POLÍTICA DE CERTIFICACIÓN DIGITO FINANCIAL TECHNOLOGY GROUP, LLC.

Persona Física

POLITICA OID: 1.3.6.1.4.1.64999.1.3.1

CONTROL DE VERSIONES

Versión	Fecha	Descripción de los cambios	Motivo
1.0	17 de septiembre de 2024	Creación inicial del documento.	Legislación
2.0	19 de diciembre de 2024	Modificación de la Sección 3.1, Sección 5.4.2, Sección 7	Solicitud del órgano regulador de República Dominicana
3.0	28 de abril de 2025	Modificación de la Sección 1.5.1, Sección 7.1	Solicitud del órgano regulador de República Dominicana
4.0	16 de marzo de 2026		Instalación de PKI
4.1	05 de mayo de 2026	Actualización integral de los Secciones	Alineación y cumplimiento estricto de los requisitos obligatorios de las normas ETSI
5.0	24 de mayo de 2026	Actualización de PKI	Implementación de mejores prácticas
6.0	30 de junio de 2026	Actualización de PKI	Incorporación de nueva Issuing
7.0	29 de julio de 2026	Modificación de Formato y nueva información siguiendo el estándar RFC 3647	Incorporación de información relacionada al campo OID perteneciente a la política que rige este perfil.

7.1	27 de octubre de 2026	Datos de activación con segundo factor de autenticación (§6.2.8 y §6.4); 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 (§1.3.3); 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 7.1, 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 7.1, 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. Introducción.

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. Propósito Del Documento.

Esta Política de Certificación tiene como propósito establecer un marco de confianza para los Solicitantes y Usuarios de los servicios de **DIGITO**, así como para los Titulares de Certificados Digitales emitidos por **DIGITO** como EC.

En ese sentido, se busca garantizar la autenticidad e integridad de la información contenida en los certificados digitales, definir los derechos y responsabilidades de **DIGITO**, los Solicitantes, Usuarios, Titulares de Certificados Digitales y las partes que confían en los certificados digitales.

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

1.2. Nombre del documento e identificación (OID)

El presente documento se denomina Política de Certificación de **DIGITO** para certificados cualificados de firma electrónica de persona física y se identifica mediante el identificador de objeto (OID) 1.3.6.1.4.1.64999.1.3.1, asignado dentro del arco privado de empresa de **DIGITO** conforme a la Taxonomía de OID de **DIGITO**.

La presente Política se fundamenta en la política QCP-n-qscd definida en la norma *ETSI EN 319 411-2*, en cumplimiento del requisito OVR-7.1-02 de la norma *ETSI EN 319 411-1*. DIGITO identifica su política mediante un OID propio, en lugar del identificador 0.4.0.194112.1.2, por tratarse de un Prestador Cualificado de Servicios de Confianza sujeto a la legislación de la República Dominicana.

La versión, la fecha de aprobación y el historial de revisiones constan en la sección de control de versiones. Toda modificación que afecte la aplicabilidad de la Política dará lugar al cambio del OID, conforme al §9.12.3.

1.3. Participantes de la ICP

La jerarquía de los certificados de la PKI incluye el *Digito Root CA* como la Autoridad de Certificación Raíz y el *Digito Issuing CA* como la Autoridad de Certificación Subordinada. El *Digito Root CA* emite certificados para el *Digito Issuing CA*, que a su vez emite certificados a las Entidades Finales (End-Entities) dentro del sistema.

En los certificados emitidos conforme a la presente Política, el Suscriptor y el Titular son la misma persona física, que actúa en nombre propio y por cuenta propia. No concurre en ellos ningún tercero contratante distinto del Titular, ni se incorporan atributos relativos a personas jurídicas.

Los certificados que vinculan a una persona física con una persona jurídica se rigen por la Política de Certificación específicamente aplicable a esa clase, identificada por su propio identificador de objeto.

1.3.1. Autoridad de Certificación (AC).

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).

