DIRECCIÓN DE GESTIÓN POR RESULTADOS

DIGER
DIRECCIÓN DE GESTIÓN POR RESULTADOS

DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN (DPC) DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE FIRMA ELECTRÓNICA

CÓDIGO	**DPC-PKI-FE-001-2025**
VERSIÓN	**1.0**
FECHA DE APROBACIÓN	**AGOSTO 2025**
APROBADO POR:	**MINISTRO ING. MARCIO SIERRA**

1. CONTROL DOCUMENTAL

ACTIVIDAD	NOMBRE	FIRMA
Elaborado por:	César Maldonado Especialista en Infraestructura	
	Raúl Aguilar Especialista en Ciberseguridad	
Responsable de Revisión Técnica	Henry Ortez Desarrollador de Sistemas	
	Dennis Vásquez Jefe de Área de Infraestructura	
Revisión	Omar Palacios Coordinador de AGEHRED	
	Ángel Orlando Paz Coordinador de Sistemas de Gobierno Digital	

2. MATRIZ CONTROL DE CAMBIOS

VERSIÓN	FECHA	TIPO DE CAMBIO	MODIFICADO POR:	DESCRIPCIÓN DEL CAMBIO
1.0.	27/8/2025	☒ NUEVA ☐ REVISIÓN ☐ MODIFICACIÓN		

CONTENIDO

1. INTRODUCCIÓN....4
2. DEFINICIONES....4
3. OBJETIVO....4
4. ALCANCE....5
5. REFERENCIAS NORMATIVAS....5
6. DESARROLLO....5
7. PUBLICACIÓN DE INFORMACIÓN Y DEPÓSITO DE CERTIFICADOS....20
8. IDENTIFICACIÓN Y AUTENTICACIÓN....21
9. REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS....35
10. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES....51
11. CONTROLES DE SEGURIDAD TÉCNICA....64
12. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS....74
13. AUDITORÍA DE CONFORMIDAD....75
14. REQUISITOS COMERCIALES Y LEGALES....76

1. INTRODUCCIÓN

La presente Declaración de Prácticas de Certificación (DPC) tiene como objetivo establecer las políticas, lineamientos y procedimientos que regulan el funcionamiento de la Infraestructura de Clave Pública (PKI) bajo la responsabilidad de la Dirección General de Gestión por Resultados (La DIGER), en su calidad de Prestador de Servicios de Certificación (PSC) del Estado de Honduras. Este documento es esencial para garantizar la transparencia, confianza y seguridad en la emisión, gestión, uso y revocación de certificados digitales.

2. DEFINICIONES

Firma Electrónica Cualificada (FEC): Firma electrónica avanzada basada en un certificado cualificado y generada mediante un dispositivo cualificado de creación de firma.

PDS (Política de Descripción del Servicio): Documento que describe los detalles del servicio de certificación, conforme a lo establecido en ETSI EN 319 411-1.

PKI (Infraestructura de Clave Pública): Conjunto de tecnologías, políticas y procedimientos para la creación, gestión, distribución, uso, almacenamiento y revocación de certificados digitales.

CA (Autoridad de Certificación): Entidad que emite y gestiona certificados digitales bajo los lineamientos establecidos.

RA (Autoridad de Registro): Entidad responsable de validar la identidad de los suscriptores antes de la emisión de certificados.

Suscriptor: Persona natural o jurídica que es titular de un certificado digital emitido por la DIGER.

3. OBJETIVO

Establecer los criterios, responsabilidades, condiciones técnicas y requisitos de seguridad aplicables a la emisión, gestión, uso y revocación de certificados electrónicos cualificados de firma electrónica, emitidos por La DIGER, garantizando la interoperabilidad, integridad, autenticidad y no repudio de las transacciones electrónicas realizadas bajo su marco de confianza.

4. ALCANCE

Esta declaración aplica a todos los actores involucrados en la emisión, gestión y uso de los certificados cualificados de firma electrónica emitidos por La DIGER, incluyendo a:

- Autoridades de Certificación (CA)
- Autoridades de Registro (RA)
- Personal autorizado de LA DIGER
- Suscriptores de certificados
- Terceros que interactúan con los servicios de certificación

5. REFERENCIAS NORMATIVAS

El presente documento se basa en el cumplimiento de las siguientes normas, leyes y estándares aplicables a los servicios de certificación y firma electrónica:

- Ley sobre Firmas Electrónicas vigente en la República de Honduras.
- Reglamento de la Ley sobre Firmas Electrónicas, emitido por la autoridad competente.
- Normas Técnicas ETSI aplicables a Prestadores Cualificados de Servicios de Confianza, en especial:
  - ETSI EN 319 401: Marco General para los Prestadores de Servicios de Confianza.
  - ETSI EN 319 411-1: Requisitos para los Prestadores de Servicios de Certificación que emiten certificados.
  - ETSI EN 319 412 (partes 1 a 5): Perfil de los certificados electrónicos.
- Política de Certificación (CP) y la Declaración de Prácticas de Certificación (CPS) de La DIGER.
- Otras directrices y políticas internas de seguridad de la información adoptadas por La DIGER.

6. DESARROLLO

Este documento declara las prácticas de certificación de firma electrónica de la Dirección de Gestión por Resultados, en adelante “La DIGER”.

6.1 LOS CERTIFICADOS QUE SE EMITEN SON:

6.11 DE PERSONA NATURAL

- Certificado de Persona Natural en software
- Certificado de Persona Natural en HSM centralizado
- Certificado de Persona Natural Operador de Registro en Token

- Certificado de Persona Natural Operador de Registro en HSM Centralizado
- Certificado de Persona Natural Perteneciente en Software
- Certificado de Persona Natural Perteneciente en HSM centralizado
- Certificado de Persona Natural Colegiado en Software
- Certificado de Persona Natural Colegiado en HSM centralizado

6.12 DE REPRESENTANTE DE PERSONA JURÍDICA ANTE LAS ADMINISTRACIONES PÚBLICAS:

- De firma de persona Natural Representante de Persona Jurídica ante las administraciones en Software.
- De firma de persona Natural Representante de Persona Jurídica ante las administraciones en HSM centralizado.
- De persona Natural Representante de Persona Jurídica ante las administraciones en Software.
- De persona Natural Representante de Persona Jurídica ante las administraciones en HSM centralizado.

6.13 DE SELLO DE EMPRESA

- Certificado cualificado de Sello Electrónico en software.
- Certificado cualificado de Sello Electrónico en HSM centralizado.

6.14 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

El presente documento establece la Declaración de Practicas de Certificación dedicada a la expedición de certificados electrónicos de Dirección de Gestión Por Resultados, en adelante LA DIGER.

6.2 IDENTIFICADORES DE CERTIFICADOS

LA DIGER ha asignado a cada política de certificado un identificador de objeto (IDO), para su identificación por las aplicaciones.

Número IDO	Tipo de certificados
	Persona Natural
1.3.6.1.4.1.63071.1.1.1	Certificado de Persona Natural ciudadano en Software
1.3.6.1.4.1.63071.1.1.2	Certificado de Persona Natural ciudadano en HSM centralizado
1.3.6.1.4.1.63071.1.1.3	Certificado de Persona Natural Operador de Registro en Token
1.3.6.1.4.1.63071.1.1.4	Certificado de Persona Natural Operador de Registro en HSM Centralizado
	Persona Natural Perteneciente
1.3.6.1.4.1.63071.1.2.1	Certificado de Persona Natural Perteneciente en Software
1.3.6.1.4.1.63071.1.2.2	Certificado de Persona Natural Perteneciente en HSM centralizado

	Persona Física Colegiado
1.3.6.1.4.1.63071.1.3.1	Certificado de Persona Natural Colegiado en Software
1.3.6.1.4.1.63071.1.3.2	Certificado de Persona Natural Colegiado en HSM centralizado
	Persona Física Representante
1.3.6.1.4.1.63071.1.4.1	De firma de persona Natural Representante de Persona Jurídica ante las administraciones en Software
1.3.6.1.4.1.63071.1.4.2	De firma de persona Natural Representante de Persona Jurídica ante las administraciones en HSM centralizado
1.3.6.1.4.1.63071.1.5.1	De persona Natural Representante de Persona Jurídica ante las administraciones en Software
1.3.6.1.4.1.63071.1.5.2	De persona Natural Representante de Persona Jurídica ante las administraciones en HSM centralizado
1.3.6.1.4.1.63071.1.6.1	De Sello Electrónico en Software
1.3.6.1.4.1.63071.1.6.2	De Sello Electrónico en HSM centralizado

En caso de contradicción entre esta Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas.

6.3 PARTICIPANTES EN LOS SERVICIOS DE CERTIFICACIÓN

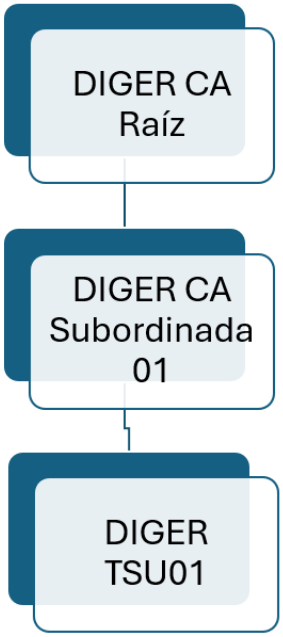
6.3.1 PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

El prestador de servicios electrónicos de certificación es la persona, física o jurídica, que expide y gestiona certificados para entidades finales, empleando una autoridad de certificación, o presta otros servicios relacionados con la firma electrónica.

La DIGER es un prestador de servicios de certificación, que actúa de acuerdo con lo dispuesto en el Decreto No. 149-2013 sobre la Ley Sobre Firmas Electrónicas, así como Acuerdo Ejecutivo Número 41-2014 Reglamento de la Ley sobre Firmas Electrónicas.

Asimismo, cumple con los requisitos exigidos por el Sistema de Gestión de la Seguridad de la Información implementado por La DIGER.

Para la prestación de los servicios de certificación, La DIGER ha establecido una jerarquía de entidades de certificación:



6.3.2 LA DIGER CA RAÍZ

Se trata de la Autoridad de Certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave público ha sido auto firmado.

Datos de identificación:

CN:	LA DIGER CA Raíz
Huella digital:	905c466f5aa0fc5fa4b8d24bdea815a0f07fa8b7
Válido desde:	lunes, 9 de junio de 2025
Válido hasta:	viernes, 10 de junio de 2050
Longitud de clave RSA:	4.096 bits

6.3.3 LA DIGER CA Subordinada 01

Se trata de la Autoridad de certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por La DIGER CA Raíz.

Datos de identificación:

CN:	LA DIGER CA Subordinada 01
Huella digital:	dc439f2f302ba564a9c9fbb32929cc2cfbf923a8
Válido desde:	lunes, 9 de junio de 2025
Válido hasta:	miércoles, 9 de junio de 2038
Longitud de clave RSA:	4.096 bits

6.3.3 LA DIGER TSU01

Datos de identificación:

CN:	LA DIGER TSU01
Huella digital:	[completar]
Válido desde:	[dd/mm/aaaa]
Válido hasta:	[dd/mm/aaaa]

6.4 AUTORIDAD DE REGISTRO

Una Autoridad de Registro de La DIGER es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado.
- Gestionar la generación de claves y la emisión del certificado.
- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

6.4.1 PODRÁN ACTUAR COMO RA DE LA DIGER:

- Cualquier entidad autorizada por la DIGER.
- La DIGER directamente.

