COLEGIO DE NOTARIOS DE LIMA

Proyecto **Entidad de Certificación**

Título **Declaración de Prácticas y Política de Certificación del Colegio de Notarios de Lima**

Realizado por	**COLEGIO DE NOTARIOS DE LIMA**
Dirigido a	**INDECOPI**
Aprobado por	
Fecha	**08/08/2016** **Versión** **1.0**

ÍNDICE

1 INTRODUCCIÓN

El Colegio de Notarios de Lima (CNL), es una persona jurídica de Derecho Público, creada por la Ley Nº 16607, mediante Resolución Suprema Nº 345-88-JUS del 02 de octubre de 1988, que incorpora a los Notarios de Lima.

Como Entidad de Certificación Digital - EC, el CNL provee servicios de emisión, distribución y revocación de certificados digitales.

La infraestructura tecnológica y operativa de la EC del CNL es provista por la Agencia Notarial de Certificación (ANCERT). Dicha infraestructura ha obtenido la certificación Webtrust for Certification Authorities, y es verificada anualmente por auditores autorizados.

Junto a los servicios de certificación digital, el CNL brinda los servicios de registro o verificación de sus clientes, tanto en el caso de personas jurídicas como naturales.

2 OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas que utiliza el CNL para la administración de sus servicios como Entidad de Certificación Digital – EC, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI, en calidad de Autoridad Administrativa Competente de la Infraestructura Oficial de la Firma Electrónica del Perú.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital brindados por el CNL a través de la ANCERT, la cual cuenta con la certificación Webtrust Program for Certification Authorities emitida por AICPA/CICA.

La ANCERT como proveedor de infraestructura y gestión de operaciones de los servicios de la EC del CNL, asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital provistos por la EC del CNL.

4 DEFINICIONES Y ABREVIACIONES

Entidad de Certificación - EC	Entidad que presta servicios de emisión, revocación, modificación, suspensión de certificados digitales en el marco de la regulación establecida por la IOFE.
Entidad de Registro - ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital.
Política de Certificación	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de

	usuarios definida.
Titular	Entidad que requiere los servicios provistos por la EC del CNL y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

4.1 PARTICIPANTES.

4.1.1 ENTIDAD DE CERTIFICACIÓN COLEGIO DE NOTARIOS DE LIMA (EC CNL)

El CNL, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

Al CNL, como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la ACC a fin de poder ingresar a la IOFE.

4.1.2 AUTORIDAD DE REGISTRO COLEGIO DE NOTARIOS DE LIMA (ER CNL)

El CNL, brinda también los servicios de Entidad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

En su condición de ER, el CNL realiza sus funciones a través de labores coordinadas entre dos sujetos:

- Colegio de Notarios de Lima: Persona jurídica que incorpora a los Notarios de Lima, y que en sus funciones como ER se encarga del levantamiento de datos, comprobación de estos respecto a un solicitante para la emisión de certificación digital, la aceptación y autorización de las solicitudes para la emisión de certificados digitales, así como de la aceptación y autorización de las solicitudes de revocación, modificación, suspensión de certificados digitales.
  Notario: Profesional del Derecho que está autorizado a dar fe de los actos y contratos que ante él se celebran.
- Personal de la Notaría: Personal de confianza adscrito a una Notaría, el mismo que se encarga de participar en las labores de emisión, suspensión y revocación de certificados digitales.

4.1.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL E INFRAESTRUCTURA (ANCERT)

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación CNL, entre sus principales funciones se encuentran las siguientes:

- Garantizar la seguridad, disponibilidad y calidad de las operaciones de gestión de los certificados digitales de los usuarios finales.
- Garantizar la seguridad de las claves de la EC Raíz del CNL y las EC Subordinadas durante todo su ciclo de vida.
- Garantizar la disponibilidad y accesibilidad de los servicios de consulta de estado de revocación de los certificados digitales
- Garantizar la protección de los datos personales de los usuarios finales.
- Garantizar la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que ofrece el CNL son provistos, en un contrato de tercerización, por la Agencia Notarial de Certificación ANCERT S.L.U. con Número de Identificación Fiscal nº B-83395988, autorizada por el Ministerio de Industria de España.

La Agencia Notarial de Certificación ANCERT S.L.U. es un proveedor de servicios de certificación establecidos en España que expide certificados reconocidos de acuerdo con todos los requisitos aplicables de la Directiva 1999/93 /EC.

4.1.4 TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta CPS.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por el CNL conforme a lo establecido en la Política de Certificación.

4.1.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

4.1.6 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un certificado emitido bajo esta CPS.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

4.1.7 TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación del CNL a un titular. El Tercero que confía, a su vez puede ser o no titular.

4.1.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el certificado.

5 SERVICIOS DE CERTIFICACIÓN DIGITAL

El CNL brinda los servicios de emisiónrevocación y distribución de los certificados digitales.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritos en la Declaración de Prácticas y la Política de Certificación del CNL:

http://www.notarios.org.pe/

6 RESPONSABILIDADES

La ANCERT como proveedor de infraestructura y gestión de operaciones de los servicios de la EC del CNL, asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital provistos por la EC del CNL.

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por la ANCERT de acuerdo a su documento Declaración de Prácticas de Certificación Certificados Notariales, publicado en:

http://www.ancert.com/liferay/web/ancert/politica-de-certificacion-y-dpcs

El CNL es responsable de exigir y supervisar las operaciones de los servicios de la EC del CNL que son administrados por la ANCERT.

Como Entidad de Registro, el CNL es responsable de la correcta identificación de las personas naturales o jurídicas y de la seguridad en la entrega de certificados digitales, siempre que esta sea realizada por los Operadores de Registro autorizados.

Las peticiones, quejas o reclamos sobre los servicios prestados por el CNL a través de la ANCERT son recibidas directamente por el CNL como prestador de servicios digitales o a través de nuestra Entidad de Registro. La línea telefónica para la atención a titulares y terceros para consultas relacionadas con el servicio que dispone el CNL es permanente. Estos reclamos serán comunicados en un lapso no mayor de 5 días a la ANCERT, para su debida atención.

7 USO DEL CERTIFICADO

7.1 USO PERMITIDO DEL CERTIFICADO

El uso adecuado de los certificados emitidos se encuentra especificado en Política General de Certificación del CNL.

Los certificados emitidos bajo esta CPS pueden ser utilizados con los siguientes propósitos:

- Identificación del Titular que firma un documento o que se autentica para acceder a un sistema: El Titular del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el certificado.

- Integridad del documento firmado: La utilización del certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.

- No repudio de origen: Con el uso de este certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

Cada política de certificación está identificada por un único identificador de objeto (OID) que además incluye el número de versión.

7.2 USO PROHIBIDO DEL CERTIFICADO Y EXCLUSIÓN DE RESPONSABILIDAD

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta CPS y concretamente en las Políticas de Certificación.

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

Se consideran indebidos aquellos usos que no están definidos en esta CPS y en consecuencia para efectos legales, el CNL y la ANCERT quedan eximidos de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de certificados digitales según esta CPS.

Asimismo, los certificados deberán emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados pueden contener límites adicionales uso en forma de atributos dentro del campo Subject Directory Attributes, así como en las condiciones generales de uso de los certificados.

Los terceros deben considerar estas limitaciones antes de confiar en los certificados. Aunque los certificados de entidad final se pueden emplear, con algunas excepciones, para el cifrado o descifrado de documentos electrónicos, se advierte que dichos usos se realizan bajo la exclusiva responsabilidad del suscriptor.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de usos limitados y/o prohibidos quedan a cargo del suscriptor.

En ningún caso podrá el suscriptor, el poseedor de claves o los terceros perjudicados reclamar a la Agencia Notarial de Certificación, o al Consejo General del Notariado, compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados para los usos limitados y/o prohibidos.

8 PERSONA DE CONTACTO

Datos de la Entidad de Certificación Digital y Registro:

Nombre: COLEGIO DE NOTARIOS DE LIMA

Dirección: Av. Giuseppe Garibaldi 339 – 343 Jesús María

Domicilio: Lima

Teléfono: +51 (01) 319-0700 / 461-0016

Correo electrónico: notarioslima@notarios.org.pe

Página Web: www.notarios.org.pe

Datos de la Entidad Prestadora de Servicios de Certificación Digital:

Nombre: AGENCIA NOTARIAL DE CERTIFICACIÓN S.L. UNIPERSONAL

Dirección: Plaza Xavier Cugat 2, Ed. A 08174 Sant Cugat de Vallès

Domicilio: España

Teléfono: +34 (93) 584 83 00

Fax: +34 (93) 584 83 23

Correo electrónico: ehernandez@notariado.org

Página Web: www.ancert.com

9 RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por el CNL, son responsables de revisar la presente CPS y las Políticas de Certificación, a fin de ser enterados de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

10 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE CP Y CPS

El CNL administra los documentos de Declaración de Prácticas, y todos los documentos normativos de la EC del CNL.

Para cualquier consulta contactar:

- Nombre: Gerardo Marvin García Martínez
- Cargo: Jefe del Área de Tecnología
- Dirección de correo electrónico: ggarcia@notarios.org.pe

11 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Certificación Digital– CPS del CNL, la Política y Plan de Privacidad, así como la Declaración de Prácticas y Política General de Certificación del CNL y otra documentación relevante son publicados en la dirección:

www.notarios.org.pe

Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por el Responsable de la EC del CNL antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Los documentos referidos a la Declaración de Prácticas y Políticas de Certificación de los proveedores del CNL, así como la Declaración de Prácticas de las ER con las que tiene filiación serán publicados en la dirección:

www.notarios.org.pe

12 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

Certificado Raíz del CNL

http://www.notarios.org.pe/

Certificados Subordinadas del CNL

http://www.notarios.org.pe/

Lista de Certificados Revocados (CRL)

http://pki.notarios.org.pe/crl

Servicio OCSP

http://pki.notarios.org.pe/ocsp

Declaración de Prácticas de Certificación (CPS)

http://www.notarios.org.pe/

12.1 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Responsable de la EC del CNL es el encargado de la autorización de la publicación de la CPS y es responsable de asegurar la integridad y disponibilidad de la información publicada en:

www.notarios.org.pe

12.2 PLAZO O FRECUENCIA DE LA PUBLICACIÓN

Certificado Raíz

El certificado raíz se publicará y permanecerá en la página Web de la EC del CNL durante todo el tiempo en que se estén prestando servicios de certificación digital.

