DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN
DIGITO FINANCIAL TECHNOLOGY, LLC.

CONTROL DE VERSIONES

Versión	Fecha	Descripción de los cambios	Motivo	
1.0	19 de diciembre de 2024	Creación inicial del documento.	Legislación	
2.0	28 de abril de 2025	Modificación de la Sección 1.5.1, Sección 7.1	Solicitud del órgano regulador de República Dominicana	
3.0	16 de marzo de 2026		Cambio de PKI	
3.1	05 de mayo de 2026	Actualización integral de los Secciones	Alineación y cumplimiento estricto de los requisitos obligatorios de las normas ETSI	
4.0	24 de junio de 2026	Actualización de PKI	Implementación de mejores prácticas	
5.0	30 de junio de 2026	Actualización de PKI	Incorporación de nueva Issuing	GGT EP IR

1. INTRODUCCIÓN.

La presente Declaración de Prácticas de Certificación tiene por objeto establecer los procedimientos y controles que regirán la emisión, gestión y revocación de certificados digitales por parte DIGITO FINANCIAL TECHNOLOGY, LLC (en lo adelante DIGITO) como Entidad de Certificación (EC) en República Dominicana.

1.1. PROPÓSITO DEL DOCUMENTO.

Este documento 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, basado en la normativa vigente en materia y en las mejores prácticas internacionales.

1.2. CONTENIDO Y ALCANCE DEL DOCUMENTO.

Esta Declaración de Prácticas de Certificación aplica a todos los certificados digitales emitidos por DIGITO para Certificados de Autoridad de Certificación, Autoridad Subordinada, Autoridades de Registro y Certificados de personas físicas. De igual forma, aplica para los servicios de autenticación ofrecidos por DIGITO.

1.3. DEFINICIONES Y SIGLAS.

1.3.1. DEFINICIONES.

Las siguientes definiciones son utilizadas por DIGITO para la interpretación del presente documento, 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.

- Duración del Certificado: Período de tiempo durante el cual un certificado digital es válido antes de necesitar renovación.

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

1.3.2. SIGLAS.

Las siguientes siglas son utilizadas por DIGITO para la interpretación de la presente Declaración de Prácticas 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.

1.5. PARTICIPANTES - JERARQUÍA DE CERTIFICADOS DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI).

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.

1.5.1. 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).

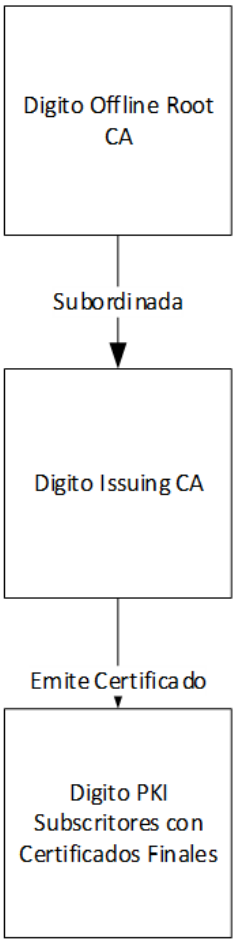
CN: **DIGITO ROOT CA**
Hash SHA256: A855459DCCB649DB801D52B5FDF63988E98AD3970F7C6C345116223A688896BB
Válido desde el 22 de junio 2026 hasta el 17 de junio de 2046
Longitud de Clave RSA 4096 – SHA256

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 SHA256 y está técnicamente restringido mediante el uso de la extensión Extended Key Usage (EKU - extKeyUsage).

CN: **DIGITO ISSUING CA DO 02**
Hash SHA256:8CEA4726AFAE80F7B292BABDA0A003B5F991B68324BA3CD09CC575B6DA585CF2
Válido desde el 30 de junio 2026 hasta 27 de junio 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*).



1.5.2. 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, en este caso DIGITO. La función de un LRA es aprobar y gestionar las solicitudes de certificados, verificar la identidad de los solicitantes y garantizar que cumplan con los requisitos de seguridad establecidos antes de emitir los certificados correspondientes.

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

1.5.3. TITULARES DE CERTIFICADOS.

Un Certificado Digital es un documento digital emitido y firmado digitalmente por una entidad de certificación, que identifica unívocamente a su titular durante el periodo de vigencia del certificado, y que se constituye en prueba de que dicho titular es fuente u originador del contenido de un documento digital o mensaje de datos que incorpore su certificado asociado.

1.5.4. TERCEROS QUE CONFÍAN.

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

1.5.4.1. 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.

1.5.5. TIPOS DE CERTIFICADOS PARA ENTIDADES FINALES.

DIGITO emitirá los siguientes tipos de certificados digitales para entidades finales:

- Certificados Personales: son certificados digitales utilizados por individuos para identificarse electrónicamente en entornos en línea. Estos certificados se emiten a personas físicas y se utilizan para realizar firmas digitales, autenticación en línea y cifrado de comunicaciones. Los certificados personales suelen contener información como el nombre del titular, su clave pública, el nombre de la entidad emisora y la fecha de vencimiento del certificado.

- Certificados para Representante privado o público: son certificados digitales utilizados por individuos para firmar como representante de una entidad pública o privada. Este certificado asegura la autenticidad y la integridad de las firmas digitales, proporcionando un medio seguro para firmar documentos en nombre de la entidad correspondiente.

1.5.6. POLÍTICAS DE INFRAESTRUCTURA

Estas políticas aplican a certificados de CA y serán los OIDs que aparezcan dentro de los certificados de las entidades de certificación (CA) para identificarlas

Tipo	OID
Root CA Policy	1.3.6.1.4.1.64999.1.0.1
Issuing CA Policy	1.3.6.1.4.1.64999.1.0.2

1.5.7. NIVELES DE GARANTÍA DE CERTIFICADOS.

Nivel de Garantía	Tipo de Certificado	OID de Política
Básico	**Ninguno identificado actualmente**	**1.3.6.1.4.1.64999.1.1.1**
Medio	**Certificados TLS/SSL**	**1.3.6.1.4.1.64999.1.2.1**
Medio	**Certificados TLS del Servidor RSE**	**1.3.6.1.4.1.64999.1.2.2**
Medio	**Certificado de LRA/SCO (sólo cuando se administran certificados de seguridad medios y básicos)**	**1.3.6.1.4.1.64999.1.2.3**
Medio	**Certificado TLS del Servidor TSA**	**1.3.6.1.4.1.64999.1.2.4**
Alto	**Qualified Electronic Signature / Seal**	**1.3.6.1.4.1.64999.1.3.1**
Alto	**Estampado de Tiempo Cualificado**	**1.3.6.1.4.1.64999.1.3.2**

Alto	**Certificados de RA/LRA para Acceso Operacional**	**1.3.6.1.4.1.64999.1.3.3**
Alto	**Certificado de Firmante OCSP (OCSP Responder)**	**1.3.6.1.4.1.64999.1.3.4**

1.5.8. DURACIÓN DE LOS CERTIFICADOS DIGITALES.

DIGITO establece que la duración de los certificados de entidades finales podrán ser de 12, 24 o 36 meses. Después de la expiración del certificado digital, el mismo no será considerado válido y necesitará ser renovado.

1.5.9. CONTENIDO DE LOS CERTIFICADOS DIGITALES.

De conformidad con la normativa vigente, y como Política interna de DIGITO, el certificado digital contendrá información relevante tales:

- Firma digital de la Entidad de Certificación;
- Nombre y dirección electrónica del titular del certificado;
- Identificación del titular del certificado nombrado en el certificado;
- Nombre, dirección electrónica y lugar donde realiza actividades Certificación;
- Antecedentes de la autorización obtenida;
- Clave pública del titular del certificado;
- Metodología utilizada para verificar la firma digital del titular del certificado;
- Número de serie del certificado;
- Fecha y hora de emisión y expiración del certificado;
- Identificación de la Política de Certificación bajo la cual el certificado fue emitido.

1.6. USOS DEL CERTIFICADO DIGITAL.

1.6.1. USOS APROPIADOS DE LOS CERTIFICADOS DIGITALES EMITIDOS POR DIGITO.

Los usos apropiados de los Certificados Digitales emitidos por DIGITO son los siguientes:

- Firmas Digitales.
- Cifrado de datos y comunicaciones.
- Acceso y realización de transacciones seguras.
- Identificación en línea o autenticación en plataformas digitales.

1.6.2. USOS NO AUTORIZADOS DE LOS CERTIFICADOS DIGITALES EMITIDOS POR DIGITO.

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

1.7. RESPONSABILIDADES DE LA ENTIDAD DE CERTIFICACIÓN.

De conformidad con el marco normativo vigente, las entidades de certificación tendrán, entre otras, las siguientes obligaciones:

- Emitir certificados conforme a lo solicitado o acordado por el suscriptor;
- Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales;
- Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;
- Garantizar la prestación permanente del servicio de entidad de certificación;
- Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;
- Efectuar los avisos y publicaciones conforme a lo establecido en la ley y sus reglamentos;
- Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y, en general, sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;
- Actualizar sus elementos técnicos para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas, la conservación y archivo de documentos soportados en mensajes de datos y todo otro servicio autorizado, sujeto a los reglamentos necesarios para garantizar la protección a los consumidores de sus servicios;
- Facilitar la realización de las auditorías por parte del Instituto Dominicano de las Telecomunicaciones (INDOTEL);
- Publicar en un repositorio su práctica de auditoría de certificación, sujeto a los términos y condiciones dispuestos en los reglamentos.

Además de lo anterior, DIGITO como política interna, establece las siguientes obligaciones:

- Verificar la identidad del firmante: La entidad debe llevar a cabo procesos y procedimientos adecuados para verificar la identidad del firmante antes de emitir un certificado digital. Esto ayuda a prevenir fraudes y garantiza que la firma sea atribuible a la persona correcta.
- Garantizar la seguridad de la infraestructura: La entidad debe mantener una infraestructura segura y confiable para garantizar la integridad y privacidad de los certificados digitales. Esto implica mantener actualizados los sistemas y protegerlos contra posibles ataques cibernéticos.
- Preservar la validez de los certificados: La entidad es responsable de garantizar la validez de los certificados digitales emitidos. Esto implica revocar los certificados en caso de que se detecte un uso indebido o se comprometa la seguridad de los mismos.
- Brindar soporte y asistencia técnica: La entidad debe proporcionar soporte y asistencia técnica a los usuarios de certificados digitales. Esto puede incluir resolver problemas técnicos,

proporcionar información sobre el uso adecuado de los certificados y ayudar en la renovación o revocación de los mismos.

1.8. 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.

1.8.1. AUTORIDAD DE POLÍTICAS (AP).

DIGITO FINANCIAL TECHNOLOGY GROUP, LLC.

1.8.2. 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: info@digito.do

2. PUBLICACIÓN Y REPOSITORIOS.

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:

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

2.2. PUBLICACIÓN DE LA INFORMACIÓN.

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.

2.3. FRECUENCIA DE LA PUBLICACIÓN.

Vida útil del CRL(Raíz CA): 1 año – sin conexión.
Vida útil del CRL(CA subordinada): Publicado una vez cada 6 horas, con los próximos períodos de actualización programados especificados cada 72 horas

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS.

Los repositorios antes mencionados son de libre acceso para su consulta del público en general. Sin embargo, DIGITO cuenta con los recursos y procedimientos necesarios para restringir el acceso a estos repositorios con fines diferentes a la consulta por parte de personas ajenas a DIGITO.

3. IDENTIFICACIÓN Y AUTENTICACIÓN.

3.1. TIPOS DE NOMBRES.

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

- AC Raiz: CN = Digito Root CA OU = Certification Authorities O = Digito Group C = DO
- AC Subordinada: cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO

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

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

3.1.1. EMPLEO DE SEUDÓNIMOS.

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

3.1.2. UNICIDAD DE LOS NOMBRES.

Cada certificado emitido por DIGITO cuenta con un nombre único que lo distingue y avala su autenticidad. Garantizamos que cada Titular de un Certificado sea identificado con su cédula de identidad y electoral en nuestro sistema, evitando duplicidades y garantizando la integridad de nuestros procesos de emisión y validación de certificados.

3.2. AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA FÍSICA.

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, los cuales son:

- Dev Portal
- Digito ID
- Digito Firma

- Digito SDK

La forma de autenticación en el ecosistema de DIGITO, se basa en un algoritmo de identificación utilizando el estándar RS 265, 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.

3.2.1. REQUISITOS PARA LA AUTENTICACIÓN DE LA IDENTIDAD.

Para realizar el proceso de autenticación de identidad se necesita:

1. Ser mayor de edad.
2. Poseer cédula de identidad y electoral.
3. Poseer un dispositivo con una cámara de vídeo con mínimo 2 megapíxeles y acceso a internet.
4. Poseer dispositivo (ej. celular) con capacidad de conectividad celular para recibir mensajes de texto SMS.