La DIGER formalizará contractualmente las relaciones entre ella y cada una de las entidades que actúen como autoridad de registro de la DIGER.

La entidad que actúe como autoridad de registro de la DIGER podrá autorizar a una o varias personas como operador de la RA para operar con el sistema de emisión de certificados de la DIGER en nombre de la autoridad de registro.

La autoridad de registro podrá delegar las funciones de identificación de los suscriptores y/o firmantes, previo acuerdo de colaboración en el que se acepte la delegación de estas funciones. La DIGER deberá autorizar de manera expresa dicho acuerdo de colaboración.

Podrán actuar como autoridades de registro las entidades expresamente designadas por La DIGER mediante contrato y habilitación formal. No se permite la designación unilateral por parte de los suscriptores.

6.5 ENTIDADES FINALES

Las entidades finales son las personas u organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de autenticación y firma electrónica.

Serán entidades finales de los servicios de certificación de la DIGER las siguientes:

1. Suscriptores del servicio de certificación.
2. Firmantes.
3. Partes usuarias.

6.5.1 SUSCRIPTORES DEL SERVICIO DE CERTIFICACIÓN

Los suscriptores del servicio de certificación son:

- Las instituciones, empresas u organizaciones que los adquieren a la DIGER (directamente o a través de un tercero) para su uso en su ámbito propio y se encuentran identificados en los certificados.
- Las personas naturales que adquieren los certificados para sí mismas, y se encuentran identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio electrónico de certificación es, por tanto, el cliente del prestador de servicios de certificación, de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en las normas técnicas europeas aplicables a la expedición de certificados electrónicos cualificados.

6.5.2 FIRMANTES

Los firmantes son las personas naturales que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma electrónica, siendo típicamente los empleados, representantes legales o voluntarios, así como otras personas vinculadas a los suscriptores; incluyendo las personas al servicio de las administraciones públicas, en los certificados de empleado público.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación inequívoco, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por el prestador de servicios electrónicos de certificación, por lo que las personas naturales identificadas en los correspondientes certificados son las únicas responsables de su protección y deberían considerar las implicaciones de perder una clave privada.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la autenticación, también se emplea el término más genérico de "persona natural identificada en el certificado", siempre con pleno respeto al cumplimiento de la regulación de firma electrónica en relación con los derechos y obligaciones del firmante.

6.5.3 PARTES USUARIAS

Las partes usuarias son las personas y las organizaciones que reciben firmas electrónicas y certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en la página web de la entidad de certificación.

6.6 USO DE LOS CERTIFICADOS

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

6.7 USOS PERMITIDOS PARA LOS CERTIFICADOS

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, disponibles en el sitio: https://www.diger.gob.hn

Certificado de Persona Natural ciudadano en Software

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.1.1. Es un certificado que se emite para la firma electrónica y autenticación, de acuerdo con la política de certificación NCP con el OID 0.4.0.2042.1.1.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

- Autenticación en sistemas de control de acceso.
- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Firma digital (Digital Signature, para realizar la función de autenticación)
ii. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
iii. Key Encipherment

6.7.1 CERTIFICADO DE PERSONA NATURAL CIUDADANO EN HSM CENTRALIZADO

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.1.2. Es un certificado que se emite para la firma electrónica y autenticación, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.
Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

- Autenticación en sistemas de control de acceso.
- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Firma digital (Digital Signature, para realizar la función de autenticación)
ii. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
iii. Key Encipherment

6.7.2 CERTIFICADO DE PERSONA NATURAL OPERADOR DE REGISTRO EN TOKEN

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.1.3 Es un certificado que se emite para firma electrónica y autenticación, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.
Adicionalmente, este certificado que se emite en token permite la autenticación en la plataforma de la Autoridad de Registro de La DIGER, para que los operadores de registro puedan llevar a cabo las actividades de gestión de la plataforma, así como el proceso de validación de la identidad y de emisión de cualesquiera perfiles de certificados.

- Autenticación en sistemas de control de acceso.
- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Firma digital (Digital Signature, para realizar la función de autenticación)
ii. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
iii. Key Encipherment

6.7.3 CERTIFICADO DE PERSONA NATURAL OPERADOR DE REGISTRO EN HSM CENTRALIZADO

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.1.4 Es un certificado que se emite para firma electrónica y autenticación, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.

Adicionalmente, este certificado que se emite en HSM Centralizado permite la autenticación en la plataforma de la Autoridad de Registro de LA DIGER, para que los operadores de registro puedan llevar a cabo las actividades de gestión de la plataforma, así como el proceso de validación de la identidad y de emisión de cualesquiera perfiles de certificados.

- Autenticación en sistemas de control de acceso.
- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:
El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Firma digital (Digital Signature, para realizar la función de autenticación)
ii. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
iii. Key Encipherment

6.7.4 CERTIFICADO DE PERSONA NATURAL PERTENECIENTE EN SOFTWARE

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.2.1. Es un certificado que se emite para la firma electrónica y autenticación, de acuerdo con la política de certificación NCP con el OID 0.4.0.2042.1.1.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

- Autenticación en sistemas de control de acceso.
- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Firma digital (Digital Signature, para realizar la función de autenticación)
ii. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
iii. Key Encipherment

6.7.5 CERTIFICADO DE PERSONA NATURAL PERTENECIENTE EN HSM CENTRALIZADO

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.2.2. Es un certificado que se emite para la firma electrónica y autenticación, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

- Autenticación en sistemas de control de acceso.
- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Firma digital (Digital Signature, para realizar la función de autenticación)
ii. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
iii. Key Encipherment

6.7.6 CERTIFICADO DE PERSONA NATURAL COLEGIADO EN SOFTWARE

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.3.1. Es un certificado que se emite para la firma electrónica y autenticación, de acuerdo con la política de certificación NCP con el OID 0.4.0.2042.1.1.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

- Autenticación en sistemas de control de acceso.

- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Firma digital (Digital Signature, para realizar la función de autenticación)
ii. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
iii. Key Encipherment

6.7.7 CERTIFICADO DE PERSONA NATURAL COLEGIADO EN HSM CENTRALIZADO

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.3.2. Es un certificado que se emite para la firma electrónica y autenticación, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

- Autenticación en sistemas de control de acceso.
- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Firma digital (Digital Signature, para realizar la función de autenticación)
ii. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
iii. Key Encipherment

6.7.8 CERTIFICADO DE FIRMA DE PERSONA NATURAL, REPRESENTANTE DE PERSONA JURÍDICA ANTE LAS ADMINISTRACIONES EN SOFTWARE

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.4.1. Es un certificado que se emite para firma electrónica, de acuerdo con la política de certificación NCP con el OID 0.4.0.2042.1.1.

Este certificado de representante emitido en software garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y

una entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la firma electrónica, es decir, la firma electrónica que se basa en un certificado y que ha sido generada para la firma por parte del representante.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

6.7.9 CERTIFICADO DE FIRMA DE PERSONA NATURAL, REPRESENTANTE DE PERSONA JURÍDICA ANTE LAS ADMINISTRACIONES EN HSM CENTRALIZADO

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.4.2. Es un certificado que se emite para firma electrónica, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.

Este certificado de representante emitido en HSM Centralizado, garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la firma electrónica, es decir, la firma electrónica que se basa en un certificado y que ha sido generada para la firma por parte del representante.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

6.7.10 CERTIFICADO DE PERSONA NATURAL REPRESENTANTE DE PERSONA JURÍDICA ANTE LAS ADMINISTRACIONES EN SOFTWARE

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.5.1. Es un certificado que se emite para firma electrónica y autenticación, de acuerdo con la política de certificación NCP con el OID 0.4.0.2042.1.1.

Este certificado de representante emitido en software garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la firma electrónica, es decir, la firma electrónica que se basa en un certificado y que ha sido generada para la firma por parte del representante.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

6.7.11 CERTIFICADO DE PERSONA NATURAL REPRESENTANTE DE PERSONA JURÍDICA ANTE LAS ADMINISTRACIONES EN HSM CENTRALIZADO

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.5.2. Es un certificado que se emite para firma electrónica y autenticación, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.

Este certificado de representante emitido en HSM Centralizado, garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la firma electrónica, es decir, la firma electrónica que se basa en un certificado y que ha sido generada para la firma por parte del representante.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- Firma de correo electrónico seguro.
- Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

i. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

6.7.12 CERTIFICADO DE SELLO ELECTRÓNICO EN SOFTWARE

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.6.1. Es un certificado que se emite de acuerdo con la política de certificación NCP con el OID 0.4.0.2042.1.1.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

6.7.13 CERTIFICADO DE SELLO ELECTRÓNICO EN HSM CENTRALIZADO

Este certificado dispone del OID 1.3.6.1.4.1.63071.1.6.2, Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment.

6.8 LÍMITES Y PROHIBICIONES DE USO DE LOS CERTIFICADOS

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la regulación aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, disponibles en la web de La DIGER.

El empleo de los certificados digitales en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos con las entidades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a La DIGER, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

LA DIGER no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de La DIGER emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

6.9 ADMINISTRACIÓN DE LA POLÍTICA

6.9.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Dirección de Gestión Por Resultados, DIGER.

6.9.2 DATOS DE CONTACTO DE LA ORGANIZACIÓN

Dirección de Gestión Por Resultados, DIGER: Boulevard Fuerzas Armadas, contiguo al Banco Central de Honduras, consultas@diger.gob.hn Teléfono +504-2240-1400

6.9.3 PROCEDIMIENTOS DE GESTIÓN DEL DOCUMENTO

El sistema documental y de organización de La DIGER garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

7. PUBLICACIÓN DE INFORMACIÓN Y DEPÓSITO DE CERTIFICADOS

6.1 DEPÓSITO(S) DE CERTIFICADOS

La DIGER dispone de un depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de La DIGER, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 0 de esta Declaración de Prácticas de Certificación.

7.2 PUBLICACIÓN DE INFORMACIÓN DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

LA DIGER publica las siguientes informaciones, en su depósito:

- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados aplicables.
- La declaración de prácticas de certificación.
- Los textos de divulgación (Policy Disclosure Statements - PDS), como mínimo en español e inglés.

7.3 FRECUENCIA DE PUBLICACIÓN

La información del prestador de servicios de certificación, incluyendo las políticas y la declaración de prácticas de certificación, se publica en cuanto se encuentra disponible.

Los cambios en la declaración de prácticas de certificación se rigen por lo establecido en la sección 0 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en esta declaración de prácticas de certificación.