Certificado de EC Subordinada

El certificado de la EC Subordinada se publicará y permanecerá en la página Web de la EC del CNL durante todo el tiempo en que se estén prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

El CNL publicará en la página Web, la lista de certificados revocados en los eventos y con la periodicidad definidas en la sección Frecuencia de emisión de las CRLs.

Declaración de Prácticas de Certificación (CPS)

Con autorización del Responsable de la EC del CNL y el INDECOPI, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados al INDECOPI y publicados en la página Web de la Entidad de Certificación del CNL junto con la nueva versión. La Auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

12.3 CONTROLES DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad del CNL que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas al CNL.

13 IDENTIFICACIÓN Y AUTENTICACIÓN

13.1 NOMBRES

13.1.1 TIPOS DE NOMBRES

Todos los certificados contienen un nombre diferenciado de la organización y/o persona, identificados en el certificado, definido de acuerdo con lo previsto en la Recomendación ITU-TX.501 y contenido en el campo *Subject Name*.

Los certificados contienen nombres alternativos de las personas y organizaciones identificadas en los certificados, principalmente en el campo *Subject Alternative Name*.

Las circunstancias personales y atributos de las personas y organizaciones identificadas en los certificados se incluyen en atributos predefinidos en normas y especificaciones técnicas ampliamente utilizadas en el sector o sectores de actividad donde deban emplearse los certificados, así como en atributos definidos de forma específica por la ANCERT, principalmente en el campo *Subject Director y Attributes.*

La descripción de los Distinguished Name (DN) para cada tipo de certificado cubiertos por esta CPS, están detallados en la Política de Certificación.

13.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

Los nombres de los certificados son comprensibles e interpretados de acuerdo con la legislación aplicable a los nombres de las personas físicas y jurídicas titulares de los certificados, según se indica en el componente Country del nombre.

Los nombres incluidos en los certificados son tratados de acuerdo con las siguientes normas:

- Se codifica el nombre tal y como aparece en la documentación acreditativa.

- Se pueden eliminar los acentos, para garantizar la mayor compatibilidad técnica posible.

- Los nombres pueden ser adaptados y reducidos, al objeto de garantizar el cumplimiento de los límites de longitud aplicables a cada campo del certificado.

13.1.3 ANONIMATO Y SEUDOANONIMATO DE LOS TITULARES

En el caso de Certificados Notariales no se emiten certificados anónimos.

El uso de seudónimos únicamente está permitido en los Certificados Notariales de Facturación Electrónica.

13.1.4 LONGITUD MÁXIMA DE LOS CAMPOS

La ANCERT, como prestador de servicios del CNL, emplea los siguientes esquemas de nombres, para la longitud máxima de los campos:

Componente del nombre	X.520	RFC 5280
Common Name	64	64
Country Name	04	02
Locality Name	128	128
Name	128	?
Given Name	?	16
Surname	64	40
Title	64	64
Organization Name	64	64
Organizational Unit Name	64	32
Serial Number	64	64
State Or Province Name	128	128
Pseudonym	128	128

13.1.5 SINGULARIDAD DE LOS NOMBRES

El DN de los certificados digitales emitidos es único.

13.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS RECONOCIDAS.

La ANCERT, como prestador de servicios del CNL, no está obligada a recopilar o solicitar evidencia en relación con la posesión o titularidad de marcas registradas u otros signos distintivos antes de la emisión de los certificados. Esta política se extiende al uso y empleo de nombres de dominio.

14 VALIDACIÓN INICIAL DE LA IDENTIDAD

14.1 MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA

Esta sección describe los métodos a emplear para demostrar que se posee la clave privada correspondiente a la clave pública objeto de certificación.

El método de demostración de posesión de la clave privada será PKCS #10, otra prueba criptográfica equivalente o cualquier otro método fiable aprobado por la ANCERT.

Este requisito no se aplica cuando el par de claves es generado por la Entidad de Registro, por delegación del suscriptor, durante el proceso de personalización o de entrega del dispositivo seguro de creación de firma al suscriptor o poseedor de claves.

En este caso, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del dispositivo seguro y del correspondiente certificado y par de claves almacenados en su interior.

14.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA)

Los procedimientos de autenticación de la identidad de una persona jurídica son descritos en el documento de Declaración de Prácticas de Registro o Verificación del CNL – RPS.

No obstante a lo anterior, el CNL y la ANCERT, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

14.3 AUTENTICACIÓN DE UNA IDENTIDAD INDIVIDUAL (PERSONA NATURAL)

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en el documento de Declaración de Prácticas de Registro o Verificación del CNL – RPS.

No obstante a lo anterior, el CNL y la ANCERT, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

14.4 INFORMACIÓN DE TITULAR NO VERIFICADA

Bajo ninguna circunstancia el CNL omitirá las labores de verificación que conduzcan a la identificación del Titular y que se traduce en la solicitud de exhibición de los documentos mencionados para organizaciones y personas naturales.

14.5 CRITERIOS PARA LA INTEROPERABILIDAD

El CNL únicamente emitirá certificados a EC Subordinadas, que estén directamente vinculadas y operadas por proveedores autorizados por el CNL.

15 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES

15.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE-EMISIÓN DE RUTINA

La EC del CNL no realiza el servicio de re-emisión de certificados.

15.2 IDENTIFICACIÓN Y AUTENTICACIÓN TRAS UNA REVOCACIÓN

Debido a que una revocación implica la expedición de un nuevo certificado, el CNL realiza un nuevo proceso de autenticación del solicitante.

Los procedimientos de autenticación son descritos en el documento de Declaración de Prácticas de Registro o Verificación del CNL– RPS.

16 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

La ANCERT, como prestador de servicios del CNL, atiende las peticiones de revocación de conformidad con las causales de revocación especificadas en la sección Circunstancias para la revocación de un certificado en esta CPS y autentica la identidad de quien solicita la revocación del certificado.

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en el documento de Declaración de Prácticas de Registro o Verificación CNL – RPS.

16.1 VALIDACIÓN PARA LA RE-EMISIÓN RUTINARIA DE CERTIFICADOS

La EC del CNL no realiza el servicio de re-emisión de certificados.

16.2 VALIDACIÓN PARA LA RENOVACIÓN DE CERTIFICADOS TRAS LA REVOCACIÓN

No resulta aplicable, debido a que el CNL no renueva en ningún caso certificados que han sido revocados.

16.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN

La ANCERT, como prestador de servicios del CNL, autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada, mediante los siguientes métodos:

- Presencialmente ante Notario, cumpliendo los mismos requisitos que para la solicitud de emisión de certificado, en cuanto a la identificación y la titularidad del certificado a revocar.

- Mediante la firma digital válida de la solicitud de revocación realizada con el certificado a revocar, previa autorización contractual del suscriptor o titular.

17 REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS

17.1 SOLICITUD DEL CERTIFICADO

Antes de la emisión y entrega de un certificado, existe una solicitud de certificado, a instancia de parte interesada.

Existen los siguientes tipos de solicitudes:

1) Pre-solicitud, que consiste en una solicitud, electrónica o presencial, de un certificado (no contiene clave pública, ni se encuentra firmada digitalmente).

2) Solicitud, que se realiza presencialmente, y que en todo caso produce una petición técnica y electrónica de certificado por la entidad de registro, con generación de claves o sobre una clave pública aportada por el solicitante PKCS#10 o mecanismo compatible, con la clave pública del usuario y su firma digital, al objeto de demostrar la posesión dela clave privada.

17.2 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Están legitimados para solicitar la emisión de un certificado:

1) El futuro suscriptor que sea persona física.

2) El representante de una persona jurídica, incluyendo un órgano colegiado de una entidad, mediante la actuación de todos los miembros del mismo.

Adicionalmente, cuando el solicitante sea un representante de la persona jurídica que solicita certificados para otras personas físicas, comparece ante el Operador de Registro, identificando a las personas físicas que vayan a resultar identificadas en los certificados y que ostentarán la condición de poseedores de claves.

Los certificados se solicitarán para estos, en función del ámbito de representación que tengan previamente concedido en los documentos públicos de los que resulte su representación, y dentro de las facultades de delegación de facultades que ostente la persona que actúe como solicitante.

Las facultades de representación que recojan directa o indirectamente los certificados tienen que corresponderse, como máximo, con las que ostenten los solicitantes en los documentos públicos de los que traigan causa.

En la concesión, el Operador de Registro comprueba, igualmente, que el Solicitante actuó como representante de la persona jurídica poderdante en el momento de otorgarse el apoderamiento en virtud del cual se concede el certificado. La recepción del certificado tiene que realizarse, necesariamente, por el poseedor de claves, y debe constar por diligencia en la póliza que documente el registro de la emisión.

17.3 PROCESO DE REGISTRO Y RESPONSABILIDADES

La fase de solicitud del certificado comprende con carácter general la personación ante un Operador de Registro, para la comprobación y confirmación de la identidad personal del solicitante, así como la aportación de la documentación que corresponda, la cumplimentación de formularios, y suscripción de los contratos que se establezcan.

Durante esta fase, el Operador de Registro asegura que las solicitudes de certificado son completas, precisas y están debidamente autorizadas, e informa al suscriptor o al poseedor de claves, según proceda, de los términos y condiciones aplicables al certificado.

La citada información se comunica en soporte duradero, en papel o electrónicamente y en lenguaje fácilmente comprensible.

A la solicitud se acompaña la documentación justificativa de la identidad y otras circunstancias del solicitante, del futuro suscriptor y del poseedor de claves, según proceda.

También se acompaña una dirección física, u otros datos, que permiten contactar al solicitante, al futuro suscriptor y al poseedor de claves, según proceda.

18 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

18.1 REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Las funciones de autenticación y verificación de la identidad del solicitante son realizadas por el CNL en calidad de Entidad de Registro, encargada de autorizar la emisión

del certificado, quien comprueba si la información suministrada es auténtica y si la documentación anexa cumple con los requisitos definidos para cada tipo de certificado de acuerdo con su documento RPS.

18.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

Si una vez verificada la identidad del solicitante, la información suministrada cumple con los requisitos establecidos por esta CPS, se aprueba la solicitud. Si no es posible la identificación plena de la identidad del solicitante o no existe autenticidad plena de la información suministrada, se niega la solicitud y no se emite el certificado. El CNL no asume ninguna responsabilidad por las consecuencias que puedan derivarse de la no aprobación de la emisión de un certificado digital y así lo acepta y reconoce el solicitante al que le haya sido negada la expedición del respectivo certificado.