3.2.2. AUTENTICACIÓN AUTOMÁTICA DE LA PERSONA FÍSICA.

El procedimiento de autenticación de identidad automática con la plataforma DIGITO cuenta con los siguientes pasos:

1. El solicitante accede a la plataforma de DIGITO a través del Aplicativo Cliente proporcionado por la entidad que requiere la verificación de identidad.
2. El solicitante seguirá las instrucciones para registrarse y crear una cuenta utilizando su dirección de correo electrónico.
3. Luego de haberse registrado, el solicitante proporcionará la información requerida por la plataforma de DIGITO para realizar la verificación de identidad. Esto incluye sus datos personales como nombre completo, fecha de nacimiento, número de identificación y número de teléfono. De igual forma, se le solicitará capturar su documento nacional de identidad de ambos lados.
4. Posteriormente, se le solicitará acceso a la cámara del solicitante para que realice el proceso de verificación de identidad con su imagen.
5. La plataforma DIGITO utiliza tecnología avanzada de verificación de identidad, que incluye el reconocimiento facial y la verificación de la autenticidad de documentos, para comparar la información proporcionada por el solicitante con fuentes de datos confiables y se compara la foto del solicitante con la imagen en el documento.
6. Una vez que la verificación de identidad se ha completado, la plataforma de DIGITO proporciona internamente un informe de verificación al Aplicativo Cliente que indica si la misma fue exitosa o no.
7. El operador del Aplicativo Cliente tiene acceso a los resultados de la verificación.
8. En caso de que la verificación haya sido exitosa, el solicitante se encuentra registrado como Usuario de la plataforma de DIGITO y cuenta con un Digito ID.

9. En caso de que la verificación no sea exitosa, DIGITO puede realizar pasos adicionales de verificación manual o comunicarse con el solicitante para obtener más información o aclaraciones.

3.2.3. MÉTODOS DE AUTENTICACIÓN.

Existen un conjunto de autenticaciones predeterminadas que son requeridas para que la solicitud sea aprobada. Cada autenticación tiene una combinación de controles que permiten a DIGITO establecer coincidencia para que sea exitosa.

Tipo de Verificación	**Interfaz de programación**	**Descripción**
Cédula de identidad y electoral	Verificación documento de identidad	Se le pide al solicitante que presente la cédula de identidad y electoral. DIGITO inspecciona el documento de identidad para verificar su autenticidad y extrae la información relevante para su uso en el proceso de verificación de identidad.
Número de Teléfono	Verificación con número de teléfono	Se pide al solicitante que proporcione un número de teléfono. DIGITO envía un código de confirmación PIN vía SMS para confirmar que está en poder del solicitante.
Facial	Verificación facial	Se pide al solicitante que siga el proceso de verificación facial utilizando una cámara. Este proceso verifica que la persona esté viva y sea real. El rostro capturado en el proceso se compara con el rostro en el documento de identidad.

3.2.4. INFORMACIÓN DE 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. AUTENTICACIÓN DE IDENTIDAD PARA LAS SOLICITUDES DE RENOVACIÓN DE CERTIFICADOS.

Para la identificación y autenticación de las solicitudes de renovación 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 presente Política de Certificación.

3.2.6. AUTENTICACIÓN DE IDENTIDAD PARA LAS SOLICITUDES DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN DE CERTIFICADOS.

DIGITO establece que los datos, documentos y evidencias biométricas o documentales recopilados y validados durante el proceso de autenticación inicial de la persona física (conforme a los métodos descritos en la sección 3.2.2) tendrán un período máximo de validez operativa de **seis (6) meses (180 días)** calendario.

Durante este plazo de seis meses, DIGITO podrá reutilizar dichas validaciones previas para procesar nuevas solicitudes de emisión o reemisión de certificados digitales para el mismo titular sin necesidad de exigirle repetir el proceso completo de enrolamiento físico o telematizado, siempre y cuando se cumplan de manera estricta las siguientes condiciones normativas:

El método tecnológico y los controles de seguridad utilizados en la validación original deben seguir siendo considerados válidos, vigentes y técnicamente seguros bajo las prácticas operativas actuales de DIGITO al momento de la nueva emisión. Si un procedimiento de verificación ha sido discontinuado por sospechas o incidentes de seguridad, los datos asociados no podrán ser reutilizados bajo ninguna circunstancia.

Integridad de los Datos: DIGITO comprobará internamente que no existan alertas de compromiso de seguridad, fallecimiento o disputas legales sobre la identidad del titular registradas en el sistema centralizado de *User Digito ID* o notificaciones externas a la entidad. La vigencia interna de la documentación de soporte (como la Cédula de Identidad y Electoral) debe ser válida durante todo el ciclo de vida del certificado a emitir.

4. CICLO DE VIDA DE LOS CERTIFICADOS DIGITALES Y REQUISITOS OPERACIONALES.

A continuación se establecen los lineamientos y procedimientos necesarios para solicitar, emitir, renovar y revocar certificados digitales, asegurando que se cumplan los estándares de seguridad y autenticación requeridos por el marco normativo vigente y los estándares internacionales.

4.1. SOLICITUD DE UN CERTIFICADO DIGITAL.

El procedimiento de solicitud de un certificado digital se realiza agotando los siguientes pasos:

- Una vez el usuario cuente con su Digito ID, solicita certificados digitales a través del Aplicativo Cliente.
- Deberá leer y comprender los requisitos y condiciones establecidos para realizar la solicitud de certificado.
- Completará el formulario de solicitud con la información requerida.

- Adjuntará los documentos adicionales necesarios según lo indicado en los requisitos.
- El usuario deberá revisar cuidadosamente toda la información ingresada y los documentos adjuntos para asegurarte que estén correctos y completos.
- Envía la solicitud completada y los documentos adjuntos a la entidad de certificación a través del Aplicativo Cliente.
- El usuario recibirá la confirmación de recepción de la solicitud. Esto puede ser en forma de un correo electrónico, SMS o una notificación en Aplicativo Cliente.
- Una vez que DIGITO haya procesado tu solicitud y verificado los documentos, el usuario recibirá una notificación indicando que debe firmar un Acuerdo de Uso de Certificados Digitales.
- El usuario accederá a un Aplicativo Cliente para firmar el Acuerdo de Uso de Certificados Digitales, a través de una firma simple.
- El usuario recibirá una notificación indicando que su certificado digital ha sido emitido o no.

4.2. EMISIÓN DE CERTIFICADOS.

DIGITO llevará a cabo el siguiente procedimiento para la verificación de una solicitud de certificado digital:

1. Una vez el usuario envía una solicitud de certificado digital proporcionando la información requerida, DIGITO (AC o RA) verifica su identidad utilizando métodos de autenticación señalados en el presente documento.
2. DIGITO (AC o RA) valida la solicitud de certificado, verificando que la información proporcionada sea correcta y además se cumplan los requisitos necesarios para obtener el certificado digital.
3. Una vez validada la solicitud, DIGITO (AC o RA) genera el certificado digital utilizando su infraestructura de clave pública (PKI). Esto implica la creación de una clave privada para el usuario, que se guarda de forma segura, y una clave pública, que se incluye en el certificado.
4. DIGITO firma digitalmente el certificado utilizando su propia clave privada. Esto garantiza la autenticidad, confiabilidad e integridad del certificado, ya que cualquier alteración posterior sería detectada.
5. DIGITO almacena el certificado del solicitante en un *Hardware Security Module (HSM)*.

4.3. ACEPTACIÓN DEL CERTIFICADO DIGITAL.

DIGITO establece que la aceptación del certificado digital deberá realizarse mediante un acto explícito, voluntario e inequívoco. El proceso y los requisitos de aceptación se diferencian según el tipo de perfil de certificado a emitir:

4.3.1. CERTIFICADOS EMITIDOS A PERSONAS NATURALES PARA USO INDIVIDUAL

Para los certificados donde el suscriptor y el sujeto son la misma persona física, la aceptación del certificado podrá manifestarse mediante cualquiera de los siguientes actos:

- La firma del Acuerdo de Uso de Certificados Digitales.
- La aceptación electrónica expresa de los términos y condiciones aplicables en el portal de registro.

- El uso voluntario del certificado digital una vez que el suscriptor haya aceptado expresamente las condiciones de emisión y uso correspondientes.
- La firma del documento de aceptación o conformidad correspondiente emitido por DIGITO.

4.3.2. CERTIFICADOS EMITIDOS A PERSONAS NATURALES EN REPRESENTACIÓN DE PERSONAS JURÍDICAS (REPRESENTANTES)

De conformidad con los requisitos regulatorios, cuando el suscriptor (la organización o persona jurídica) y el sujeto (la persona física representante o empleado) sean entidades diferentes, el acuerdo de uso del certificado estará dividido obligatoriamente en dos partes independientes y acumulativas:

- **Parte A - Ratificación del Suscriptor (La Organización):** El representante legal o persona autorizada por la persona jurídica deberá ratificar formalmente la solicitud de emisión de los certificados asociados a su organización. Mediante este acto, la organización acepta los términos del servicio y asume la obligación de notificar de manera inmediata a DIGITO la solicitud de revocación del certificado en caso de cese de la relación laboral, cambio de funciones del sujeto, o revocación de las facultades otorgadas.
- **Parte B - Ratificación del Sujeto (El Firmante):** La persona física que actuará como sujeto del certificado deberá manifestar su consentimiento y aceptación expresa de manera individual, previa o simultánea a la fase de generación de sus claves. Mediante este acto, el sujeto acepta la vinculación de su identidad con la organización y se compromete formalmente a la custodia y control exclusivo de sus datos de creación de firma y mecanismos de activación (PIN, contraseñas o segundos factores de autenticación).

La emisión y entrega definitiva del certificado de representante quedará estrictamente condicionada a la validación técnica y contractual de ambas partes del acuerdo.

4.3.3. GARANTÍAS DE ACEPTACIÓN

Al momento de aceptar un certificado, el Titular del certificado garantiza que:

- a) La firma digital autenticada mediante este, estará bajo su control exclusivo;
- b) Que ninguna persona tendrá acceso al procedimiento de generación de la firma digital;
- c) Que la información contenida en el certificado es verdadera y corresponde a la suministrada por éste a la entidad de certificación.

4.3.4. REGLA GENERAL DE NO ACEPTACIÓN TÁCITA

Para todos los perfiles de certificados, la ausencia de objeción, el transcurso del tiempo o la falta de respuesta por parte del suscriptor o del sujeto no constituirán, bajo ninguna circunstancia, una aceptación tácita del certificado digital ni de las condiciones asociadas al mismo.

4.4. PUBLICACIÓN DEL CERTIFICADO.

Los certificados Raíz e intermedios no se actualizan frecuentemente y estarán disponible para descarga a través del portal de DIGITO.

Los certificados para entidades finales estarán disponibles para ser consultados durante su uso en firmas. No serán publicados directamente en ningún repositorio.

4.5. NOTIFICACIÓN DE LA EMISIÓN DE CERTIFICADOS A OTRAS ENTIDADES DE CERTIFICACIÓN.

DIGITO no emite notificaciones de la emisión de certificados a otras Entidades de Certificación.

4.6. RENOVACIÓN DE UN CERTIFICADO DIGITAL.

La renovación de certificados se refiere a la emisión de un certificado para sustituir uno que esté revocado o expirado.

4.6.1. PROCEDIMIENTO DE RENOVACIÓN DE UN CERTIFICADO DIGITAL.

El procedimiento de renovación del certificado digital se realiza agotando los siguientes pasos:

El titular del certificado digital debe iniciar el proceso de renovación contactando a través de la plataforma en línea de DIGITO. Para ello, es necesario proporcionar la información necesaria, como el número de cédula de identidad o el identificador del certificado.

- DIGITO verificará la identidad del usuario de acuerdo a los procedimientos de autenticación automática o manual establecidos. A tales fines, **se permitirá la reutilización y el consumo de las validaciones de identidad preexistentes en el sistema siempre que estas se encuentren dentro del límite de veinticuatro (24) horas posteriores a la verificación anterior**. Si la última verificación del titular excede dicho plazo, el sistema forzará obligatoriamente al solicitante a agotar un nuevo proceso de validación de identidad en tiempo real.
- Una vez que se ha verificado la identidad, DIGITO validará la solicitud conforme el procedimiento de Emisión de Certificados y generará el nuevo certificado digital en caso de aprobarla.
- DIGITO firmará digitalmente el nuevo certificado.
- DIGITO almacenará el nuevo certificado del solicitante en un HSM.
- El Titular del Certificado recibirá una notificación indicando que su certificado digital ha sido renovado correctamente.
- En caso de no aprobar la solicitud de renovación por alguna de las razones expuestas en el presente documento como causas de revocación, el Solicitante recibirá una notificación indicando que su certificado digital no ha sido renovado. Si la causa es subsanable, el solicitante contará con siete (7) días calendario para tales fines. Vencido dicho plazo, DIGITO evaluará nuevamente conforme los pasos anteriores.

4.7. ACEPTACIÓN DEL CERTIFICADO DIGITAL POR RENOVACIÓN.

La aceptación del certificado digital por renovación se manifiesta de la misma manera que el certificado anterior.

La renovación no solo confirma la validez del certificado, sino también la aceptación de la responsabilidad continua del titular. Esto implica el compromiso de cumplir las normativas y requisitos exigidos durante su utilización.

4.8. NOTIFICACIÓN DE LA EMISIÓN DE CERTIFICADOS A OTRAS ENTIDADES DE CERTIFICACIÓN.

DIGITO no emite notificaciones de la renovación de certificados a otras Entidades de Certificación.