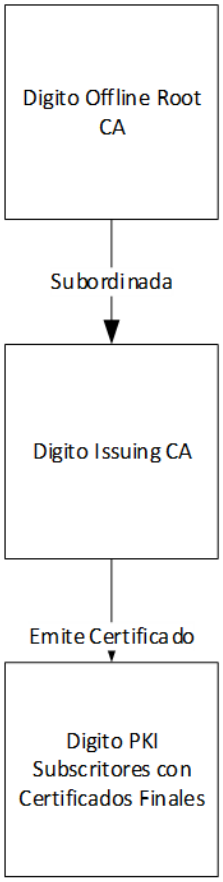
CN: DIGITO ROOT CA
Hash SHA256:
A855459DCCB649DB801D52B5FDF63988E98AD3970F7C6C345116223A688896BB
Válido desde el 22 de junio de 2026 hasta el 17 de junio de 2046
Longitud de Clave RSA 4096 – SHA256

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

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. 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.

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, que en la presente Política coincide con el Titular.

1.3.4. Terceros que confían

Para los fines de esta política, 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.

1.4. Uso de los certificados

1.4.1. Usos Apropiados De Los Certificados Digitales Emitidos Por Digito

Los certificados emitidos conforme a la presente Política se destinan a la firma electrónica cualificada por personas físicas actuando en nombre propio y por cuenta propia.

Su uso comprende la creación de firmas electrónicas cualificadas con los efectos previstos en la Normativa Vigente, sobre documentos y mensajes de datos en los que el Titular actúa a título personal.

Los certificados incorporan la extensión *keyUsage* con los valores *digitalSignature* y *nonRepudiation*, conforme al §6.1.7 y al §7.1.2, y no incorporan *extendedKeyUsage*.

Estos certificados no acreditan vínculo institucional alguno del Titular con persona jurídica, ni incorporan atributos organizacionales. Los certificados que incorporan tales atributos se rigen por la Política de Certificación identificada mediante el OID *1.3.6.1.4.1.64999.1.3.4*.

Las restantes clases de certificado emitidas por **DIGITO**, así como el servicio de sellado de tiempo cualificado, se enumeran en el §1.4.1 de la Declaración de Prácticas de Certificación.

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

Los certificados emitidos conforme a la presente Política no podrán utilizarse:

a) Para el cifrado de información ni para el establecimiento de claves de sesión, conforme al §4.12.2.

b) Para la firma de código.

c) Para acreditar la representación de una persona jurídica o la pertenencia del Titular a una organización.

d) Con posterioridad a la expiración del certificado o a su revocación, conforme al §4.5.1.

e) Para fines distintos de los previstos en el §1.4.1, o excediendo los límites establecidos en la presente Política.

El uso del certificado para fines no autorizados exonera a **DIGITO** de responsabilidad conforme al §9.8.

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 PC.

Corresponde a la Autoridad de Políticas de **DIGITO** determinar si la presente Política de Certificación satisface los requisitos establecidos en cada una de las Políticas de Certificación que **DIGITO** soporta.

El dictamen se emite con carácter previo a la aprobación de cualquier versión de la presente 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 PC

La aprobación de la presente Política y de sus modificaciones sigue el procedimiento siguiente:

• Elaboración de la propuesta por el área responsable, con identificación de los cambios respecto de la versión vigente.

• Revisión por la Autoridad de Políticas, incluido el dictamen del §1.5.3.

• Aprobación por el órgano de dirección de **DIGITO**, con autoridad final conforme al requisito REQ-6.1-06 de la ETSI EN 319 401, documentada mediante su firma en la sección de aprobación del documento, con posterioridad a la firma de la Autoridad de Políticas.

• Comunicación previa a suscriptores y terceros que confían cuando el cambio pueda afectar la aceptación del servicio, conforme al §9.12.2.

• Publicación inmediata de la versión aprobada en el repositorio, conforme al §2.2.

• Notificación al INDOTEL en los supuestos y plazos previstos por la Normativa Vigente.

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 Política se revisa, como mínimo, con periodicidad anual, con independencia de que existan o no 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.

- **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.

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

- **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.

1.6.2. Siglas.

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

- AC - Autoridad de Certificación (o CA por sus siglas en inglés).
- EC - Entidad de Certificación.
- PKI - Infraestructura de Clave Pública (Public Key Infrastructure).
- TSA - Autoridad de Sellado de Tiempo (Time Stamping Authority).
- HSM - Módulo de Seguridad de Hardware (Hardware Security Module).
- RA - Autoridad de Registro.
- LRA - Autoridad de Registro Local.
- UMS - Servicio de Gestión de Usuarios (User Management Service).
- CSR - Solicitud de firma de certificado (Certificate signing request).
- AP - Autoridad de Políticas.