Igualmente, el CNL se reserva el derecho de no emitir certificados a pesar que la identificación del solicitante y/o la información suministrada por este haya sido plenamente autenticada, cuando la emisión de un certificado en particular por razones de orden legal y/o de conveniencia comercial, buen nombre o reputación de EC del CNL pueda poner en peligro el sistema de certificación digital.

En caso que una solicitud sea aprobada por la ER, se realizará lo siguiente:

- Se comunicará a la EC su aprobación para la emisión del certificado. Para ello se deben implementar los mecanismos de seguridad necesarios para establecer una comunicación segura entre la EC y la ER durante el proceso de emisión del certificado y generación del par de claves.
- La ER del CNL requerirá al suscriptor la firma de un contrato de conformidad personal de dichas responsabilidades, así como de conformidad por parte de los titulares en cuyo nombre actúa el suscriptor.

18.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

El plazo para la aprobación de una solicitud por parte de la ER del CNL, es de tres (3) días hábiles desde el momento de recibir la documentación e información completa. El tiempo de entrega del certificado digital una vez recibida la solicitud completa es de cinco (5) días hábiles.

19 EMISIÓN DE CERTIFICADOS

19.1 ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS

Para la emisión de un certificado el Operador de Registro (OR), actuando como Entidad de Registro, debe acceder a la aplicación de emisión de certificados. El acceso a la aplicación está protegido, identificando al OR mediante su certificado digital. La aplicación

comprueba que el OR, una vez autenticado, está autorizado para emitir certificados notariales. De esta forma se asegura que la comunicación entre la RA y la CA se lleva a cabo de forma segura.

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado. Las acciones a seguir para la emisión de las claves y el certificado son distintas, según si el soporte para su almacenamiento es una tarjeta criptográfica o bien un módulo de maquinaria de seguridad o una aplicación informática.

En todos los casos, ANCERT como proveedor de servicios del CNL:

- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.

- Protege la confidencialidad e integridad de los datos de registro, especialmente en caso de que sean intercambiados electrónicamente con el solicitante, durante la pre-solicitud.

- Indica la fecha y la hora en que se expide el certificado.

- En los casos en que el CNL aporta el dispositivo seguro de creación de firma, como la tarjeta criptográfica, emplea un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al solicitante o al poseedor de claves, según proceda.

- Utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

- Asegura que el certificado es emitido por sistemas que utilizan protección contra falsificación y, cuando genera claves privadas, que garantizan la confidencialidad de las claves durante el proceso de generación de dichas claves.

19.1.1. EMISIÓN EN TARJETA CRIPTOGRÁFICA

Las acciones a seguir son las siguientes:

1. El OR introduce en el lector de tarjetas su tarjeta criptográfica con el certificado que le autentica como Entidad de Registro y accede a la aplicación de registro.

2. Una vez autenticado, el OR introduce en el lector de tarjetas la tarjeta criptográfica del poseedor de claves, que previamente le ha sido entregada por el citado OR junto a los códigos PIN y PUK correspondientes en sobre cerrado.

3. El OR completa el formulario de registro con los datos que le debe aportar el solicitante y solicita la emisión del certificado.

4. En este momento, la aplicación de registro solicita el PIN correspondiente a la tarjeta criptográfica del solicitante, para activar el procedimiento de generación de claves.

5. En ese momento se genera el par de claves en la tarjeta criptográfica del suscriptor, enviando la petición a la ANCERT, la cual genera el certificado y lo remite al ordenador del OR vía SSL, quedando almacenado automáticamente en la tarjeta criptográfica del suscriptor.

19.1.2. EMISIÓN EN MÓDULO DE MAQUINARIA DE SEGURIDAD O EN APLICACIÓN INFORMÁTICA

Las acciones a seguir para la emisión en este soporte son las siguientes:

1. El solicitante debe presentar al OR el archivo en formato PKCS10 que contiene la petición de certificado.

2. El OR procede a introducir en el lector de tarjetas su tarjeta criptográfica con el certificado que le autentica como OR autorizado a emitir Certificados Notariales y accede a la aplicación de registro.

3. El OR comprueba, mediante las herramientas que le proporciona la ANCERT, que el archivo facilitado por el solicitante corresponde con la información aportada y el perfil del certificado.

4. Si los datos son correctos completa el formulario de petición de certificado y envía la petición a la ANCERT.

5. En un plazo máximo de 48 horas, el solicitante puede obtener su Certificado descargándolo de la dirección:

www.ancert.com.

19.2 NOTIFICACIÓN AL SOLICITANTE POR LA EC DE LA EMISIÓN DEL CERTIFICADO

La ANCERT, en calidad de proveedor de servicios del CNL, notifica en el acto de emisión o posteriormente la emisión del certificado al suscriptor o, en su caso, al poseedor de claves.

En certificados de sistemas o certificados de otros tipos emitidos a claves generadas en dispositivos seguros que estuvieran previamente en poder del solicitante, se notifica que el certificado se encuentra disponible en un plazo máximo de 48 horas, y que el solicitante puede obtener su Certificado Notarial descargándolo de la dirección:

www.ancert.com

20 ACEPTACIÓN DEL CERTIFICADO

20.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

La aceptación del certificado por parte del suscriptor se entiende producida desde el momento de su emisión y entrega al mismo por la ANCERT y firma ante el OR del correspondiente contrato.

Al aceptar el certificado el suscriptor también acepta además las normas de uso y las condiciones contenidas en la presente Declaración de Prácticas de Certificación.

En todo caso, al aceptar un Certificado emitido por el CNL, el suscriptor del mismo declara:

a) Que toda la información entregada durante el procedimiento de solicitud del certificado es verdadera.

b) Que el certificado será usado exclusivamente para fines legales y autorizados por el CNL, de acuerdo a la presente Declaración de Prácticas de Certificación y siempre dentro del ámbito determinado en cada Política de Certificación.

c) Que asegura su exclusivo control sobre los Datos de creación de Firma que se correspondan con los Datos de verificación de Firma incluidos en su certificado emitido por

la ANCERT y vinculados a su identidad personal, lo que en todo caso y a título meramente enunciativo, incluirá las acciones y medidas necesarias para prevenir su pérdida, revelación, modificación, o uso por tercero distinto del suscriptor.

El CNL considera válido todo certificado aceptado por el suscriptor y publicado en su Depósito de Certificados correspondiente, siempre que no haya caducado y que no conozca ninguna causa de revocación que le afecte.

20.2 PUBLICACIÓN DEL CERTIFICADO POR LA EC

Una vez emitido el certificado, la ANCERT publica automáticamente una copia del mismo en el Depósito de Certificados correspondiente.

20.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES

El CNL no notifica la emisión de certificados a terceros.

21 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO

21.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR

El titular del certificado emitido y de la clave privada asociada acepta las condiciones de uso establecidas en esta CPS por el solo hecho de haber solicitado la emisión del certificado y solo podrá emplearlos para los usos explícitamente mencionados y autorizados en la presente CPS y de acuerdo con lo establecido en los campos "Extended Key Usage" de los certificados. Por consiguiente, los certificados emitidos y la clave privada no deberán ser usados en otras actividades que estén por fuera de los usos mencionados. Una vez perdida la vigencia del certificado, el titular está obligado a no seguir usando la clave privada asociada al mismo. Con base en lo anterior, desde ya acepta y reconoce el titular, que en tal sentido será el único responsable por cualquier perjuicio pérdida o daño que cause a terceros por el uso de la clave privada una vez expirada la vigencia del certificado. El CNL no asume ningún tipo de responsabilidad por los usos no autorizados.

El titular o suscriptor deberá notificar a la EC o ER del CNL los siguientes casos:

1. La pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador, token criptográfico o tarjeta inteligente).
2. El compromiso potencial de su clave privada.
3. La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
4. Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

Asimismo, el titular y suscriptor deberán dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado.

21.1.1 OBLIGACIONES DEL SUSCRIPTOR Y EN SU CASO, POSEEDOR DE CLAVES

El CNL obliga al suscriptor, mediante las condiciones generales de emisión, a:

- En caso que el suscriptor genere sus propias claves, a:

  a) Generar sus claves de suscriptor empleando un algoritmo reconocido como aceptable para la firma electrónica reconocida.

  b) Crear las claves dentro del dispositivo seguro de creación de firma.

  c) Emplear longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica reconocida.

- Facilitar a la EC del CNL y a sus entidades de registro información completa y adecuada, en especial en lo relativo al procedimiento de registro.

- Manifestar su consentimiento previo a la emisión y entrega de un certificado, así como a su publicación en el Depósito y cuando, proceda, a la notificación de la emisión a terceros.

- Cumplir las obligaciones que se establecen para el suscriptor en la presente Declaración de Prácticas de Certificación.

- Emplear el certificado de acuerdo con lo establecido en esta Declaración de Prácticas de Certificación.

- Ser diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, no cediendo el uso de la clave privada a ninguna otra persona.

- Comunicar a la ANCERT y a cualquier persona que el suscriptor o el poseedor de claves crea que pueda confiar en el certificado, sin retrasos injustificables:

  a) La pérdida, el robo o el compromiso potencial de su clave privada o del dispositivo seguro.

  b) La pérdida de control sobre su clave privada o del dispositivo seguro, debido al compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo seguro de creación de firma) o por cualquier otra causa.

  c) Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor o el poseedor de claves.

- Dejar de emplear la clave privada transcurrido el periodo de vigencia.

- Transferir a los poseedores de claves las obligaciones específicas de los mismos.

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la ANCERT ni del CNL, sin permiso previo por escrito.

- No comprometer intencionadamente la seguridad de los servicios de certificación de la ANCERT ni del CNL, sin permiso previo por escrito.

El suscriptor del certificado de firma electrónica que genere firmas digitales empleando la clave privada correspondiente a su clave pública listada en el certificado reconoce, en el debido documento jurídico, que tales firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas.

21.1.2 RESPONSABILIDAD CIVIL DEL SUSCRIPTOR DE CERTIFICADO

El CNL obliga al suscriptor y, en su caso, al poseedor de claves, mediante las condiciones generales de emisión, a garantizar:

- En caso de que el suscriptor fuese el solicitante del certificado, 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 esta Declaración de Prácticas de Certificación.

- Que cada firma digital creada empleando la clave pública listada en el certificado es la firma digital del suscriptor y que el certificado ha sido aceptado y se encuentra operativo (no ha expirado ni ha sido revocado) en el momento de creación de la firma.