4.9. REVOCACIÓN DE UN CERTIFICADO DIGITAL.

La revocación de certificados es el proceso de invalidar un certificado previamente emitido por DIGITO, antes de la fecha de su expiración.

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. TIPOS DE REVOCACIÓN DE UN CERTIFICADO DIGITAL.

DIGITO establece que estos son los tipos de revocación que pueden aplicarse a un certificado digital emitido por nuestra entidad de certificación:

1. Revocación voluntaria: Este tipo de revocación ocurre cuando el titular del certificado solicita de manera voluntaria la revocación. El titular debe presentar una solicitud por escrito para la revocación del certificado, y se llevarán a cabo los procedimientos de verificación de identidad y evaluación de la solicitud antes de proceder con la revocación.

2. Revocación obligatoria: Este tipo de revocación es impuesta por DIGITO, como Entidad de Certificación, en los casos en los que se detecta un mal uso evidente o actividades fraudulentas asociadas con el certificado, violación de nuestra política de uso de certificados digitales, por vulneración de clave privada, acciones legales, por cambios en la información del titular y por fallecimiento, declaración de ausencia, entre otros.

4.9.2. CAUSAS DE REVOCACIÓN.

De conformidad con la normativa vigente, así como la Política interna de DIGITO, las causas por las cuales se puede revocar un certificado digital emitido por DIGITO, son las siguientes:

- **Uso indebido:** El certificado será revocado si se detecta que ha sido utilizado de manera incorrecta, ilegal o fraudulenta. Esto incluye el uso del certificado para actividades delictivas como, sin que sea limitativo, falsificación de identidad o la realización de transacciones no autorizadas.
- **Vulneración de la clave privada:** Si existe evidencia de que la clave privada asociada al certificado ha sido vulnerada, se procederá a su revocación. Esto puede ocurrir en caso de acceso no autorizado a la clave privada, o si se detecta que la clave ha sido expuesta o comprometida de alguna manera.
- **Cambio de información:** Si los datos de identificación del titular del certificado han cambiado y ya no son válidos, se procederá a la revocación del certificado. Esto puede incluir cambios en el nombre, la dirección de correo electrónico u otros detalles que afecten la autenticidad del certificado.
- **Incumplimiento de políticas por el Titular:** Si se determina que el titular del certificado ha incumplido alguna de las políticas o normas establecidas por DIGITO en relación con el uso de certificados digitales, se procederá a su revocación. Esto puede incluir el incumplimiento de políticas de seguridad, uso indebido de sistemas o violaciones de confidencialidad.
- **Pérdida de cumplimiento normativo o técnico del Certificado o de la CA:** De conformidad con los requisitos obligatorios del estándar **ETSI EN 319 411-1**, DIGITO revocará de oficio cualquier certificado vigente si determina, detecta o es notificada de que el certificado emitido no cumple, o ha dejado de cumplir, con las especificaciones técnicas, perfiles de certificado o requisitos de seguridad contemplados en esta CP/CPS, o bajo el marco regulatorio legal aplicable bajo el cual fue emitido.
- **Acciones legales:** En caso de que una autoridad competente presente una orden judicial o una solicitud oficial para revocar un certificado en particular, se seguirán los procedimientos legales correspondientes.
- **En caso de fallecimiento:** Se procederá a revocar de forma automática el certificado y se invalidará todas las facultades y derechos asociados al mismo. DIGITO deberá ser notificada del fallecimiento del titular del certificado digital a través de un documento fehaciente como un acta de defunción.
- **Por ausencia o desaparición definitivamente declarada por autoridad competente, de acuerdo a lo prescrito por el derecho común:** Se procederá a revocar de forma automática el certificado y se invalidará todas las facultades y derechos asociados al mismo. DIGITO deberá ser notificada de la declaración de ausencia definitiva del titular del certificado digital a través de un medio fehaciente.
- **Por el cese de actividades de la entidad de certificación.**

DIGITO se reserva el derecho de revocar un certificado en cualquier momento si se detectan una o varias de las causas mencionadas anteriormente, de acuerdo con las circunstancias y las políticas establecidas.

4.9.3. PROCEDIMIENTOS DE REVOCACIÓN DE UN CERTIFICADO DIGITAL.

A continuación describe los pasos a seguir para llevar a cabo la revocación de un certificado digital:

- Solicitud de revocación: El titular de un certificado o una persona autorizada debe presentar una solicitud por escrito para la revocación del certificado. La solicitud debe incluir información

relevante, como el número de serie del certificado, la fecha de emisión y una descripción detallada de la razón de la revocación.

- Verificación de la identidad: Para garantizar la autenticidad de la solicitud, se llevará a cabo un proceso de verificación de la identidad del solicitante. Esto puede incluir la presentación de documentos de identidad válidos. El tiempo de procesamiento de la revocación iniciará una vez DIGITO haya validado razonablemente la autenticidad e integridad de la solicitud presentada. Verificación de la identidad: Para garantizar la autenticidad de la solicitud, se llevará a cabo un proceso de verificación de la identidad del solicitante. Esto puede incluir la presentación de documentos de identidad válidos.
- Evaluación de la causa de revocación: DIGITO evaluará la razón proporcionada para la revocación del certificado. Se verificará si la causa se ajusta a las políticas y criterios establecidos para la revocación, como el uso indebido, la vulneración de la clave privada o el incumplimiento de las políticas de seguridad. En los casos relacionados con compromiso de clave privada, fraude, uso indebido, pérdida de control del dispositivo criptográfico o incidentes de seguridad críticos, DIGITO podrá ejecutar la revocación inmediata por personal autorizado, priorizando la protección de la infraestructura y de terceros que confían en el certificado.
- Revisión y aprobación: Un comité o equipo designado podrá revisar posteriormente las solicitudes de revocación procesadas, con el objetivo de validar el cumplimiento de las políticas internas, la trazabilidad del proceso y la adecuada justificación de la revocación realizada. DIGITO podrá solicitar información adicional al solicitante cuando sea necesario, siempre que esto no retrase injustificadamente el procesamiento de solicitudes críticas de revocación.Un comité o equipo designado revisará la solicitud de revocación y tomará una decisión fundamentada sobre su aprobación. Se considerarán todos los factores relevantes, y se podrá solicitar información adicional al solicitante si es necesario.
- Tiempos de procesamiento de revocación: DIGITO garantizará que toda solicitud válida de revocación será procesada y reflejada en los mecanismos públicos de validación correspondientes, incluyendo CRL y/u OCSP, en un plazo máximo de 24 horas desde su recepción y validación. Las solicitudes relacionadas con incidentes críticos de seguridad serán procesadas con prioridad inmediata por personal autorizado designado por DIGITO. DIGITO mantendrá mecanismos operativos adecuados para la recepción y procesamiento de solicitudes de revocación fuera del horario laboral cuando sea requerido.
- Revocación del certificado: En caso de que la solicitud sea aprobada, se procederá a revocar el certificado digital. Esto implicará la eliminación de la validez del certificado y su inclusión en una lista de certificados revocados.
- Comunicación de la revocación: Se notificará al titular del certificado sobre la revocación a través de un aviso por correo electrónico u otro medio de comunicación seguro. El aviso incluirá información detallada sobre la revocación, la razón de la misma y las implicaciones que esto puede tener en el uso del certificado.
- Actualización de repositorios: DIGITO garantizará la actualización oportuna de los servicios CRL y/u OCSP para asegurar que el estado revocado del certificado se encuentre disponible públicamente dentro de los plazos establecidos por las normas y estándares aplicables. DIGITO se encargará de actualizar los repositorios y sistemas pertinentes para reflejar la revocación del certificado, de manera que otros usuarios y sistemas confíen en esta información actualizada.

4.10. MODIFICACIÓN DE CERTIFICADOS.

DIGITO no realiza modificaciones de certificados. Toda modificación conlleva la emisión de un nuevo certificado, bajo el procedimiento de emisión de certificados establecido en el presente documento.

4.11. SUSPENSIÓN Y REACTIVACIÓN DE CERTIFICADOS.

DIGITO no realiza suspensiones y reactivaciones de certificados. La suspensión de un certificado se tratará como una revocación y por ende, para contar con un certificado válido, se deberá solicitar la emisión de un nuevo certificado, bajo el procedimiento de emisión de certificados establecido en el presente documento.

4.12. VENCIMIENTO O EXPIRACIÓN DEL CERTIFICADO DIGITAL.

Una vez finalizado el periodo de validez del certificado digital, el mismo no podrá ser utilizado para lo establecido en la Sección 1.6. En ese caso, se debe proceder a la renovación del mismo siguiendo el procedimiento establecido en el presente documento.

4.13. RESPONSABILIDADES DEL TITULAR DE UN CERTIFICADO.

De conformidad con la normativa vigente, así como por política interna de DIGITO, son responsabilidades y deberes de los titulares de certificados digitales:

- Recibir el acceso a las claves por parte de la entidad de certificación o generar las claves, utilizando un sistema de seguridad exigido por la entidad de certificación;
- Suministrar información completa, precisa y verídica a la entidad de certificación, así como mantenerla actualizada;
- Aceptar los certificados emitidos por la entidad de certificación, demostrando aprobación de sus contenidos mediante el envío de estos a una o más personas o solicitando la publicación de estos en repositorios;
- Mantener el control del acceso a la clave privada y reservado del conocimiento de terceras personas;
- Efectuar oportunamente las correspondientes solicitudes de renovación o revocación.
- Utilizar el certificado digital de manera responsable, siendo utilizado únicamente para los fines previstos y de acuerdo con las leyes y regulaciones aplicables.
- Notificar cualquier compromiso de seguridad: Si el titular del certificado sospecha o descubre que su clave privada ha sido comprometida o utilizada de manera no autorizada, debe notificar de inmediato a la entidad emisora del certificado digital.
- Cumplir con las políticas y regulaciones: El titular del certificado debe cumplir con las políticas y regulaciones establecidas por DIGITO y las autoridades competentes.
- Cooperar en investigaciones y disputas: Si se presenta una disputa legal o se requiere la colaboración en una investigación, el titular del certificado debe cooperar y proporcionar la información necesaria, de acuerdo con las leyes y regulaciones aplicables.

Los titulares de certificados digitales serán responsables por la falsedad o error en la información suministrada a la entidad de certificación y que es objeto material del contenido del certificado. También serán responsables en los casos en los cuales no den oportuno aviso de revocación de sus certificados.

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES.

5.1 CONTROLES DE SEGURIDAD FÍSICA.

DIGITO establece controles de seguridad física para evitar el acceso físico no autorizado o el daño a la información y las instalaciones de procesamiento de información de la entidad. Estos controles abarcan todas las oficinas y ubicaciones de DIGITO y a todas las partes externas con acceso físico a las instalaciones propias o alquiladas de DIGITO.

5.1.1. PERÍMETRO DE SEGURIDAD FÍSICA.

Las oficinas físicas y las instalaciones de procesamiento de DIGITO cumplen con todos los estándares de materiales de construcción para paredes, ventanas, puertas y mecanismos de control de acceso. Algunas zonas interiores pueden identificarse como áreas seguras donde el acceso físico está aún más restringido a un personal autorizado de DIGITO.

5.1.2. CONTROLES DE ENTRADA FÍSICA.

Las oficinas y las instalaciones de procesamiento de DIGITO están protegidas por controles de entrada apropiados para garantizar que solo se permite el acceso al personal autorizado. Siempre que sea posible, los sistemas de control de acceso de DIGITO estarán vinculados a un sistema centralizado que proporcione control de acceso inteligente para el personal individual. Los accesos deben registrarse y revisarse adecuadamente según sea necesario de acuerdo con el riesgo. Se utilizarán cámaras en las instalaciones de DIGITO.

5.1.2.1. PROTECCIÓN DE OFICINAS, SALAS E INSTALACIONES.

La seguridad física para oficinas, salas e instalaciones se encuentran diseñadas para proteger contra robos, mal uso, amenazas ambientales, acceso no autorizado y otras amenazas que atenten contra la confidencialidad, integridad y disponibilidad de datos y sistemas de DIGITO.

5.1.2.2. ÁREAS SEGURAS / GESTIÓN DE VISITANTES.

DIGITO no permite el acceso de visitantes, personal de entrega, técnicos de soporte externo y otros agentes externos a áreas seguras sin escolta y / o supervisión adecuada. Los terceros que se encuentren en áreas seguras deberán firmar su entrada y salida en un registro de visitantes y serán escoltados o monitoreados por el personal de DIGITO.

5.1.3. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES.

Las instalaciones de DIGITO cuentan con protección física contra desastres naturales, ataques maliciosos o accidentes. Las áreas seguras están monitoreadas mediante el uso de sistemas de videovigilancia.

Además, el acceso de visitantes y terceros a áreas seguras se encuentra restringido para reducir el riesgo de pérdida y robo de información.

