actualizaciones y parches, con aplicación priorizada en función de la severidad conforme al §5.4.8.

g) Separación de los entornos de producción, preproducción y desarrollo. Los datos de producción no se emplean en los restantes entornos salvo previa anonimización.

Los sistemas que albergan las funciones de emisión y de gestión de claves se dedican exclusivamente a dichas funciones y no ejecutan aplicaciones ajenas a ellas.

El entorno de desarrollo opera sobre una infraestructura de clave pública independiente, cuyos certificados se identifican mediante los identificadores de la rama 5.9 de la Taxonomía de OID y no producen efecto jurídico alguno. Dicho entorno podrá ser accedido por terceros con finalidad demostrativa o de integración técnica; sus certificados incorporan en su denominación y en el calificador *userNotice* una indicación expresa de su carácter de prueba, y no incorporan las declaraciones de certificado cualificado del §7.1.

6.5.2. Calificación de seguridad informática

DIGITO no somete sus sistemas a esquemas de calificación distintos de las evaluaciones del §5.4.8 y de la evaluación de conformidad del capítulo 8.

6.6. Controles técnicos del ciclo de vida

Los sistemas que soportan los servicios de certificación se desarrollan, adquieren, implantan y mantienen con sujeción a controles que aseguran su integridad y su adecuación a los requisitos de seguridad aplicables.

6.6.1. Controles de desarrollo de sistemas

El desarrollo y la modificación de los sistemas se practican conforme a un procedimiento documentado que comprende el análisis de requisitos, incluidos los de seguridad, las pruebas previas a la puesta en producción y la aprobación formal del despliegue.

Los despliegues en producción se practican por personal distinto de quien desarrolló la modificación, y quedan registrados conforme al §5.4.1.

El software adquirido a terceros se obtiene de fuentes fiables y se verifica su integridad con anterioridad a su instalación.

6.6.2. Controles de gestión de seguridad

DIGITO mantiene un sistema de gestión de la seguridad de la información que comprende la identificación y clasificación de los activos, el análisis y tratamiento de riesgos, y la revisión periódica de la eficacia de los controles implantados.

La configuración de los sistemas se documenta y su integridad se verifica periódicamente, de modo que sea posible detectar modificaciones no autorizadas.

Los cambios en la configuración de las Autoridades de Certificación y de los perfiles de certificado se someten al control multipersona del §5.2.2.

6.6.3. Controles de seguridad del ciclo de vida

Los sistemas se mantienen en versiones soportadas por sus proveedores. **DIGITO** planifica su sustitución con anterioridad al fin del soporte.

La política criptográfica de **DIGITO** se revisa periódicamente conforme al §6.1.5, y su modificación se practica conforme al §5.6.

6.7 Controles de seguridad de red

Los sistemas que soportan los servicios de certificación se segmentan en redes diferenciadas en función de su criticidad, de modo que los que albergan las

funciones de emisión y de gestión de claves no resulten accesibles directamente desde redes públicas.

El tráfico entre segmentos se restringe a las comunicaciones expresamente autorizadas, y se somete a filtrado y a monitorización con generación de alertas.

El dispositivo criptográfico que alberga la clave privada de la Autoridad de Certificación Raíz se mantiene permanentemente desconectado de toda red, y sus operaciones se practican únicamente en el marco de las ceremonias del §5.2.2.

Las comunicaciones con los servicios accesibles desde redes públicas, en particular el repositorio y el servicio de consulta del estado, se protegen mediante protocolos criptográficos vigentes.

Los componentes de la infraestructura alojados en entornos de terceros se someten a los mismos controles, conforme al §5.3.7.

6.8 Sellado de tiempo

La sincronización horaria de los sistemas que soportan los servicios de certificación se rige por el §5.5.5.

DIGITO presta el servicio de sellado de tiempo cualificado conforme a la política identificada en el §1.2 y a la norma ETSI EN 319 421. Los sellos emitidos se ajustan al perfil de la norma ETSI EN 319 422, y consignan en el campo policy de la estructura TSTInfo el identificador de dicha política.

Las unidades de sellado de tiempo emplean claves privadas alojadas en módulos criptográficos conforme al §6.2.1.

La precisión del reloj se declara en el campo *accuracy* de los sellos emitidos, conforme al IETF RFC 3161, con el valor establecido en la Política de Sellado de Tiempo.

La pérdida de trazabilidad respecto de UTC, o la superación de la desviación declarada, determina el cese inmediato de la emisión de sellos hasta su restablecimiento y verificación.

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1. Perfil del certificado

El presente apartado establece el perfil de los certificados emitidos por las Autoridades de Certificación de **DIGITO**. El perfil concreto de cada clase de certificado de entidad final se establece en el capítulo 7 de la Política de Certificación aplicable, que prevalece conforme al §1.4.1.

7.1.1. Números de versión

Los certificados se emiten conforme a la versión 3 del formato X.509, según el IETF RFC 5280.

7.1.2. Extensiones del Certificado

7.1.2.1. PERFIL DE CERTIFICADO DE AC RAÍZ DE DIGITO

CAMPO/EXTENSIÓN	¿CRÍTICO?	VALORES	COMENTARIOS
Campos Básicos del Certificado			
Version	N/A	V3 (2)	Version 3
serialNumber	N/A	Asignado por la CA	
Signature Algorithm	N/A	Sha256RSA	
Issuer	N/A	cn=Digito Root CA, ou=Certification Authorities, o=Digito Group, c=DO	
Validity	N/A	notBefore and notAfter are both included in UTCTime format YYMMDDHHMMSSZ	20 años
Subject	N/A	Same as issuer	
subjectPublicKeyInfo	N/A	RSA encryption ;4096-bit modulus 2^16+1 public exponent	
Extensiones			
keyUsage	Sí	Certificate Signing, Off-line CRL Signing, CRL Signing	
subjectKeyIdentifier	No	SM CA includes hash of the subjectPublicKey component of the subjectPublicKeyInfo field of the certificate	
basicConstraints	Sí	CA = TRUE pathLenConstraint = None	