- 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 a título de prestador de servicios de certificación ni en ningún otro caso.

- Que sólo creará firmas digitales mientras tenga la seguridad que ninguna persona no autorizada ha tenido jamás acceso a su clave privada.

- Que el suscriptor es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada y, en su caso, de generar correctamente dicha clave y emplear un dispositivo seguro de firma.

21.2 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

21.2.1 OBLIGACIONES DEL TERCERO QUE CONFÍA EN CERTIFICADOS

El CNL obliga al tercero que confía en certificados, mediante las condiciones generales de uso, a:

- 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 ANCERT ni del CNL sin permiso previo por escrito.

- No comprometer intencionadamente la seguridad de los servicios de certificación de la ANCERT ni del CNL, sin permiso previo por escrito.

- En relación con los certificados que permiten la firma electrónica, reconocer que las firmas electrónicas válidamente verificadas con los certificados son firmas electrónicas equivalentes a firmas manuscritas.

21.2.2 RESPONSABILIDAD CIVIL DEL TERCERO QUE CONFÍA EN CERTIFICADOS

La ANCERT, como prestador de servicios del CNL, obliga al tercero que confía en el certificado, mediante las condiciones generales de uso, a reconocer:

- 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.

22 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

El CNL y la ANCERT, no atiende requerimientos de renovación de un certificado sin cambio de claves.

23 MODIFICACIÓN DE CERTIFICADOS

Los certificados digitales emitidos por la ANCERT como proveedor de servicios del CNL, no pueden ser modificados. A cambio el titular debe solicitar la emisión de uno nuevo. En este evento y por una única vez se expedirá nuevo certificado al titular sin costo adicional de la emisión, por el tiempo faltante para el vencimiento original, cobrando solamente el valor del dispositivo criptográfico si a ello hubiere lugar.

La modificación de certificados se trata como una nueva emisión de certificado.

24 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

24.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

El titular reconoce y acepta que los certificados deben ser revocados cuando ocurra cualquiera de las siguientes circunstancias:

- Circunstancias que afectan a la información contenida en el certificado:
  a) Modificación de alguno de los datos contenidos en el certificado.
  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.
- Circunstancias que afectan a la seguridad de la clave o del certificado:
  a) Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad 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 ANCERT, 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 del suscriptor o del poseedor de claves.
  d) Acceso o utilización no autorizados, por un tercero, de la clave privada del suscriptor o del poseedor de claves.
  e) El uso irregular del certificado por el suscriptor o del poseedor de claves, o la falta de diligencia en la custodia de la clave privada.
- Circunstancias que afectan a la seguridad del dispositivo criptográfico:
  a) Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
  b) Pérdida o inutilización por daños del dispositivo criptográfico.
  c) Acceso no autorizado, por un tercero, a los datos de activación del suscriptor o del poseedor de claves.
- Circunstancias que afectan al suscriptor o al poseedor de claves:
  a) Finalización de la relación jurídica entre la ANCERT, el CNL y el suscriptor.
  b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor o del poseedor de claves.
  c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
  d) Infracción por el suscriptor o del poseedor de claves, de sus obligaciones, responsabilidad y garantías, establecidas en las condiciones generales de emisión correspondientes o en esta Declaración de Prácticas de Certificación.
  e) La incapacidad sobrevenida o el fallecimiento del suscriptor o del poseedor de claves.
  f) En caso de certificados de colectivo, 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 poseedor de claves.
  g) Solicitud del suscriptor de revocación del certificado.
- Otras circunstancias:

a) La modificación de la Declaración de Prácticas de Certificación que no sea aceptada por el suscriptor del certificado.
b) La terminación del servicio por la ANCERT.

Si la entidad a la que se dirige la solicitud de revocación no dispone de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso, puede decidir su suspensión.

- Uso indebido de la clave privada del titular de conformidad con lo expuesto en la CPS.
- Por orden judicial o de entidad administrativa competente.
- Por incumplimiento en el pago de los valores por los servicios de certificación, acordados entre el solicitante y el Colegio de Notarios de Lima.
- Por revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Por decisión de la legislación respectiva.

No obstante, las causales anteriores, el Colegio de Notarios de Lima, también podrá revocar certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial, buen nombre de EC del Colegio de Notarios de Limay/o idoneidad legal o moral de todo el sistema de certificación.

24.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

El titular, un Tercero que confía o cualquier persona interesada cuando tenga constancia demostrable de conocimiento de hechos y causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta CPS y que comprometan la clave privada:

- El titular o suscriptor del certificado.
- La EC que emitió el certificado.
- Un juez que de acuerdo a la Ley decida revocar el certificado.
- Un tercero que tenga pruebas fehacientes del uso indebido del certificado, el compromiso de clave u otro motivo de revocación mencionado en la Ley, los reglamentos de acreditación y el presente documento

24.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

La entidad que precise revocar un certificado debe solicitarlo a la ANCERT, al CNL o, en su caso, a cualquier entidad de registro de las autorizadas, comprensiva de la siguiente información:

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

24.4 PERIODO DE GRACIA DE SOLICITUD DE REVOCACIÓN

Previa validación de la autenticidad de una solicitud de revocación, ANCERT como proveedor del servicio brindado para el CNL, procederá en forma inmediata con la revocación solicitada, dentro de los horarios de oficina de este. En consecuencia, no existe un periodo de gracia que permita al solicitante cancelar la solicitud. Si se trató de una falsa alarma, el titular debe solicitar un certificado nuevo, pues el certificado revocado perdió su validez inmediatamente fue validada la solicitud de revocación.

24.5 PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

La solicitud de revocación de un certificado digital debe ser atendida con la máxima urgencia, sin que su revocación tome más de 24 horas una vez validada la solicitud.

24.6 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

Los terceros que confían en certificados 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 Entidad de Certificación del CNL.

El CNL y ANCERT suministran información a los terceros que confían en certificados acerca de cómo y dónde encontrar la Lista de Revocación de Certificados correspondiente; entre otros métodos, mediante la inclusión de la dirección web de publicación de las listas dentro de los propios certificados emitidos.

24.7 FRECUENCIA DE EMISIÓN DE LAS CRLS

El CNL, a través del proveedor de servicios ANCERT, emite una nueva CRL al menos cada 24 horas. Adicionalmente, se emitirá una nueva CRL en un periodo de tiempo no superior a 15 minutos después de la suspensión o revocación de un certificado.

Se indica en la CRL el momento programado de emisión de una nueva CRL, si bien se puede emitir una CRL antes del plazo indicado en la CRL anterior.

Los certificados revocados que expiran son retirados de la CRL transcurridos sesenta días desde su expiración.

24.8 TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS

De forma alternativa, los terceros que confían en certificados pueden consultar su estado en el Depósito de certificados de la ANCERT, que se encuentra disponible las 24 horas de los 7 días de la semana, en la dirección web:

http://pki.notarios.org.pe/crl/CACNL.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control del CNL, este realizará sus mejores esfuerzos para asegurar que este servicio se mantenga inactivo el mínimo tiempo posible.

24.9 REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ON-LINE

Para obtener la información del estado de revocación de un certificado en un momento dado, se puede hacer la consulta en línea en la dirección:

http://pki.notarios.org.pe/ocsp

Para lo cual se debe contar con un software que sea capaz de operar con el protocolo RFC2560.

24.10 REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS

El compromiso de la clave privada de una Entidad de Certificación de la Clase Notariales se notifica, en la medida de lo posible, a todos los participantes en los servicios de certificación del Colegio de Notarios de Lima y a los Notarios participantes.

Dicha notificación se produce, al menos, mediante la publicación de la información en el Depósito de la Agencia Notarial de Certificación.

24.11 NOTIFICACIÓN DE LA REVOCACIÓN DE UN CERTIFICADO

El suscriptor cuyo certificado haya sido revocado debe ser informado de dicho hecho, así como, en su caso, del levantamiento de la suspensión, por lo que la ANCERT, como prestador de servicios del CNL, notificará dicha información por correo electrónico o postal o incluso por teléfono cuando no haya sido posible la notificación en alguna de las dos formas anteriores.

No obstante, lo dispuesto en el párrafo anterior, la notificación se entenderá debidamente cumplida cuando haya sido realizada por correo electrónico a la dirección que aparezca en el certificado y que, por tanto, habrá sido admitida previamente por el usuario del certificado.

Si no obstante el sistema produjera un mensaje de error o rechazara la comunicación, se entenderá que la ANCERT ha cumplido suficientemente la notificación cuando esta haya sido sellada. A fin de justificar ulteriormente el cumplimiento de la debida diligencia, la ANCERT conservará durante quince (15) años el comprobante electrónico de haber realizado la comunicación de la revocación o suspensión.

La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá accesible en el directorio de Listas de Revocación de Certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

25 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

25.1 CARACTERÍSTICAS OPERACIONALES

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, a través del Depósito de los certificados, y a través del servicio OCSP.

25.2 DISPONIBILIDAD DEL SERVICIO

Los servicios de comprobación de estado de certificados se encuentran disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

25.3 FINALIZACIÓN DE LA VIGENCIA DE UN CERTIFICADO

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

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, en los casos y con la antelación que determina esta Declaración de Prácticas de Certificación.

26 CUSTODIA Y RECUPERACIÓN DE CLAVES

26.1 ALMACENAMIENTO DE LA CLAVE PRIVADA DEL TITULAR

La ANCERT, como prestador de servicios del CNL, no deposita ni puede recuperar claves de suscriptores o poseedores de claves, con excepción de las claves de los certificados de cifrado, que se encuentran depositadas en la ANCERT, con controles de seguridad apropiados que impiden su acceso no autorizado por terceras personas.

Las claves de cifrado sólo se pueden recuperar a solicitud de la persona física identificada en el certificado, y en caso de mandamiento judicial, mediante el correspondiente procedimiento implantado por la ANCERT.

27 CONTROLES FÍSICOS DE LA INSTALACION, GESTIÓN Y OPERACIONALES

27.1 CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA A TRAVÉS DE LA ANCERT COMO PRESTADOR DE SERVICIOS DEL CNL

27.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

La ANCERT, como prestador de servicios del CNL, debe disponer de instalaciones que protejan físicamente la prestación de, al menos, los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos.

La protección física se logrará mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación. La parte de las instalaciones compartida con otras organizaciones debe encontrarse fuera de estos perímetros.