5.1.4. SEGURIDAD FÍSICA DEL CENTRO DE DATOS (DATA CENTER) DE DIGITO.

DIGITO mantiene la contratación de un data center diseñado para instalar equipos de alta tecnología. El mismo cuenta con un servicio de vigilancia las 24 horas todos los días, a los fines de monitorear interrupciones, fallas, eventos críticos y anomalías en la red que pueden afectar la disponibilidad de la infraestructura de DIGITO. Además, dispone de suministro de electricidad y aire acondicionado para que las operaciones sean confiables e ininterrumpidas.

Las instalaciones se encuentran protegidas contra daños por exposición al agua y disponen de alta seguridad preventiva contra incendios.

El data center implementa soluciones de recuperación de desastres y continuidad de negocio.
Al igual que las oficinas de DIGITO, el data center cuenta con acceso inteligente para el personal, acceso restringido a áreas seguras, cámaras de vigilancia, además de sistemas de detección de intrusos.

5.2. CONTROLES DE RECURSOS HUMANOS.

DIGITO ha diseñado e implementado, desde el área de Recursos Humanos, una serie de controles preventivos y correctivos para asegurar el cumplimiento de sus políticas. Estos controles que deben ser claros, equitativos y no discriminatorios, buscan garantizar un ambiente de trabajo seguro y productivo para alcanzar objetivos.

5.2.1. VERIFICACIÓN DE ANTECEDENTES.

Los controles de verificación de antecedentes del personal de DIGITO se llevarán a cabo de acuerdo con el Código de Trabajo de la República Dominicana y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que debe acceder y los riesgos que puede percibir como colaborador de DIGITO. La investigación previa podrá incluir verificaciones de antecedentes penales, a menos que lo prohíba la ley.

5.2.2. EVALUACIÓN DE HABILIDADES Y COMPETENCIAS.

Las habilidades y la competencia de los colaboradores y contratistas de DIGITO serán evaluadas por el personal de recursos humanos y el encargado de contratación o sus designados como parte del proceso de contratación. Las habilidades y competencias requeridas se enumerarán en las descripciones de puestos. Las evaluaciones de competencia pueden incluir verificaciones de referencias, educación y verificaciones de títulos, certificaciones, pruebas técnicas y entrevistas.

Todos los colaboradores de DIGITO, se someterán a una revisión anual del desempeño que incluirá una evaluación del desempeño laboral, competencia en el puesto, cumplimiento de las políticas y código de conducta de la entidad, así como logros de los objetivos específicos del puesto.

5.2.3. TÉRMINOS Y CONDICIONES DE EMPLEO.

DIGITO informará oportunamente a colaboradores y terceros sobre sus políticas, funciones y responsabilidades de seguridad de la información. Los colaboradores y terceros con acceso a la información de la entidad firmarán un acuerdo de confidencialidad o no divulgación adecuado. Estos acuerdos establecerán responsabilidades para las vulneraciones de seguridad de la información según sea necesario. Los colaboradores y los terceros deberán seguir todas las políticas de seguridad de la información de DIGITO.

5.2.4. RESPONSABILIDADES DE DIGITO.

DIGITO será responsable de asegurar que las políticas y procedimientos de seguridad de la información se revisen anualmente, se distribuyan y estén disponibles, y que los colaboradores y contratistas cumplan con esas políticas y procedimientos durante la duración de su empleo o compromiso.
El cumplimiento de las políticas y procedimientos de seguridad de la información se evaluarán como parte del proceso de revisión del desempeño cuando corresponda.

5.2.5. CONCIENCIA, EDUCACIÓN Y CAPACITACIÓN.

Los colaboradores de DIGITO deberán completar capacitaciones relativas a sus puestos de trabajo, asi como a seguridad de la información y protección de datos personales, según corresponda. DIGITO deberá monitorear la finalización de las capacitaciones.

5.2.6. PROCESO DISCIPLINARIO.

Los colaboradores de DIGITO que incumplan las políticas de DIGITO estarán sujetos al proceso disciplinario progresivo, incluyendo la terminación del empleo o contrato, en caso de ser necesario.

5.3. ROLES Y RESPONSABILIDADES.

5.3.1. AUTORIDAD DE REGISTRO DE DIGITO, AUTORIDAD DE REGISTRO LOCAL DE DIGITO.

DIGITO define claramente los roles y responsabilidades que son esenciales para el establecimiento, la implementación, el mantenimiento y la mejora continua de los sistemas de DIGITO, incluyendo el de gestión de la seguridad de la información:

- Rol de Autoridad de Registro de DIGITO (RAs):

El rol RA se asigna a los colaboradores de DIGITO autorizados a emitir y administrar todos los tipos de certificados definidos en la AC Subordinada.

- Rol Autoridad de registro local de DIGITO (LRAs):

El rol LRA se asigna a los colaboradores de DIGITO que tendrán capacidades limitadas de RA. Por ejemplo, solo pueden estar autorizados a emitir un tipo de certificado específico y solo se les puede permitir administrar suscriptores PKI asociados con un grupo o división específica dentro de DIGITO.

Los LRAs pueden utilizar el Servicio de Gestión de Usuarios (UMS) de Servicios de Administración (AS) para realizar sus actividades de administración de certificados para emitir y administrar certificados.

5.3.2. CONSEJO DE SEGURIDAD DE LA INFORMACIÓN.

DIGITO cuenta con un Consejo de Seguridad de la Información conformado por la Dirección Ejecutiva, la Dirección de Operaciones, el Oficial de Seguridad de la Información, el Oficial de Protección de Datos y la Dirección de Tecnología de la Información (como administrador y operador de sistemas).

La Dirección Ejecutiva y la Dirección de Operaciones tienen la autoridad de impulsar la seguridad de la información en la entidad a nivel financiero, funcional y operativo.

El Oficial de Seguridad de la Información es el encargado de la gestión de la seguridad de la información en toda la entidad, así como de mantener la comunicación a todos los directivos sobre el estado de la misma. La persona asignada a este rol es responsable de realizar actividades de autoevaluación que confirmarán que la función RAs se ejecuta según los procedimientos operativos y las políticas relevantes.

De igual forma, puede consultar las auditorías generadas por la AC y las aplicaciones RA utilizando las siguientes aplicaciones:

- UMS;
- Informes de infraestructura de clave pública; y
- Archivos de registro almacenados en los servidores RA locales (por ejemplo, TSA).

El Oficial de Protección de Datos tiene la autoridad para impulsar la privacidad de los datos en DIGITO a nivel funcional y operativo. Es responsable de la coordinación de las actividades de privacidad de los datos en toda la entidad.

El equipo de la Dirección de Tecnología de la Información está compuesto por individuos que administran las actividades diarias de cumplimiento y monitoreo necesarias para lograr, mantener y mejorar los sistemas de DIGITO, incluyendo el de seguridad de la información.

5.3.2.1. RESPONSABILIDADES DEL CONSEJO DE SEGURIDAD DE LA INFORMACIÓN.

Responsabilidad	**Frecuencia**
Supervisar las principales iniciativas para mejorar la seguridad de la información.	Anualmente o según sea necesario
Confirmar que los objetivos de la seguridad de la información sean establecidos, compatibles y actualizados basados en la dirección estratégica de la organización.	Anualmente
Revisar las acciones correctivas y las mejoras para lograr sus objetivos previstos.	Anualmente
Monitorear el progreso de la comunicación, implementación, acción correctiva y planes de mejora de la seguridad de la información.	Anualmente
Revisar los incidentes de seguridad de la información y apoyar la resolución según su función.	Según sea necesario
Proporcionar recursos adecuados (es decir, presupuesto, humano, equipo, software) para establecer, operar y mejorar el SGSI.	Anualmente
Aprobación de las políticas de seguridad de la información.	Anualmente o según sea necesario

Aprobación del plan de tratamiento de riesgos correspondiente a los resultados de la evaluación de riesgos. el plan de tratamiento de riesgos.	Anualmente
Comunicar la importancia del SGSI y la criticidad de la mejora continua.	Anualmente
Realización de la revisión de administración del SGSI, según su función	Anualmente
Revisar los resultados de las pruebas técnicas y las auditorías internas y externas del SGSI.	Anualmente
Identificar, gestionar y apoyar al personal que opera el SGSI.	Continuamente

5.3.2.2. RESPONSABILIDADES DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN.

Responsabilidad	**Frecuencia**
Evaluar cumplimiento de los procedimientos realizados por los RAs	Según sea necesario
Mantener informado al Consejo de Seguridad de la Información (Autoridad de Políticas)	Según sea necesario
Supervisar todas las iniciativas SGSI para la organización.	Continuamente
Supervisar la ejecución del plan de comunicación / implementación, auditorías internas, revisión de administración y acciones / mejoras correctivas	Continuamente
Mantener la supervisión del SGSI.	Continuamente
Confirmar que el Consejo de SGSI está informado de los cambios materiales en el perfil de riesgo de la organización o los controles clave.	Según sea necesario
Revisar, actualizar y confirmar que las políticas del SGSI son actuales y cumplen con los objetivos.	Anualmente
Supervisar la ejecución de la auditoría interna del SGSI y otras auditorías y pruebas técnicas.	Anualmente
Solicitar recursos (es decir, presupuesto, humanos, equipos, software) necesarios para establecer, operar y mejorar el SGSI.	Anualmente
Comunicar la importancia del SGSI y la importancia de la mejora continua dentro de su función.	Anualmente
Implementar y coordinar capacitación y concientización sobre seguridad.	Anualmente
Gestión de los documentos y registros del SGSI.	Continuamente

5.3.2.3. RESPONSABILIDADES DE LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN.

Responsabilidad	**Frecuencia**
Implementar, mantener y operar los servidores RA locales (por ejemplo, TSA).	Continuamente
Asegúrese de que los servicios de RA se operan según la Política de Certificación.	Continuamente
Mantenimiento del sistema de DIGITO.	Según sea necesario
Definir, monitorear y reportar la comunicación, implementación, mejora, planes de acción correctiva y métricas de medición de efectividad.	Según sea necesario
Hacer un seguimiento de todos los incidentes notificados para su resolución y compartir oportunidades de aprendizaje con todas las funciones aplicables	Según sea necesario
Identificar los cambios y su impacto en el contexto interno / externo de la entidad, las partes interesadas, el alcance, los límites y los objetivos.	Continuamente
Responsable del respaldo de datos	Según sea necesario

Notificar al Oficial de Seguridad de la Información sobre cualquier problema relacionado con la competencia del personal que apoya al SGSI	Según sea necesario
Coordinar y gestionar la ejecución de las auditorías internas / externas y tratamiento de no conformidades.	Anualmente
Facilitar evaluaciones de riesgos y pruebas técnicas.	Anualmente
Personal de apoyo que está implementando y operando controles administrados y pertenecientes a su función respectiva.	Continuamente
Implementar acciones correctivas y mejoras para los controles administrados y propiedad de su respectiva función.	Continuamente
Medir e informar sobre la efectividad de los controles del SGSI administrados y propiedad de su función respectiva	Anualmente y Según sea necesario
Soporte a los usuarios	Según sea necesario
Participar en auditorías internas, revisiones de gestión y auditorías externas.	Según sea necesario

5.3.3. AUDITOR INTERNO.

La selección del auditor o auditores internos estará a cargo de la Dirección Ejecutiva. Los auditores serán evaluados y seleccionados en base a su objetividad e imparcialidad en el proceso de auditoría. El auditor o auditores deben estar capacitados y calificados para realizar la auditoría interna de una Entidad de Certificación y de un Sistema de Gestión de Seguridad de la Información. Los auditores serán evaluados en base a su educación y experiencia para validar su competencia.

Se debe garantizar que existe una separación adecuada de funciones al elegir un auditor, es decir, el auditor no puede haber implementado, operado o revisado ninguno de los controles bajo auditoría.

Los auditores internos llevarán a cabo el programa de auditoría con los insumos que le aporte el Oficial de Seguridad de la Información y las demás Direcciones de DIGITO.
.
Las principales responsabilidades del auditor interno son las siguientes:

- Planificar las auditorías internas según la frecuencia y cronograma definidos.
- Llevar a cabo la auditoría interna según el plan de auditoría y compartir los resultados de los hallazgos para revisión y aprobación.
- Asegurar la confidencialidad e integridad de los datos de auditoría y la evidencia de respaldo dentro del control del auditor.
- Proporcionar todos los registros de auditoría según se solicite.

5.3. PROCEDIMIENTOS PARA EL REGISTRO DE AUDITORÍAS.

5.3.1. TIPOS DE EVENTOS REGISTRADOS.

- Logs de eventos;
- CSR
- Logs de interacción con el sistema.

5.3.2. AUDITORÍA Y MONITOREO DEL SISTEMA.

La PKI de DIGITO tendrá disponibles las siguientes fuentes de información de registro y auditoría:

- Servicio de Gestión de Usuarios (UMS): las auditorías de la AC contienen información sobre las actividades de creación y administración de usuarios, así como de eventos específicos de la AC, tales como:

    - Copia de seguridad de la AC,
    - Estado del servicio y base de datos de la AC,
    - Verificación de integridad de base de datos,
    - Emisión de CRLs,
    - Politícas.

Los RAs, LRAs y el Oficial de Seguridad de la Información tienen acceso a esta aplicación después de la autenticación positiva del certificado.

- Aplicación de informes PKI: Los RAs y el Oficial de Seguridad de la Información tendrán acceso a esta aplicación web para generar informes a partir de los archivos de registro de la AC.