7.4 CONTROL DE ACCESO

La DIGER no limita el acceso de lectura a las informaciones establecidas en la sección 7.2, pero establece controles para impedir que personas no autorizadas puedan añadir,

modificar o borrar registros del depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

LA DIGER emplea sistemas fiables para el depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

8. IDENTIFICACIÓN Y AUTENTICACIÓN

8.1 REGISTRO INICIAL

Tipos de nombres

Todos los certificados contienen un nombre distintivo (DN o *distinguished name*) conforme al estándar X.509 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la Persona Natural identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

8.1.2 CERTIFICADO DE PERSONA NATURAL CIUDADANO EN SOFTWARE

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.3 CERTIFICADO DE PERSONA NATURAL CIUDADANO EN HSM CENTRALIZADO

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.4 CERTIFICADO DE PERSONA NATURAL OPERADOR DE REGISTRO EN TOKEN

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.5 CERTIFICADO DE PERSONA NATURAL OPERADOR DE REGISTRO EN HSM CENTRALIZADO

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante

Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.6 CERTIFICADO DE PERSONA NATURAL PERTENECIENTE EN SOFTWARE

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.7 CERTIFICADO DE PERSONA NATURAL PERTENECIENTE EN HSM CENTRALIZADO

Country (C)	Estado[1]
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante

1 El campo “Estado” corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que está vinculado (por ser empleado, miembro, socio u otra vinculación), con independencia de la nacionalidad del trabajador.

Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.8 CERTIFICADO DE PERSONA NATURAL COLEGIADO EN SOFTWARE

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.9 CERTIFICADO DE PERSONA NATURAL COLEGIADO EN HSM CENTRALIZADO

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.10 CERTIFICADO DE FIRMA DE PERSONA NATURAL, REPRESENTANTE DE PERSONA JURÍDICA ANTE LAS ADMINISTRACIONES EN SOFTWARE

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.11 CERTIFICADO DE FIRMA DE PERSONA NATURAL, REPRESENTANTE DE PERSONA JURÍDICA ANTE LAS ADMINISTRACIONES EN HSM CENTRALIZADO

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.12 CERTIFICADO DE PERSONA NATURAL REPRESENTANTE DE PERSONA JURÍDICA ANTE LAS ADMINISTRACIONES EN SOFTWARE

Country (C)	Estado o departamento donde la organización está registrada.
Organization (O)	Organización a la que está vinculado el firmante

Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.13 CERTIFICADO DE PERSONA NATURAL REPRESENTANTE DE PERSONA JURÍDICA ANTE LAS ADMINISTRACIONES EN HSM CENTRALIZADO

Country (C)	Estado[2]
Organization (O)	Organización a la que está vinculado el firmante
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Identificación de la Organización a la que está vinculado el firmante
Title	Título o especialidad de firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Documento de Identidad, Cédula, u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

8.1.14 CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO EN SOFTWARE

Country (C)	Estado donde la entidad está registrada la Organización
Organization (O)	Nombre de la Organización
Organization Unit (OU)	Indica la naturaleza del certificado

2 El campo “Estado” corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que está vinculado (por ser empleado, miembro, socio u otra vinculación), con independencia de la nacionalidad del trabajador.

Organization Identifier	Número de identificación fiscal de la Organización a la que está vinculado el sello electrónico
Surname	Apellidos del responsable del certificado
Given Name	Nombre del responsable del certificado
Serial Number	Número de identificación fiscal de la Organización a la que está vinculado el sello electrónico
Common Name (CN)	Nombre del sistema automático

8.1.15 CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO EN HSM CENTRALIZADO

Country (C)	Estado donde la entidad está registrada la Organización
Organization (O)	Nombre de la Organización
Organization Unit (OU)	Indica la naturaleza del certificado
Organization Identifier	NIF o Número de identificación fiscal de la organización a la que está vinculado el sello electrónico
Surname	Apellidos del responsable del certificado
Given Name	Nombre del responsable del certificado
Serial Number	Número de identificación fiscal de la organización a la que está vinculado el sello electrónico
Common Name (CN)	Nombre del sistema automático

Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

Emisión de certificados del set de pruebas y certificados de pruebas en general

En el caso que los datos indicados en el DN o Subject fueran ficticios (ej. “Test Organization”, “Test Nombre”, “Apellido1”) o se indique expresamente palabras que denoten su invalidez (ej. “TEST”, “PRUEBA” o “INVALIDO”), se considerará al certificado sin validez legal y por lo tanto sin responsabilidad alguna sobre LA DIGER. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y permitir al ente regulador su evaluación.

8.1.16 EMPLEO DE ANÓNIMOS Y SEUDÓNIMOS

En ningún caso se pueden utilizar seudónimos para identificar una entidad, empresa u organización, ni a un firmante. Así mismo, en ningún caso se emiten certificados anónimos.

8.1.16.1 INTERPRETACIÓN DE FORMATOS DE NOMBRES

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo "país" o "estado" será el del suscriptor del certificado.

Los certificados cuyos suscriptores sean personas jurídicas, entidades u organismos de la administración pública, muestran la relación entre estas y una Persona Natural, con independencia de la nacionalidad de la Persona Natural.

En el campo "número de serie" se incluye el Documento de identidad, Cédula u otro número de identificación idóneo del firmante, reconocido en derecho.

8.1.16.2 UNICIDAD DE LOS NOMBRES

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de La DIGER.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del número del Número de Identificación Fiscal, o equivalente, en el esquema de nombres.

Un suscriptor puede solicitar múltiples certificados siempre que la combinación de valores (identificador legal, OID de política, soporte del certificado) sea única:

- Cédula de Identidad u otro identificador legalmente válido de la Persona Natural.
- Número de Identificación Fiscal u otro identificador legalmente válido del suscriptor.
- Tipo de certificado (OID de identificador de política de certificación).
- Soporte del certificado (software, HSM centralizado o Token)

Como excepción esta DPC permite emitir un certificado cuando coincida Cédula del suscriptor, Identificación del firmante, Tipo de certificado, Soporte del certificado, con un certificado activo, siempre que exista algún elemento diferenciador entre ambos, en los campos cargo (title) y/o departamento (Organizational Unit)

8.1.16.3 RESOLUCIÓN DE CONFLICTOS RELATIVOS A NOMBRES

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

La DIGER no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, al que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte en el documento contractual que formaliza el servicio.

8.2 VALIDACIÓN INICIAL DE LA IDENTIDAD

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre La DIGER y el suscriptor, momento en el que queda verificada la existencia del suscriptor mediante su documento oficial de identidad o las escrituras correspondientes, al igual que los poderes de actuación de la persona que presente como representante si fuese el caso. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

En el caso de personas naturales identificadas en certificados cuyo suscriptor sea una persona jurídica, sus identidades se validarán mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a La DIGER, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

8.2.2 PRUEBA DE POSESIÓN DE CLAVE PRIVADA

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor, en certificados de sello, o por el firmante, en certificados de firma.

8.2.3 VALIDACIÓN DE LA IDENTIDAD

Para lo solicitud de certificados, los operadores de registro de La DIGER verificarán la identidad del firmante a la que se le expide el certificado (véase la persona natural o

representante autorizado de la persona jurídica), así como cualquier atributo especifico de la persona natural o jurídica con la que tenga relación o vinculación.

Para la verificación se procederá directamente o bien por medio de un tercero de conformidad con el derecho nacional, de acuerdo con los siguientes métodos:

- En presencia de la persona natural o de un representante autorizado de la persona jurídica. Se podrá prescindir de la personación cuando la solicitud de expedición de un certificado haya sido legitimada en presencia notarial.
- Mediante el uso de los datos contenidos en una cartera digital de identidad y/o atributos verificados mediante dicha cartera, que permita acreditar, tanto la identidad como los atributos de la persona a identificar.

8.2.4 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN, EMPRESA O ENTIDAD MEDIANTE REPRESENTANTE

Las Personas Naturales con capacidad de actuar en nombre de las personas jurídicas o entidades sin personalidad jurídica, públicas o privadas, que sean suscriptoras de certificados, podrán actuar como representantes de estas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la Persona Natural y la organización de la que se trate, que exige su reconocimiento por La DIGER, la cual se realizará mediante el siguiente procedimiento:

1. El representante del suscriptor deberá acreditar su identidad por uno de los métodos de identificación especificados en el apartado 8.2. de tal manera que:
    - Si se identifica presencialmente ante un operador o persona autorizada de una Autoridad de Registro de La DIGER:
        - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
        - Acreditando el carácter y facultades que alegue poseer.
    - Si se identifica electrónicamente a través del sistema de cartera digital y/o wallet usado por LA DIGER.
        - Proporcionando su información mediante el sistema de compartir credenciales proporcionado por el propio sistema de cartera digital usada por La DIGER.
        - Acreditando el carácter y facultades que alegue poseer.

2. El representante proporcionará la siguiente información y sus correspondientes soportes acreditativos:
    - Sus datos de identificación, como representante:
        - Nombre y apellidos
        - Lugar y fecha de nacimiento

- Documento: Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.

- Los datos de identificación del suscriptor al que representa:
  - Denominación o razón social.
  - Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.
  - Documento: Documento acreditativo de la identificación fiscal de la entidad.
  - Documento: Documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.
- Los datos relativos a la representación o la capacidad de actuación que ostenta:
  - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin si resulta aplicable.
  - El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:
    - TOTAL. Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.
    - PARCIAL. Representación o capacidad parcial. Esta comprobación se podrá realizar mediante copia auténtica electrónica de la escritura notarial de apoderamiento, en los términos de la normativa notarial.

3. El operador o personal autorizado de la Autoridad de Registro de LA DIGER comprobará la identidad del representante actuando del siguiente modo:
   - Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
     - Documento de identidad aportado.
     - Documentación que acredite su representación.
   - Cuando la identificación se haya realizado a través del sistema de cartera digital y/o wallet usado por La DIGER:
     - Verificación de las credenciales proporcionadas por parte del sistema de cartera digital y/o wallet.
     - Revisión del contenido de las credenciales compartidas; si faltasen, se solicitará completar la información.

4. El operador o personal autorizado de la Autoridad de Registro de La DIGER verificará la información suministrada para la autenticación y le devolverá cuando corresponda la documentación original aportada.

5. Alternativamente, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar al operador o personal autorizado de la Autoridad de Registro La DIGER, en cuyo caso los pasos 3 y 4 anteriores no serán precisos.

La prestación del servicio de certificación digital se formaliza mediante el oportuno contrato entre La DIGER y el suscriptor, debidamente representado.

8.2.7 VALIDACIÓN DE LA IDENTIDAD

Para la solicitud de certificados, el operador o personal autorizado de la autoridad de registro La DIGER comprobará la identidad de la persona natural identificada en la solicitud del certificado, actuando del siguiente modo:

- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
  - Documento de identidad aportado
- Cuando la identificación se haya realizado a través del sistema de cartera digital y/o wallet usado por La DIGER:
  - Verificación de las credenciales proporcionadas por parte del sistema de cartera digital y/o wallet.
  - Revisión del contenido de las credenciales compartidas; si faltasen, se solicitará completar la información.

Durante este trámite se confirma rigurosamente la identidad de la persona natural identificada en el certificado. Por este motivo, en todos los casos en que se expide un certificado se acredita ante un operador de registro la identidad de la persona natural firmante ya sea presencialmente o mediante la cartera digital.

La autoridad de registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de los datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

8.2.8 VINCULACIÓN DE LA PERSONA NATURAL

La justificación documental de la vinculación de una persona natural identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización) de cada una de las personas públicas y privadas a las que están vinculadas.

8.2.9 INFORMACIÓN DE SUSCRIPTOR NO VERIFICADA

La DIGER no incluye ninguna información de suscriptor no verificada en los certificados a excepción del correo electrónico del suscriptor o firmante.