7.1.2.2. PERFIL DEL CERTIFICADO DE AC SUBORDINADA

Campo/Extensión	¿Crítico?	Valores	Comentarios
Base certificate fields			
Version	N/A	V3 (2)	
serialNumber	N/A	Asignado por la CA	
Signature	N/A	Sha256RSA	
Issuer	N/A	cn=Digito Root CA, ou=Certification Authorities, o=Digito Group, c=DO	
Validity	N/A	notBefore y notAfter en formato UTCTime YYMMDDHHMMSSZ	10 años
Subject	N/A	cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO	
subjectPublicKeyInfo	N/A	RSA encryption; 4096-bit modulus 2^16+1 public exponent	
Extensiones			
cRLDistribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digito.do/CRLs/DigitoRootCA.crl CRL Issuer: Directory Address: C=DO O=Digito Group OU=Certification Authorities CN=Digito Root CA	
authorityInfoAccess	No	[1]Authority Info Access	

Campo/Extensión	¿Crítico?	Valores	Comentarios
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.digito.do/CAs/DigitoRootCA.crt	
keyUsage	Sí	Certificate Signing, CRL Signing	
authorityKeyIdentifier	No	keyIdentifier presente authorityCertIssuer	
subjectKeyIdentifier	No	SM CA includes hash of the subjectPublicKey component of the subjectPublicKeyInfo field of the certificate	
basicConstraints	Sí	CA boolean = TRUE pathLenConstraint = 0	
certificatePolicies	No	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.64999.1.0.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://cps.digito.do	1.3.6.1.4.1.64999.1.0.2

7.1.2.3. PERFIL DEL CERTIFICADO DE ENTIDAD FINAL

Los perfiles de los certificados de entidad final se establecen en el capítulo 7 de cada Política de Certificación, según la clase:

Clase	Política
Certificado cualificado de firma de persona física	1.3.6.1.4.1.64999.1.3.1
Certificado cualificado de firma de persona física con responsabilidad institucional	1.3.6.1.4.1.64999.1.3.4

La presente Declaración establece los perfiles de los certificados de las Autoridades de Certificación y de los componentes de la infraestructura, así como los elementos comunes a todas las clases.

Cuando la Política aplicable prevea la incorporación de atributos organizacionales, éstos se construyen conforme al §3.1.4 y a la norma ETSI EN 319 412-1.

7.1.2.4. PERFIL DEL CERTIFICADO DEL RESPONDEDOR OCSP

Campo	**Certificados del Respondedor OCSP**
Nombre de Perfil	OCSP-DIGITO
X.509 Version	3
Tipo de certificado	End Entity-OCSP Certificate
Validez de Certificado	2 años
Minimum Key Length	RSA-2048/SHA-256
Subject DN Attributes	cn= OCSP-[CA], ou= Services, o= Digito Group, c= DO
Allowed Subject Alt Name	N/A
Key Usage	Digital Signature (c)
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9) OCSP No Check Enabled (1.3.6.1.5.5.7.48.1.5)

7.1.2.5. PERFIL DEL CERTIFICADO DE LA AUTORIDAD DE SELLADO DE TIEMPO

Field	Certificados de Timestamping
Nombre de Perfil	tsa_h_5y_nodir-CP
OID	1.3.6.1.4.1.64999.1.3.2
X.509 Version	3
Tipo de certificado	End Entity-Timestamping Certificate
Validez de Certificado	5 años
Minimum Key Length	RSA-4096/SHA-256
Subject DN Attributes	cn= TSA-Server, ou= Applications, o= Digito Group, c= DO
Subject Alternative Name	RFC 822: Dirección de correo electrónico
AIA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.digito.do/CAs/DigitoIssuingCADO02.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digito.do
CDP	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.digito.do/CRLs/DigitoIssuingCADO02.crl [2]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: cn=CRL

Field	Certificados de Timestamping
	cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO
Key Usage	digitalSignature
Extended Key Usage	timestamping (critical) {1.3.6.1.5.5.7.3.8}
Certificate Policies Extension	Policy Identifier= Garantia Alta 1.3.6.1.4.1.64999.1.3.2
Key and Certificate Storage	Llave privada generada y guardada en HSM

7.1.2.6. DECLARACIONES DE CERTIFICADO CUALIFICADO

La extensión *qcStatements* (OID 1.3.6.1.5.5.7.1.3) de los certificados cualificados contiene:

Declaración	OID	Función
QcCompliance	0.4.0.1862.1.1	Certificado cualificado, en formato procesable, conforme a la Normativa Vigente.
QcType (esign)	0.4.0.1862.1.6.1	Certificado de firma electrónica
QcSSCD	0.4.0.1862.1.4	Clave en QSCD, en formato procesable, conforme a la Normativa Vigente.
QcCClegislation	0.4.0.1862.1.7	Valor=DO: cualificado bajo legislación distinta de la normativa de la Unión Europea
QcRetentionPeriod	0.4.0.1862.1.3	**Veinte (20) años**, conforme

		al §5.5.2
QcPDS	0.4.0.1862.1.5	Localización del PDS, con al menos una entrada en inglés y una en español

Se incorpora asimismo el identificador de semántica de persona física (OID 0.4.0.194121.1.1) mediante la declaración *id-qcs-pkixQCSyntax-v2*.

7.1.3. Identificadores de objeto de los algoritmos

Algoritmo de firma: sha256WithRSAEncryption (1.2.840.113549.1.1.11). Algoritmo de clave pública: rsaEncryption (1.2.840.113549.1.1.1), con las longitudes del §6.1.5.

7.1.4. Formas de nombre

Los Nombres Distintivos se construyen conforme al §3.1 y a la Política aplicable.

a) Autoridades de Certificación. Incorporan *countryName*, *organizationName*, *organizationalUnitName* y commonName. La unidad organizativa Certification Authorities distingue a las Autoridades de Certificación de los restantes componentes.

b) Componentes de la infraestructura. Incorporan la unidad organizativa correspondiente a su función: Services para el respondedor OCSP, Applications para las unidades de sellado de tiempo.

c) Entidades finales. Conforme al §7.1.4 de la Política aplicable.

Los atributos se consignan en mayúsculas, sin acentos ni caracteres especiales, salvo cuando la fuente oficial de la que proceden los incluya.

7.1.5. Restricciones de nombre

No estipulado. Los certificados emitidos conforme a la presente Declaración de Prácticas de Certificación no incorporan la extensión *nameConstraints*.