Los usuarios se autenticarán en la aplicación de informes PKI utilizando el ID de usuario y las contraseñas proporcionadas por la PKI.

- RAs y el Oficial de Seguridad de la Información tendrán acceso a los archivos de registro generados por los servidores locales en TSA.

5.4. ARCHIVOS DE REGISTRO.

5.4.1. TIPOS DE ARCHIVOS DE REGISTRO.

DIGITO conservará los siguientes registros:

- Emisión de certificados Raíz;
- Emisión de certificados de tiempo;
- Emisión de certificados Autoridad Subordinada;
- Emisión de certificados usuario;
- Revocación de certificados Raíz;
- Revocación de certificados de tiempo;
- Revocación de certificados Autoridad Subordinada;
- Revocación de certificados usuario;
- Expiración de los certificados;
- CRL;
- Certificados emitidos y revocados;
- Documentación de respaldo del proceso de autenticación de identidad;
- Datos de la auditoría.

5.4.2. PERIODO DE CONSERVACIÓN DE REGISTROS.

Los registros de certificados serán mantenidos por el período que establezca el marco normativo vigente. Esta retención de datos estará en conformidad con los requisitos legales aplicables durante ese tiempo.

Los datos proporcionados por los Titulares de Certificados Digitales, y los documentos de apoyo, serán conservados por DIGITO por el período que establezca el marco normativo vigente desde la revocación o expiración de los certificados, incluyendo su almacenamiento local.

DIGITO conservará los registros de certificados digitales, información de auditoría, registros operacionales, eventos de seguridad, evidencia de validación, solicitudes de emisión, revocación, renovación y demás documentación de soporte relacionada con los servicios de confianza prestados, por un período mínimo de veinte (20) años contados a partir de la expiración o revocación del certificado digital correspondiente.

Los datos proporcionados por los titulares de certificados digitales, así como los documentos de soporte y evidencias asociadas al proceso de identificación, validación y aceptación, serán conservados durante el mismo período, conforme a las medidas de seguridad y confidencialidad establecidas por DIGITO y la normativa aplicable.

DIGITO podrá conservar determinados registros por períodos superiores cuando sea requerido por disposiciones legales, regulatorias, contractuales, requerimientos judiciales o necesidades de preservación de evidencia asociada a incidentes de seguridad, auditorías o investigaciones.

Los registros conservados deberán mantenerse protegidos contra alteración, destrucción no autorizada, pérdida y acceso indebido durante todo el período de retención establecido.

5.4.3. PROTECCIÓN DE REGISTROS.

DIGITO ha tomado las medidas necesarias para garantizar la confidencialidad de la información y la protección de los datos personales de los suscriptores de certificados digitales siguiendo las líneas generales establecidas en el documento DTI-PROC-05 - Procedimiento de revisión de firewall y acceso a redes y el registro de eventos de sistema.

Los registros están protegidos de tal manera que solo las personas autorizadas pueden acceder a ellos de acuerdo a nuestro documento DTI-POL-09 - roles y responsabilidades de Seguridad de la Información Se garantiza la protección contra la visualización, modificación, eliminación u otras formas de manipulación.

5.4.4. COPIA DE SEGURIDAD DE LOS ARCHIVOS DE REGISTRO.

Todos los registros de eventos se respaldan en un sistema centralizado para su posterior visualización. A estos eventos se les realiza un respaldo de acuerdo al procedimiento DTI-PROC-07 - Procedimiento Respaldo de Información.

Todos los archivos de registro son replicados en el datacenter de recuperación de desastre siguiendo de igual manera el mismo procedimiento antes mencionado.

5.4.5. SELLADO DE TIEMPO.

La CA emite el certificado para la Autoridad de Sellado de Tiempo (TSA) de DIGITO. Los servidores de TSA procesarán las solicitudes de marca de tiempo utilizando el protocolo de marca de tiempo (TSP) como se describe en RFC.3161

El sellado de tiempo se encuentra alineado con los estándares ETSI EN 319 421, ETSI TS 319 422 y CEN TS 419 261.

5.4.5.1. SINCRONIZACIÓN DE TIEMPO.

El tiempo para los servicios de DIGITO se obtienen del servicio de servidor NTP de diferentes proveedores asegurando la mejor precisión disponible. Los servidores se mantienen actualizados con la hora UTC −4, mediante sincronización a través del protocolo NTP v4, conforme al estándar RFC 5905 “Network Time Protocol Version 4: Protocol and Algorithms Specification”.

5.4.5.2. CONFIGURACIÓN DE AUTORIDAD DE MARCA DE TIEMPO.

Los servidores TSA recibirán un certificado TSA por parte de la AC Subordinada de DIGITO. Los certificados TSA tendrán una vida útil de cinco (5) años e incluirán una clave pública RSA-4096. A los certificados TSA se les asignará los siguientes DN: cn=TSA-Server-<unique name>, ou=Applications, o=Digito Group, c=DO

Los certificados de servidor TSA serán emitidos por la AC Subordinada de DIGITO utilizando las aplicaciones web CSR-Solicitante/Aprobador por un RA/LRA autorizado.

6. CONTROLES DE SEGURIDAD TÉCNICA.

6.1. GENERACIÓN DE PAR DE CLAVES.

La gestión o administración de claves se refiere a generar, almacenar, distribuir y revocar de manera segura las claves criptográficas utilizadas en algoritmos de encriptación de los certificados digitales. La gestión y administración de claves incluye los siguientes aspectos:

- Generación de claves: Las claves se generan utilizando algoritmos criptográficos y generadores de números aleatorios.
- Almacenamiento de claves: Las claves deben almacenarse de manera segura para evitar el acceso no autorizado. DIGITO utiliza módulos de seguridad de hardware (HSM) o dispositivos de almacenamiento criptográficamente protegidos.
- Uso de claves: Las claves se utilizan para encriptación, desencriptación, firmas digitales y otras operaciones criptográficas. El uso de claves deberá cumplir con Políticas de Seguridad de DIGITO.
- Revocación de claves: Cuando una clave se ve comprometida o ya no es necesaria, se debe revocar para evitar un uso no autorizado. Se utiliza la revocación de certificados para este procedimiento. Las listas de revocación de certificados (CRL) serán el medio para indicar que una clave ya no es válida.

DIGITO genera un par de claves criptográficas compuesto por una clave pública y una clave privada. Estas claves son únicas y se generan utilizando algoritmos criptográficos seguros.

DIGITO, además, implementa medidas de seguridad adecuadas para proteger las claves privadas generadas. Esto puede incluir el almacenamiento seguro de las claves en entornos controlados y protegidos, utilizando técnicas como el cifrado y la gestión segura de claves.

DIGITO lleva a cabo un registro completo de la generación de claves criptográficas, incluyendo información como la fecha y hora de generación, el solicitante de las claves y cualquier otra información relevante.

6.1.1 MÓDULOS CRIPTOGRÁFICOS.

6.1.1.1. GENERACIÓN Y ALMACENAMIENTO DE CLAVES DE AC RAÍZ.

Los pares de claves de AC Raíz se generarán y almacenarán en *Root CA HSM.* Los HSM utilizados por la Infraestructura de Clave Pública serán el Luna S790 HSM 7 fabricado por Thales Group. Este HSM es un módulo criptográfico evaluado por FIPS 140-3 nivel 3, Criterios Comunes EAL 4+.

6.1.1.2. EMISIÓN DE ALMACENAMIENTO DE CLAVES DE AC SUBORDINADA.

Estos pares de claves se generarán y almacenarán en el clúster de HSM de la AC Subordinada. Los HSM empleados son módulos de Luna S790 HSM 7. Este HSM es un módulo criptográfico evaluado por FIPS 140-3 nivel 3, Criterios Comunes EAL 4+.

6.1.1.3. ALMACENAMIENTO DE CLAVES DIGITO RA, LRA Y OFICIAL DE SEGURIDAD DE LA INFORMACIÓN.

- Los RAs de DIGITO tendrán sus claves y certificados generados y almacenados en tokens USB de Gemalto (SafeNet). Estos tokens y módulos criptográficos cuentan con la certificación FIPS 140-2 de nivel 2.

- Los LRA de DIGITO autorizados para emitir y administrar certificados de seguridad básica, media y alta tendrán sus claves y certificados generados y almacenados en tokens USB de Gemalto (SafeNet). Estos tokens y módulos criptográficos cuentan con la certificación FIPS 140-2 de nivel 2.

- Los RA de DIGITO autorizados para emitir y gestionar certificados de seguridad básica y media tendrán sus claves y certificados generados y almacenados en software (EPF).

- El Oficial de Seguridad de la Información tendrá sus claves y certificados generados y almacenados en el software (EPF).

6.1.1.4. ENTIDADES FINALES DE DIGITO.

Las entidades finales de DIGITO pueden almacenar claves criptográficas en los siguientes contenedores:

- Contenedores de certificados y claves (por ejemplo: MS CAPI, Java Key Store y similares);;
- Contenedor de claves y certificados PKCS #12; y
- Otros contenedores aprobados por la Autoridad de Políticas.

Los módulos criptográficos y los contenedores de claves y certificados deben ser aprobados por la Autoridad de Políticas antes de ser utilizados.

6.1.1.5. CAMBIO DE CLAVE PRIVADA.

En el caso de que deba realizarse un cambio de clave privada, se procederá a generar un nuevo certificado con una nueva clave privada que se utilizará para reemplazar la anterior. Esto se hará siguiendo el procedimiento de solicitud y emisión de certificados digitales establecidos en el presente documento.

El nuevo certificado y la clave privada correspondiente deben ser actualizados en los sistemas y aplicaciones que utilizan el certificado. Esto asegura que las comunicaciones futuras se realicen utilizando la nueva clave privada.

6.2. DISPONIBILIDAD DE LA CADENA DE CONFIANZA E INFORMACIÓN DE REVOCACIÓN.

Los terceros que confían podrán consultar los certificados de la AC Raíz y la AC Subordinada en la página web de DIGITO https://digito.do
La información de revocación (CRLs) y los certificados de la AC se replican al mismo tiempo entre diferentes servidores web ubicados en los data center contratados por DIGITO y en la Red de Distribución de Contenido (*Content Delivery Network - CDN,* por sus siglas en inglés). Esto garantiza que la información de revocación y los datos necesarios para validar las cadenas de confianza estén disponibles cuando sea necesario.

6.3. ALGORITMOS DE CIFRADO Y LONGITUD DE CLAVE.

- DIGITO ha seleccionado los algoritmos de cifrado RSA-4096 y SHA-256 y la longitud de la clave para su AC Raíz.
- DIGITO ha seleccionado los algoritmos de cifrado RSA-4096 y SHA-256 y la longitud de clave para su AC Subordinada.
- DIGITO ha seleccionado los algoritmos de cifrado RSA-2048 y SHA-256 y la longitud de la clave para sus certificados de entidad final.
- DIGITO ha seleccionado los algoritmos de cifrado RSA-4096 y SHA-256 y la longitud de clave para sus certificados de estampado de tiempo.
- DIGITO ha confirmado que sus aplicaciones habilitadas para ILP admitirán certificados de AC con claves RSA-2048.
- DIGITO ha confirmado que sus aplicaciones habilitadas para PKI admitirán SHA-256.

6.3.1. PROTOCOLO DE CONTINGENCIA ANTE LA DEGRADACIÓN O COMPROMISO DE ALGORITMOS CRIPTOGRÁFICOS

De conformidad con las exigencias de la norma **ETSI EN 319 411-1**, DIGITO mantiene un proceso continuo de monitoreo del estado del arte criptográfico y de las recomendaciones emitidas por los organismos internacionales de estandarización (como ETSI y NIST).

En el caso de que se determine de manera imprevista que alguno de los algoritmos o longitudes de clave vigentes de la PKI (ej. RSA-2048, RSA-4096 o SHA-256) ha dejado de ser criptográficamente suficiente, seguro o robusto frente a nuevos vectores de ataque o capacidades de cómputo, DIGITO activará de forma inmediata el siguiente protocolo de desuso criptográfico prematuro dentro de su Plan de Recuperación de Desastres:

- **1. Cese Inmediato de Emisiones:** Se procederá a deshabilitar de forma inmediata en la CA la emisión de cualquier nuevo certificado utilizando el algoritmo, suite criptográfica o longitud de clave identificada como vulnerable.
- **2. Notificación Obligatoria de Emergencia:** DIGITO notificará de manera prioritaria a la Autoridad de Supervisión competente, a los organismos de certificación de conformidad, a sus suscriptores y a las partes confiantes (*relying parties*) en un **plazo máximo de veinticuatro (24) horas** tras la confirmación del compromiso del algoritmo, detallando el alcance del riesgo técnico.
- **3. Revocación Mandatoria:** DIGITO ejecutará la revocación obligatoria y masiva de la totalidad de los certificados vigentes (incluyendo, si fuera necesario, los certificados de las AC Subordinadas y de las entidades finales) cuyas claves públicas dependan del algoritmo degradado o comprometido.
- **4. Transición y Re-emisión de Infraestructura:** El Comité de Seguridad de la PKI iniciará un plan de migración tecnológica acelerado para reemplazar las llaves afectadas. Esto incluirá la generación de nuevos pares de claves para las AC y la re-emisión de los certificados de los usuarios utilizando algoritmos alternativos que ofrezcan una seguridad matemática adecuada y vigente (por ejemplo, migración total a criptografía de curva elíptica [ECC] o longitudes de clave superiores).