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 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*, en cumplimiento de 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

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 Políticas de Certificación y la Declaración de Prácticas 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 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:

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 de componentes de la infraestructura incorporan los atributos propios de su función, conforme al §7.1 de la presente Política.

3.1.2. Necesidad de que los nombres sean significativos

Los Nombres Distintivos consignados en los certificados emitidos por **DIGITO** son significativos: identifican de forma comprensible a la persona física 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

DIGITO no permite el uso de seudónimos por parte de los Titulares de Certificados.

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 lo establecido en la norma ETSI EN 319 412-1, incorporada por la Normativa Vigente. En particular, el atributo *serialNumber* de persona física se compone del prefijo de tres caracteres correspondiente al tipo de documento (IDC para cédula de identidad y electoral, PAS para pasaporte), seguido del código de país conforme a la norma ISO 3166, un guión, y el número de documento.

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 conforme a la presente Política.

Un mismo Titular podrá ostentar simultáneamente certificados vigentes acreditados mediante distintos tipos de documento de identidad, conforme al §3.1.4, así como más de un certificado acreditado mediante un mismo documento.

Cada emisión exige una validación de identidad propia conforme al §3.2.7. La existencia de un certificado vigente no exime de dicha validación respecto de una emisión posterior, ni permite la reutilización de la evidencia obtenida en la emisión anterior fuera de la ventana establecida en dicho apartado.

Cada certificado se asocia a un par de claves propio y exclusivo, y a datos de activación independientes, conforme al §6.1.1 y al §6.4.3.

Todos los certificados de 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

No está estipulado. Los certificados emitidos conforme a la presente Política se expiden a personas físicas actuando en nombre propio y no incorporan atributos relativos a personas jurídicas. La autenticación de la identidad de

organizaciones se rige por la Política de Certificación aplicable a las clases de certificado que incorporen tales atributos.

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 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

No estipulado. Las solicitudes de certificado conforme a la presente Política son presentadas por el propio Titular, actuando en nombre propio, sin intervención de solicitante autorizado alguno.

La validación de la autoridad de quien solicita un certificado por cuenta de un tercero se rige por la Política de Certificación aplicable a esa clase de certificado.

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, y validación biométrica, a través de los servicios ofrecidos por la Junta Central Electoral de la República Dominicana, conforme a la Normativa Vigente. Estos servicios resultan 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 periódicamente 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 en la verificación de la identidad del Titular podrá reutilizarse en solicitudes posteriores durante las **veinticuatro (24) horas** siguientes a su obtención.

Excedido dicho plazo, **DIGITO** practicará un nuevo proceso completo de validación de identidad en tiempo real, sin que resulte admisible el consumo de validaciones preexistentes.

Dentro de dicha ventana podrá emitirse un máximo de **un (1) certificado** sobre una misma validación de identidad, 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

No procede la renovación respecto de un certificado revocado o caducado.

La obtención de un certificado nuevo por el mismo Titular exige la repetición íntegra del procedimiento de registro e identificación establecido en el §3.2, con independencia de la causa que hubiere motivado la revocación o de la antigüedad de la evidencia de identidad previamente obtenida.

No resulta admisible en estos supuestos la identificación mediante certificado, ni el consumo de validaciones de identidad preexistentes.

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

Para la identificación y autenticación de las solicitudes de revocación de certificados, se llevará a cabo el procedimiento de autenticación de identidad automática con la plataforma **DIGITO** o el proceso de autenticación de identidad manual, establecidos en la Declaración de Prácticas de Certificación.

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

4.1. Solicitud de Certificado

El procedimiento de solicitud de certificados, los sujetos legitimados para presentarla y las responsabilidades derivadas del proceso de inscripción se rigen por el §4.1 de la Declaración de Prácticas de Certificación de **DIGITO**.

4.1.1. Quién puede presentar una solicitud

Podrán presentar una solicitud de certificado la persona física que vaya a ser Titular del certificado, actuando en nombre propio

No se admiten solicitudes presentadas por terceros, ni por representantes, mandatarios o apoderados del Titular, sin perjuicio de los supuestos de representación legal de personas con capacidad restringida que **DIGITO** atienda conforme a la normativa aplicable.