La ANCERT establecerá 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.

La política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación deberá establecer prescripciones para las siguientes contingencias, que se documentarán sucintamente en la Declaración de Prácticas de Certificación:

- 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 antirrobos.

- Allanamiento y entrada no autorizada.

- Recuperación del desastre.

- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

27.1.2 ACCESO FÍSICO

La ANCERT deberá establecer al menos cuatro (4) niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias del prestador de servicios de certificación donde se lleven a cabo procesos relacionados con el ciclo de vida del certificado, será necesaria la autorización previa, identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Esta identificación, ante el sistema de control de accesos, deberá realizarse mediante reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.

La generación de claves criptográficas de las Entidades de Certificación, así como su almacenamiento, deberá realizarse en dependencias específicas para estos fines, y requerirán de acceso y permanencia duales.

27.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Los equipos informáticos del prestador de servicios de certificación deberán estar convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.

Las instalaciones contarán con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener el suministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas informáticos.

Los equipos informáticos deberán estar ubicados en un entorno donde se garantice una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

27.1.4 EXPOSICIÓN AL AGUA

La ANCERT deberá disponer de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad, en el caso de que las condiciones de ubicación de las instalaciones lo hagan necesario.

27.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Todas las instalaciones y activos de la ANCERT deben contar con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos, y soportes que almacenen claves de los prestadores de servicios de certificación, deberán contar con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

27.1.6 SISTEMA DE ALMACENAMIENTO

El almacenamiento de soportes de información debe realizarse de forma que se garantice tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se haya establecido.

Deberá contarse para ellos con dependencias o armarios ignífugos.

El acceso a estos soportes, incluso para su eliminación, deberá estar restringido a personas específicamente autorizadas.

27.1.7 ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

La eliminación de soportes, tanto papel como magnéticos, se deberá realizar mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procederá al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, este deberá someterse a un tratamiento físico de destrucción.

27.1.8 BACKUP FUERA DE LA INSTALACIÓN

Periódicamente, la ANCERT almacenará copia de respaldo de los sistemas de información, en dependencias físicamente separadas de aquellas en las que se encuentran los equipos.

27.2 CONTROLES DE PROCEDIMIENTO

27.2.1 ROLES DE CONFIANZA

La ANCERT deberá identificar, en su política de seguridad, funciones o roles con la condición de fiables.

Las personas que deban ocupar tales puestos deberán ser formalmente nombrados por la alta dirección del prestador de servicios de certificación.

Las funciones fiables deberán incluir:

- Personal responsable de la seguridad.
- Administradores del sistema.
- Operadores del sistema.
- Auditores del sistema.

27.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Las funciones fiables identificadas en la sección anterior y en la política de seguridad, y sus responsabilidades asociadas, serán documentadas en descripciones de puestos de trabajo, y descritas de forma sucinta en la Declaración de Prácticas de Certificación correspondiente.

Dichas descripciones deberán realizarse teniendo en cuenta que debe existir una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando sea posible.

Para determinar la sensibilidad de la función, se tendrán en cuenta los siguientes elementos:

- Deberes asociados a la función.
- Nivel de acceso.
- Monitorización de la función.

- Formación y concienciación.
- Habilidades requeridas.

27.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

La ANCERT deberá identificar y autenticar al personal antes de acceder a la correspondiente función fiable.

27.2.4 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Las siguientes tareas deberán ser realizadas, al menos, por dos personas:

- Gestión del acceso físico.
- Gestión de aplicaciones informáticas del prestador.
- Gestión de configuración y control de cambios.
- Gestión del archivo.
- Gestión de bienes de equipo criptográfico.
- Generación de certificados de autoridad de certificación.

27.3 CONTROLES DE PERSONAL

27.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

La ANCERT, en calidad de prestador de servicios del CNL, deberá emplear personal cualificado y con la experiencia necesaria, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

Este requisito se aplicará al personal de gestión, especialmente en relación con procedimientos de personal de seguridad.

La calificación y la experiencia podrán suplirse mediante una formación y entrenamiento apropiados.

El personal en puestos fiables deberá encontrarse libre de intereses personales que entre en conflicto con el desarrollo de la función que tenga encomendada.

No se podrá asignar a un puesto fiable o de gestión a una persona que no sea idóneo para el puesto, especialmente por haber sido condenada por delito o falta que afecte a su idoneidad para el puesto. Por este motivo, se deberá realizar una investigación, de acuerdo con lo establecido en la sección siguiente, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación de que realmente se hizo el trabajo alegado.
- Morosidad.
- Hasta donde lo permite la legislación vigente, antecedentes penales.

27.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

La ANCERT deberá realizar la investigación antes de que la persona sea contratada y/o acceda al puesto de trabajo.

En la solicitud para el puesto de trabajo se informará acerca de la necesidad de someterse a una investigación previa.

Se deberá advertir de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

Se deberá obtener consentimiento inequívoco del afectado por la investigación previa y procesar y proteger todos sus datos personales de acuerdo con la LOPD y su Reglamento de desarrollo. La investigación se repetirá cada tres años.

27.3.3 REQUISITOS DE FORMACIÓN

La ANCERT deberá formar al personal en puestos fiables y de gestión, hasta que alcancen la calificación necesaria.

La formación deberá incluir los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.

- Versiones de maquinaria y aplicaciones en uso.

- Tareas que debe realizar la persona.

- Gestión y tramitación de incidentes y compromisos de seguridad.

- Procedimientos de continuidad de negocio y emergencia.

27.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

La ANCERT deberá realizar una actualización en la formación del personal al menos cada dos años.

27.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

La ANCERT podrá establecer métodos de rotación laboral para la prestación del servicio en turnos, con el objeto de cubrir las necesidades de 24x7 del servicio.

27.3.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS

La ANCERT deberá disponer de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, que deberá encontrarse adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias podrán incluir la suspensión y el despido de la persona responsable de la acción dañina.

27.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

La ANCERT podrá contratar profesionales para cualquier función, incluso para un puesto fiable, en cuyo caso deberá someterse a los mismos controles que los restantes empleados.

En el caso de que el profesional no deba someterse a tales controles, deberá estar constantemente acompañado por un empleado fiable, cuando se encuentre en las instalaciones de la ANCERT.

27.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

La ANCERT suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de que sea suficientemente competente a tenor de lo establecido.

27.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

27.4.1 TIPOS DE EVENTOS REGISTRADOS

La ANCERT, como prestador de servicios del CNL, debe guardar registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado de los sistemas.

- Inicio y terminación de la aplicación de autoridad de certificación o de autoridad de registro central.

- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.

- Generación y cambios en las claves de la Entidad de Certificación.

- Cambios en las políticas de emisión de certificados.

- Intentos de entrada y salida del sistema.

- Intentos no autorizados de entrada en la red de la Entidad de Certificación.

- Intentos no autorizados de acceso a los ficheros del sistema.

- Intentos fallidos de lectura en un certificado, y de lectura y escritura en el Depósito de certificados.

- Eventos relacionados con el ciclo de vida del certificado, como solicitud, emisión, revocación y renovación de un certificado.

- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.

La ANCERT debe también guardar, ya sea manual o electrónicamente, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.

- Los 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 o del poseedor de claves.

- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.

27.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

Los registros de auditoría se examinarán por lo menos una vez al mes en busca de actividad sospechosa o no habitual.

El procesamiento de los registros de auditoría consistirá en una revisión de los registros la cual incluye la verificación de que los registros 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 llevadas a cabo a partir de la revisión de auditoría también deben ser documentadas.

27.4.3 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

Los registros de auditoría se deben retener en el recinto durante por lo menos dos meses después de procesarlos y a partir de ese momento se archivarán.

27.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los ficheros de registros, tanto manuales como electrónicos, deben protegerse de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

27.4.5 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

Se deberán generar, al menos, copias incrementales de respaldo de registros de auditoría diariamente y copias completas semanalmente.

27.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

- Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría deberá ser, al menos, un sistema interno de la ANCERT, compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado.

27.4.7 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

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

Se podrá comunicar si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

27.4.8 ANÁLISIS DE VULNERABILIDADES

Los eventos en el proceso de auditoría deberán ser guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados a través de un examen de esos eventos monitorizados.

Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente de acuerdo con su definición en el plan de auditoría o documento que lo sustituya, de la ANCERT.

27.5 ARCHIVO DE REGISTROS

27.5.1 TIPOS DE EVENTOS ARCHIVADOS

La ANCERT, en calidad de prestador de servicios del CNL, debe guardar todos los eventos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación del mismo.

Se debe guardar un registro de lo siguiente:

- Tipo de documento presentado en la solicitud del certificado.

- Número de identificación único proporcionado por el documento anterior.

- Identidad de la entidad que procesa la solicitud de certificado.

- La ubicación de las copias de solicitudes de certificados y del documento firmado por el suscriptor o por el poseedor de las claves, según proceda.

27.5.2 PERIODO DE CONSERVACIÓN

La ANCERT debe guardar los registros especificados en la sección anterior de esta política de forma permanente, con un mínimo de quince (15) años.

27.5.3 PROTECCIÓN DE ARCHIVOS

La ANCERT debe:

- Mantener la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.

- Archivar los datos anteriormente citados de forma completa y confidencial.

- Mantener la privacidad de los datos de registro del suscriptor o del poseedor de las claves, según proceda.

27.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

La ANCERT debe realizar copias de respaldo incrementales diarias de todos sus documentos electrónicos. Debe, además, realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, debe guardar los documentos en papel, en un lugar fuera de las instalaciones de la propia ANCERT para casos de recuperación de datos.

27.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

La ANCERT debe emitir los certificados y las CRLs con información fiable de fecha y hora. No será necesario que esta información se encuentre firmada digitalmente.

27.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

La ANCERT debe disponer de un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones.

27.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA.

Solo personas autorizadas por la ANCERT podrán tener acceso a los datos de archivo, ya sea en las mismas instalaciones de la ANCERT o en su ubicación externa.

27.6 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

27.6.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

La ANCERT, como prestador de servicios del CNL, debe desarrollar, mantener, probar y, si es necesario, ejecutar un plan de emergencia para el caso de que ocurra un desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, el cual indique cómo restaurar los servicios de los sistemas de información.

La ANCERT debe restaurar los servicios críticos dentro de las 24 horas siguientes al desastre. Estos servicios son los siguientes:

- Revocación de certificados.

- Publicación de información de revocación de los certificados.