8.2.10 AUTENTICACIÓN DE LA IDENTIDAD DE UNA RA Y SUS OPERADORES

Para la constitución de una nueva autoridad de registro, LA DIGER realiza las verificaciones necesarias para confirmar la existencia de la entidad u organización de la que se trate. Para ello, La DIGER podrá utilizar exhibición de documentos o utilizar sus propias fuentes de información.

Igualmente, La DIGER directamente o a través de su autoridad de registro, verifica y valida la identidad de los operadores de las autoridades de registro, para lo cual estas últimas envían a La DIGER la documentación de identificación correspondientes al nuevo operador, juntamente con su autorización para actuar como tal.

En el caso de que el operador desee emitirse un certificado de cualquier otro tipo de perfil de certificado, siempre que cumpla las condiciones para poderse emitir, no podrá actuar como operador de registro para la solicitud de dicho certificado, debiendo ser dicho operador de registro una persona distinta a la solicitante del certificado.

La DIGER se asegura que los operadores de la autoridad de registro reciben la formación suficiente para el desarrollo de sus funciones, lo cual verifica con la evaluación correspondiente. Dicha formación y evaluación puede ser ejecutada por la autoridad de registro previamente autorizada por La DIGER.

Para la prestación de los servicios, La DIGER se asegura de que los operadores de autoridad de registro acceden al sistema mediante autenticación fuerte con certificado digital.

8.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN

8.3.1 VALIDACIÓN PARA LA RENOVACIÓN RUTINARIA DE CERTIFICADOS

Antes de renovar un certificado, el operador o personal autorizado de la autoridad de registro la DIGER comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona natural identificada en el certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son:

- El uso del código "CRE" o "ERC" relativo al certificado anterior, o de otros métodos de autenticación personal, que consiste en información que sólo conoce la persona natural identificada en el certificado, y que le permite renovar de forma automática su certificado, siempre que no se haya superado el plazo máximo legalmente establecido.
- El empleo del certificado vigente para su renovación y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 8.2.

8.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE RENOVACIÓN

Antes de renovar un certificado, el operador o personal autorizado de la autoridad de registro la DIGER comprobará que la información empleada en su día para verificar la identidad y los restantes datos del suscriptor y de la persona natural identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona natural identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 8.2.

8.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

La DIGER o un operador o personal autorizado de la autoridad de registro autentica las peticiones e informes relativos a la revocación, suspensión o reactivación de un certificado, comprobando que provienen de una persona autorizada.

La identificación de los suscriptores y/o firmantes en el proceso de revocación, suspensión o reactivación de certificados podrá ser realizada por:

- El suscriptor y/o firmante:

- Identificándose y autenticándose mediante el uso del Código de Revocación (ERC o ERC) a través de la página web de La DIGER en horario 24x7.
- Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la suspensión o revocación, a juicio de La DIGER y/o Autoridades de Registro.

Las autoridades de registro de La DIGER: deberán identificar al firmante y/o suscriptor ante una petición de revocación, suspensión o reactivación según los propios medios que considere necesarios. Se considerará que se ha identificado correctamente:

- Mediante solicitud enviada por el firmante, firmada con el propio certificado.
- Mediante solicitud firmada por el suscriptor o su representante, acreditando su identidad y facultades.

Cuando en horario de oficina el suscriptor desee iniciar una petición de revocación y existan dudas para su identificación, su certificado pasa a estado de suspensión.

9. REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS

9.1 SOLICITUD DE EMISIÓN DE CERTIFICADO

9.1.2 LEGITIMACIÓN PARA SOLICITAR LA EMISIÓN

El solicitante del certificado sea persona natural o jurídica, debe firmar un contrato de prestación de servicios de certificación con La DIGER.

Asimismo, con anterioridad a la emisión y entrega de un certificado, debe existir una solicitud de certificados ya sea en el mismo contrato, en un documento específico de hoja de solicitud de certificados o ante la autoridad de registro.

Cuando el solicitante es una persona distinta al suscriptor, debe existir una autorización del suscriptor para que el solicitante pueda rHealizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por dicho solicitante en nombre propio en el caso de certificados para Persona Natural, o bien en nombre del suscriptor en el caso de que el suscriptor sea la entidad, empresa u organización de derecho público o privado.

9.2.3 PROCEDIMIENTO DE ALTA Y RESPONSABILIDADES

La DIGER recibe solicitudes de certificados, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se instrumentan mediante un formulario en formato papel o electrónico, de manera individual o por lotes, o mediante la conexión con bases de datos externas, o a través de una capa de *Web Services* cuyo destinatario es La DIGER.

En el caso de certificados cuyo suscriptor sea una entidad, empresa u organización de derecho público o privado que actúe como una Autoridad de Registro de La DIGER, podrá gestionar directamente las solicitudes accediendo a los sistemas informáticos de La DIGER y generar los certificados correspondientes para la propia entidad, empresa u organización o para sus miembros.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la Persona Natural identificada en el certificado, de acuerdo con lo establecido en la sección 8.2. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la Persona Natural identificada en el certificado.

9.3 PROCESAMIENTO DE LA SOLICITUD DE CERTIFICACIÓN

9.3.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Una vez recibida una petición de certificado, LA DIGER se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, La DIGER verifica la información proporcionada, verificando los aspectos descritos en la sección 8.2.

En caso de un certificado cualificado, la documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la extinción del certificado o la finalización del servicio prestado, incluso en caso de pérdida anticipada de vigencia por revocación.

9.3.2 APROBACIÓN O RECHAZO DE LA SOLICITUD

En caso de que los datos se verifiquen correctamente, la DIGER debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Autoridad de Certificación, de las Autoridades de Registro o de los suscriptores, la DIGER denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, la DIGER denegará la solicitud definitivamente.
La DIGER notifica al solicitante la aprobación o denegación de la solicitud.

9.3.3 PLAZO PARA RESOLVER LA SOLICITUD

La DIGER atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

9.4 EMISIÓN DEL CERTIFICADO

9.4.1 ACCIONES DE LA CA DURANTE EL PROCESO DE EMISIÓN

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, La DIGER:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo de las claves por parte del usuario, no pudiendo la propia LA DIGER o sus Autoridades de Registro deducirlas o utilizarlas en ningún modo.

9.4.2 NOTIFICACIÓN DE LA EMISIÓN AL SUSCRIPTOR

La DIGER notifica la emisión del certificado al suscriptor y/o a la persona natural identificada en el certificado y el método de generación/descarga.

9.5 ENTREGA Y ACEPTACIÓN DEL CERTIFICADO

9.5.1 RESPONSABILIDADES DE LA CA

Durante este proceso, el operador o personal autorizado de la autoridad de registro en la DIGER debe realizar las siguientes actuaciones:

- Acreditar definitivamente la identidad de la persona natural identificada en el certificado, de acuerdo con lo establecido en las secciones 8.2.
- Disponer del Contrato de Prestación de Servicios de Certificación (PSC) debidamente firmado por el suscriptor.
- Entregar la hoja de entrega y aceptación del certificado a la persona natural identificada en el certificado con los siguientes contenidos mínimos:
    - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la declaración de prácticas de certificación aplicable, como sus obligaciones, facultades y responsabilidades.
    - Información acerca del certificado.
    - Reconocimiento, por parte del firmante, de recibir el certificado y/o los mecanismos para su generación/descarga y la aceptación de los citados elementos.
    - Régimen de obligaciones del firmante.
    - Responsabilidad del firmante.
    - Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
    - La fecha del acto de entrega y aceptación.

  Toda esta información podrá incluirse en el propio contrato de prestación de servicios de certificación. Dicho lo cual, cuando se produzca la firma del contrato de prestación de servicios de certificación por el suscriptor, se entenderá perfeccionada la entrega y aceptación del certificado y, en su caso, de los medios de generación o descarga asociados.
- Obtener la firma de la persona identificada en el certificado.

Las Autoridades de Registro son las encargadas de realizar estos procesos, debiendo registrar documentalmente los anteriores actos y conserva los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a la DIGER, así como los originales cuando la DIGER precise de acceso a los mismos.

9.5.2 CONDUCTA QUE CONSTITUYE ACEPTACIÓN DEL CERTIFICADO

Cuando se haga entrega de la hoja de aceptación, la aceptación del certificado por la persona natural identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación.

Cuando la generación y entrega del certificado se lleve a cabo a través del procedimiento automatizado definido por La DIGER, la aceptación del certificado por la persona natural identificada en el mismo se produce mediante la firma del contrato de prestación de servicios de certificación utilizando el propio certificado.

9.5.3 PUBLICACIÓN DEL CERTIFICADO

La DIGER publica el certificado en el depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes y siempre que la DIGER disponga de la autorización de la persona natural identificada en el certificado.

9.5.4 NOTIFICACIÓN DE LA EMISIÓN A TERCEROS

La DIGER no realiza ninguna notificación de la emisión a terceras entidades.

9.6 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

9.6.1 USO POR EL FIRMANTE

La DIGER obliga a:

- Facilitar a la DIGER información completa y adecuada, conforme a los requisitos de esta declaración de prácticas de certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados.
- Comunicar a la DIGER, autoridades de registro y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.

La DIGER obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la declaración de prácticas de certificación.
- Que ninguna persona no autorizada ha tenido acceso a las credenciales de activación a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni lista de revocación de certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

9.7 USO POR EL SUBSCRIPTOR

9.7.1 OBLIGACIONES DEL SUSCRIPTOR DEL CERTIFICADO

La DIGER obliga contractualmente al suscriptor a:

- Facilitar a la autoridad de certificación información completa y adecuada, conforme a los requisitos de esta declaración de prácticas de certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Comunicar a la DIGER, autoridades de registro y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
    - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas naturales identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de estas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la DIGER, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de la DIGER.

9.7.2 RESPONSABILIDAD CIVIL DEL SUSCRIPTOR DE CERTIFICADO

La DIGER obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la declaración de prácticas de certificación.
- Que ninguna persona no autorizada ha tenido acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

9.7.3 USO POR EL TERCERO QUE CONFÍA EN CERTIFICADOS

9.7.4 OBLIGACIONES DEL TERCERO QUE CONFÍA EN CERTIFICADOS

LA DIGER informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la DIGER, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la DIGER.

9.7.5 RESPONSABILIDAD CIVIL DEL TERCERO QUE CONFÍA EN CERTIFICADOS

La DIGER informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

9.8 RENOVACIÓN DE CERTIFICADOS

La renovación de los certificados exige la renovación de claves, por lo que debe atenderse a lo establecido en la sección 0.

9.9 RENOVACIÓN DE CLAVES Y CERTIFICADOS

9.9.1 CAUSAS DE RENOVACIÓN DE CLAVES Y CERTIFICADOS

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación.

Se consideran al menos dos posibilidades para la renovación de certificados:

- Proceso de renovación, que se efectuará del mismo modo que la emisión de un nuevo certificado.
- Proceso de renovación online (a través de internet), que se detalla a continuación.

9.9.10 PROCEDIMIENTO DE RENOVACIÓN ONLINE DE CERTIFICADOS

CIRCUNSTANCIAS PARA LA RENOVACIÓN ONLINE

Solamente se podrá proceder a la renovación online del certificado si se cumplen las condiciones siguientes:

- La Autoridad de Registro y/o la DIGER dispone del servicio de renovación online.
- El certificado con el que se firma la renovación esté vigente, es decir, no haya caducado, no esté revocado ni suspendido.