7.1.6. Identificador de objeto de la política

La extensión *certificatePolicies* contiene exclusivamente el identificador de la política aplicable, asignado dentro del arco de **DIGITO** conforme a la Taxonomía de OID y enumerado en el §1.2.

El certificado de la Autoridad de Certificación Raíz tiene como identificador 1.3.6.1.4.1.64999.1.0.1 y se designa su régimen con finalidad documental.

7.1.7. Uso de la extensión Policy Constraints

No estipulado. Los certificados no incorporan la extensión *policyConstraints*.

7.1.8. Sintaxis y semántica de los calificadores de política

La extensión certificatePolicies incorpora dos calificadores: el calificador DPS, con el localizador de la presente Declaración; y el calificador userNotice, cuyo campo explicitText contiene la denominación del tipo de certificado y las limitaciones de uso aplicables.

El texto descriptivo se consigna exclusivamente en dicho campo y no en atributo alguno del Nombre Distintivo.

En los certificados emitidos en el entorno de prueba conforme al §6.5.1, el campo explicitText incorpora la indicación expresa de su carácter de prueba y de su carencia de validez jurídica.

7.1.9. Semántica de procesamiento de la extensión crítica

La extensión certificatePolicies no se marca como crítica.

7.2. Perfil de la CRL

Las listas de revocación emitidas por las Autoridades de Certificación de **DIGITO** se ajustan al perfil de los apartados siguientes.

7.2.1 Números de versión

Las listas de revocación se emiten conforme a la versión 2 del formato X.509, según el IETF RFC 5280.

7.2.2. Extensiones de la CRL y de sus entradas

Campo/Extensión	Valor	Descripción
Campos: General		
Versión	V2	Indica el certificado de la versión
Emisor	DN de la CA que emite el certificado	Emisor (DN)
fecha efectiva	inicio de validez están incluidos en el formato UTCTime Dia, mes DD,YYYY HH:MM:SS AM	Fecha y hora de efectividad de la lista
Siguiente actualización	Fecha y hora están incluidos en el formato UTCTime Dia, mes DD,YYYY HH:MM:SS AM	fecha y hora de siguiente actualización
Algoritmo de firma	SHA256 RSA	Algoritmo de firma
Numero de CRL	Numero de lista	Número de lista en formato hexadecimal
Certificados Expirados en CRL (expiredCertsOnCRL)	Presente (Valor: NULL) *Criticidad: No crítica*	Extensión requerida por ETSI EN 319 411-2. Indica explícitamente que la CRL retiene y sigue listando los certificados revocados aun después de que estos han expirado, garantizando la consulta histórica.
Campos:lista base		
Numero de serial	Serial de certificado	Número en hexadecimal del certificado
Fecha de revocación	fecha: Dia, mes DD,YYYY HH:MM:SS AM	fecha de revocación

La lista se emite y publica con independencia de que se hayan practicado o no revocaciones en el período, a fin de que las partes que confían dispongan siempre de información de estado vigente.

7.3. Perfil OCSP

DIGITO presta el servicio de consulta del estado conforme al protocolo OCSP definido en el IETF RFC 6960, en los términos del §4.10.

7.3.1. Números de versión

Las peticiones y respuestas se ajustan a la versión 1 del protocolo.

7.3.2. Extensiones OCSP

Las respuestas son firmadas por un respondedor cuyo certificado es emitido por la Autoridad de Certificación emisora de los certificados sobre los que informa, conforme al IETF RFC 6960, cláusula 4.2.2.2. Dicho certificado incorpora:

a) La extensión extendedKeyUsage con el valor *id-kp-OCSPSigning*.

b) La extensión id-pkix-ocsp-nocheck, que exime a las partes que confían de comprobar el estado de revocación del propio certificado del respondedor.

Contenido de las respuestas. Las respuestas incorporan el certificado del respondedor y su cadena de certificación, a fin de que las partes que confían puedan verificarlas sin obtener información adicional.

Las respuestas no incorporan el campo *nextUpdate*, indicando así que la información de estado se encuentra disponible de forma continua y que no procede su almacenamiento en caché, conforme al §4.10.1.

No se incorpora la extensión *ArchiveCutOff*, por proveerse la disponibilidad de la información de estado con posterioridad a la expiración mediante la conservación de las entradas en las listas de revocación conforme al §4.9.8.

Estados devueltos. El respondedor devuelve *good*, *revoked* o *unknown*. Devuelve *unknown* respecto de los números de serie que no consten en su base de información. **DIGITO** no emite en ningún caso respuestas de estado *good* respecto de números de serie no emitidos por sus Autoridades de Certificación.

Alcance del servicio. El servicio se presta respecto de los certificados emitidos por las Autoridades de Certificación Subordinadas. El estado de los certificados emitidos por la Autoridad de Certificación Raíz se consulta exclusivamente

mediante la lista de revocación del §4.9.7, dada su condición permanentemente fuera de línea.

8. AUDITORÍA DE CONFORMIDAD Y OTRAS EVALUACIONES

8.1. Frecuencia o circunstancias de la evaluación

Los servicios de **DIGITO** se someten a evaluación de conformidad por un Organismo de Evaluación de la Conformidad, conforme a la Normativa Vigente y a la norma ETSI EN 319 403.

La evaluación se practica:

a) Con carácter previo al inicio de la prestación de los servicios, y con anterioridad a la incorporación de una clase de certificado o de un servicio de confianza nuevo.

b) Con la periodicidad que establezca la normativa aplicable para el mantenimiento de la autorización, y en todo caso con una frecuencia no superior a **veinticuatro (24) meses.**

c) Con ocasión de toda modificación sustancial de la infraestructura, de los procedimientos o de la presente Declaración que pueda afectar a la conformidad.

d) Cuando lo requiera el INDOTEL en ejercicio de sus facultades de supervisión.

DIGITO practica adicionalmente auditorías internas con periodicidad anual, ejecutadas por el Auditor Interno conforme al §8.2, cuyo alcance comprende las materias del §8.4.

8.2. Identidad y cualificación del evaluador

La evaluación de conformidad se practica por un Organismo de Evaluación de la Conformidad acreditado conforme a la normativa aplicable y reconocido por el INDOTEL, con competencia acreditada en la evaluación de prestadores de servicios de confianza conforme a las normas ETSI EN 319 401, ETSI EN 319 411-1 y ETSI EN 319 411-2.

