COLEGIO DE NOTARIOS DE LIMA

Proyecto **Entidad de Registro**

Título **Declaración de Prácticas y Política de Registro 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 Registro Digital - ER, el CNL se encarga de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

La infraestructura tecnológica y operativa de la ER 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 certificación, servicio de valor añadido de intermediación digital y sellado de tiempo.

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 Registro o Verificación – ER, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Registro o Verificación – ER" 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 registro y verificación de la identidad brindados por la ER del 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 de certificados digitales. Constituye función del CNL el mantener un archivo de toda la información de los solicitantes de certificados digitales, lo cual incluye pero no se encuentra limitado a: contratos de los suscriptores, solicitantes de los procesos de emisión o revocación de certificados digitales, debidamente suscritas por los interesados. El CNL realiza estas funciones a través de las Notarías. Las especificaciones y detalles y procedimientos son los señalados en su organigrama estructural y funcional.
  Notario: Profesional del Derecho que está autorizado a dar fe de los actos y contratos que ante él se celebran. Es responsable de la formalización de la

voluntad de los otorgantes, la redacción de los instrumentos a los que confiere autenticidad, la conservación de los originales y expedición de los traslados correspondientes. Su función también comprende la comprobación de hecho y la tramitación de asuntos no contenciosos previstos en la ley de la materia. Asimismo, compete al notario, de conformidad con lo establecido en el inciso h) del artículo 94° del Decreto Legislativo N° 1049 (Decreto Legislativo del Notariado); la función de constatación de la identidad para efectos de la prestación de servicios de certificación digital. Para esto último, resulta necesario que el Notario previamente acredite ante el CNL una capacitación mínima en la materia y que haya suscrito el correspondiente convenio.

- Personal de la Notaría: Personal de confianza adscrito a una Notaría, el mismo que se encarga de participar en las labores de emisión y revocación de certificados digitales. Para poder realizar dichas funciones, es requisito indispensable que este personal cuente previamente con la capacitación y acreditación por parte del CNL.

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 la Declaración de Prácticas de Certificación del CNL.

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 la Declaración de Prácticas de Certificación del CNL.

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 bajo la Declaración de Prácticas 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 emisión, revocación 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:

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 la 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 la Declaración de Prácticas de Certificación del CNL 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.

Asimismo, el uso de los certificados dependerá del tipo de usuario que solicite un certificado digital. Estos usuarios pueden clasificarse en:

- Notario: Usuario interno que utiliza los certificados para autenticarse y obtener el acceso al SISGEN y para firmar los documentos digitales para el envío a la SUNAT/UIF/ROS, y emitir respuestas de las Alertas Notariales al Poder Judicial/otros.
- Oficial de cumplimiento: Usuario interno que utiliza los certificados para autenticarse y obtener el acceso al SISGEN y firmar los documentos digitales para el envío del ROS.
- Personal de notaría: Usuario interno que utiliza los certificados para el acceso al SISGEN para el envío a la SUNAT/UIF, y emitir respuestas de las Alertas Notariales al Poder Judicial/otros.
- Personal de entidades externas: Usuario externo del CNL que utiliza los certificados para el acceso al SISGEN y para realizar la solicitud de personas investigadas.

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 Declaración de Prácticas de Certificación y concretamente en las Políticas de Certificación del CNL.

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 la Declaración de Prácticas de Certificación del CNL 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 la Declaración de Prácticas de Certificación del CNL.

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 Declaración de Prácticas de Certificación, las Políticas de Certificación y la Declaración de Prácticas de Registro, 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 RPS

El CNL administra los documentos de Declaración de Prácticas y Política de Registro, y todos los documentos normativos de la ER 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 Registro Digital – RPS 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 ER 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 ERs con las que tiene filiación serán publicados en la dirección:

www.notarios.org.pe

12 IDENTIFICACIÓN Y AUTENTICACIÓN

12.1 NOMBRES

12.1.1 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 Directory Attributes.

La descripción de los Distinguished Name (DN) para cada tipo de certificado cubiertos por la Declaración de Prácticas de Certificación y están detallados en la Política de Certificación del CNL.

12.1.2 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.

12.1.3 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.

12.1.4 SINGULARIDAD DE LOS NOMBRES

El DN de los certificados digitales emitidos es único.

12.1.5 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.