La ubicación de los sistemas de recuperación de desastres debe disponer de las protecciones físicas de seguridad detalladas en el plan de seguridad.

La base de datos de recuperación de desastres utilizada por la ANCERT debe estar sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el plan de seguridad.

Los equipos de recuperación de desastres deben tener las medidas de seguridad físicas especificadas en el plan de seguridad, equivalentes a las de las instalaciones principales.

27.7 CESE DE UNA EC O ER

27.7.1 ENTIDAD DE CERTIFICACIÓN

El CNL informará a todos los titulares, con una anticipación de treinta (30) días, sobre la terminación de su actividad o actividades, la fecha precisa de cesación y las consecuencias jurídicas de esta respecto de los certificados expedidos. Si por causas de fuerza mayor el servicio es suspendido temporalmente, el CNL informará al titular dentro de las veinticuatro (24) horas siguientes de ocurrido el incidente.

Los registros competentes de los certificados emitidos a los ciudadanos y empresas privadas serán mantenidos hasta ser cumplido el plazo de diez (10) años.

27.7.2 ENTIDAD DE REGISTRO O VERIFICACIÓN

En el caso de cese de actividades de la Entidad de Registro o Verificación, se debe informar con un (1) mes de anticipación tanto al INDECOPI como a los titulares, suscriptores y terceros que confían.

28 CONTROLES TÉCNICOS DE SEGURIDAD

28.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

28.1.1 GENERACIÓN DEL PAR DE CLAVES.

- **Generación del par de claves de la EC Raíz**

La ANCERT, como prestador de servicios del CNL, cuando actúe como Entidad de Certificación raíz, generará y firmará su propio par de claves y procederá a la generación de las claves de cada Entidad de Certificación subordinada, todo ello de acuerdo con la ceremonia de claves, dentro del perímetro de alta seguridad destinado específicamente a esta tarea.

Los pares de claves de las Entidades de Certificación (raíz o subordinadas) deben ser generados empleando hardware criptográfico que cumpla ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14167 partes 1 a 4, según proceda; o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes.

Los pares de claves de los suscriptores y de los operadores y administradores de las entidades de registro, deberán generarse siempre en dispositivos criptográficos que cumplan ISO 15408:

EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14167 partes 1 a 4, según proceda; o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes, excepto en el caso de los certificados de firma electrónica avanzada o de los certificados de sistemas. Dichos dispositivos seguros podrán ser tarjetas criptográficas, tokens USB criptográficos, o cualquier otro tipo de dispositivo, en especial maquinaria de seguridad (HSM), que cumpla con los requisitos de seguridad establecidos por la normativa vigente para los dispositivos seguros.

- **Generación del par de claves de las EC subordinadas de la ANCERT**

La generación del par de claves de las EC subordinadas de la ANCERT se realiza dentro de la sala criptográfica del proveedor de servicios de la ANCERT bajo el protocolo de ceremonia de generación de claves. Para el almacenamiento de la clave privada subordinada se utiliza un dispositivo criptográfico homologado FIPS 140-1 nivel 3 con control dual.

28.1.2 ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES

La clave privada del suscriptor o del poseedor de claves, deberá serle entregada debidamente protegida mediante un dispositivo criptográfico que cumpla lo establecido en ISO 15408: EAL 4+ (o superior), de acuerdo con lo establecido en CEN CWA 14169 o criterios de seguridad equivalentes, excepto en el caso de los certificados de firma electrónica avanzada o de los certificados de sistemas.

28.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública es enviada a la ANCERT, en calidad de prestador de servicios del CNL, como parte de la petición de solicitud del certificado digital en formato PKIX-CMP.

28.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA EC A TERCEROS ACEPTANTES

Las claves de las Entidades de Certificación deben ser comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen.

La clave pública de cada Entidad de Certificación se publicará en el Depósito, en forma de certificado autofirmado o firmado por otra Entidad de Certificación, junto a una declaración referente a que la clave autentica a la Entidad de Certificación.

Se deberán establecer medidas adicionales para confiar en los certificados autofirmados, como la comprobación de la huella digital del certificado.

Los usuarios podrán acceder al Depósito para obtener las claves públicas de las Entidades de Certificación.

Adicionalmente, en aplicaciones S/MIME, el mensaje de datos podrá contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

28.1.5 TAMAÑO DE LAS CLAVES

La longitud de las claves de las Entidades de Certificación será al menos de 4096 bits, mientras que la de los restantes tipos de certificados será de al menos 2048 bits.

28.1.6 PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

La ANCERT, como prestador de servicios del CNL, podrá establecer métodos de comprobación de la calidad de los parámetros de las claves públicas.

28.1.7 USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509)

La ANCERT, como prestador de servicios del CNL, deberá incluir la extensión *Key Usage* en todos los certificados, indicando los usos permitidos de las correspondientes claves privadas.

28.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

28.2.1 CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos utilizados en la creación de claves utilizadas por EC Raíz de la Entidad de Certificación del CNL cumplen los requisitos establecidos de acuerdo con FIPS 140-1 Nivel 3.

28.2.2 CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

El acceso a las claves privadas de las Entidades de Certificación, se deberá requerir necesariamente del concurso simultáneo de dos (2) dispositivos criptográficos protegidos por una clave de acceso, de entre cuatro (4) dispositivos.

La clave de acceso será conocida únicamente por una persona responsable de ese dispositivo.

Ninguna de ellas conocerá más que una de las claves de acceso.

Los dispositivos criptográficos quedarán almacenados en las dependencias del prestador de servicios de certificación, y para su acceso será necesaria una persona adicional.

28.2.3 CUSTODIA DE LA CLAVE PRIVADA

Únicamente se podrán custodiar copias de respaldo de las claves privadas de los certificados de entidad final cuyo uso exclusivo sea el cifrado.

No se custodian otras claves privadas de los suscriptores.

28.2.4 BACKUP DE LA CLAVE PRIVADA

La clave privada de las Entidades de Certificación deberá contar con una copia de respaldo realizada, almacenada en dependencia independiente de aquella donde se almacena habitualmente, y recuperada en su caso, por personal sujeto a la política de confianza del personal. Este personal debe ser expresamente autorizado a estos fines, y debe limitarse a aquel que necesite hacerlo.

Los controles de seguridad a aplicar a las copias de respaldo de las Entidades de Certificación deberán ser de igual o superior nivel a los que se aplican a las claves habitualmente en uso.

Cuando las claves se almacenen en un módulo hardware de proceso dedicado, deberán proveerse los controles oportunos para que estas nunca puedan abandonar el dispositivo.

28.2.5 ARCHIVO DE LA CLAVE PRIVADA

Las claves privadas de las Entidades de Certificación serán archivadas al final de su periodo de operación, de forma permanente.

No se archivarán claves privadas de firma electrónica de usuarios finales.

28.2.6 ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO

Las claves privadas se podrán generar directamente en los módulos criptográficos o en módulos criptográficos externos, de los que se exportarán las claves cifradas para su introducción en los módulos de producción.

Las claves privadas de las Entidades de Certificación quedarán almacenadas en ficheros cifrados con claves fragmentadas y en dispositivos criptográficos (de las que no podrán ser extraídas). Dichos dispositivos serán empleados para introducir la clave privada en el módulo criptográfico.

28.2.7 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de cada Entidad de certificación se activará mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección Control por más de una persona (n de m) sobre la clave privada.

La clave privada del suscriptor se activará mediante la introducción del PIN en el dispositivo criptográfico o aplicación de firma.

28.2.8 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Para certificados de firma digital, cuando se retire el dispositivo criptográfico del lector o se desconecte del ordenador, o la aplicación que lo utilice finalice la sesión, será necesaria nuevamente la introducción del PIN.

28.2.9 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

Las claves privadas serán destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

28.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

28.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Las Entidades de Certificación archivarán sus claves públicas de forma permanente.

28.3.2 PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES

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

Como excepción, la clave privada podrá continuar empleándose para el descifrado de documentos, incluso tras la expiración del certificado.

28.4 DATOS DE ACTIVACIÓN

28.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

En los casos en que la ANCERT facilita al suscriptor un dispositivo seguro de creación de firma, entonces los datos de activación del dispositivo, deben ser generados de forma segura por el prestador de servicios de certificación.

28.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

La ANCERT podrá generar y facilitar al suscriptor los datos de activación del dispositivo seguro de creación de firma empleando procedimientos seguros, como la entrega presencial o a distancia, en cuyo caso los datos de activación deberán ser distribuidos separadamente del propio dispositivo de creación de firma (por ejemplo, entregándose en momentos diferentes, o por rutas diferentes).

28.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulación.

28.5 CONTROLES DE SEGURIDAD INFORMÁTICA

28.5.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

Se deberá garantizar que el acceso los sistemas está limitado a individuos debidamente autorizados. En particular:

- Se debe garantizar una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo gestión de cuentas de usuarios, auditoría y modificaciones o denegación de acceso oportunas.

- Se debe garantizar que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas, incluyendo la

separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema estará restringido y estrechamente controlado.

- El personal deberá ser identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.

- El personal será responsable y deberá poder justificar sus actividades, por ejemplo, mediante un archivo de eventos.

- Deberá evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento (por ejemplo, ficheros borrados) que queden accesibles a usuarios no autorizados.

- Los sistemas de seguridad y monitorización deben permitir una rápida detección, registro y actuación ante intentos de acceso irregular o no autorizado a sus recursos (por ejemplo, mediante sistema de detección de intrusiones, monitorización y alarma)

- El acceso a los depósitos públicos de la información (por ejemplo, certificados o información de estado de revocación) deberá contar con un control de accesos para modificaciones o borrado de datos.

28.5.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

Las aplicaciones de autoridad de certificación y de registro empleadas por la ANCERT deberán ser fiables, debiendo acreditarse dicha condición, por ejemplo, mediante una certificación de producto contra un perfil de protección adecuado, conforme a la norma ISO15408, o equivalente.

28.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

28.6.1 CONTROLES DE DESARROLLO DE SISTEMAS

Se deberá realizar un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones de autoridad de certificación y de registro, para garantizar que los sistemas son seguros.

Se emplearán procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

28.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

La ANCERT, como prestador de servicios del CNL, deberá mantener un inventario de todos los activos informativos y realizará una clasificación de los mismos, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se auditará de forma periódica, de acuerdo con lo establecido en la sección Frecuencia de la auditoría de conformidad.

Se realizará un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenamiento para los activos informativos.