6.4. CONTROL DE SEGURIDAD DE MÁS DE UNA PERSONA SOBRE LA CLAVE PRIVADA.

DIGITO implementa un control de protección de la clave privada mediante la participación de múltiples personas. Para activar la clave privada de la AC Raíz, se requiere la participación de más de la mitad del personal designado para realizar estas actividades.

6.5. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES.

6.5.1. PERÍODOS DE UTILIZACIÓN DE LAS CLAVES PÚBLICA Y PRIVADA.

El período de uso del par de claves y certificado digital será de 12, 24 o 36 meses, a partir de la fecha de emisión. Al término de este período, el titular deberá renovar su certificado digital.

6.6. CONTROLES DE SEGURIDAD INFORMÁTICA Y DE RED.

DIGITO emplea los siguientes controles de seguridad informática y de red:

- **Firewall:** DIGITO ha implementado firewalls de próxima generación (NGFW) en alta disponibilidad para controlar el tráfico entrante y saliente, así como para las políticas de seguridad que protegen contra ataques de red, como intrusiones y tráfico malicioso adicional con sistemas de SOC.
- **Filtrado de contenido web**: DIGITO utiliza herramientas de filtrado de contenido web para bloquear el acceso a sitios web maliciosos o no autorizados, así como para controlar y monitorear el tráfico web para detectar amenazas.
- **Sistema de antivirus**: DIGITO utiliza una solución de ciberseguridad avanzada de antivirus y protección de malware para proteger a los equipos, servidores y sistemas de posibles ataques de softwares maliciosos.
- **Prevención de intruso:** DIGITO ha implementado sistemas de prevención de intrusiones (IPS) para detectar y bloquear intentos de intrusión en la red, como escaneos de puertos, ataques de denegación de servicio (DDoS) y exploits de vulnerabilidades conocidas.
- **VPN (Redes Privadas Virtuales):** DIGITO utiliza VPN para establecer conexiones seguras entre ubicaciones remotas y/o usuarios remotos, cifrando el tráfico y protegiendo la comunicación frente a posibles interceptaciones.
- **Segmentación de red:** DIGITO ha segmentado las redes en diferentes VLANs para limitar la exposición a ataques y reducir la superficie de ataque, y utiliza firewalls internos para controlar el tráfico entre segmentos.
- **Gestión de parches y actualizaciones**: DIGITO ha creado procedimientos para mantener actualizados todos los sistemas y aplicaciones con los últimos parches de seguridad y actualizaciones de software disponibles para proteger contra vulnerabilidades conocidas y mitigar los riesgos de explotación.
- **Cifrado de datos:** Implementa cifrado de datos para proteger la confidencialidad de la información sensible, tanto en reposo como en tránsito, utilizando algoritmos de cifrado robustos y técnicas de gestión de claves seguras.

6.7. CONTROLES TÉCNICOS DEL CICLO DE VIDA.

6.7.1. CONTROLES DE DESARROLLO.

DIGITO cuenta con la Política de Seguridad de Operaciones DTI-POL-10 y la Política de Desarrollo Seguro DTI-POL-13, que describen las reglas para la adquisición, cambios y desarrollo de software y sistemas que se aplicarán en la Entidad de Certificación.

6.7.2. CONTROLES DE GESTIÓN DE SEGURIDAD.

DIGITO cuenta con la Política del Sistema de Gestión de Seguridad de la Información DTI-SGSI-02 y la Política de Seguridad de la Información DTI-POL-08, mediante las cuales se describe el uso aceptable y la protección de la información y los activos de DIGITO. En ese sentido, estas políticas aplican al uso de información, dispositivos electrónicos y de computación, así como recursos de red para realizar negocios con DIGITO o interactuar con redes internas y sistemas comerciales, ya sean propiedad o arrendados por DIGITO. Todos los colaboradores, contratistas y consultores de DIGITO son responsables de ejercer su buen juicio con respecto al uso apropiado de estos activos.

6.7.2.1. CLASIFICACIÓN Y GESTIÓN DE INFORMACIÓN.

DIGITO cuenta con la Política de Gestión de Datos DTI-POL-05, mediante la cual se clasifican los datos y

los sistemas de información de acuerdo con los requisitos legales, la sensibilidad y la importancia del negocio para garantizar que la información reciba el nivel de protección adecuado.

Los niveles de protección serán: Confidencial, Restringido y Público.

6.7.2.2. RESPUESTA DE INCIDENCIAS.

DIGITO cuenta con el Plan de Respuesta ante Incidentes DTI-POL-07, para la gestión de incidentes y eventos de seguridad de la información. El mismo ofrece orientación para los colaboradores de DIGITO sobre respuesta a incidentes que pueden haber descubierto o están respondiendo ante un incidente de tecnología.

6.7.2.3. GESTIÓN DE ACCESOS.

DIGITO cuenta con la Política de Control de Acceso DTI-POL-01, mediante la cual se determinará el tipo y nivel de acceso otorgado a los colaboradores, contratistas y consultores de DIGITO (usuarios individuales) según el "principio de privilegio mínimo". Este principio establece que a los usuarios solo se les concede el nivel de acceso absolutamente necesario para realizar sus funciones, y está determinado por los requisitos comerciales y de seguridad de DIGITO**.** Los permisos y derechos de acceso no otorgados expresamente estarán prohibidos por defecto.

6.7.3. POLÍTICA DE CRIPTOGRAFÍA.

DIGITO cuenta con la Política de Criptografía DTI-POL-04, mediante la cual evalúa los riesgos inherentes al procesamiento y almacenamiento de datos e implementa controles criptográficos para mitigar esos riesgos cuando se considere apropiado.

DIGITO utiliza módulos de seguridad de hardware (HSM) o dispositivos de almacenamiento criptográficamente protegidos, tal como se describe en este documento.

6.7.4. FUENTES DE TIEMPO.

El tiempo para los servicios de DIGITO se obtienen del servicio de NTP server de diferentes proveedores asegurando la mejor precisión disponible. Los servidores se mantienen actualizados con la hora UTC −4, mediante sincronización a través del protocolo NTP v4, conforme al estándar RFC 5905 “Network Time Protocol Version 4: Protocol and Algorithms Specification”.

6.7.5. CAMBIO DE ESTADO DE UN DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA (QSCD).

DIGITO consta en su infraestructura varios equipos QSDC certificados. En el caso de que se lleve a cabo cualquier modificación en las características operativas o de seguridad de un dispositivo QSCD, se realizará una evaluación exhaustiva para determinar las posibles implicaciones sobre su funcionalidad y la integridad de las firmas electrónicas avanzadas que produce. Es crucial reconocer que un cambio en el estado operativo de un QSCD puede ser el resultado de diversas circunstancias. Por ejemplo, las actualizaciones de software pueden introducir modificaciones en las capacidades y comportamiento del dispositivo, lo que podría afectar la generación y verificación de las firmas electrónicas avanzadas.

Además, cualquier forma de manipulación física no autorizada o fallo técnico en el dispositivo puede comprometer su seguridad y precisión, lo que a su vez puede incidir en la confianza en las firmas electrónicas generadas se llevarán a cabo las acciones necesarias para asegurar que el dispositivo continúe cumpliendo con los estándares de seguridad y funcionalidad requeridos para la creación de firmas electrónicas avanzadas incluyendo hasta su sustitución.

7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS.

7.1. PERFIL DE CERTIFICADO DE AC RAÍZ DE DIGITO.

CAMPO/EXTENSIÓN	¿CRÍTICO?	VALORES	COMENTARIOS
Campos Básicos del Certificado			
Version	N/A	V3 (2)	Version 3
serialNumber	N/A	Asignado por la CA	505fedf35914388c5dfab081a59bd3c0f770c71e
Signature Algorithm	N/A	**Sha256RSA**	
Issuer	N/A	cn=Digito Root CA, ou=Certification Authorities, o=Digito Group, c=DO	
Validity	N/A	**notBefore** and **notAfter** are both included in **UTCTime** format YYMMDDHHMMSSZ	20 años
Subject	N/A	Same as issuer	
subjectPublicKey Info	N/A	**RSA encryption** ;4096-bit modulus 2^16+1 public exponent	
Extensiones			
keyUsage	Sí	Certificate Signing, Off-line CRL Signing, CRL Signing	
subjectKeyIdentifier	No	SM CA includes hash of the **subjectPublicKey** component of the **subjectPublicKeyInfo** field of the certificate	
basicConstraints	Sí	**CA** = **TRUE**	

Campo/Extensión	¿Crítico?	Valores	Comentarios
		pathLenConstraint = **None**	

7.2. PERFIL DEL CERTIFICADO DE AC SUBORDINADA.

Campo/Extensión	¿Crítico?	Valores	Comentarios
Base certificate fields			
Version	N/A	V3 (2)	
serialNumber	N/A	Asignado por la CA	16a6b4c37f24235dd357e5c16c6fcbf8ad3464aa
Signature	N/A	**Sha256RSA**	
Issuer	N/A	cn=Digito Root CA, ou=Certification Authorities, o=Digito Group, c=DO	
Validity	N/A	**notBefore** y **notAfter** en formato **UTCTime** YYMMDDHHMMSSZ	10 años
Subject	N/A	cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO	
subjectPublicKeyInfo	N/A	**RSA encryption**; 4096-bit modulus 2^16+1 public exponent	
Extensiones			
cRLDistributionPoints	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digito.do/CRLs/DigitoRootCA.crl CRL Issuer: Directory Address: C=DO O=Digito Group OU=Certification Authorities CN=Digito Root CA	
authorityInfoAccess	No	[1]Authority Info Access	

Campo/Extensión	¿Crítico?	Valores	Comentarios
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.digito.do/CAs/DigitoRootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digito.do	
keyUsage	Sí	Certificate Signing, CRL Signing	
authorityKeyIdentifier	No	**keyIdentifier presente** **authorityCertIssuer**	
subjectKeyIdentifier	No	SM CA includes hash of the **subjectPublicKey** component of the **subjectPublicKeyInfo** field of the certificate	
basicConstraints	Sí	**CA boolean** = TRUE **pathLenConstraint** = 0	
certificatePolicies	No	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.64999.1.0.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://cps.digito.do	1.3.6.1.4.1.64999.1.0.2

7.3. PERFIL DE CERTIFICADOS DE SUSCRIPTOR DE DIGITO PRODUCCIÓN.

7.3.1 - Certificados TLS/SSL - Medio.

Field	SSL/TLS Servers Medium Assurance – 3 años
Nombre de Perfil en uso	SSL_tls_3y_nodir-CP
OID	1.3.6.1.4.1.64999.1.2.1
X.509 Version	3
Tipo de certificado	End Entity-SSL/SSL Server
Validez de Certificado	3 años
Minimum Key Length	RSA-2048/SHA-256
Subject DN Attributes	cn= [Server Name], ou= SSL Servers, o= Digito Group, c= DO
AIA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.digito.do/CAs/DigitoIssuingCADO02.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digito.do
CDP	[1]CRL Distribution Point Distribution Point Name: **Full Name:** URL=http://crl.digito.do/CRLs/DigitoIssuingCADO02.crl

Field	SSL/TLS Servers Medium Assurance – 3 años
	Full Name: Directory Address: cn=CRL cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO
Key Usage	digitalSignature keyEncipherment
Extended Key Usage	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; id-kp-serverAuth {1.3.6.1.5.5.7.3.1};
Certificate Policies Extension	Policy Identifier= Garantia Media 1.3.6.1.4.1.64999.1.2.1
Key and Certificate Storage	Web server key and certificate stores (e.g. MS CAPI, Java key store, etc.)

7.3.2 - Certificados TLS del Servidor RSE - Medio

Field	RSE and SAE Servers Medium Assurance – 3 años
Nombre de Perfil	RSE tls 3y nodir-CP
OID	1.3.6.1.4.1.64999.1.2.2
X.509 Version	3
Tipo de certificado	End Entity-SSL/TLS Server
Validez de Certificado	3 años
Minimum Key Length	RSA-2048/SHA-256
Subject DN Attributes	cn= [Server Name], ou= SSL Servers, o= Digito Group, c= DO
AIA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.digito.d

Field	RSE and SAE Servers Medium Assurance – 3 años
	o/CAs/DigitoIssuingCADO02.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digito.do
CDP	[1]CRL Distribution Point Distribution Point Name: **Full Name:** URL=http://crl.digito.do/CRLs/DigitoIssuingCADO02.crl Directory Address: cn=CRL cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO
Key Usage	digitalSignature keyEncipherment
Extended Key Usage	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; id-kp-serverAuth {1.3.6.1.5.5.7.3.1};
Certificate Policies Extension	Policy Identifier= Garantia Media 1.3.6.1.4.1.64999.1.2.2
Key and Certificate Storage	Signing Automation and Remote Signing Engines servers key stores (.jks)

7.3.3 - Certificado de LRA/SCO - Medio.