En todo caso, la emisión requiere el consentimiento expreso del Titular en los términos del §4.1.2.

4.1.2. Proceso de Inscripción y Responsabilidades

El proceso de inscripción comprende la identificación del solicitante, la verificación de su identidad conforme al §3.2.3, la aceptación de los términos y condiciones aplicables y la obtención del consentimiento del Titular.

Dado que el Suscriptor y el Titular son la misma persona conforme al §1.3, la aceptación de los términos y condiciones y el consentimiento se otorgan en un único acto, mediante la firma del Acuerdo de Uso de Certificados Digitales o la aceptación electrónica expresada en el portal de registro.

DIGITO conserva la evidencia del consentimiento y de la aceptación de los términos por el plazo establecido en el §5.5.2 de la Declaración de Prácticas de Certificación.

4.2. Procesamiento de la solicitud de certificado

Recibida la solicitud, **DIGITO** ejecuta las funciones de identificación y autenticación previstas en el capítulo 3 y resuelve su aprobación o rechazo conforme a los §4.2.2 y §4.2.3.

4.2.1. Ejecución de las funciones de I&A

La ejecución de las funciones de identificación y autenticación previas a la aprobación de una solicitud se rige por el §4.2.1 de la Declaración de Prácticas de Certificación de **DIGITO**. Ninguna solicitud se aprueba antes de haberse completado satisfactoriamente las funciones aplicables del capítulo 3.

4.2.2. Aprobación o rechazo de solicitudes

DIGITO aprobará la solicitud cuando se hayan completado satisfactoriamente todas las verificaciones exigidas por el capítulo 3 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.

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

DIGITO procesará las solicitudes de certificado en un plazo no superior a **cinco (5) días** hábiles desde la recepción de la documentación completa. En los procedimientos de identificación remota desatendida, el procesamiento es inmediato una vez superadas satisfactoriamente las comprobaciones automatizadas.

4.3. Emisión de Certificado

Las actuaciones de la Autoridad de Certificación durante la emisión y la notificación al Titular se rigen por los §4.3.1 y §4.3.2 de la Declaración de Prácticas de Certificación de **DIGITO**.

4.3.1. Actuaciones de la AC durante la emisión

Aprobada la solicitud, **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 la emisión de su certificado, o el rechazo de la solicitud, por el canal de comunicación registrado en su expediente. El procedimiento se establece en el §4.3.2 de la Declaración de Prácticas de Certificación.

4.4. Aceptación del certificado

La conducta que constituye aceptación del certificado, su publicación y la notificación a terceros se rigen por los §4.4.1 a §4.4.3 de la Declaración de Prácticas de Certificación de **DIGITO**. No se admite la aceptación tácita.

4.4.1. Conducta que constituye aceptación

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

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.

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 al mismo.

Con la aceptación, el Titular asume las garantías establecidas en el §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 emitidos conforme a la presente Política 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

4.5.1. Uso de la clave privada por el titular

- 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**, las partes que confían deben:

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.

Las partes que confían deben 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.

Las partes que confían quedan sujetas 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 Política, 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 autónomo del ciclo de vida del certificado.

A los efectos de la presente Política, 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 de certificados es el proceso de invalidar un certificado previamente emitido por **DIGITO**, antes de la fecha de su expiración.

En la Declaración de Prácticas de Certificación se establecen los lineamientos y procedimientos necesarios para revocar un certificado. **DIGITO** AC publica una Lista de Revocación de Certificados (CRL) y opcionalmente proporciona un servicio de Protocolo de Estado de Certificado en Línea (OCSP). La CRL es una lista actualizada regularmente de certificados revocados que puede ser verificada por las partes para comprobar el estado de un certificado. Por otro lado, el OCSP permite verificar en tiempo real el estado de revocación mediante una consulta al servidor de la AC.

Por tanto, revocar un certificado implica la invalidación del mismo, su eliminación de los repositorios de confianza, su no utilización en transacciones o comunicaciones seguras y su presencia en las Listas de Revocación de Certificados (CRL). Es responsabilidad del titular del certificado informar de inmediato cualquier situación que pueda justificar una revocación y seguir los procedimientos establecidos por **DIGITO** para gestionar la revocación de un certificado digital.