13 SOLICITUD DE EMISIÓN DE CERTIFICADOS DIGITALES

13.1 SOLICITUD DE CERTIFICADOS A PERSONA JURÍDICA

13.1.1 SERVICIOS BRINDADOS

La ER del CNL brinda los siguientes servicios a personas jurídicas:

a) Atención de solicitudes de emisión y revocación de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

Los certificados brindados por la ER del CNL corresponden a las Entidades de Certificación acreditadas ante el INDECOPI que se encuentran publicadas en la siguiente dirección: www.notarios.org.pe

13.1.2 AUTORIZADAS PARA REALIZAR LA SOLICITUD

Aquellas que puedan sustentar su existencia y vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos. Las personas jurídicas asumen la responsabilidad de titulares de los certificados digitales que adquieren. En este caso existen los siguientes tipos de suscriptores: el representante legal y los notarios o empleados internos o externos a la empresa, que por el cargo que ocupan deben adquirir un certificado digital. En el certificado digital del representante legal quedarán registrados sus atributos o facultades, los cuales le permitirán utilizar el certificado digital para realizar transacciones en nombre y representación de la persona jurídica. Por otro lado, los certificados digitales de los funcionarios o empleados tienen atributos limitados al desenvolvimiento de sus funciones dentro de la persona jurídica.

Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad de certificados y de las firmas digitales generadas a partir de dicho certificado digital corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde el representante legal, que en nombre de la persona jurídica solicita el certificado.

13.1.3 MODALIDADES DE ATENCIÓN

El representante legal o la persona con facultades suficientes para actuar a nombre de la persona jurídica deberá comunicarse con la Entidad de Registro enviando un correo electrónico a entidadregistro@notarios.org.pe solicitando una cita de atención presencial con el OR, portando los documentos solicitados

Dicha solicitud puede ser realizada mediante un contrato de adquisición de los certificados digitales que puede ser celebrado de las siguientes formas:

- De manera presencial en las instalaciones de la ER del CNL
- De manera presencial en un lugar asignado por el solicitante en presencia de un representante de la ER

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER del CNL, utilizando un certificado digital reconocido por el INDECOPI.

13.1.4 SOLICITUD DE CERTIFICADOS DE ATRIBUTOS

En el caso de certificados de atributos, la persona jurídica se considera como aspirante a titular del certificado y los empleados vienen a ser los aspirantes a suscriptor.

El solicitante deberá especificar en la solicitud lo siguiente: su cargo, la descripción de la función para el uso del certificado, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

Un mismo suscriptor podrá efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera.

13.1.5 SOLICITUD DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

En la solicitud deberá especificarse el cargo, el propósito del certificado y el módulo criptográfico a emplear.

13.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

Conforme con la Guía de Acreditación de ER del INDECOPI, en el caso de personas jurídicas, la ER del CNL no asignará un nombre de titular que haya sido ya asignado a un titular diferente. La ER del CNL se reserva el derecho de rechazar una solicitud de emisión de certificado digital a causa de un conflicto de nombres.

Por otro lado, no le corresponde a la ER del CNL determinar si al solicitante de un certificado digital le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado digital. Asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

13.1.7 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA JURÍDICA

El solicitante deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva con el documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. La información proporcionada por los solicitantes será validada a través de la Consulta en línea a la Superintendencia Nacional de los Registros Públicos. En el caso de Notarios, se podrá verificar su identidad por medio de la plataforma SIGILUM, donde se podrá validar la firma, fotos, sellos y rúbrica del Notario solicitante.

13.1.8 CONTRATO DEL TITULAR

El Representante Legal de la persona jurídica o una persona asignada por él, debidamente acreditada, deberá firmar un contrato del titular.

A través de dicho contrato, el titular deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

13.1.9 VERIFICACIÓN DE TITULARES

El representante legal, o la persona con facultades suficientes para actuar a nombre de la persona jurídica deberá acreditar su identidad presentándose personalmente ante un Operador de Registro, ya sea en las oficinas de la Entidad de Registro o habiendo sido visitado por el Operador de Registro en su propia oficina. El solicitante tendrá que portar los instrumentos públicos o norma legal respectiva que acrediten la existencia de la persona jurídica:

- Vigencia de poder de la persona jurídica, en caso de tratarse de una empresa privada.
- Norma legal de constitución de la Entidad Pública, en caso de tratarse de una entidad del Estado Peruano.