Quién puede solicitar la renovación online de un certificado

Cualquier firmante podrá pedir la renovación online de su certificado si se cumplen las circunstancias descritas en el punto anterior.

El firmante podrá formalizar su solicitud accediendo al servicio de renovación online de certificados en la página web de la DIGER.

Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, la DIGER aprobará la solicitud de renovación del certificado y proceder a su emisión y entrega.

La DIGER notifica al solicitante la aprobación o denegación de la solicitud.

Tramitación de las peticiones de renovación online

La solicitud de una renovación del certificado se realizará de acuerdo con lo siguiente:

- Cuando el certificado digital de un usuario esté próximo a caducar, la DIGER podrá enviar una o más notificaciones distribuidas en el tiempo, invitándole a su renovación.
- El firmante se conectará al servicio de renovación de la página web de la DIGER y procederá a la solicitud de renovación. El operador de registro comprobará que la información empleada para verificar la identidad y los restantes datos del usuario identificado en el certificado continúan siendo válidos. Si cualquier información del usuario identificado en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 8.2.
- El firmante firmará la renovación de su certificado válido.
- Se procederá a la generación del nuevo par de claves y generación e importación del certificado, respetando los siguientes condicionantes:
    - Protege la confidencialidad e integridad de los datos de registro de que dispone.
    - Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
    - Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
    - Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
    - Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
    - Indica la fecha y la hora en que se expidió un certificado.
    - Garantiza el control exclusivo del usuario sobre sus propias claves, no pudiendo la propia la DIGER o sus autoridades de registro deducirlas o utilizarlas.

9.9.11 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO RENOVADO

La DIGER notifica la emisión del certificado al suscriptor y a la persona natural identificada en el certificado.

9.9.12 CONDUCTA QUE CONSTITUYE ACEPTACIÓN DEL CERTIFICADO RENOVADO

El certificado se considerará aceptado al firmar electrónicamente la renovación.

9.9.13 PUBLICACIÓN DEL CERTIFICADO RENOVADO

La DIGER publica el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

9.9.14 NOTIFICACIÓN DE LA EMISIÓN A TERCEROS

La DIGER no realiza notificación alguna de la emisión a terceras entidades.

9.10 MODIFICACIÓN DE CERTIFICADOS

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 0, 0, 0 y 0.

9.11 REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN DE CERTIFICADOS

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible. Sólo los certificados de entidad final podrán ser suspendidos.

La reactivación de un certificado supone su paso de estado suspendido a estado activo.

9.11.1 CAUSAS DE REVOCACIÓN DE CERTIFICADOS

La DIGER revoca un certificado cuando concurre alguna de las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:
   a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
   b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
   c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
   d) Alteración posterior de las circunstancias verificadas para la expedición del certificado, como por ejemplo las relativas al cargo o facultades.

2) Circunstancias que afectan a la seguridad de la clave o del certificado:
   a) Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
   b) Infracción, por la DIGER, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta declaración de prácticas de certificación.
   c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
   d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
   e) El uso irregular del certificado por la persona natural identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.
   f) Utilización de dispositivos cualificados de creación de firma que no cumplen con los estándares de seguridad mínimos y necesarios para garantizar la seguridad del certificado o sus claves privadas.

3) Circunstancias que afectan al suscriptor o a la Persona Natural identificada en el certificado:
   a) Finalización de la relación jurídica de prestación de servicios entre la DIGER y el suscriptor.
   b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona natural identificada en el certificado.
   c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.
   d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente, así como la presente declaración de prácticas de certificación.
   e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.
   f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.
   g) Solicitud formulada por el suscriptor y/o firmante del certificado, la persona natural o jurídica representada por este o un tercero autorizado, requiriendo la revocación del certificado.
   h) Terminación de la representación en los certificados electrónicos con atributo de representante. Corresponde tanto al suscriptor como al firmante, solicitar la revocación del certificado cuando exista una modificación o extinción de la relación de representación.

4) Otras circunstancias:
   a) La terminación del servicio de certificación de la autoridad de certificación de la DIGER, salvo que de acuerdo con su plan de cese se opte por transferir la gestión de los certificados a otro Prestador de Servicios de Certificación.
   b) El incumplimiento de la política de certificación sobre la que ha sido expedido el certificado.
   c) Resolución judicial o administrativa que lo ordene.
   d) El uso del certificado que sea dañino y continuado para la DIGER. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
      - La naturaleza y el número de quejas recibidas.
      - La identidad de las entidades que presentan las quejas.
      - La legislación relevante vigente en cada momento.
      - La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

9.11.2 CAUSAS DE SUSPENSIÓN DE UN CERTIFICADO

Los certificados de la DIGER pueden ser suspendidos a partir de las siguientes causas:

- Cuando así sea solicitado por el suscriptor o la persona natural identificada en el certificado.
- Resolución judicial o administrativa que ordene la suspensión.
- Cuando el HSM, no cumpla con los estándares de seguridad mínimos y necesarios para garantizar la seguridad del certificado o sus claves privadas.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al suscriptor o la Persona Natural identificada en el certificado.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, la DIGER tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

9.12.3 CAUSAS DE REACTIVACIÓN DE UN CERTIFICADO

Los certificados de La DIGER pueden ser reactivados a partir de las siguientes causas:

- Cuando el certificado se encuentre en un estado de suspendido.
- Cuando así sea solicitado por el suscriptor o la persona natural identificada en el certificado.

9.12. 4 QUIÉN PUEDE SOLICITAR LA REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

Pueden solicitar la revocación, suspensión o reactivación de un certificado:

- La persona identificada en el certificado, véase el firmante.
- El suscriptor del certificado por medio su representante legal o voluntario o tercero autorizado.

- Autoridad judicial o administrativa mediante la resolución correspondiente.

9.12.5 PROCEDIMIENTOS DE SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

La entidad que precise revocación, suspensión o reactivación un certificado puede solicitarlo a través de las siguientes vías:

- Directamente contactando a la DIGER. Los usuarios pueden enviar una petición por correo electrónico o por teléfono, o bien, dirigir un escrito a la dirección social de la DIGER, según la información proporcionada en el epígrafe 1.5. del presente documento.
- A través de la autoridad de registro del suscriptor;
- De forma autónoma mediante el servicio en línea disponible

La solicitud de revocación, suspensión o reactivación deberá incorporar la siguiente información:

- Fecha de solicitud de la revocación, suspensión o reactivación.
- Identidad del suscriptor.
- Nombre y título de la persona que pide la revocación, suspensión o reactivación.
- Información de contacto de la persona que pide la revocación, suspensión o reactivación.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, por la DIGER, de acuerdo con los requisitos establecidos en la sección 0 de esta política, antes de proceder a la revocación, suspensión o reactivación.

El servicio de revocación, suspensión o reactivación se encuentra en la página web de la DIGER en la dirección: https://www.diger.gob.hn/

En caso de que el destinatario de una solicitud de revocación, suspensión o reactivación por parte de una persona natural identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a la DIGER.

La solicitud de revocación, suspensión o reactivación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la persona natural identificada en el certificado, acerca del cambio de estado del certificado.

Tanto el servicio de gestión de revocación, suspensión o reactivación como el servicio de consulta son considerados servicios críticos y así constan en el plan de contingencias y el plan de continuidad de negocio de la DIGER.

Los sistemas vinculados a la gestión del ciclo de vida del certificado, así como a la autoridad de validación se sincronizan con una fuente de tiempo bajo UTC, al menos una vez al día.

9.12.6 PLAZO TEMPORAL DE SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

Las solicitudes de revocación, suspensión o reactivación se remitirán de forma inmediata en cuanto se tenga conocimiento.

9.12.7 PLAZO TEMPORAL DE PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

Las solicitudes de revocación, suspensión o reactivación realizadas a través del servicio online se tramitarán de manera inmediata.

Si se realiza a través de un operador de registro, se ejecutará dentro del horario ordinario de operación de la DIGER o en su caso de la autoridad de registro. En cualquier caso, las peticiones se tramitarán en un plazo no superior a 24 horas desde la recepción de esta.

En el caso de que, debido a una incidencia técnica u operativa, no se pudiere cumplir con el plazo de 24 horas, la DIGER registrará la solicitud en su sistema de tickes, asignando un número de caso único, registrando la fecha y hora de recepción de la misma, y designando un responsable para su seguimiento.
De igual forma, se indicarán los motivos específicos del retraso, así como las acciones concretas que se llevarán a cabo para asegurar la resolución de la solicitud en el menor tiempo posible.
La DIGER se pondrá en contacto con el usuario de forma inmediata notificándole:

- Que su solicitud ha sido registrada.
- Información sobre el motivo del retraso.
- Estimación del tiempo para la finalización del proceso

Asimismo, la DIGER mantendrá al usuario informado del progreso de su solicitud mediante actualizaciones periódicas hasta su resolución. El solicitante podrá ponerse en contacto con la DIGER a través de los datos de contacto especificados en el epígrafe 1.5.2. del presente documento.
Una vez procesada la solicitud, la DIGER notificará al usuario, confirmando el resultado de la revocación, suspensión o reactivación.
Finalmente, la DIGER procederá a cerrar el ticket abierto relacionado con la incidencia.

9.12.8 OBLIGACIÓN DE CONSULTA DE INFORMACIÓN DE REVOCACIÓN O SUSPENSIÓN DE CERTIFICADOS

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la lista de revocación de certificados más reciente emitida por la autoridad de certificación de la DIGER.

Las listas de revocación de certificados se publican en el depósito de la autoridad de certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

La DIGER CA ROOT

- http://crl1.diger.gob.hn/tsp/crl/arl_diger.crl
- http://crl2.diger.gob.hn/tsp/crl/arl_diger.crl

La DIGER CA Subordinada 01

- http://crl1.La DIGER.gob.hn/tsp/crl/digerCA1.crl
- http://crl2.La DIGER.gob.hn/tsp/crl/digerCA1.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- http://ocsp1.diger.gob.hn/tsp/ocsp/
- http://ocsp2.diger.gob.hn/tsp/ocsp/

9.12.9 FRECUENCIA DE EMISIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS (LRCS)

La DIGER emite una LRC al menos cada 24 horas.

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

9.12.10 PLAZO MÁXIMO DE PUBLICACIÓN DE LRCS

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

9.12.11 DISPONIBILIDAD DE SERVICIOS DE COMPROBACIÓN EN LÍNEA DE ESTADO DE CERTIFICADOS

De forma alternativa, los terceros que confían en certificados podrán consultar el depósito de certificados de la DIGER, que se encuentra disponible las 24 horas de los 7 días de la semana en el web de la DIGER.

Para comprobar la última CRL emitida en cada CA se debe descargar:

LA DIGER CA ROOT

- http://crl1.diger.gob.hn/tsp/crl/arl_diger.crl
- http://crl2.diger.gob.hn/tsp/crl/arl_La DIGER.crl

LA DIGER CA Subordinada 01

- http://crl1.diger.gob.hn/tsp/crl/digerCA1.crl
- http://crl2.diger.gob.hn/tsp/crl/digerCA1.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de la DIGER, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible.