El equipo evaluador cuenta con la formación y la experiencia necesarias en infraestructuras de clave pública, criptografía y seguridad de la información.

Las auditorías internas del §8.1 se practican por el Auditor Interno, en las condiciones de independencia del §5.2.4, literal a), o por un tercero contratado al efecto.

8.3. Relación del evaluador con la entidad evaluada

El Organismo de Evaluación de la Conformidad es independiente de **DIGITO**. No existe entre ambos vinculación societaria, ni relación contractual distinta de la propia evaluación, ni ninguna otra circunstancia que pueda comprometer su imparcialidad, conforme a la norma ETSI EN 319 403.

DIGITO no contrata con el Organismo de Evaluación servicios de consultoría, asesoramiento o implantación sobre las materias objeto de evaluación, ni en el período evaluado ni durante la evaluación.

El personal de **DIGITO** no participa en la determinación del resultado de la evaluación.

8.4 Materias cubiertas por la evaluación

La evaluación comprende la verificación de la conformidad de los servicios con las Políticas del §1.2, con la presente Declaración y con las normas y disposiciones aplicables, y alcanza al menos:

a) La adecuación de las Políticas y de la presente Declaración al marco normativo, y la correspondencia entre ambas conforme al §1.5.3.

b) Los procedimientos de identificación y autenticación del capítulo 3, incluidas las modalidades automática, asistida y presencial del §3.2.3 y la verificación de atributos organizacionales del §3.2.2, así como la efectividad de la separación de funciones del §5.2.4.

c) Los procedimientos del ciclo de vida del capítulo 4, con especial atención a la emisión y a la revocación, y a los plazos del §4.9.5.

d) Los controles de instalaciones, gestión y operativos del capítulo 5.

e) Los controles de seguridad técnica del capítulo 6, con especial atención a la protección de las claves privadas y a los datos de activación del §6.4.

f) Los perfiles de certificado, de lista de revocación y de respuesta OCSP del capítulo 7.

g) Las prácticas de sellado de tiempo, conforme a la norma ETSI EN 319 421.

h) La correspondencia entre lo declarado en la presente Declaración y lo efectivamente implantado.

Alcance sobre proveedores externos. La evaluación alcanza asimismo a los componentes prestados por los proveedores del §5.3.7, en los términos siguientes:

i) Respecto del operador del centro de datos y del proveedor de infraestructura en nube, mediante la revisión de sus certificaciones e informes de auditoría independiente vigentes, y de los registros de acceso físico a las jaulas de Digito.

ii) Respecto del Prestador de Sistemas de Pruebas de Identidad, mediante la revisión de su evaluación de conformidad con las normas ETSI EN 319 401 y TS 119 461, y en particular de que el alcance de dicha evaluación comprenda los procesos efectivamente empleados por **DIGITO**.

iii) Respecto del proveedor de distribución de contenido, mediante la verificación de que la configuración no comporta almacenamiento en caché de las respuestas del servicio de consulta del estado, conforme al §4.10.2.

Los contratos con dichos proveedores comprenden la sujeción a las auditorías de Digito y de los Organismos de Evaluación de la Conformidad, conforme al §5.3.7.

8.5. Acciones adoptadas ante deficiencias

Detectada una deficiencia, **DIGITO** elabora un plan de acción correctiva que identifica la causa raíz, las medidas a adoptar, el responsable de su implantación y el plazo de ejecución, y lo somete al Organismo de Evaluación de la Conformidad.

Las no conformidades mayores se subsanan con carácter prioritario y con anterioridad a la emisión del informe favorable.

Cuando una deficiencia comprometa la seguridad de los servicios o la validez de los certificados emitidos, **DIGITO** adopta de forma inmediata las medidas de contención necesarias, que podrán comprender la suspensión de la emisión y la revocación de los certificados afectados conforme al §4.9.1, y lo comunica al INDOTEL.

La ejecución de las acciones correctivas se verifica y se documenta, y su evidencia se conserva conforme al §5.5.2.

8.6. Comunicación de resultados

El informe de evaluación de conformidad se remite al INDOTEL en los plazos y condiciones establecidos por la normativa aplicable.

DIGITO publica en su repositorio la constancia vigente de conformidad, con indicación del Organismo de Evaluación emisor, del alcance de la evaluación y de su período de validez, conforme al §2.2.

El informe íntegro de evaluación tiene carácter confidencial conforme al §9.3, sin perjuicio de su comunicación al INDOTEL y a las autoridades competentes.

Los resultados de las auditorías internas tienen carácter interno y se comunican a la Autoridad de Políticas y al órgano de dirección.

9. OTROS ASUNTOS DE NEGOCIO Y LEGALES

9.1. Tarifas

DIGITO percibe las tarifas correspondientes a los servicios prestados conforme a la presente práctica de certificación, según el régimen de los apartados siguientes. Las tarifas vigentes se publican en el repositorio conforme al §2.2.

9.1.1 Tarifas de emisión

La emisión de certificados está sujeta al pago de la tarifa vigente al momento de la solicitud, según la clase de certificado solicitada.

Toda emisión de certificado constituye una emisión inicial, dado que **DIGITO** no practica la renovación ni la renovación de claves conforme a los §4.6 y §4.7. En consecuencia, no se establecen tarifas diferenciadas por concepto de renovación.

Las tarifas vigentes se publican en el repositorio conforme al §2.2, en cumplimiento de la Normativa Vigente.

Las tarifas podrán establecerse mediante acuerdo particular con el Suscriptor o con la Organización Vinculada, en cuyo caso prevalecerán las condiciones pactadas.

La prestación del servicio de sellado de tiempo se rige por las tarifas publicadas o por las condiciones particulares acordadas.

9.1.2. Tarifas de acceso al certificado

No se percibe tarifa alguna por el acceso de las partes que confían al certificado de un Titular, ni a los certificados de las Autoridades de Certificación publicados conforme al §6.1.4.

9.1.3. Tarifas de acceso a la información de estado

El acceso a la información de estado de revocación es gratuito, tanto mediante el servicio OCSP como mediante las listas de revocación, y no requiere registro ni autenticación previa, conforme al §4.10.2.