4.9.1. Circunstancias para la revocación

DIGITO revocará un certificado emitido conforme a la presente Política cuando concurra alguna de las circunstancias siguientes:

a) A solicitud del Titular, formulada 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 asociada al certificado o de los datos de activación previstos en el §6.4, así como pérdida de control de dicha 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 de identificación del Titular consignados en el certificado, de forma que dejen de ser exactos.

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 de las longitudes de clave empleados.

i) Cese de actividades de **DIGITO**, en los términos del §5.8 de la Declaración de Prácticas de Certificación.

j) Resolución del INDOTEL o de autoridad judicial o administrativa competente que así lo ordene.

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 dicho conocimiento 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 de un certificado:

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) 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.

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

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

4.9.3. Procedimiento de solicitud de revocación

El procedimiento de solicitud de revocación se encuentra disponible de forma ininterrumpida, **veinticuatro (24) horas** al día los **siete (7) días** de la semana.

Toda solicitud se autentica conforme al §3.4 y se comprueba que proceda de fuente legitimada conforme al §4.9.2, con anterioridad a practicar la revocación.

DIGITO procesa las solicitudes al momento de su recepción y publica el estado de revocación dentro del plazo del §4.9.5.

El resultado de la solicitud se notifica al Titular conforme al §4.9.2, literal a), de la presente Política, salvo imposibilidad material.

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 de esta obligación 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 de revocación al momento de su recepción, y publica el estado de revocación en un plazo máximo de **veinticuatro (24) horas**

contadas desde la recepción de la solicitud, 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 (24) horas** al día los **siete (7) 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 en un certificado emitido conforme a la presente Política deberán verificar su estado de revocación con anterioridad a otorgarle efectos, mediante el servicio OCSP cuya localización se consigna en la extensión *authorityInformationAccess* del propio certificado, o mediante la lista de revocación publicada en el punto de distribución indicado en la extensión *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 excede 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 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.

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.

La información de estado de revocación se mantiene disponible más allá del período de validez del certificado, conforme a la Normativa Vigente. 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.

Las características operativas del servicio, su disponibilidad y sus funciones se establecen en el §4.10.

4.9.10. Requisitos de comprobación en línea

Las partes que confían en un certificado emitido conforme a la presente Política deben comprobar su estado de revocación con anterioridad a otorgarle efectos.

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.

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

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 del certificado.

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.

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** activará su procedimiento de contingencia y notificará de forma inmediata al INDOTEL, a los Titulares afectados y, mediante publicación en su repositorio, a las partes que confían. La comunicación indicará 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 de la Declaración de Prácticas de Certificación.

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.

4.10. 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.

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.

El período máximo de indisponibilidad del servicio, así como las medidas de continuidad aplicables, se establecen en el §5.7 de la Declaración de Prácticas de Certificación.

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.

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 en los certificados de persona física es el propio Titular, 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 conforme a la presente Política 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 conforme a la presente Política se destinan exclusivamente 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. La descripción de los controles implantados se establece en el §5.1.1 de la Declaración de Prácticas de Certificación de **DIGITO**.

5.1.2. Acceso físico

El acceso a las instalaciones en que se prestan los servicios de certificación está restringido al personal expresamente autorizado y se somete a los controles siguientes:

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. 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 de la Declaración de Prácticas de Certificación.

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 de confianza 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.

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 en un rol de confianza requiere la verificación previa de antecedentes conforme al §5.3.2 y la formación prevista en el §5.3.3, y queda documentada de forma expresa.

5.2.2. Número de personas requeridas por tarea

Las operaciones siguientes 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 en que se ubica el dispositivo criptográfico de la Autoridad de Certificación Raíz, que requiere la presencia simultánea de al menos dos personas en roles de confianza, conforme al §5.1.2, literal c).

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

Las ceremonias de claves se documentan en acta suscrita por todos los intervinientes, con indicación de las operaciones practicadas.

5.2.3. Identificación y autenticación para cada rol

El personal que desempeña roles de confianza se identifica y autentica con anterioridad al ejercicio de las funciones asociadas al rol, 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.

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 la identidad de un solicitante no aprueba su propia verificación cuando el procedimiento exija doble control.

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

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

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 los servicios de certificación 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 que desempeña roles de confianza cuenta con la formación, los conocimientos y la 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 de antecedentes del §5.3.2 y recibido la formación del §5.3.3.