28.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

El Consejo General del Notariado podrá exigir que la ANCERT se someta a evaluaciones independientes, auditorías y, en su caso, certificaciones de seguridad del ciclo de vida de los productos que emplea.

28.7 CONTROLES DE SEGURIDAD DE LA RED

Se deberá garantizar que el acceso a las diferentes redes de la ANCERT está limitado a individuos debidamente autorizados. En particular:

- Deben implementarse controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos deberán configurarse de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la Entidad de Certificación.

- Los datos sensibles deberán protegerse cuando se intercambien a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor).

- Se debe garantizar que los componentes locales de red se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

28.8 SELLADO DE TIEMPO

Los servidores se mantienen actualizados con la hora UTC. Están sincronizados mediante el protocolo NTP (Network Time Protocol). La hora legal española es obtenida de la escala UTC de la Hora del Real Instituto y Observatorio de la Armada en San Fernando (ROA), la cual se genera mediante un algoritmo que combina información procedente de una batería de patrones atómicos de frecuencia, constituida por un máser de hidrógeno activo y cinco patrones de haz de cesio, optimizando la estabilidad y proporcionando otras características metrológicas de interés, como fiabilidad, control de la exactitud, etc.

29 PERFILES DE CERTIFICADOS, CRL Y OCSP

29.1 PERFIL DE CERTIFICADO

Los certificados de firma digital serán conformes con las siguientes normas:

- ETSI TS 101 862 v1.3.3 (2006-01): Qualified Certificate Profile, 2006

- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March2004 (siempre que no entre en conflicto con TS 101 862)

29.1.1 NÚMERO DE VERSIÓN

Los certificados emitidos por la Entidad de Certificación del CNL cumplen con el estándar X.509 Versión 3.

29.1.2 EXTENSIONES DEL CERTIFICADO

En el Anexo 2 de esta CPS se describe de forma detallada los certificados emitidos bajo esta CPS

29.1.3 KEY USAGE

El "key usage" es una extensión crítica que indica el uso del certificado de acuerdo con el RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

29.1.4 EXTENSIÓN DE POLÍTICA DE CERTIFICADOS

La extensión de "certifícate policies" del X.509 versión 3 es el identificador del objeto de esta CPS de acuerdo con la sección Identificador de objeto de la Política de Certificación de esta CPS. La extensión no es considerada como crítica.

29.1.5 NOMBRE ALTERNATIVO DEL SUJETO

La extensión "suject Alt Name" es opcional y el uso de esta extensión es "No critica".

29.1.6 RESTRICCIONES BÁSICAS

Para el caso de la ANCERT, como prestador de servicios del CNL, en el campo "Path Lenght Constraint" de certificado de las subordinadas tiene un valor de 0, para indicar que la ANCERT no permite más sub-niveles en la ruta del certificado. Es un campo crítico.

29.1.7 USO EXTENDIDO DE LA CLAVE

Esta extensión permite definir otros propósitos adicionales de la clave. Es considerada No crítica. Los propósitos más comunes son:

OID	Descripción	Tipos de Certificados
1.3.6.1.5.5.7.3.1	Autenticación de Servidor	Autenticación Agente Electrónico
1.3.6.1.5.5.7.3.2	Autenticación del Cliente	Autenticación persona Natural. Firma digital. Agente electrónico.
1.3.6.1.5.5.7.3.4	Protección de correo.	Firma Digital de persona natural y Agente Electrónico
1.3.6.1.5.5.7.3.8	Sellado de tiempo	Sellado de tiempo

1.3.6.1.4.1.311.20.2.2	Smart CardLogon	Autenticación Persona Natural.

29.1.8 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

El identificador de objeto del algoritmo de firma es 1.2.840.113549.1.1.5 SHA-1 with RSA Encryption

El identificador de objeto del algoritmo de la clave pública es 1.2.840.113549.1.1.1 rsaEncryption

29.1.9 FORMATOS DE NOMBRES.

De conformidad con lo especificado en el numeral Tipos de nombres de esta CPS.

29.1.10 RESTRICCIONES DE LOS NOMBRES.

Los nombres se deben escribir en mayúsculas y sin tildes, la letra Ñ solo se permite para los nombres de personas naturales o jurídicas.

El código del país se asigna de acuerdo al estándar ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".

29.1.11 IDENTIFICADOR DE OBJETO DE LA POLÍTICA DE CERTIFICACIÓN

El identificador de objeto de la Política de certificado correspondiente a cada tipo de certificado.

29.1.12 USO DE LA EXTENSIÓN POLICY CONSTRAINS

No se estipula.

29.1.13 SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

El calificador de la política está definido en la extensión de "Certificate Policies" y contiene una referencia al URL donde esta publicada la CPS del proveedor de servicios de certificación.

29.1.14 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICIES

No se estipula.

29.2 PERFIL DE CRL

Las CRLs emitidas por la ANCERT, como prestador de servicios del CNL, cumplen con el RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" y contienen los siguientes elementos básicos:

29.2.1 NÚMERO DE VERSIÓN

Las CRLs emitidas por la ANCERT como prestador de servicios del CNL cumplen con el estándar X.509 versión 2.

29.2.2 CRL Y EXTENSIONES CRL

La información sobre el motivo de la revocación de un certificado estará incluida en la CRL, utilizando las extensiones de la CRL y más específicamente en el campo de motivos de revocación (reason Code).

29.3 PERFIL OCSP

El servicio OCSP cumple con lo estipulado en el RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

29.3.1 NÚMERO DE VERSIÓN

Cumple con la OCSP Versión 1 del RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

29.3.2 EXTENSIONES OCSP

No aplica.

30 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

30.1 TIPOS DE EVENTOS REGISTRADOS

31.1.1. DOMINIO DE CREACIÓN DE CERTIFICADOS

La ANCERT, como prestador de servicios del CNL, guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado de los sistemas.
- Inicio y terminación de la aplicación de entidad de certificación o de entidad de registro central.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Generación y cambios en las claves de la entidad de certificación.
- Cambios en las políticas de emisión de certificados.
- Intentos de entrada y salida del sistema.
- Intentos no autorizados de entrada en la red de la entidad de certificación.
- Intentos no autorizados de acceso a los ficheros del sistema.
- Intentos fallidos de lectura en un certificado, y de lectura y escritura en el depósito de certificados.
- Eventos relacionados con el ciclo de vida del certificado, como solicitud, emisión, revocación y renovación de un certificado.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.
- La ANCERT también guarda, ya sea manual o electrónicamente, la siguiente información:
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Los 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 o del poseedor de claves.
- Posesión de datos de activación, para operaciones con la clave privada de la entidad de certificación.

31.1.2. DOMINIO DE REGISTRO DE USUARIO Y GESTIÓN DE TARJETAS EN NOTARÍA

La ANCERT por medio de la Notaría guarda la siguiente información:

- Encendido y apagado del sistema donde se aloja la entidad de registro.
- Inicio y terminación de la aplicación de entidad de registro.
- Procesamiento correcto e incorrecto de solicitudes.
- Solicitudes de emisión, renovación y revocación de certificados.

30.2 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

- En todos los dominios

Los registros de auditoría se examinan por lo menos una vez al mes en busca de actividad sospechosa o no habitual.
El procesamiento de los registros de auditoría consiste en una revisión de los registros la cual incluye la verificación de que los registros 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 llevadas a cabo a partir de la revisión de auditoría también deben ser documentadas.

30.3 IDENTIDAD/CUALIFICACIÓN DEL AUDITOR

ANCERT como prestador de servicios del CNL, somete su infraestructura y sistemas de gestión a evaluadores autorizados conforme a los Principios de Webtrust y a evaluadores autorizados por el INDECOPI.

30.4 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

La única relación establecida entre el Auditor y la Entidad auditada es la de Auditor y Auditado. La firma de Auditoría ejerce su absoluta independencia en el cumplimiento de sus actividades de auditoria y no existe conflicto de intereses pues la relación es netamente de tipo contractual.

30.5 ASPECTOS CUBIERTOS POR LOS CONTROLES

Los elementos cubiertos por la auditoría son la implementación de las prácticas de certificación, personal, procedimientos y técnicas, descritos en el anexo 2 de la presente Guía de Acreditación.

30.6 ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

Las deficiencias detectadas durante el proceso de auditoría deben ser subsanadas a través de un Plan de Mejoramiento que contenga las acciones, procedimientos o implementación de los controles requeridos para minimizar riesgos.

30.7 COMUNICACIÓN DE RESULTADOS

Una vez terminada la auditoría, la firma Auditora debe presentar el Informe de Auditoria al INDECOPI y si se requiere el CNL debe establecer un Plan de Mejoramiento.

31 OTROS ASUNTOS LEGALES Y COMERCIALES

31.1 TARIFAS

31.1.1 TARIFAS DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

Las tarifas serán definidas por el CNL de acuerdo a los contratos celebrados con sus clientes.

31.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

El acceso a la consulta del estado de los certificados emitidos, es libre y gratuito y por tanto no aplica una tarifa.

31.1.3 TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO

No se establece ninguna tarifa por el acceso a la información de estado de los certificados.

31.1.4 TARIFAS DE OTROS SERVICIOS

Una vez se ofrezcan otros servicios por parte del CNL, se publicarán en la dirección:

http://www.notarios.org.pe/

31.1.5 POLÍTICA DE REEMBOLSO

El CNL debe disponer de una Política de reintegro de la tarifa, que deberá documentar en su Declaración de Prácticas de Certificación.

31.2 RESPONSABILIDAD

ANCERT como proveedor de infraestructura y gestión de operaciones de los servicios de la EC del CNL, asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital provistos por la EC del CNL.

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por ANCERT de acuerdo a su documento Declaración de Prácticas de Certificación Certificados Notariales, publicado en:

http://www.ancert.com/liferay/web/ancert/politica-de-certificacion-y-dpcs

El CNL es responsable de exigir y supervisar las operaciones de los servicios de la EC del CNL que son administrados por ANCERT.

Como Entidad de Registro, el CNL es responsable de la correcta identificación de las personas naturales o jurídicas y de la seguridad en la entrega de certificados digitales, siempre que esta sea realizada por los Operadores de Registro autorizados.

Las peticiones, quejas o reclamos sobre los servicios prestados por el CNL a través de la Agencia Notarial de Certificación, S.L. Unipersonal "ANCERT" son recibidas directamente por el CNL como prestador de Servicios Digitales o a través de nuestra Entidad de Registro. La línea telefónica para la atención a titulares y terceros para consultas relacionadas con el servicio que dispone el CNL es permanente. Estos reclamos serán comunicados en un lapso no mayor de 5 días a ANCERT, para su debida atención.