DIGITO no percibirá tarifa alguna por dicho acceso ni establecerá restricciones que lo condicionen, sin perjuicio de las medidas técnicas necesarias para preservar la disponibilidad del servicio frente a usos abusivos, que en ningún caso impedirán la consulta legítima.

9.1.4. Tarifas por otros servicios

No se percibe tarifa alguna por la revocación de un certificado, ni por el acceso a la presente Declaración, a las Políticas de Certificación, a la Declaración de Divulgación de Prácticas ni a los términos y condiciones.

Los restantes servicios se rigen por las tarifas publicadas o por las condiciones particulares acordadas.

9.1.5. Política de reembolso

DIGITO percibe la tarifa una vez aprobada la solicitud, y no percibe tarifa alguna por solicitudes rechazadas.

Procede el reembolso cuando el certificado no llegue a emitirse por causa imputable a **DIGITO**, o cuando deba revocarse por error de emisión imputable a **DIGITO**. No procede en los demás supuestos.

Las reclamaciones relativas al reembolso se sustancian conforme al §9.13.

9.2. Responsabilidad financiera

DIGITO mantiene los recursos financieros necesarios para sostener la prestación de sus servicios, para atender las responsabilidades derivadas de su actividad y para afrontar los costes de un eventual cese conforme al §5.8, en cumplimiento del requisito REQ-6.1-02 de la norma ETSI EN 319 401.

9.2.1. Cobertura de seguro

DIGITO mantiene vigente una póliza de seguro de responsabilidad civil que cubre los daños que puedan derivarse de la prestación de sus servicios, con la cobertura mínima exigida por la normativa aplicable.

La entidad aseguradora, la cobertura contratada y su vigencia constan en la documentación aportada al INDOTEL en el procedimiento de autorización, y se mantienen actualizadas.

9.2.2. Otros activos

DIGITO dispone de recursos suficientes, adicionales a la cobertura del §9.2.1, para sostener sus obligaciones de conservación del §5.5.2 y las actuaciones derivadas de un eventual cese conforme al §5.8, incluidas las de transferencia del archivo y de mantenimiento de la información de estado.

9.2.3. Cobertura para entidades finales

La cobertura del §9.2.1 alcanza a los Titulares y a las partes que confían, dentro de los límites establecidos en el §9.8.

DIGITO no proporciona cobertura de seguro adicional en favor de los Titulares distinta de la indicada.

9.3. Confidencialidad de la información de negocio

DIGITO clasifica la información que maneja en función de su sensibilidad y aplica los controles de protección correspondientes conforme al §6.6.2.

9.3.1. Alcance de la información confidencial

Tiene la consideración de información confidencial:

a) Los expedientes de registro y la evidencia de verificación de identidad, sin perjuicio del §9.4.

b) Las claves privadas, los datos de activación y cualquier información que permita deducirlos.

c) Los registros de auditoría del §5.4.1.

d) Los procedimientos operativos internos y la documentación de configuración de los sistemas.

e) Los informes íntegros de evaluación de conformidad y de auditoría interna, conforme al §8.6.

f) Los planes de continuidad, de gestión de incidentes y de cese.

g) La información relativa a incidentes de seguridad, en tanto su divulgación pueda comprometer la seguridad de los servicios.

h) La ubicación concreta de las instalaciones, conforme al §5.1.1, y el registro de precintos del §5.1.2.

9.3.2. Información no comprendida en el ámbito de la confidencialidad

No tiene la consideración de información confidencial:

a) El contenido de los certificados emitidos y su estado de revocación.

b) Las listas de revocación publicadas.

c) La presente Declaración, las Políticas de Certificación y la Declaración de Divulgación de Prácticas.

d) Los términos y condiciones aplicables y las tarifas vigentes.

e) Los certificados de las Autoridades de Certificación y sus valores resumen.

f) La constancia de conformidad publicada conforme al §8.6.

g) La Taxonomía de OID y los identificadores en ella definidos.

h) Toda información que Digito esté obligada a publicar conforme a la normativa aplicable.

9.3.3. Responsabilidad de proteger la información confidencial

DIGITO protege la información confidencial mediante los controles de los capítulos 5 y 6, y restringe su acceso al personal que lo requiera para el ejercicio de sus funciones.

El personal y los proveedores externos quedan sujetos a obligaciones de confidencialidad conforme a los §5.3.8 y §5.3.7, que subsisten tras la terminación de la relación.

La divulgación de información confidencial únicamente procede con el consentimiento del afectado o en los supuestos del §9.4.6.

9.4. Privacidad de la información personal

El tratamiento de los datos personales por **DIGITO** se sujeta a la Normativa Vigente de protección de datos de carácter personal.

9.4.1. Plan de privacidad

DIGITO mantiene una política de privacidad que identifica los datos personales tratados, las finalidades del tratamiento, su base de licitud, los plazos de conservación, las cesiones previstas y los derechos de las personas afectadas y el modo de ejercerlos.

La política de privacidad se publica en el repositorio conforme al §2.2 y se pone en conocimiento del Titular con anterioridad a la emisión, conforme al §9.4.5.

9.4.2. Información tratada como privada

Tienen la consideración de información privada los datos personales del Titular que no se incorporan al certificado, y en particular:

a) El domicilio y los datos de contacto.

b) Las imágenes, grabaciones y datos biométricos obtenidos en el proceso de acreditación conforme al §3.2.3, incluidas las grabaciones de las sesiones de acreditación en modalidad asistida.

c) Las copias de los documentos de identidad aportados.

d) Los datos de activación y las credenciales de acceso a la plataforma.

e) El historial de operaciones del Titular en la plataforma.

f) Los datos tratados por el Prestador de Sistemas de Pruebas de Identidad del §3.2.6 por cuenta de **DIGITO**.

Dicha información se conserva conforme al §5.5.2 y con las medidas del §9.4.4.

9.4.3. Información no considerada privada

No tiene la consideración de información privada la que se incorpora al propio certificado, por su naturaleza destinada a ser conocida por cualquier tercero que verifique una firma. Comprende, en los certificados emitidos conforme a la presente Política, el nombre y los apellidos del Titular, su correo y su número de documento de identidad.