Los criterios de cualificación y experiencia exigidos para cada rol se establecen en el §5.3.1 de la Declaración de Prácticas de Certificación de **DIGITO**.

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 de la verificación se conserva conforme al §5.5.2 y con sujeción a la normativa de protección de datos personales.

5.3.3. Requisitos de formación

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

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

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.

La formación recibida 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 a la 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 de gestión de incidentes 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. Dichos proveedores quedan sujetos a las obligaciones establecidas en los contratos correspondientes, 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 certificación, 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 practicadas, con indicación de la modalidad empleada, del resultado obtenido, de las fuentes consultadas y del Operador de Registro 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.

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.

Práctica 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 Política y de la Declaración de Prácticas de Certificación 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) años 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 Política 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 se establece en el §5.5.7 de la Declaración de Prácticas de Certificación.

5.6. Cambio de claves

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

El cambio 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 de compromiso conforme al §5.7.3.

La generación del nuevo par de claves se practica en ceremonia documentada, conforme al §6.1.1 y 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 previsto en el §4.10.2, y mantiene disponible el certificado de la Autoridad de Certificación 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 de sus servicios 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 de revocación del §4.9.1, y práctica 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 Entidad de Certificación, sea voluntario o no voluntario, se sujeta al procedimiento siguiente:

a) DIGITO comunicará su intención de cesar en la actividad 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 período de preaviso, **DIGITO** cesará la emisión de certificados nuevos y mantendrá la prestación de los servicios de revocación y de consulta del estado.

c) DIGITO revocará los certificados que se encuentren pendientes de expiración a la conclusión del período de 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 de conservación del §5.5.2.

e) DIGITO adoptará las medidas necesarias para que la información de estado de revocación 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.

f) Se destruirán las claves privadas de las Autoridades de Certificación, conforme al §6.2.10, documentándose la destrucción en acta.

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.

El plan de cese, con la asignación de responsabilidades y los plazos de cada actuación, se establece en el §5.8 de la Declaración de Prácticas de Certificación.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación del par de claves

Los pares de claves empleados en los servicios prestados conforme a la presente Política se generan e instalan con sujeción a los requisitos establecidos en los apartados siguientes, y con el detalle operativo que se establece en el capítulo 6.1 de la Declaración de Prácticas de Certificación de **DIGITO**.

6.1.1. Generación del par de claves

El par de claves del Titular se genera dentro del dispositivo cualificado de creación de firma gestionado por **DIGITO**, mediante algoritmos y generadores de números aleatorios que satisfacen los requisitos del §6.1.5.

La generación se practica en el momento de la emisión del certificado y de forma exclusiva para éste. No se reutilizan pares de claves entre certificados, ni en la emisión inicial ni con ocasión de una nueva emisión al mismo Titular, conforme al §4.7.

La clave privada se genera de modo que no resulte extraíble del dispositivo, y no existe en ningún momento fuera de él, ni siquiera de forma transitoria.

Los pares de claves de las Autoridades de Certificación se generan en ceremonia documentada, con el control multipersona del §5.2.2, dentro de dispositivos criptográficos que satisfacen los requisitos del §6.2.1.

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 del certificado.

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

Los pares de claves de los Titulares emitidos conforme a la presente Política emplean el algoritmo RSA con una longitud de clave no inferior a 2048 bits, y algoritmo de resumen SHA-256.

> Los pares de claves de las Autoridades de Certificación emplean el algoritmo RSA con una longitud de clave de 4096 bits y algoritmo de resumen SHA-256.

6.1.6. Generación y calidad de los parámetros de clave pública

Los parámetros de clave pública 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 certificados emitidos conforme a la presente Política incorporan la extensión keyUsage marcada como crítica, con los valores *digitalSignature* y *nonRepudiation*, y no incorporan *extendedKeyUsage*.

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

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

Las claves privadas empleadas en los servicios prestados conforme a la presente Política se generan, almacenan y utilizan dentro de dispositivos criptográficos que satisfacen los requisitos del §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 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, y los dispositivos que las albergan permanecen desactivados fuera de dichas operaciones. El dispositivo que alberga la clave de la Autoridad de Certificación Raíz se mantiene fuera de línea de forma permanente (offline Root CA).