La DIGER suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

9.12.12 OBLIGACIÓN DE CONSULTA DE SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

9.12.13 REQUISITOS ESPECIALES EN CASO DE COMPROMISO DE LA CLAVE PRIVADA

El compromiso de la clave privada de la DIGER es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de la DIGER, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

9.12.14 PERÍODO MÁXIMO DE UN CERTIFICADO DIGITAL EN ESTADO SUSPENDIDO

El plazo máximo de un certificado digital en estado suspendido es indefinido hasta su caducidad.

9.13 FINALIZACIÓN DE LA SUSCRIPCIÓN

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta declaración de prácticas de certificación.

La DIGER puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

9.14 DEPÓSITO Y RECUPERACIÓN DE CLAVES

9.14.1 POLÍTICA Y PRÁCTICAS DE DEPÓSITO Y RECUPERACIÓN DE CLAVES

La DIGER no presta servicios de depósito y recuperación de claves.

9.14.2 POLÍTICA Y PRÁCTICAS DE ENCAPSULADO Y RECUPERACIÓN DE CLAVES DE SESIÓN

Sin estipulación.

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

10.1 CONTROLES DE SEGURIDAD FÍSICA

Se han establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones para la prestación de los servicios electrónicos de Certificación.

En concreto, la política de seguridad aplicable a los servicios electrónicos de certificación establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios electrónicos de certificación, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias de La DIGER destinadas a este fin.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24 horas, los 365 días al año y con respuesta en las 24 horas siguientes al aviso.

10.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DE LAS INSTALACIONES

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos (CPD) cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

Se dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de estos.

10.1.2 ACCESO FÍSICO

Se disponen de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al Rack) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por circuito cerrado de televisión y su archivo.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

10.1.3 ELECTRICIDAD Y AIRE ACONDICIONADO

Las instalaciones disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

10.1.4 EXPOSICIÓN AL AGUA

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

10.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Las instalaciones y activos cuentan con sistemas automáticos de detección y extinción de incendios.

10.1.6 ALMACENAMIENTO DE SOPORTES

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del CPD.

10.1.7 TRATAMIENTO DE RESIDUOS

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

10.1.8 COPIA DE RESPALDO FUERA DE LAS INSTALACIONES

Se utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

10.2 CONTROLES DE PROCEDIMIENTOS

Se garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

10.2.1 FUNCIONES FIABLES

Se han identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- Auditor Interno: Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- Administrador de Sistemas: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- Administrador de CA: Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- Operador de CA: Responsable necesario juntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.
- Operador de Registro: Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor y emitir certificados digitales.
- Oficial de Revocación: Persona responsable de realizar los cambios en el estado de un certificado, principalmente proceder con la suspensión y revocación de estos.
- Responsable de Seguridad: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, se implementan criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

10.2.2 NÚMERO DE PERSONAS POR TAREA

Se garantiza al menos dos personas para realizar las tareas relativas a la generación, recuperación y back-up de la clave privada de las Autoridades de Certificación. Igual criterio se aplica para la ejecución de tareas de emisión y activación de certificados y claves privadas de las Autoridades de Certificación, y en general cualquier manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

10.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA FUNCIÓN

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

10.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE TAREAS

Las siguientes tareas son realizadas, al menos, por dos personas:

- Las tareas propias del rol de Auditor serán incompatibles con la operación y administración de sistemas, y en general aquellas dedicadas a la prestación directa de los servicios electrónicos de certificación.
- Emisión y revocación de certificados, serán tareas incompatibles con la Administración y operación de los sistemas.
- La administración y operación de los sistemas y las CAs, serán incompatibles entre sí.

10.2.5 SISTEMA DE GESTIÓN PKI

El sistema de PKI se compone de los siguientes módulos:

- Componente/módulo de gestión de la Autoridad de Certificación Subordinada.
- Componente/módulo de gestión de la Autoridad de Registro.
- Componente/módulo de gestión de solicitudes.
- Componente/módulo de gestión de claves (HSM).
- Componente/módulo de bases de datos.
- Componente/módulo de gestión de CRL.
- Componente/módulo de gestión de la Autoridad de Validación (servicios de OCSP).

10.3 CONTROLES DE PERSONAL

10.3.1 REQUISITOS DE HISTORIAL, CALIFICACIONES, EXPERIENCIA Y AUTORIZACIÓN

Todo el personal está cualificado y/o ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

Se asegura de que el personal de registro es confiable para realizar las tareas de registro. El Administrador de Registro recibe formación para realizar las tareas de validación de las peticiones.

En general, se retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

No se asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales.
- Referencias profesionales.

En todo caso, las Autoridades de Registro podrán establecer procesos de comprobación de antecedentes diferentes, siempre preservando las políticas, siendo responsables por la actuación de las personas que autoricen en sus operaciones.

10.3.2 PROCEDIMIENTOS DE INVESTIGACIÓN DE HISTORIAL

La DIGER, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

La DIGER obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales en cumplimiento de la normativa vigente en materia de protección de datos personales.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

10.3.3 REQUISITOS DE FORMACIÓN

Se forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son revisados periódicamente, y son actualizados para su mejor y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

10.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN FORMATIVA

Se actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficiente para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

10.3.5 SECUENCIA Y FRECUENCIA DE ROTACIÓN LABORAL

No aplicable.

10.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

Se dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

10.3.7 REQUISITOS DE CONTRATACIÓN DE PROFESIONALES

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la Declaración de Prácticas de Certificación, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la

Autoridad de Certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto.

10.3.8 SUMINISTRO DE DOCUMENTACIÓN AL PERSONAL

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

10.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

10.4.1 TIPOS DE EVENTOS REGISTRADOS

Se produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de
- activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como
- recepción, uso y desinstalación de éste.
- La ceremonia de generación de claves y las bases de datos de gestión de
- claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados

individuales, o de la Persona Natural identificada en el certificado, en caso de certificados de organización.

- Posesión de datos de activación, para operaciones con la clave privada de la Autoridad de Certificación.
- Eventos relacionados con la sincronización, así como pérdida de esta en lo relativo a las fuentes fiables de tiempo usadas para proporcionar la marca de tiempo en los registros relativos a la Infraestructura de Clave Pública usada por LA DIGER para la prestación de los servicios.
- Eventos relacionados con caídas de los servicios proporcionados mediante la Infraestructura de Clave Pública usada por La DIGER para la prestación de los servicios.
- Eventos relacionados con la mal función de los equipos usados por la DIGER en lo relativo a la prestación de servicios de certificación.
- Eventos relacionados con los cortafuegos vinculados a la infraestructura de clave pública usada por la DIGER para la prestación de los servicios.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

10.4.2 FRECUENCIA DE TRATAMIENTO DE REGISTROS DE AUDITORÍA

Se revisan sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

Se mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.

- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

10.4.3 PERÍODO DE CONSERVACIÓN DE REGISTROS DE AUDITORÍA

Se almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada. No obstante, lo anterior, los registros de auditoría que tengan relación con la gestión del ciclo de vida de los certificados digitales se conservarán por el periodo máximo establecido legalmente.

10.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los logs de los sistemas:

- Están protegidos de manipulación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

10.4.5 PROCEDIMIENTOS DE COPIA DE RESPALDO

Se dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

Se tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

10.4.6 LOCALIZACIÓN DEL SISTEMA DE ACUMULACIÓN DE REGISTROS DE AUDITORÍA

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

10.4.7 NOTIFICACIÓN DEL EVENTO DE AUDITORÍA AL CAUSANTE DEL EVENTO

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

10.4.8 ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el procedimiento interno que previsto para este fin.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

10.5 ARCHIVOS DE INFORMACIONES

Se garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 0 de esta política.

10.5.1 TIPOS DE REGISTROS ARCHIVADOS

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por La DIGER (o por las entidades de registro):

- Todos los datos de auditoría de sistema.
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 0
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

La DIGER y/o las Autoridades de Registro según corresponda, serán responsables del correcto archivo de todo este material.

10.5.2 PERÍODO DE CONSERVACIÓN DE REGISTROS

Se archivan los registros especificados anteriormente durante el período que establezca la legislación vigente.

10.5.3 PROTECCIÓN DEL ARCHIVO

Se protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

Se asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

10.5.4 PROCEDIMIENTOS DE COPIA DE RESPALDO

Se dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

Como mínimo se realizan copias de respaldo incrementales diarias de todos sus documentos electrónicos y realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, la DIGER (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Autoridad de Certificación.

10.5.5 REQUISITOS DE SELLADO DE FECHA Y HORA

Los registros están fechados con una fuente fiable vía NTP.

No es necesario que esta información se encuentre firmada digitalmente.

10.5.6 LOCALIZACIÓN DEL SISTEMA DE ARCHIVO

Se dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

10.5.7 PROCEDIMIENTOS DE OBTENCIÓN Y VERIFICACIÓN DE INFORMACIÓN DE ARCHIVO

Se dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. Se proporciona la información y medios de verificación al auditor.

10.6 RENOVACIÓN DE CLAVES

Con anterioridad a que el uso de la clave privada de la AC caduque, será realizado un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará una nueva AC con una clave privada nueva y un nuevo DN. El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

Alternativamente, en el caso de Autoridades de Certificación subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves, no resultando aplicable el procedimiento antes descrito.

10.7 COMPROMISO DE CLAVES Y RECUPERACIÓN DE DESASTRE

10.7.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENCIAS Y COMPROMISOS

Se han desarrollado políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones, asegurando los servicios críticos de revocación y publicación del estado de los certificados.

10.7.8 CORRUPCIÓN DE RECURSOS, APLICACIONES O DATOS

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo con las políticas de seguridad y gestión de incidentes de la DIGER, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de la DIGER.

10.7.3 COMPROMISO DE LA CLAVE PRIVADA DE LA ENTIDAD

En caso de sospecha o conocimiento del compromiso de la DIGER, se activarán los procedimientos de compromiso de claves de acuerdo con las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

10.7.4 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Se restablecerán los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el plan de incidencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

Se dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

10.9 TERMINACIÓN DEL SERVICIO

Se asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación. En este sentido, se garantiza un mantenimiento continuo de los registros definidos en el apartado 5.5.1, por el tiempo establecido en el apartado 5.5.2 de esta Declaración de Prácticas de Certificación.

No obstante, lo anterior, si procede se ejecutarán todas las acciones que sean necesarias para transferir a un tercero o a un depósito notarial, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta Declaración de Prácticas de Certificación o la previsión legal que corresponda.

Antes de terminar sus servicios, se desarrolla un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios, para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima fijada en la regulación.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.

11.CONTROLES DE SEGURIDAD TÉCNICA

Se emplean sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

11.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

11.1.1 GENERACIÓN DEL PAR DE CLAVES

El par de claves de la entidad de certificación intermedias "La DIGER CA Subordinada 01" ha sido creada por la Autoridad de Certificación raíz "La DIGER CA Raíz" de acuerdo con los procedimientos de ceremonia de claves, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por la DIGER.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones FIPS 140-2 level 3 y Common Criteria EAL4+.