El Titular es informado expresamente, con anterioridad a la emisión y como parte del consentimiento previsto en el §4.1.2, de que dichos datos quedan incorporados de forma permanente e inmutable en cada documento que suscriba y son accesibles a cualquier tercero que lo verifique.

En aplicación del principio de minimización, **DIGITO** no incorpora al certificado datos distintos de los enumerados. En particular, la dirección y el domicilio del Titular que exige la Normativa Vigente constan en el expediente de registro y no se incorporan al certificado, en virtud de la equivalencia declarada por la Normativa Vigente.

Para los tipos de certificados que apliquen, no se considerara información privada la siguiente:

- La razón social
- El identificador de la persona jurídica
- El cargo o función del Titular
- Su 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.

9.4.4. Responsabilidad de proteger la información privada

DIGITO protege los datos personales mediante los controles técnicos y organizativos de los capítulos 5 y 6, y restringe su acceso al personal que lo requiera.

Los proveedores externos que traten datos personales por cuenta de **DIGITO** quedan sujetos a las obligaciones del §5.3.7 y a las que resulten exigibles conforme a la Normativa Vigente.

DIGITO notifica las brechas de seguridad que afecten a datos personales conforme al §5.7.1 y a la normativa aplicable.

9.4.5. Aviso y consentimiento para el uso de información privada

DIGITO informa al Titular, con anterioridad al tratamiento, de los extremos previstos en el §9.4.1, y obtiene su consentimiento expreso, informado y verificable conforme al §4.1.2.

El consentimiento comprende expresamente el tratamiento de los datos biométricos necesarios para la acreditación de identidad conforme al §3.2.3, y la incorporación al certificado de los datos del §9.4.3.

La evidencia del consentimiento se conserva conforme al §5.5.2.

El Titular puede ejercer sus derechos de acceso, rectificación, supresión, oposición y limitación en los términos de la Normativa Vigente, mediante el procedimiento publicado. El ejercicio del derecho de supresión no alcanza a la información cuya conservación resulte exigible conforme al §5.5.2, ni al contenido de los certificados ya emitidos.

9.4.6. Divulgación por proceso judicial o administrativo

DIGITO divulgará información privada cuando resulte requerida por resolución judicial o administrativa dictada por autoridad competente, o cuando lo exija la normativa aplicable.

La divulgación se limitará a la información estrictamente requerida, quedará registrada conforme al §5.4.1, y se comunicará al afectado salvo que la propia resolución o la normativa lo impidan.

9.4.7. Otras circunstancias de divulgación

Fuera de los supuestos del §9.4.6, **DIGITO** únicamente divulgará información privada con el consentimiento expreso del afectado.

La comunicación de datos a los proveedores del §5.3.7, en la medida necesaria para la prestación del servicio, no constituye divulgación a los efectos del presente apartado, y se sujeta a las obligaciones del §9.4.4.

9.5. Derechos de propiedad intelectual

DIGITO conserva la titularidad de los derechos de propiedad intelectual sobre la presente Política, sobre la Declaración de Prácticas de Certificación, sobre los identificadores de objeto asignados dentro de su arco privado de empresa y sobre sus marcas y signos distintivos.

Se autoriza la reproducción y distribución de la presente Política de forma íntegra y sin modificación, con indicación de su origen.

Los certificados emitidos son propiedad de **DIGITO,** que concede al Titular una licencia de uso no exclusiva, intransferible y limitada al período de validez, para los fines previstos en el §1.4.1.

Las claves privadas y públicas corresponden en exclusiva a sus Titulares, sin perjuicio de lo dispuesto en el §6.1.2 sobre su custodia en el dispositivo cualificado.

9.6. Manifestaciones y garantías

Las manifestaciones y garantías de cada participante se establecen en los apartados siguientes, sin perjuicio de las que resulten de la Política de Certificación aplicable a cada clase.

9.6.1. Manifestaciones y garantías de la Autoridad de Certificación

DIGITO garantiza que:

a) Presta sus servicios conforme a las Políticas del §1.2, a la presente Declaración y a la normativa aplicable.

b) Verifica la identidad del Titular conforme al capítulo 3 con anterioridad a la emisión.

c) La información consignada en el certificado se corresponde con la verificada al momento de la emisión.

d) Emite los certificados conforme al perfil del capítulo 7 y de la Política aplicable.

e) Las claves privadas de los Titulares se generan y custodian en un dispositivo cualificado de creación de firma y se mantienen bajo control exclusivo del Titular conforme al §6.4.

f) Revoca los certificados en los supuestos y plazos del §4.9, y mantiene disponible la información de estado conforme al §4.10.

g) Conserva la información conforme al §5.5.2.

h) No accede a las claves privadas de los Titulares ni dispone de mecanismo alguno para utilizarlas.

i) Emite sellos de tiempo conforme a la política del §1.2 y a la norma ETSI EN 319 421.

DIGITO no garantiza extremos distintos de los enumerados, conforme al §9.7.

9.6.2. Manifestaciones y garantías de la Autoridad de Registro

Las Autoridades de Registro y Autoridades de Registro Locales garantizan que practican la verificación de la identidad y de los atributos conforme al capítulo 3, que conservan la evidencia obtenida y que tramitan las solicitudes conforme a los procedimientos establecidos.

DIGITO responde de las actuaciones de las Autoridades de Registro que operen bajo su responsabilidad, conforme al §5.3.7.

9.6.3. Manifestaciones y garantías del Titular

Al aceptar el certificado, el Titular garantiza que:

a) La firma digital autenticada mediante el certificado estará bajo su control exclusivo.

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

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

Son asimismo obligaciones del Titular:

d) Suministrar información completa, precisa y verídica, y mantenerla actualizada.

e) Custodiar sus datos de activación y no divulgarlos a terceros, conforme al §6.4.2.

f) Utilizar el certificado únicamente para los fines del §1.4.1 y durante su período de validez.

g) Solicitar la revocación de forma inmediata en los supuestos del §4.9.4.

h) Cumplir las políticas y condiciones establecidas por **DIGITO** y por las autoridades competentes.

i) Cooperar y proporcionar la información necesaria en caso de disputa legal o de requerimiento de colaboración en una investigación.

j) Mantener la confidencialidad de sus credenciales de acceso a la plataforma y responder de la actividad que ocurra en su cuenta.