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 emitidos conforme a la presente Política es de **treinta y seis (36) meses**.

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 de Certificación 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.

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 de certificación de **DIGITO** se someten a controles de seguridad proporcionados al riesgo, cuyo detalle se establece en el capítulo 6.5 de la Declaración de Prácticas de Certificación.

6.5.1. Requisitos técnicos específicos

Los sistemas que soportan los servicios de certificación 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.

6.5.2. Calificación de seguridad informática

DIGITO no somete sus sistemas a esquemas de calificación de seguridad informática distintos de las evaluaciones de vulnerabilidad 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.

Los equipos y soportes retirados del servicio se someten a los procedimientos de eliminación del §5.1.7.

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 conforme a la presente Política. Los perfiles de los certificados de las Autoridades de Certificación se establecen en el §7.1 de la Declaración de Prácticas de Certificación.

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

Extensión	Crítica	Contenido
keyUsage	Si	digitalSignature, nonRepudiation
extendedKeyUsage	N/A	No se incorpora
certificatePolicies	No	OID de la presente Política, con calificadores DPC y userNotice
qcStatements	No	Conforme al §7.1.2.1
authorityInformationAccess	No	OCSP
cRLDistributionPoints	No	Punto de distribución de la CRL
subjectKeyIdentifier	No	Conforme al RFC 5280
authorityKeyIdentifier	No	Conforme al RFC 5280
basicConstraints	Si	cA=FALSE
rfc822Name	Si	Dirección de correo electrónico dominio del titular.
calssuers	N/A	http://pki.digito.do/CAs/DigitoIssuingCADO02.crt

No se incorporan extensiones distintas de las enumeradas.

7.1.2.1. Declaraciones de certificado cualificado

La extensión *qcStatements* (OID 1.3.6.1.5.5.7.1.3) contiene:

Declaración	OID	Función

QcCompliance	0.4.0.1862.1.1	Indica que el certificado es 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	La clave reside 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, a fin de que las aplicaciones de validación interpreten correctamente el formato del atributo serialNumber.

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

El Nombre Distintivo se compone exclusivamente de:

Atributo	**Contenido**	**Ejemplo**
countryName	Código ISO 3166 del país del documento de identidad del Titular	DO

commonName	Nombre completo, para presentación	Nombre + Apellido
surname	Apellidos según documento de identidad	APELLIDO
givenName	Nombres según documento de identidad	NOMBRE
serialNumber	Conforme a EN 319 412-1, cap. 5.1.3	IDC/PAS+countryName +[-]cedula de identidad de la persona/numero de pasaporte

El prefijo del atributo *serialNumber* es IDC cuando la identidad se acredite mediante cédula de identidad y electoral, y PAS cuando se acredite mediante pasaporte, seguido en ambos casos del código de país del documento, un guión y el número de 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, no admitiéndose cédulas o documentos equivalentes de otros países al momento de la presente Política.

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

7.1.5. Restricciones de nombre

No estipulado. Los certificados emitidos conforme a la presente Política no incorporan la extensión nameConstraints.

7.1.6. Identificador de objeto de la política

La extensión certificatePolicies contiene exclusivamente el OID de la presente Política, asignado dentro del arco privado de DIGITO. El OID correspondiente para esta politica es 1.3.6.1.4.1.64999.1.3.1.

La presente Política se fundamenta en la política QCP-n-qscd de la norma ETSI EN 319 411-2, conforme al §1.2.

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 DPC, con el localizador de la Declaración de Prácticas de Certificación publicada por **DIGITO**; 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.

7.1.9. Semántica de procesamiento de la extensión crítica

La extensión certificatePolicies no se marca como crítica.

7.2. Perfil de la CRL

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

Las listas incorporan las extensiones *authorityKeyIdentifier*, *cRLNumber* y *ExpiredCertsOnCRL*, esta última conforme al §4.9.8 y con la fecha correspondiente al inicio de validez del certificado de la Autoridad de Certificación emisora.

Las entradas incorporan la fecha de revocación y, cuando proceda, el código de motivo. No se emplea el código certificateHold, por no practicar **DIGITO** la suspensión de certificados conforme al §4.9.13.

7.3. Perfil OCSP

DIGITO presta el servicio de consulta del estado conforme al protocolo OCSP definido en el IETF RFC 6960.