Field	Certificados de LRA/SCO para Acceso Operacional - Medio- Medium Assurance – 3 años
Nombre de Perfil	lra-sco_m_req_app-CP
OID	1.3.6.1.4.1.64999.1.2.3
X.509 Version	3
Tipo de certificado	End Entity-LRA/SCO Certificate
Validez de Certificado	3 años
Minimum Key Length	RSA-2048/SHA-256
Subject DN Attributes	cn= [Nombre del LRA o SCO], ou= Administrator, o= Digito Group, c= [pais de jurisdiccion]
Allowed Subject Alt Name	Email Address
AIA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.digito.do/CAs/DigitoIssuingCADO02.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digito.do
CDP	[1]CRL Distribution Point Distribution Point Name: **Full Name:** URL=http://crl.digito.do/CRLs/DigitoIssuingCADO02.crl

Field	Certificados de LRA/SCO para Acceso Operacional - Medio- Medium Assurance – 3 años
	Directory Address: cn=CRL cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO
Key Usage	Digital Signature Key encipherment
Extended Key Usage	clientAuthentication {1.3.6.1.5.5.7.3.2}
Certificate Policies Extension	Policy Identifier= Garantia Alta 1.3.6.1.4.1.64999.1.3.3
Key and Certificate Storage	Encrypted Hard Drive

7.3.4 - Certificado TLS del Servidor TSA - Medio

Field	Certificado TLS del Servidor TSA- Medium Assurance – 3 años
Nombre de Perfil en Uso	Digito-CSRREQ-TSA-CP
OID	1.3.6.1.4.1.64999.1.2.4
X.509 Version	3
Tipo de certificado	End Entity-SSL/TLS Server
Validez de Certificado	3 años
Minimum Key Length	RSA-4096/SHA-256
Subject DN Attributes	cn= [Server Name], ou= SSL Servers, o= Digito Group, c= DO
AIA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.digito.do/CAs/DigitoIssuingCADO02.crt

Field	Certificado TLS del Servidor TSA- Medium Assurance – 3 años
	[2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digito.do
CDP	[1]CRL Distribution Point Distribution Point Name: **Full Name:** URL=http://crl.digito.do/CRLs/DigitoIssuingCADO02.crl **Full Name:** Directory Address: cn=CRL cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO
Key Usage	digitalSignature keyEncipherment
Extended Key Usage	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; id-kp-serverAuth {1.3.6.1.5.5.7.3.1};
Certificate Policies Extension	Policy Identifier= Garantia Media 1.3.6.1.4.1.64999.1.2.4
Key and Certificate Storage	TimeStamp Authorization (TSA) Server

7.3.5 - Qualified Electronic Signature / Seal - Alto

Field	Qualified Electronic Signature / Seal - High Assurance – 3 años
Nombre de Perfil	digsig 3y nodir-CP
OID	1.3.6.1.4.1.64999.1.3.1
X.509 Version	3
Tipo de certificado	End Entity-Qualified Electronic Signature / Seal Certificate
Validez de Certificado	3 años
Minimum Key Length	RSA-2048/SHA-256
Subject DN Attributes	cn= [Nombre + Apellido], serialNumber= <Tipo de documento + código país + cédula>ou= People ID, o= Digito Group, c= DO
Allowed Subject Alt Name	Email Address
AIA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.digito.do/CAs/DigitoIssuingCADO02.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digito.do
CDP	[1]CRL Distribution Point Distribution Point Name: **Full Name:**

Field	Qualified Electronic Signature / Seal - High Assurance – 3 años
	URL=http://crl.digito.do/CRLs/DigitoIssuingCADO02.crl Directory Address: cn=CRL cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO
Key Usage	digitalSignature, nonrepudiation
Extended Key Usage	n/a
Certificate Policies Extension	Policy Identifier= Garantia Alta [1) 1.3.6.1.4.1.64999.1.3.1 [2) PRIVATE KEY GENERATED IN QUALIFIED ELECTRONIC SIGNATURE/SEAL CREATION DEVICE (QSCD) 1.3.6.1.5.5.7.1.3
DN Qualifier	CERTIFICADO CUALIFICADO EN LA NUBE PARA PERSONA FISICA; CLAVE PRIVADA GENERADA EN DISPOSITIVO CUALIFICADO DE CREACION DE FIRMA (QSCD).
QC Statements	qcstatements=1.3.6.1.5.5.7.1.3 Qualified Certificate according to ETSI EN 319 412-5 Qualified Certificate Country Code Legislation: DO Retention Period: 20 Years Private key resides in QSCD

Field	Qualified Electronic Signature / Seal - High Assurance – 3 años
Key and Certificate Storage	Llave privada generada y guardada en HSM

7.3.6 - Estampado de Tiempo Cualificado - Alto

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

Field	Certificados de Timestamping - High Assurance – 5 años
	Distribution Point Name: **Full Name:** URL=http://crl.digito.do/CRLs/DigitoIssuingCADO02.crl [2]CRL Distribution Point Distribution Point Name: **Full Name:** Directory Address: cn=CRL cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO
Key Usage	digitalSignature
Extended Key Usage	timestamping (critical) {1.3.6.1.5.5.7.3.8}
Certificate Policies Extension	Policy Identifier= Garantia Alta 1.3.6.1.4.1.64999.1.3.2
Key and Certificate Storage	Llave privada generada y guardada en HSM

7.3.7 - Certificados de RA/LRA para Acceso Operacional - Alto

Field	Certificados de RA/LRA para Acceso Operacional - Alto- High Assurance – 3 años
Nombre de Perfil	ra h req app-CP
OID	1.3.6.1.4.1.64999.1.3.3
X.509 Version	3
Tipo de certificado	End Entity-RA/LRA Certificate
Validez de Certificado	3 años
Minimum Key Length	RSA-2048/SHA-256

Field	Certificados de RA/LRA para Acceso Operacional - Alto- High Assurance – 3 años
Subject DN Attributes	cn= [RA Name], ou= Administrator, o= Digito Group, c= DO
Allowed Subject Alt Name	Email Address
AIA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.digito.do/CAs/DigitoIssuingCADO02.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digito.do
CDP	[1]CRL Distribution Point Distribution Point Name: **Full Name:** URL=http://crl.digito.do/CRLs/DigitoIssuingCADO02.crl **Full Name:** Directory Address: cn=CRL cn=Digito Issuing CA DO 02, ou=Certification Authorities, o=Digito Group, c=DO
Key Usage	Digital Signature Key encipherment
Extended Key Usage	clientAuthentication {1.3.6.1.5.5.7.3.2}

Field	Certificados de RA/LRA para Acceso Operacional - Alto- High Assurance – 3 años
Certificate Policies Extension	Policy Identifier= Garantia Alta 1.3.6.1.4.1.64999.1.3.3
Key and Certificate Storage	Encrypted Hard Drive

7.3.8 - Certificados de Firmante OCSP (OCSP Responder) - Alto

Field	Certificados de RA/LRA para Acceso Operacional - Alto- High Assurance – 3 años
Nombre de Perfil	OCSP-DIGITO
X.509 Version	3
Tipo de certificado	End Entity-OCSP Certificate
Validez de Certificado	2 años
Minimum Key Length	RSA-2048/SHA-256
Subject DN Attributes	cn= OCSP-[CA], ou= Services, o= Digito Group, c= DO
Allowed Subject Alt Name	N/A
Key Usage	Digital Signature (c)
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9) OCSP No Check Enabled (1.3.6.1.5.5.7.48.1.5)
Certificate Policies Extension	Policy Identifier= Garantia Alta 1.3.6.1.4.1.64999.1.3.4

7.5. PERFIL DE LA CRL.

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

8. AUDITORÍAS DE CONFORMIDAD.

DIGITO cuenta con el Procedimiento para Auditorías Interna DTI–SGSI-07, que bajo su propio criterio, cubrirá todos los elementos del Sistema de Gestión de Seguridad de la Información (SGSI) para todos los activos de información.

De igual forma, DIGITO podrá contratar los servicios de un proveedor independiente y especializado para la realización de auditorías externas. Estas auditorías deberán abarcar como mínimo:

- Cumplimiento normativo;
- Gestión de Seguridad;
- Prácticas de emisión, gestión, renovación y revocación de certificados;
- Auditorías internas.

DIGITO se compromete a proporcionar toda la información y documentación necesaria para la realización de estas auditorías, así como la disponibilidad del personal para entrevistas y pruebas de control.

Los hallazgos y recomendaciones de la auditoría serán compartidos con el Consejo de Seguridad de la Información, para fines de implementación y seguimiento.

9. TARIFAS COMERCIALES.

DIGITO no ha establecido tarifas para la prestación de sus servicios a los solicitantes, usuarios y titulares de certificados.

10. CAPACIDAD FINANCIERA.

DIGITO cuenta con la capacidad económica y financiera suficiente y demostrable para prestar los servicios autorizados como entidad de certificación, de conformidad con la legislación vigente.

11. COBERTURA DE SEGURO.

DIGITO cuenta con un seguro apropiado en los términos que señala el artículo 16 del Reglamento de Aplicación de la Ley No. 126-02 y el Instituto Dominicano de las Telecomunicaciones (INDOTEL).

12. PLAN DE CONTINGENCIA.

El Plan de Contingencia de DIGITO abarca todos sus procesos críticos, incluyendo:

- Emisión de certificados

- Gestión de auditorías
- Mantenimiento de registros
- Control de documentos
- Seguridad de la información

12.1. GESTIÓN DE INCIDENTES Y VULNERABILIDADES.

DIGITO realiza un análisis exhaustivo de los riesgos internos y externos que puedan afectar sus operaciones. Por tanto, ha establecido políticas y procedimientos de seguridad para el manejo de incidentes y vulnerabilidades en su infraestructura y sistemas:

- Plan de respuesta ante incidentes DTI-POL-07;
- Politica de Gestion de Riesgos DTI-POL-12;
- Procedimiento de Gestión de vulnerabilidades DTI-PROC-08.

12.1.1 NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

- Notificación de incidentes de seguridad: DIGITO notificará a las autoridades supervisoras, organismos reguladores y demás entidades pertinentes sobre cualquier incidente de seguridad, vulneración de integridad, compromiso criptográfico o interrupción significativa de los servicios de confianza que pueda afectar la confiabilidad de los certificados digitales, los servicios prestados o la información de los suscriptores.
- Dicha notificación será realizada sin demora injustificada y, cuando aplique conforme a las normativas vigentes y estándares aplicables, dentro de un plazo máximo de 24 horas desde la detección o confirmación inicial del incidente.
- DIGITO mantendrá procedimientos internos para la clasificación, escalamiento, tratamiento y seguimiento de incidentes de seguridad, conforme a los lineamientos establecidos en sus políticas y procedimientos internos de gestión de incidentes y riesgos.
- Cuando corresponda, DIGITO también podrá informar a los suscriptores, terceros confiantes y demás partes afectadas sobre incidentes que puedan impactar la validez, integridad o confianza de los certificados digitales y servicios relacionados.

13. RECUPERACIÓN DE DESASTRES.

La infraestructura de DIGITO está configurada para la recuperación ante desastres. Los módulos de seguridad de hardware (HSM) y los servidores de manejo de los módulos de seguridad y aplicación están desplegados en un centro de datos secundario de DIGITO.

Las Base de datos y Servidores aplicaticación esta desplegados para asegurar la continuidad del servicio, se ha realizado las configuraciones de replicación y la redundancia necesarias para garantizar la alta disponibilidad y la tolerancia a fallos de los servidores

13.1. REPLICACIÓN Y RESPALDO DE DATOS.

Los datos de PKI se replicarán desde el centro de datos principal al centro de datos secundario y los servicios pueden conmutar cuando los se declara un desastre.

La PKI designa todos los sistemas como "con estado" o "sin estado". Los sistemas con estado son sistemas donde se almacena información que se requiere para las operaciones normales o que puede tener un impacto en la postura de seguridad. Por ejemplo, las CAs y su infraestructura de soporte se consideran con estado. Los datos con estado se replican en el sitio secundario en tiempo real para estar disponibles de inmediato en caso de que surja una situación de conmutación por error. Las copias de seguridad del sistema también se realizan para todos los sistemas con estado y se transfieren al sitio secundario. De acuerdo con el contrato de DIGITO, las copias de seguridad se completarán al menos una noche por semana, y las copias de seguridad incrementales se crearán las seis noches restantes. Estas copias de seguridad se copiarán en la instalación secundaria.

14. CONTINUIDAD DEL NEGOCIO.

DIGITO cuenta con la Política de continuidad negocio (BCP) y de recuperación ante desastres (DRP) DTI-POL-03, para que en caso de interrupciones prolongadas del servicio causadas por factores fuera de nuestro control (por ejemplo, desastres naturales, eventos provocados) se puedan restaurar los servicios en la mayor brevedad posible y en un marco de tiempo mínimo.

En caso de una interrupción importante de los servicios de producción y un desastre que afecte la disponibilidad y/o la seguridad de la oficina, todo el personal de DIGITO deberá trabajar de forma remota desde sus hogares o desde cualquier lugar seguro.