Cuando intervenga una Organización Vinculada, en las clases cuya Política así lo prevea, ésta asume las obligaciones que dicha Política establezca, y en particular las relativas a la autenticidad de la documentación aportada y a la comunicación de los cambios que afecten a la información del certificado.

El Titular responde de la falsedad o del error en la información suministrada y de la omisión o retraso en el aviso de revocación, conforme al §9.9 y a la Normativa Vigente.

9.6.4. Manifestaciones y garantías de las partes que confían

Las partes que confían garantizan que, con anterioridad a otorgar efectos a un certificado:

a) Comprueban su estado de revocación conforme al §4.9.10.

b) Verifican la cadena de certificación hasta el certificado raíz de **DIGITO**.

c) Verifican que el certificado se encontraba vigente en la fecha de la firma, mediante sello de tiempo cualificado cuando la verificación sea posterior a su expiración.

d) Comprueban que el uso se corresponde con el previsto en el §1.4.1 y con los límites del certificado.

e) Conocen y aceptan la presente Política y las limitaciones del §9.8.

La omisión de estas comprobaciones excluye la condición de tercero de buena fe exento de culpa a los efectos de la Normativa Vigente.

9.6.5. Manifestaciones y garantías de otros participantes

Los proveedores externos que intervienen en la prestación garantizan el cumplimiento de las obligaciones asumidas contractualmente conforme al §5.3.7, y mantienen vigentes las certificaciones y evaluaciones de conformidad declaradas.

9.7. Exención de garantías

DIGITO no garantiza extremos distintos de los del §9.6.1. En particular, no garantiza:

a) La idoneidad del certificado para finalidad distinta de las del §1.4.1.

b) El contenido, la veracidad o los efectos jurídicos de los documentos suscritos por el Titular.

c) La capacidad, facultades o legitimación del Titular para el acto que suscribe.

d) El comportamiento de las aplicaciones de terceros empleadas para generar o verificar firmas.

e) La disponibilidad de redes o servicios de terceros ajenos a su control.

f) La aceptación del certificado por terceros.

9.8. Limitaciones de responsabilidad

DIGITO responde de la correcta ejecución de las verificaciones descritas en la presente Declaración y en la Política aplicable, conforme a la documentación aportada y en el momento en que fueron practicadas.

DIGITO no responde de:

a) La inautenticidad, falsedad o inexactitud de la documentación aportada, cuando tales vicios no fueran detectables mediante los procedimientos previstos.

b) La omisión o el retraso del Titular o de la Organización Vinculada en la solicitud de revocación conforme al §4.9.4.

c) El uso del certificado para fines distintos de los previstos o excediendo sus límites.

d) Los daños derivados de que la parte que confía haya omitido las comprobaciones del §9.6.4.

e) El uso de la clave privada por tercero que hubiere accedido a los datos de activación del Titular por causa imputable a éste.

f) Los daños derivados de la indisponibilidad de servicios de terceros ajenos a su control, sin perjuicio de los compromisos del §4.10.2.

Las presentes limitaciones se publican en la presente Declaración y son oponibles a las partes que confían, quienes las aceptan por el hecho de utilizar los servicios de validación de **DIGITO.**

Lo anterior se entiende sin perjuicio del deber de revocar del §4.9.2, que no admite limitación ni exclusión por acuerdo entre las partes, y de las responsabilidades que resulten indisponibles conforme a la normativa aplicable.

9.9. Indemnizaciones

El Titular mantendrá indemne a **DIGITO** frente a las reclamaciones de terceros derivadas de la falsedad o inexactitud de la información suministrada, del incumplimiento de su obligación de solicitar la revocación, del uso del certificado excediendo sus límites y del incumplimiento de las obligaciones del §9.6.3.

Las partes que confían mantendrán indemne a **DIGITO** frente a los daños derivados de la omisión de las comprobaciones del §9.6.4.

9.10. Vigencia y terminación

9.10.1. Vigencia

La presente Declaracion entra en vigor desde su publicación en el repositorio conforme al §2.2, y permanece vigente hasta su sustitución por una versión posterior o hasta su derogación expresa.

9.10.2. Terminación

La presente Política se extingue por su sustitución, por su derogación expresa acordada por la Autoridad de Políticas, o por el cese de actividades de **DIGITO** conforme al §5.8.

9.10.3. Efecto de la terminación y supervivencia

Extinguida la Declaración, subsisten las obligaciones de **DIGITO** respecto de los certificados emitidos bajo su vigencia, en particular las de revocación, disponibilidad de la información de estado conforme al §4.10.2 y conservación conforme al §5.5.2.

Las versiones sucesivas se conservan conforme al §5.5.1, literal g), a fin de permitir determinar el régimen aplicable a cada certificado en función de la fecha de su emisión.

9.11. Notificaciones y comunicaciones individuales

Las notificaciones de **DIGITO** al Titular relativas a la emisión, aceptación, rechazo y revocación se practican por el canal de comunicación registrado en su expediente y surten plenos efectos conforme al régimen de validez de la comunicación electrónica.

La proximidad de la expiración del certificado no se comunica mediante notificación individual. **DIGITO** pone dicha información a disposición del Titular a través de la plataforma, que muestra el estado de vigencia de sus certificados con indicación diferenciada según la proximidad de la fecha de expiración, conforme a los umbrales siguientes:

a) Estado normal, cuando restan más de treinta **(30) días** naturales para la expiración.
b) Estado de advertencia, cuando restan **treinta (30) días** naturales o menos.
c) Estado crítico, cuando restan **siete (7) días** naturales o menos.

Los umbrales son parámetros de la plataforma y su modificación no requiere la de la presente Declaración.

Corresponde al Titular consultar el estado de vigencia y solicitar la emisión de un certificado nuevo con anterioridad a la expiración. La disponibilidad de dicha indicación no traslada a **DIGITO** deber alguno de aviso individual, y la falta de consulta no altera la fecha de expiración ni genera derecho a prórroga ni indemnización.

9.12. Modificaciones del documento

9.12.1. Procedimiento de modificación

El procedimiento es el del §1.5.4. Corresponde a la Autoridad de Políticas calificar cada modificación como sustancial o no sustancial, a los efectos de los §9.12.2 y §9.12.3.