La DIGER CA Raíz	4.096 bits	25 años
La DIGER CA Subordinada 01	4.096 bits	13 años
- Certificados de entidad final	2.048 bits	Hasta 5 años

Los documentos texto de divulgación (PKI Disclosure Statement-PDS) de todos los perfiles de certificados digitales indicados en el presente documento, se encuentran accesibles bajo el enlace https://www.diger.gob.hn/

11.1.2 GENERACIÓN DEL PAR DE CLAVES DEL FIRMANTE

Las claves del firmante pueden ser generadas por él mismo mediante dispositivos hardware y/o softwares autorizados por la DIGER. Las claves no generadas en un HSM serán generadas por el firmante. La DIGER nunca genera claves fuera de un HSM para ser enviadas al firmante. Como norma general las claves no generadas en un HSM serán generadas por el firmante. No obstante, lo anterior, la DIGER podrá generar claves fuera de un HSM para ser puestas a disposición del firmante mediante métodos seguros que garanticen que únicamente el firmante es quien tiene acceso a ellas.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

11.1.3 ENVÍO DE LA CLAVE PRIVADA AL FIRMANTE

En certificados emitidos en HSM la clave privada se generará y se almacena debidamente protegida en el interior de dicho dispositivo cualificado.

En certificados en software, el envío de la clave privada se realiza de la manera que se describe a continuación:

Si la clave privada del firmante se genera y se almacena en el sistema informático que utiliza este firmante cuando realiza la solicitud del certificado, en este caso no se realiza el envío de clave privada, debido a que esta se "autogenera", garantizando así el control exclusivo de la clave por parte del usuario.

Si la clave privada del firmante se genera en los sistemas certificados de la DIGER, la misma se pone a disposición del firmante mediante mecanismos y protocolos seguros, garantizando que únicamente el firmante tiene acceso a la misma, asegurando el control exclusivo de la clave por parte del usuario.

En ambos casos, la DIGER no almacena, guarda, custodia ni tiene la capacidad de deducir la clave privada de los certificados en software.

En certificados en HSM Centralizado la clave privada del firmante se genera en un área privada del firmante en un HSM remoto. Las credenciales de acceso a la clave privada son introducidas por el propio firmante, no siendo almacenadas ni susceptibles de capacidad de deducción o intercepción por el sistema de generación y custodia remota. La clave privada no se envía al firmante, es decir, nunca abandona el entorno de seguridad que garantiza el control exclusivo de la clave privada por parte del firmante.

11.1.4 ENVÍO DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

El método de remisión de la clave pública al prestador de servicios electrónicos de certificación es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por la DIGER.

11.1.5 DISTRIBUCIÓN DE LA CLAVE PÚBLICA DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Las claves de la DIGER son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el depósito.

Los usuarios pueden acceder al depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las autoridades de certificación raíz y subordinadas estarán a disposición de los usuarios en la página web de la DIGER.

Tamaños de claves

- La longitud de las claves de la autoridad de certificación raíz es de 4096 bits.

- La longitud de las claves de la autoridad de certificación subordinadas es de 4096 bits.
- La longitud de las claves de los certificados de entidad final es de 2048 bits.

11.1.6 GENERACIÓN DE PARÁMETROS DE CLAVE PÚBLICA

La clave pública de las autoridades de certificación raíz, subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.
Así las cosas, los certificados emitidos por la DIGER respetan en todo momento los limites vinculados a cada campo de certificado, a tenor del apartado 4.2 de dicho estándar.

11.1.7 COMPROBACIÓN DE CALIDAD DE PARÁMETROS DE CLAVE PÚBLICA

- Longitud del Módulo = 4096 bits
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

11.1.8 GENERACIÓN DE CLAVES EN APLICACIONES INFORMÁTICAS O EN BIENES DE EQUIPO

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

11.1.9 PROPÓSITOS DE USO DE CLAVES

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final son exclusivamente para la firma digital, el no repudio y cifrado de datos.

11.2 PROTECCIÓN DE LA CLAVE PRIVADA

112.1 ESTÁNDARES DE MÓDULOS CRIPTOGRÁFICOS

En relación con los módulos que gestionan claves de la DIGER y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

11.2.2 CONTROL POR MÁS DE UNA PERSONA (N DE M) SOBRE LA CLAVE PRIVADA

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta Declaración de Prácticas de Certificación, en concreto existe una política de 3 de 6 personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

11.2.3 DEPÓSITO DE LA CLAVE PRIVADA

La DIGER no almacena copias utilizables por medios propios de las claves privadas de los firmantes.

11.2.4 INTRODUCCIÓN DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Las claves privadas se generan directamente en los módulos criptográficos de producción de la DIGER.

Las claves privadas de la Autoridad de Certificación se almacenan cifradas en los módulos criptográficos de producción de la DIGER.

11.2.5 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de la DIGER se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas autorizadas de acuerdo con esta Declaración de Prácticas de Certificación.

Las claves de la AC se activan por un proceso de m de n (3 de 6). La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC.

11.2.6 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Para la desactivación de la clave privada de la DIGER se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

11.2.7 MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de la DIGER. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad. Respecto a las claves privadas de los firmantes se procederá acorde a los establecido en el plan de cese.

11.2.8 CLASIFICACIÓN DE MÓDULOS CRIPTOGRÁFICOS

Ver la sección 0 clasificación

11.3 Otros aspectos de gestión del par de claves

113.1 ARCHIVO DE LA CLAVE PÚBLICA

Se archivan las claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 0 de este documento.

11.3.1 PERÍODOS DE UTILIZACIÓN DE LAS CLAVES PÚBLICA Y PRIVADA

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

Como excepción y en caso de existir, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

11.4 DATOS DE ACTIVACIÓN

11.4.1 GENERACIÓN E INSTALACIÓN DE DATOS DE ACTIVACIÓN

Los datos de activación de los dispositivos que protegen las claves privadas de la DIGER son generados de acuerdo con lo establecido en la sección 0 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada.

Asimismo, la DIGER genera de forma segura los datos de activación.

11.4.2 PROTECCIÓN DE DATOS DE ACTIVACIÓN

Los datos de activación de los dispositivos que protegen las claves privadas de las autoridades de certificación raíz y subordinadas, están protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una o varias contraseñas lo más completas y complejas posible. El firmante debe recordar dicha(s) contraseña(s).

11.5 CONTROLES DE SEGURIDAD INFORMÁTICA

Se emplean sistemas fiables para ofrecer sus servicios de certificación. Se han realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, la DIGER aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de la DIGER, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

11.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURIDAD INFORMÁTICA

Cada servidor incluye las siguientes funcionalidades:

- Control de acceso a los servicios de las autoridades de certificación subordinadas y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor, de las autoridades de certificación subordinadas y datos de auditoría.
- Auditoria de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de las Autoridades de certificación subordinadas.
- Mecanismos de recuperación de claves y del sistema de las autoridades de certificación subordinadas.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

11.5.2 EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA

Las aplicaciones de autoridad de certificación y de registro empleadas por la DIGER son fiables.

11.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

11.6.1 CONTROLES DE DESARROLLO DE SISTEMAS

Las aplicaciones son desarrolladas e implementadas por la DIGER de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

11.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

Se desarrollan las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

La DIGER exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de certificación.

11.6.3 CLASIFICACIÓN Y GESTIÓN DE INFORMACIÓN Y BIENES

La DIGER mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de la DIGER detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: SIN CLASIFICAR, USO INTERNO y CONFIDENCIAL.

11.6.4 OPERACIONES DE GESTIÓN

La DIGER dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad de la DIGER se desarrolla en detalle el proceso de gestión de incidencias.

La DIGER tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

11.6.5 TRATAMIENTO DE LOS SOPORTES Y SEGURIDAD

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

11.6.5 PLANIFICACIÓN DEL SISTEMA

El departamento de Sistemas mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

11.6.7 REPORTES DE INCIDENCIAS Y RESPUESTA

Se dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

11.6.8 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Se definen actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

11.6.9 GESTIÓN DEL SISTEMA DE ACCESO

Se realizan todos los esfuerzos que razonablemente están en el alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.
En particular:

AC General

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- Se dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- Se dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada.

Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

11.6.6 GESTIÓN DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRÁFICO

La DIGER se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

La DIGER registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

Se realizan test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema, así como sus modificaciones y actualizaciones son documentadas y controladas.

Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

11.7 CONTROLES DE SEGURIDAD DE RED

Se protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

11.8 CONTROLES DE INGENIERÍA DE MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

12.PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

12.1 PERFIL DE CERTIFICADO

Todos los certificados cualificados emitidos bajo esta política cumplen con el estándar X.509 versión 3 y el RFC 3739 y los diferentes perfiles descritos en la norma EN 319 412.
La documentación relativa a los perfiles de la norma EN 319 412 puede solicitarse a la DIGER.

12.1 .1 NÚMERO DE VERSIÓN

La DIGER emite certificados X.509 Versión 3

12.1 .2 EXTENSIONES DEL CERTIFICADO

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la página web de la DIGER (https://www.diger.gob.hn)

De esta forma se permite mantener unas versiones más estables de la declaración de prácticas de certificación y desligarlos de los frecuentes ajustes en los perfiles.

12.1 .3 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

12.1 .4 FORMATO DE NOMBRES

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

12.1 .5 RESTRICCIÓN DE LOS NOMBRES

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos.

12.1 .6 IDENTIFICADOR DE OBJETO (OID) DE LOS TIPOS DE CERTIFICADOS

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 0

12.2 PERFIL DE LA LISTA DE REVOCACIÓN DE CERTIFICADOS

12.2.1 NÚMERO DE VERSIÓN

Las CRL emitidas por la DIGER son de la versión 2.

Perfil de OCSP

Según el estándar IETF RFC 6960.

13.AUDITORÍA DE CONFORMIDAD

La DIGER ha comunicado el inicio de su actividad como prestador de servicios de certificación autorizado por el Instituto de la propiedad de Honduras.

13.1 FRECUENCIA DE LA AUDITORÍA DE CONFORMIDAD

La DIGER lleva a cabo auditorías que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

13.2 IDENTIFICACIÓN Y CALIFICACIÓN DEL AUDITOR

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

13.3 RELACIÓN DEL AUDITOR CON LA ENTIDAD AUDITADA

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con la DIGER.

13.4 LISTADO DE ELEMENTOS OBJETO DE AUDITORÍA

La auditoría verifica respecto a la DIGER:

a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.

b) Que la entidad cumple con los requerimientos de la declaración de prácticas de certificación y otra documentación vinculada con la emisión de los distintos certificados digitales.
c) Que la declaración de prácticas de certificación y demás documentación jurídica vinculada, se ajusta a lo acordado por la DIGER y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información

En particular, los elementos objeto de auditoría serán los siguientes:

a) Procesos de las Autoridades de Certificación, Autoridades de Registro y elementos relacionados.
b) Sistemas de información.
c) Protección del centro de proceso de datos.
d) Documentos.

13.5 ACCIONES A EMPRENDER COMO RESULTADO DE UNA FALTA DE CONFORMIDAD

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solventen dichas deficiencias.

Si la DIGER es incapaz de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Seguridad que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la Autoridad de Certificación y regenerar la infraestructura.
- Terminar el servicio de la Autoridad de Certificación.
- Otras acciones complementarias que resulten necesarias.

Tratamiento de los informes de auditoría:
Los informes de resultados de auditoría se entregan al comité de seguridad en un plazo máximo de 15 días tras la ejecución de la auditoría.