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 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.

Las respuestas no incorporan el campo *nextUpdate*, conforme al §4.10.1, ni la extensión *ArchiveCutOff*, conforme al §4.10.3.

El certificado del respondedor incorpora la extensión id-kp-OCSPSigning en su campo extendedKeyUsage y la extensión id-pkix-ocsp-nocheck, conforme al IETF RFC 6960.

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.

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.
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 prestados con la presente Política, con la Declaración de Prácticas de Certificación y con las normas y disposiciones aplicables, y alcanza al menos:

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

b) Los procedimientos de identificación y autenticación del capítulo 3, incluidos los practicados por proveedores externos conforme al §5.3.7.

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

d) Los controles de instalaciones, gestión y operativos del capítulo 5, incluidos los ejecutados por el operador del centro de datos.

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.

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

g) La correspondencia entre lo declarado en la presente política y lo efectivamente implantado.

El literal g) comprende la verificación de que los proveedores externos que intervienen en la prestación mantienen vigentes las certificaciones y evaluaciones declaradas en el §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 Política, 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, 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

Los restantes servicios prestados por **DIGITO** se rigen por las tarifas publicadas en su repositorio o por las condiciones particulares acordadas.

No se percibe tarifa alguna por la revocación de un certificado, ni por el acceso a la presente Política y a la Declaración de Prácticas de Certificación.

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 de certificación, 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 de los Titulares y la evidencia de verificación de identidad, sin perjuicio de lo dispuesto en el §9.4.

b) Las claves privadas y los datos de activación, así como 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 y de gestión de incidentes.

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 Política, la Declaración de Prácticas 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 obtenidos en el proceso de registro que no se incorporan al certificado, y en particular:

a) El domicilio y los datos de contacto del Titular.

b) Las imágenes, grabaciones y datos biométricos obtenidos en el proceso de acreditación de identidad conforme al §3.2.3.

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 de protección 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 la Normativa Vigente.

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 §4.12.

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.

9.6.1. Manifestaciones y garantías de la Autoridad de Certificación

DIGITO garantiza que:

a) Presta sus servicios conforme a la presente Política, a la Declaración de Prácticas de Certificación 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.

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.

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 enumerados en el §9.6.1. En particular, no garantiza:

a) La idoneidad del certificado para una finalidad determinada 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, las facultades o la 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 Política y en la Declaración de Prácticas de Certificación, 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 por el Titular, cuando tales vicios no fueran detectables mediante los procedimientos de verificación previstos.

b) La omisión o el retraso del Titular 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 Política 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 Política 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 Política, 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, la aceptación, el rechazo y la revocación de certificados 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 Política.

Corresponde al Titular consultar el estado de vigencia de sus certificados y solicitar la emisión de uno 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 por el Titular no altera la fecha de expiración ni genera derecho a prórroga ni indemnización.

Corresponde al Titular mantener actualizados sus datos de contacto en la plataforma.

9.12. Modificaciones del documento

9.12.1. Procedimiento de modificación

El procedimiento de modificación es el establecido en el §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

El identificador de objeto se modificará cuando el cambio afecte la aplicabilidad de la Política, en particular cuando altere los requisitos de identificación y autenticación, el perfil del certificado, el período de validez, los usos autorizados o el régimen de responsabilidad.

No afecta a la aplicabilidad, y por tanto no comporta cambio de identificador, la incorporación de instrumentos adicionales de acreditación de la identidad del Titular que mantengan el mismo nivel de aseguramiento.

Las modificaciones que no afecten la aplicabilidad se reflejan mediante el cambio del número de versión.

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 Política 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 Política y la Declaración de Prácticas de Certificación 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 la presente Política 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 electrónicas 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 previstos en la Normativa Vigente.

DIGITO se somete a la supervisión del INDOTEL y a las evaluaciones de conformidad del capítulo 8.

9.16. Disposiciones misceláneas

9.16.1. Acuerdo completo

La presente Política, la Declaración de Prácticas de Certificación, la Declaración de Divulgación de Prácticas y los términos y condiciones aceptados por el Titular constituyen el régimen aplicable a la prestación de los servicios.

En caso de discrepancia entre dichos documentos, prevalecerá el orden siguiente: la presente Política; la Declaración de Prácticas de Certificación; 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