Anualmente se realizará una prueba de recuperación de desastres, incluyendo una prueba de los procesos de restauración de las copias de seguridad.

15. CESE DE ACTIVIDADES.

DIGITO podrá finalizar la prestación de sus servicios de manera voluntaria o no voluntaria, para lo cual seguirá el Procedimiento Interno de Cese de Actividades DTI-PROC-15.

15.1. CESE DE ACTIVIDADES VOLUNTARIO.

En el caso de que DIGITO decida finalizar la prestación de sus servicios de manera voluntaria, solicitará al órgano regulador, con noventa (90) días hábiles de anticipación, la cancelación de su autorización, comunicando el destino de los certificados emitidos como Entidad de Certificación.

De igual forma, con una antelación no menor a noventa (90) días hábiles, DIGITO notificará a los titulares de los certificados la fecha efectiva del cese de operaciones y la identidad de la Entidad de Certificación sucesora que asumirá la continuidad de los servicios o la custodia de la información.

De conformidad con las exigencias obligatorias de la norma **ETSI EN 319 411-1**, **la transferencia de los certificados y datos asociados a una tercera entidad se ejecutará de forma exclusiva para aquellos titulares que hayan otorgado su consentimiento explícito, positivo e informado durante el proceso de registro e inducción inicial (onboarding).** Para aquellos titulares que no hayan otorgado dicho consentimiento explícito en su registro inicial, o que manifiesten expresamente su oposición tras la notificación de cese, DIGITO procederá de la siguiente manera:

- Sus certificados vigentes serán revocados de oficio antes del cese de actividades.
- Sus datos personales y registros de auditoría no serán transferidos a la entidad sucesora bajo ningún concepto; en su lugar, serán destruidos o archivados de forma segura y aislada por DIGITO (o por el custodio legal designado) únicamente para cumplir con los periodos de retención legales y auditorías posteriores exigidas por la normativa vigente.

DIGITO se compromete a mantener las obligaciones establecidas en la normativa vigente relativas a la protección, confidencialidad y debido uso de la información suministrada por los titulares de certificados hasta la finalización total de sus operaciones y el cierre de sus repositorios.

15.2. CESE DE ACTIVIDADES NO VOLUNTARIO.

La cancelación de la autorización será notificada a los titulares de certificados en un plazo máximo de veinticuatro (24) horas. En caso de que la Entidad de Certificación se encuentre en situación de traspasar los certificados a otra Entidad de Certificación, informará tal situación en un plazo de quince (15) días hábiles mediante comunicación escrita. Dicho plazo comenzará a contar desde la recepción de notificación.

15.3 CONSERVACIÓN DEL REGISTRO DE CERTIFICADOS.

DIGITO conservará las informaciones aportadas por los titulares de certificados por el tiempo que establezca la normativa vigente en la materia, contado a partir de la revocación o expiración de los certificados.

En el caso de los registros de todos los certificados emitidos, en los cuales se indican las fechas de emisión, expiración y los registros revocación, DIGITO los conservará por el tiempo que establezca la normativa vigente en la materia, contado a partir de la revocación o expiración de los certificados.
En el caso de que DIGITO cese sus actividades y transfiera dichas informaciones a otra Entidad de Certificación o a una empresa especializada en la custodia de datos electrónicos debidamente autorizada por el Instituto Dominicano de las Telecomunicaciones (INDOTEL), la misma deberá conservar estos datos y registros por el tiempo faltante para completar sus respectivos plazos de conservación.

15.4 Emisión de la Lista de Revocación de Certificados (CRL) Final

De conformidad con los requisitos obligatorios establecidos en el estándar **ETSI EN 319 411-2**, en caso de que DIGITO determine el cese definitivo de sus actividades como Prestador de Servicios de Confianza para una o más de sus Autoridades de Certificación (CA), se ejecutará de forma obligatoria el siguiente procedimiento criptográfico antes del desmantelamiento de la infraestructura técnica:

- **1. Revocación previa de Certificados Vigentes:** DIGITO procederá a la revocación de oficio de la totalidad de los certificados finales que permanezcan vigentes a la fecha efectiva del cese, utilizando la causa de revocación correspondiente a "Cese de operaciones de la CA" (*cessationOfOperation*).
- **2. Generación de la CRL Final:** Inmediatamente después de la revocación masiva, y antes de proceder a la destrucción de las claves privadas de la CA o a la baja del HSM, el Administrador de la PKI generará y firmará digitalmente una **última Lista de Revocación de Certificados (CRL Final)**.
- **3. Configuración del Campo `nextUpdate` (Vigencia Infinita):** Esta CRL Final se emitirá configurando de forma mandatoria el campo nextUpdate (fecha de próxima actualización) con el valor estandarizado **`99991231235959Z`** (31 de diciembre del año 9999, a las 23:59:59 UTC), indicando explícitamente que la validez de dicha lista es permanente e infinita, y que no habrá publicaciones posteriores.
- **4. Publicación y Mantenimiento del Repositorio:** DIGITO garantizará, ya sea por medios propios o a través de la entidad pública/privada que asuma la custodia de sus activos (de acuerdo al plan de cese aprobado), que esta CRL Final permanezca accesible de forma pública y gratuita en la URL indicada en la extensión *CRL Distribution Points* (CDP) de los certificados, durante el periodo legalmente exigido por la autoridad regulatoria local tras el cese de operaciones.

16. RESOLUCIÓN DE CONFLICTOS.

DIGITO se acoge a las disposiciones y procedimientos dictados por el Instituto Dominicano de las Telecomunicaciones (INDOTEL) para la resolución de conflictos y protección de los derechos de los usuarios y consumidores.

17. POLÍTICA DE PRIVACIDAD.

17.1. INFORMACIÓN RECOPILADA.

DIGITO solicitará y recopilará los siguientes datos personales: Nombre, documento de identidad (incluyendo foto), dirección de correo electrónico, números de contacto, foto de perfil, así como un video grabado por el Solicitante, Usuario y Titular del Certificado. Además, DIGITO podría recopilar otras informaciones tales como dispositivo utilizado y su ubicación, sistema operativo, tiempo en la

plataforma, así como cualquier información que nos proporcione o haya creado durante su uso. De igual forma, se podrá recopilar cualquier información proporcionada durante algún contacto con el Departamento de Soporte o Asistencia al Usuario de DIGITO.

No obstante, DIGITO nunca solicitará o recopilará información sobre números de cuentas bancarias, tarjetas de crédito o débito al momento de completar el registro en nuestra plataforma.

17.2. VERIFICACIÓN DE LA INFORMACIÓN RECOPILADA.

A los fines de verificar los datos personales recopilados, DIGITO se apoyará de proveedores públicos o privados, nacionales e internacionales, autorizados a recopilar esta información, a tales fines el Solicitante, Usuario o Titular del Certificado nos autoriza a realizar las indagaciones necesarias para confirmar su identidad.

17.3. USO DE LA INFORMACIÓN RECOPILADA.

DIGITO utilizará la información con el fin principal de realizar la verificación de datos personales y mantener un registro de usuarios, de conformidad con la legislación vigente sobre protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.

Además, DIGITO utilizará dicha información para obtener mejores controles de calidad para la seguridad del Solicitante, Usuario o Titular del Certificado y mejorar su experiencia con el Departamento de Soporte Asistencia al Usuario. Tales como verificación de identidad durante el uso de Soporte al Usuario, respuesta a preguntas realizadas por el Usuario, análisis de tráfico y mejorar nuestros productos.

17.4. VALIDEZ DE LA COMUNICACIÓN ELECTRÓNICA.

Las comunicaciones electrónicas tales como avisos en la Plataforma de DIGITO, correos electrónicos, mensajes de texto SMS o por aplicaciones de mensajería electrónica y chats, así como otros medios disponibles de acuerdo con el avance de la tecnología, se consideran comunicaciones electrónicas válidas, legalmente vinculantes y satisfactorias como medios de prueba de las distintas interacciones o eventualidades que ocurran en el marco de la prestación del Servicio, siempre y cuando se realicen por los canales de comunicación oficiales de DIGITO.

17.5. USO COMPARTIDO DE TU INFORMACIÓN.

DIGITO no compartirá, venderá o distribuirá a terceros los datos suministrados por el Solicitante, Usuario y Titular del Certificado sin su consentimiento. No obstante, se podrá compartir la información suministrada, incluyendo aquellas de carácter personal, a requerimiento de las autoridades competentes y en cumplimiento con las leyes vigentes en la República Dominicana. En estos casos, el Solicitante, Usuario y Titular del Certificado descarga a DIGITO de cualquier responsabilidad por la entrega y el manejo de la información provista.

17.6. ACEPTACIÓN DE POLÍTICA DE PRIVACIDAD.

Con el acceso, uso, navegación o registro en la Plataforma de DIGITO, el Solicitante, Usuario y Titular del Certificado declara que ha leído, entendido y aceptado la presente Política de Privacidad. En caso de no encontrarse de acuerdo, no podrá utilizar los servicios de DIGITO.

17.7. CONTROL DE LA INFORMACIÓN PERSONAL.

DIGITO toma todas las medidas de seguridad que están a su alcance para proteger la información y garantizar la disponibilidad, integridad y confidencialidad de las mismas.

El Solicitante, Usuario o Titular del Certificado tendrá acceso a sus derechos de acceso, rectificación, cancelación y oposición, escribiendo a soporte@digito.com.do

18. CONDICIONES DE USO.

Al acceder y utilizar DIGITO, el Solicitante, Usuario o Titular del Certificado acepta cumplir con estos Términos y Condiciones de Uso en todo su contenido y está sujeto a ellos. En caso de no estar acuerdo en su totalidad o con algún punto en específico, no será posible utilizar los servicios de DIGITO.
Las siguientes condiciones se consideran esenciales para el uso de los servicios de DIGITO:

- Permiso de uso: Se otorga un permiso de uso que es limitado, no exclusivo y revocable para acceder y utilizar los servicios que ofrecemos. Este permiso no abarca autorizaciones para modificar, copiar, distribuir, transmitir, mostrar, realizar, reproducir, publicar, licenciar, crear, transferir o vender cualquier contenido o información obtenida de DIGITO sin consentimiento expreso y por escrito.

- Registro: Es necesario crear una cuenta para acceder a los servicios de DIGITO. En tal sentido, se debe proporcionar información precisa y actualizada al registrarse. El Solicitante, Usuario o

Titular del Certificado es responsable de mantener la confidencialidad de su cuenta (usuario y contraseña), y de toda la actividad que ocurra en ella.

- Contenido del Solicitante, Usuario o Titular del Certificado: Al utilizar los servicios de DIGITO, el Solicitante, Usuario o Titular del Certificado es responsable del contenido que envía, carga o publica y garantiza que tiene los derechos necesarios para hacerlo.

- Propiedad intelectual: Todos los derechos de propiedad intelectual asociados a DIGITO incluyendo pero no limitado a diseños, logotipos, texto, gráficos, imágenes, videos, software y demás contenidos, son propiedad exclusiva de nuestra empresa y está protegido por derechos de propiedad intelectual y leyes de derechos de autor. Queda estrictamente prohibida cualquier reproducción, distribución o utilización no autorizada de dichos contenidos.

- Enlaces a Terceros: El Solicitante, Usuario o Titular del Certificado puede acceder a los servicios de DIGITO a través de enlaces de sitios web de terceros que no están bajo nuestro control. No somos responsables de los contenidos de estos sitios ni de cualquier daño que pueda surgir del uso de los mismos.

19. PUBLICACIÓN.

La presente Declaración de Práctica de Certificación estará disponible públicamente en el sitio web de DIGITO.

20. VIGENCIA.

La presente Declaración de Práctica de Certificación entrará en vigor a partir de la fecha de su publicación y estará sujeta a revisiones periódicas por parte de DIGITO, que se reserva el derecho de modificarla en cualquier momento, y las modificaciones entrarán en vigor a partir de la fecha de su publicación.

Gabriella Gómez Tolari	Emily Perez	Irving Rivas
Gabriella Gómez Tolari	Emily Perez	Irving Rivas
2026-07-03	2026-07-03	2026-07-03

Audit trail

Details

FILE NAME	[DRAFT] DIGITO - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN v5.0 - 7/3/26, 2:58 PM
STATUS	Signed
STATUS TIMESTAMP	2026/07/03 19:52:27 UTC

Activity

SENT	emily.perez@digito.com.do **sent** a signature request to: • Gabriella Gómez Tolari (gabriella.gomez@digito.com.do) • Irving Rivas (irving.rivas@digito.com.do) • Emily Perez (emily.perez@digito.com.do)	2026/07/03 18:58:42 UTC
SIGNED	**Signed** by Emily Perez (emily.perez@digito.com.do)	2026/07/03 19:06:14 UTC
SIGNED	**Signed** by Gabriella Gómez Tolari (gabriella.gomez@digito.com.do)	2026/07/03 19:52:27 UTC
SIGNED	**Signed** by Irving Rivas (irving.rivas@digito.com.do)	2026/07/03 19:45:04 UTC
COMPLETED	This document has been signed by all signers and is **complete**	2026/07/03 19:52:27 UTC

The email address indicated above for each signer may be associated with a Google account, and may either be the primary email address or secondary email address associated with that account.