9.12.2. Mecanismo y período de notificación

Las modificaciones que puedan afectar la aceptación del servicio se publican en el repositorio con una antelación no inferior a **treinta (30) días** naturales respecto de su entrada en vigor, conforme al requisito REQ-6.1-09 de la norma ETSI EN 319 401. Las restantes surten efecto desde su publicación.

9.12.3. Circunstancias en que debe cambiarse el OID

Las modificaciones del perfil de certificado que no comporten cambio del identificador de la Política conforme a los párrafos anteriores se aplican con carácter prospectivo, exclusivamente a los certificados emitidos con posterioridad a su implementación técnica.

No afectan la validez de los certificados vigentes ni requieren su revocación o reemisión, conforme al requisito REV-6.3.9-02 de la norma ETSI EN 319 411-1, salvo que concurra alguna de las circunstancias que dicho requisito califica como causal de revocación: que el certificado deje de ser conforme con la Política bajo la que fue emitido, que sobrevenga un cambio que afecte su validez, o que el criptosistema empleado deje de garantizar el vínculo entre el Titular y su clave pública.

En tales supuestos, la revocación se rige por el §4.9.1.

9.13. Disposiciones de resolución de conflictos

Las controversias derivadas de la prestación de los servicios se someterán en primer término al procedimiento de reclamación de **DIGITO**, atendido a través de su Centro de Atención al Consumidor y al Usuario, conforme a la Normativa Vigente.

El Centro de Atención atiende a través del correo electrónico **soporte@digito.do** y de los demás canales publicados en el repositorio conforme al §2.2.

Las reclamaciones podrán presentarse dentro del plazo de **treinta (30) días** calendario contados desde la fecha en que se genere el hecho que las origina, conforme a la Normativa Vigente.

DIGITO responderá a la reclamación en un plazo no mayor a **veinte (20) días** calendario contados desde su presentación, y notificará su decisión al reclamante por escrito dentro de dicho plazo, conforme a la Normativa Vigente.

DIGITO no podrá negarse a recibir reclamaciones ni condicionar su presentación o conocimiento al pago previo de contraprestación alguna, conforme a la Normativa Vigente.

Las reclamaciones se inscriben en el registro previsto en la Normativa Vigente, que se conserva por un período de **seis (6) meses** desde su recepción, prorrogable automáticamente cuando la decisión sea recurrida ante la Dirección Ejecutiva del INDOTEL.

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, conforme a la Normativa Vigente.

Las decisiones de **DIGITO** sobre las reclamaciones podrán ser recurridas mediante Recurso de Queja ante la Dirección Ejecutiva del INDOTEL, conforme a la Normativa Vigente, sin perjuicio de la facultad del reclamante de acudir a los tribunales competentes de la República Dominicana.

9.14. Ley aplicable

La presente Declaración se rige por el derecho de la República Dominicana, y en particular por la Normativa Vigente en materia de comercio electrónico, documentos, firmas digitales y servicios electrónicos de confianza.

La remisión a normas técnicas de la European Telecommunications Standards Institute y a especificaciones del Internet Engineering Task Force se practica a los efectos técnicos previstos en la Normativa Vigente, sin que ello comporte la sujeción de **DIGITO** al ordenamiento jurídico de la Unión Europea.

9.15. Cumplimiento de la ley aplicable

DIGITO declara que la presente Declaración y las Políticas derivadas se ajustan a la Normativa Vigente en la República Dominicana en materia de servicios electrónicos de confianza, firma electrónica y protección de datos personales.

Los certificados emitidos conforme a las Políticas de firma electrónica tienen la consideración de Certificados Cualificados de Firma Electrónica conforme a la Normativa Vigente, que los considera equivalentes a los certificados digitales regulados en ella.

Las firmas generadas mediante dichos certificados y con los datos de creación custodiados conforme al capítulo 6 tienen la consideración de Firma Electrónica Cualificada, con los efectos que les atribuye la Normativa Vigente.

DIGITO se somete a la supervisión del INDOTEL y a las evaluaciones del capítulo 8.

9.16. Disposiciones misceláneas

9.16.1. Acuerdo completo

La presente Declaración, las Políticas de Certificación, la Declaración de Divulgación de Prácticas y los términos y condiciones aceptados constituyen el régimen aplicable a la prestación de los servicios.

En caso de discrepancia prevalecerá el orden siguiente: la Política de Certificación aplicable; la presente Declaración; los términos y condiciones; las condiciones particulares acordadas.

9.16.2. Cesión

DIGITO no cede los derechos y obligaciones derivados de la prestación de sus servicios sin autorización previa del INDOTEL. Toda transmisión se practicará preservando los derechos de los Titulares y las obligaciones de conservación del §5.5.2, y se comunicará conforme al §9.12.2.

El Titular no puede ceder ni transferir su certificado ni los derechos derivados del mismo, por corresponder de forma personalísima a la persona identificada en él.

9.16.3. Divisibilidad

La declaración de nulidad o ineficacia de cualquiera de las disposiciones de la presente Política no afectará a la validez de las restantes, que continuarán siendo aplicables. La disposición afectada será sustituida por aquella que resulte conforme a la normativa aplicable y más próxima a la finalidad perseguida.

9.16.4. Ejecución

La falta de ejercicio por **DIGITO** de cualquiera de los derechos o facultades previstos en la presente Política no comportará su renuncia ni impedirá su ejercicio posterior. El régimen de costas se rige por la normativa procesal aplicable.

9.16.5. Fuerza mayor

DIGITO no responderá del incumplimiento de sus obligaciones cuando obedezca a causas de fuerza mayor o caso fortuito, entendidas como acontecimientos imprevisibles o inevitables ajenos a su control.

Acaecida tal circunstancia, **DIGITO** adoptará las medidas del §5.7 y comunicará la situación a los Titulares, a las partes que confían y al INDOTEL.

La fuerza mayor no exonera del deber de revocar del §4.9.2 ni de mantener la información de estado del §4.10.2, respecto de los cuales **DIGITO** aplicará las medidas de continuidad del §5.7.4 a fin de restablecer el servicio en el menor plazo posible.

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