14.REQUISITOS COMERCIALES Y LEGALES

14.1 TARIFAS

14.1.1 TARIFA DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

La DIGER puede establecer una tarifa por la emisión o por la renovación de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

14.1.2 TARIFA DE ACCESO A CERTIFICADOS

La DIGER no ha establecido ninguna tarifa por el acceso a los certificados.

14.1.3 TARIFA DE ACCESO A INFORMACIÓN DE ESTADO DE CERTIFICADO

La DIGER no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

14.1.4 TARIFAS DE OTROS SERVICIOS

Sin estipulación.

14.1.5 POLÍTICA DE REINTEGRO

Sin estipulación.

14.2 CAPACIDAD FINANCIERA

La DIGER dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401-1 7.12 c), con relación a la gestión de la finalización de los servicios y plan de cese.

14.2.1 COBERTURA DE SEGURO

La DIGER dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo a la normativa vigente aplicable.

14.2.2 OTROS ACTIVOS

Sin estipulación.

14.3 CONFIDENCIALIDAD

14.3.1 INFORMACIONES CONFIDENCIALES

Las siguientes informaciones son mantenidas confidenciales por LA DIGER:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Autoridad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Planes de seguridad.

- Documentación de operaciones, archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

14.3.2 INFORMACIONES NO CONFIDENCIALES

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Autoridad de Certificación.
- El nombre y los apellidos de la Persona Natural identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la Persona Natural identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

14.3.4 DIVULGACIÓN DE INFORMACIÓN DE SUSPENSIÓN Y REVOCACIÓN

Véase la sección anterior.

14.3.5 DIVULGACIÓN LEGAL DE INFORMACIÓN

La DIGER divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

La DIGER indicará estas circunstancias en la política de privacidad prevista en la sección 0.

14.3.5 DIVULGACIÓN DE INFORMACIÓN POR PETICIÓN DE SU TITULAR

La DIGER incluye, en la política de privacidad prevista en la sección 0, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la Persona Natural identificada en el certificado, directamente a los mismos o a terceros.

14.3.6 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Sin estipulación.

14.4 PROTECCIÓN DE DATOS PERSONALES

La DIGER garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales.

En cumplimiento de esta, la DIGER ha documentado en esta declaración de prácticas de certificación los aspectos y procedimientos de seguridad y organizativos, con el fin de garantizar que todos los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

A continuación, se detalla toda la información necesaria con respecto al tratamiento de datos personales realizado por La DIGER:

Responsable del tratamiento

Dirección de Gestión por Resultados
Dirección: Boulevard Fuerzas Armadas
Contiguo al Banco Central de Honduras
Delegado de Protección de datos
Correo electrónico: consultas@diger.gob.hn

Finalidad del tratamiento

La DIGER trata los datos de carácter personal facilitados para llevar a cabo los servicios electrónicos solicitados, concretamente la expedición de certificados electrónicos, todo ello de acuerdo con lo previsto en la Declaración de Prácticas de Certificación (DPC) de LA DIGER, la cual se encuentra disponible en el siguiente enlace: https://www.diger.gob.hn

Las finalidades de tratamiento de datos relativos al servicio son las siguientes:

- Identificación de los suscriptores y/o firmantes de los certificados electrónicos.
- Expedición y gestión de certificados electrónicos.
- Gestión del ciclo de vida del certificado (suspensión, renovación, reactivación y revocación).

- Comunicaciones relativas al servicio.
- Custodia y mantenimiento del archivo relativo al certificado electrónico.
- Gestión administrativa, contable y de facturación derivada de la contratación.

Legitimación del tratamiento

La legitimación del tratamiento de datos personales para la prestación de servicios de certificación para la expedición de certificados se basa en la ejecución de un contrato de los servicios solicitados, donde el usuario es parte de este.

Datos tratados y conservación

Las categorías de datos personales tratados por la DIGER, a título enunciativo, pero no limitativo, comprenden:

- Datos identificativos: nombre, apellidos y número oficial de identidad.
- Datos profesionales: organización, departamento y/o cargo.
- Datos de contacto: dirección postal, correo electrónico y número de teléfono.
- Datos relativos a la identidad o identificación de los usuarios: fotografías y/o cuando corresponda el patrón biométrico facial, con la finalidad de poder llevar a cabo el proceso de vídeo identificación de la DIGER.

Los datos personales se conservarán hasta la finalización de la relación contractual y posteriormente, durante los plazos legalmente exigidos acorde a cada caso. Como norma general, los datos personales relativos al SERVICIO se conservarán durante el tiempo legamente establecido.

Los datos personales se almacenarán en las instalaciones seguras de la DIGER ubicadas en Honduras.

Transferencia de datos

Los datos pueden ser puestos a disposición de terceros, dentro del territorio de Honduras, con motivo de la prestación de servicios contratados por el usuario (por ejemplo proveedores de alojamiento de datos (CPD), servicios de apoyo en la identificación, empresas del grupo, etc.), todo ello al amparo del correspondiente contrato de encargo de tratamiento de datos personales, garantizando en todo momento unas medidas de seguridad idóneas que aseguren la debida protección de los datos personales de los usuarios.
Sin perjuicio de lo anterior, como norma general los datos personales únicamente se cederán a terceros bajo obligación legal.

Como norma general, no se realizarán transferencias internacionales.

Derechos de los usuarios

Los usuarios podrán ejercitar sus derechos de confirmación, acceso, rectificación, supresión, cancelación, limitación, oposición y portabilidad.

- Confirmación. Todos los usuarios tienen derecho a obtener confirmación sobre si LA DIGER está tratando datos personales que les conciernan.

- Acceso y rectificación. Los usuarios tienen derecho a acceder a todos sus datos personales, así como solicitar la rectificación de aquellos que sean inexactos o erróneos.

- Supresión y cancelación. Los usuarios podrán solicitar la supresión/cancelación de los datos cuando, entre otros motivos, éstos no sean necesarios para los fines para los que fueron recogidos.

- Limitación y oposición. El usuario podrá solicitar la limitación del tratamiento para que sus datos personales no se apliquen en las operaciones que correspondan. En determinadas circunstancias y por motivos relacionados con su situación particular, el usuario podrá oponerse al tratamiento de datos, estando la DIGER obligada a dejar de tratarlos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

- Portabilidad. Los interesados podrán solicitar que sus datos personales les sean enviados o bien se transmitan a otro responsable, en un formato electrónico estructurado y de uso habitual.

Para ejercer sus derechos, los usuarios pueden enviar una petición a la dirección de correo electrónico o bien dirigir un escrito a la dirección indicada en el apartado 1.5. En dicha petición, deberán adjuntar copia de su cédula de identidad e indicar claramente cuál es el derecho que se desea ejercer.

14.5 DERECHOS DE PROPIEDAD INTELECTUAL

14.5.1 PROPIEDAD DE LOS CERTIFICADOS E INFORMACIÓN DE REVOCACIÓN

Únicamente la DIGER goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por la DIGER contienen un aviso legal relativo a la propiedad de estos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

14.5.2 PROPIEDAD DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Únicamente la DIGER goza de derechos de propiedad intelectual sobre esta declaración de prácticas de certificación.

14.5.3 PROPIEDAD DE LA INFORMACIÓN RELATIVA A NOMBRES

El suscriptor y, en su caso, la persona natural identificada en el certificado conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido (DN) del certificado, formado por las informaciones especificadas en la sección 0.

14.5.4 PROPIEDAD DE CLAVES

Los pares de claves son propiedad de los suscriptores de los certificados.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

14.6 OBLIGACIONES Y RESPONSABILIDAD CIVIL

14.6.1 OBLIGACIONES DE LA DIGER

La DIGER garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la Declaración de Prácticas de Certificación, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento.

La DIGER presta los servicios electrónicos de certificación conforme con esta Declaración de Prácticas de Certificación.

La DIGER informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia los textos de divulgación (PDS) de cada uno de los certificados adquiridos.

El documento de texto de divulgación, también denominado PDS3 el contenido del anexo A de la ETSI EN 319 411-1 v1.1.1 (2016-02), documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

La DIGER vincula a suscriptores, poseedores de claves y terceros que confían en certificados, mediante dicho texto de divulgación o PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Autoridad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 0
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Autoridad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Autoridad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas, disponible en: https://www.diger.gob.hn
- Ley aplicable y jurisdicción competente.
- Si la Autoridad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

14.6.2 GARANTÍAS OFRECIDAS A SUSCRIPTORES Y TERCEROS QUE CONFÍAN EN CERTIFICADOS

3 “PKI Disclosure Statement”, o declaración de divulgación de PKI aplicable.

LA DIGER, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

La DIGER, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Autoridad de Certificación de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación de este.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- Que los servicios de revocación y el empleo del depósito cumplen con todos los requisitos materiales establecidos en la declaración de prácticas de certificación.

La DIGER, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 0.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, la DIGER garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona natural identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la autoridad de certificación, con los límites que se establezcan.

14.6.3 RECHAZO DE OTRAS GARANTÍAS

La DIGER rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 0.

14.6.4 LIMITACIÓN DE RESPONSABILIDADES

La DIGER limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados por la Autoridad de Certificación.

14.6.5 CLÁUSULAS DE INDEMNIDAD

14.6.5.1 CLÁUSULA DE INDEMNIDAD DE SUSCRIPTOR

La DIGER incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Autoridad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Autoridad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

14.6.5.2 CLÁUSULA DE INDEMNIDAD DE TERCERO QUE CONFÍA EN EL CERTIFICADO

La DIGER incluye en el texto de divulgación o PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Autoridad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

14.6.5.3 CASO FORTUITO Y FUERZA MAYOR

La DIGER no será responsable en ningún caso bajo situaciones que incurran en caso fortuito y en caso de fuerza mayor.

Se entiende por caso fortuito como aquella situación o suceso que sea imposible de prever, o que, previsto, sea inevitable respecto de su mitigación. Adicionalmente, se entiende por fuerza mayor aquellas situación o suceso que es inevitable de hacer efectivas sus circunstancias, imprevisible y extraordinario en su origen, emanante de un ámbito ajeno e irresistible.

Por ello, la DIGER no será responsable bajo ningún concepto en situación de guerra, desastres naturales, funcionamiento disfuncional de servicios eléctricos, redes o infraestructura informática, por causa no imputable a la DIGER.

14.6.5.4 LEY APLICABLE

La DIGER establece, en el contrato de suscriptor y en el texto de divulgación o PDS, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley de Honduras.

14.6.5.5 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

La DIGER establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la autoridad de certificación vela porque, al menos los requisitos contenidos en las secciones obligaciones y responsabilidad; auditoría de conformidad y confidencialidad continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

14.6.5.6 CLÁUSULA DE JURISDICCIÓN COMPETENTE

La DIGER establece, en el contrato de suscriptor y en el texto de divulgación o PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces hondureños.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

14.6.5.7 RESOLUCIÓN DE CONFLICTOS

La DIGER establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, los procedimientos de mediación y resolución de conflictos aplicables.

La presente declaración será revisada cada año o cuando se requiera por la máxima autoridad de la DIGER, funcionario delegado o haya cambios significativos.

Este documento fue aprobado por el ministro de la Dirección de Gestión por Resultados, el día 27 de agosto del año 2025.