31.3 EXONERACIÓN DE RESPONSABILIDAD

La EC del CNL no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de fuerza mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente CPS y sus Anexos.
- Por el uso indebido o fraudulento de los certificados o CRLs emitidos por la Entidad de Certificación.
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el incumplimiento de las obligaciones establecidas para el Titular o Terceros que confían en la normativa vigente, la presente CPS y sus Anexos.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación/suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Titular.
- Fraude en la documentación presentada por el solicitante.

31.4 RESPONSABILIDADES FINANCIERAS

31.4.1 COBERTURA DEL SEGURO

La ANCERT, como prestador de servicios del CNL, deberá disponer de una garantía de cobertura de su responsabilidad civil suficiente, bien mediante un seguro de responsabilidad civil profesional por errores y omisiones, bien mediante una fianza o aval.

La cuantía garantizada deberá ser de 3.000.000 de euros o superior.

31.4.2 SEGURO O GARANTÍA DE COBERTURA PARA LAS ENTIDADES FINALES

Sin estipulación.

31.5 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

31.5.1 ÁMBITO DE LA INFORMACIÓN CONFIDENCIAL

Las siguientes informaciones, como mínimo, serán mantenidas confidenciales por la ANCERT:

- 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 la ANCERT.

- Registros de transacciones, incluyendo los registros completos y los registros de auditoría delas transacciones.

- Registros de auditoría interna y externa, creados y/o mantenidos por la ANCERT y sus auditores.

- Planes de continuidad de negocio y de emergencia.

- Política y planes de seguridad.

- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.

- Toda otra información identificada como "Confidencial".

31.5.2 INFORMACIÓN NO CONFIDENCIAL

La siguiente información será considerada no confidencial:

- Los certificados emitidos o en trámite de emisión.

- La vinculación del suscriptor a un certificado emitido por una Entidad de Certificación.

- El nombre y los apellidos del suscriptor del certificado o del poseedor de claves, según proceda, así como cualesquiera 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 del suscriptor del certificado o del poseedor de claves, según proceda, o la dirección de correo electrónico que corresponda.

- 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 (CRLs), así como las restantes informaciones de estado de revocación.

- La información contenida en el Depósito.

- Toda otra información que no esté indicada en la sección anterior de esta política.

31.5.3 DEBER DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Mediante el presente documento la ANCERT, como prestador de servicios del CNL, establece las medidas de seguridad a implantar para la protección de los datos de carácter personal, contenidos en sus ficheros que contengan de carácter personal, de acuerdo con la legislación vigente en materia de Protección de Datos de carácter personal.

Como se ha dicho, la ANCERT, directamente o a través de las Entidades de Registro, recaba datos de carácter personal de los solicitantes/suscriptores, con el fin de identificarlos y prestarles los servicios de certificación interesados. Dada la naturaleza de este tipo de datos, según indica el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, la ANCERT debe adoptar medidas de seguridad de nivel básico.

La vigencia del Documento de Seguridad se inicia desde su realización y ordenación de las medidas de seguridad hasta su modificación, en su caso.

Este documento asegura la aplicación de las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal objeto de tratamiento en los Ficheros responsabilidad de la ANCERT, para evitar su alteración, pérdida, tratamiento o acceso no autorizado y ser utilizados para una finalidad legítima.

Con el Documento de Seguridad, la ANCERT implanta la normativa de seguridad a los equipos y máquinas encargados del tratamiento automatizado de los Ficheros, centros o locales de tratamiento, red, personal, usuarios, puestos de trabajo, programas o aplicaciones y soportes o dispositivos de almacenamiento.

Todo el personal de la ANCERT que intervenga directa o indirectamente en el tratamiento automatizado de los datos de carácter personal está obligado a cumplir y a respetar las disposiciones establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD y, en especial, lo establecido en el presente documento.

Todo el personal autorizado para acceder a los datos es informado de sus obligaciones y responsabilidades, así como del contenido de su contenido.

31.6 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

31.6.1 POLÍTICA DE PRIVACIDAD

La ANCERT, como prestador de servicios del CNL, precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales.

La ANCERT ha desarrollado una política de intimidad, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, y documenta en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al documento de seguridad previsto en el Real Decreto 994/99, de11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad. Esta Declaración de Prácticas de Certificación tiene la consideración de documento de seguridad.

31.6.2 INFORMACIÓN TRATADA COMO PRIVADA

La información personal suministrada por el titular y que es requerida para la aprobación del certificado digital es considerada información de carácter privado.

31.6.3 INFORMACIÓN NO CALIFICADA COMO PRIVADA

La información personal suministrada por el titular y que es contenida en el certificado digital no es considerada información de carácter privado.

31.6.4 RESPONSABILIDAD DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

La ANCERT, como prestador de servicios del CNL, es responsable y cuenta con los adecuados mecanismos de seguridad y control para garantizar la protección, confidencialidad y debido uso de la información suministrada por el titular.

31.6.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR DATOS DE CARÁCTER PERSONAL

Los datos de carácter personal no podrán ser comunicados a terceros, sin la debida notificación y consentimiento de su dueño.

31.6.6 REVELACIÓN EN EL MARCO DE UN PROCESO ADMINISTRATIVO O JUDICIAL

Los datos de carácter personal podrán ser comunicados cuando se requieran por parte de una autoridad competente en el marco de un proceso administrativo o judicial sin la debida notificación y consentimiento de su dueño, de conformidad con la legislación peruana.

31.7 DERECHOS DE PROPIEDAD INTELECTUAL

La ANCERT, como prestador de servicios del CNL, es la única entidad que goza de los derechos de propiedad intelectual sobre los certificados que emite, concediendo 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 usos autorizado y legítimos de acuerdo con esta Declaración de Prácticas de Certificación.

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

Los OID propiedad de la Agencia Notarial de Certificación han sido registrados en la IANA (Internet Assigned Number Authority) bajo la rama 1.3.6.1.4.1., habiéndose asignado el número 18920 (ANCERT), siendo dicha información pública en:

http://www.iana.org/assignments/enterprise-numbers

Igualmente queda prohibido el uso total o parcial de cualquiera de los OID asignados a la ANCERT salvo para los usos previstos en los Certificados o en el Depósito de Certificados.

Queda prohibida cualquier extracción y/o reutilización de la totalidad o de una parte sustancial de los contenidos o de las bases de datos que la ANCERT pone a disposición de los suscriptores de certificados.

31.8 OBLIGACIONES

31.8.1 OBLIGACIONES DE LA EC

La ANCERT, en calidad de prestador de servicios del CNL, garantiza bajo su plena responsabilidad que cumple con todos los requisitos establecidos en cada política de certificado para la que emite certificados.

Es la única entidad responsable del cumplimiento de los procedimientos descritos en esta Declaración de Prácticas de Certificación, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.

La ANCERT presta sus servicios de certificación conforme con esta Declaración de Prácticas de Certificación vigente, en la que se detallan sus funciones, procedimientos de operación y medidas de seguridad.

Antes de la emisión y entrega del certificado al suscriptor, se le informa de los términos y condiciones relativos al uso del certificado, de su precio – cuando se establece – y de sus limitaciones de uso.

Este requisito se cumple, entre otros medios, mediante un "Texto divulgativo de la política de certificado" aplicable, publicado y transmisible electrónicamente, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

Se vincula a suscriptores, poseedores de claves y terceros que confían en certificados mediante condiciones generales de emisión y uso de certificados, que se encuentran en lenguaje escrito y comprensible, y que tienen los siguientes contenidos mínimos:

- Indicación de la política aplicable, con indicación de si los certificados se expiden al público y de la necesidad de empleo de dispositivo seguro.

- 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, para la provisión del dispositivo seguro de creación de firma y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.

- Límites de uso del certificado de esta Declaración de Prácticas de Certificación.

- 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 ANCERT.

- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la ANCERT 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.

- Ley aplicable y jurisdicción competente.

- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

La ANCERT debe asumir otras obligaciones incorporadas directamente en el certificado o incorporadas por referencia.

31.8.2 OBLIGACIONES DE LA ER

Las ER son las entidades delegadas por la EC para realizar la labor de identificación y registro, por lo tanto la ER está obligada en los términos definidos en esta Declaración de Prácticas de Certificación a:

- Conocer y dar cumplimiento a lo dispuesto en la presente CPS y en la Política de Certificación correspondiente a cada tipo de certificado.
- Custodiar y proteger su clave privada.
- Comprobar la identidad de los Solicitantes y Titulares de certificados digitales.
- Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
- Archivar y custodiar la documentación suministrada por el solicitante o titular, durante el tiempo establecido por la legislación vigente.
- Respetar lo dispuesto en los contratos firmados entre el CNL y el titular.
- Identificar e informar a la EC las causas de revocación suministradas por los solicitantes sobre los certificados digitales vigentes.

31.8.3 OBLIGACIONES DEL TITULAR

La ANCERT, en las condiciones generales de emisión y uso de certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

La ANCERT, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la ANCERT y, en su caso, por la entidad de registro.

- 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 del mismo.

- Que los certificados cumplen con todos los requisitos materiales establecidos de 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.

31.8.4 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

La Agencia Notarial de Certificación, como mínimo, garantiza 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.

- 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, cuando emita un certificado de firma electrónica, garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado reconocido, de acuerdo con el artículo 11 de la Ley 59/2003, de 19 de diciembre.

- La responsabilidad de la ANCERT, con los límites legales que se establezcan.

32 CONFORMIDAD CON LA LEY APLICABLE

El CNL es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación de Entidades de Certificación, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales -Ley27269, para el reconocimiento legal de los servicios de valor añadido emitidos bajo las directrices definidas en el presente documento.

33 BIBLIOGRAFÍA

a) Declaración de Prácticas de Certificación Digital
b) Guía de Acreditación de Prestadores de Servicios de Valor Añadido, INDECOPI
c) Ley de Firmas y Certificados Digitales –Ley 27269
d) Decreto Supremo 026-2016
e) Decreto Supremo 052-2008
f) Decreto Supremo 070-2011
g) Decreto Supremo 105-2012
h) Declaración de Prácticas de Certificación ANCERT v3
i) Declaración de Prácticas de Registro Colegio de Notarios de Lima
j) Política de Certificación del CNL