En ambos casos, la persona asignada para realizar la solicitud deberá portar los siguientes documentos y sustentos:

- Documento que evidencie la vigencia de su nombramiento en el cargo.
- Documento que acredite sus facultades para solicitar los certificados digitales.
- Documento oficial de identidad.
- Cargo y propósito de la emisión del certificado digital

Asimismo, en presencia del Operador de Registro se verificará la identidad del solicitante mediante el servicio de Consulta En Línea de la Superintendencia Nacional de Registros Públicos. En el caso de un Notario se llevará a cabo la verificación de identidad por medio de la plataforma SIGILUM, dónde se podrá validar la firma, fotos, sellos y rúbrica del Notario solicitante.

El Representante Legal de la persona jurídica o una persona asignada por él, deberá firmar el contrato del titular.

Luego, el contrato y los documentos sustentatorios, serán registrados y almacenados en el archivo físico, siendo responsabilidad del Responsable de la ER su custodia.

En caso de no aprobarse dicha solicitud, el OR documentará las razones que generaron el rechazo.

En caso de ser exitosa, el OR realizará la confirmación por llamada telefónica al emisor de la solicitud para que, posteriormente, sea registrado de forma adecuada.

13.2 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

13.2.1 SERVICIOS BRINDADOS

La ER del CNL brinda los siguientes servicios a personas naturales:

- Atención de solicitudes de emisión y revocación de certificados para personas naturales de nacionalidad peruana.
- Atención de solicitudes de emisión y revocación de certificados de atributos para personas naturales de nacionalidad extranjera.

Los certificados corresponden a las Entidades de Certificación acreditadas que se encuentran publicadas en la siguiente dirección: www.notarios.org.pe

13.2.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

Aquellas que tienen plena capacidad de ejercicio de sus derechos civiles. Las personas naturales asumirán la responsabilidad de titulares y suscriptores de los certificados digitales que adquieren.

13.2.3 MODALIDADES DE ATENCIÓN

Las personas naturales deberán comunicarse con la Entidad de Registro enviando un correo electrónico a entidadregistro@notarios.org.pe solicitando una cita de atención presencial con el OR, portando los documentos solicitados

Dicha solicitud puede ser realizada mediante un contrato de adquisición de los certificados digitales que puede ser celebrado de las siguientes formas:

- De manera presencial en las instalaciones de la ER del CNL
- De manera presencial en un lugar asignado por el solicitante en presencia de un representante de la ER

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER del CNL, utilizando un certificado digital reconocido por el INDECOPI.

13.2.4 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento, portando el original de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro. No se admitirán fotocopias u otro tipo de documento.

13.2.5 CONTRATO DEL SUSCRIPTOR

El solicitante deberá firmar un contrato del suscriptor, el cual contiene las obligaciones que deben cumplir los suscriptores de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas, establecidas por las ER del CNL en coordinación con la EC, así como las consecuencias de no cumplir con el acuerdo.

Este contrato deberá ser firmado de manera digital o manuscrita por el solicitante, para luego ser archivado por la ER del CNL.

A través de dicho contrato, el suscriptor deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

13.2.6 VERIFICACIÓN DE SUSCRIPTORES

- El solicitante, aspirante a suscriptor del certificado digital, deberá acreditar su identidad presentándose personalmente ante un Operador de Registro, ya sea en las oficinas de la Entidad de Registro o habiendo sido visitado por el Operador de Registro en su propia oficina, portando su Documento de Identidad Oficial vigente (DNI o Carné de Extranjería) y documentos que correspondan al tipo de usuario, tal y como se detalla a continuación:

	Nombre	**Descripción**	**Requisitos específicos de sustento**	**Sistema de autenticación**
	Notario	Usuario interno que utiliza los certificados para autenticarse y obtener el acceso al SISGEN y para firmar los documentos digitales para el envío a la SUNAT/UIF/ROS, y emitir respuestas de las Alertas Notariales al Poder Judicial/otros.	- Convenio - Constancia de habilidad emitida por el Colegio al que pertenece	- Consulta biométrica IDENTIFICA - Consulta En Línea del RENIEC - Consulta a la plataforma SIGILUM
	Oficial de cumplimiento	Usuario interno que utiliza los certificados para autenticarse y obtener el acceso al SISGEN y firmar los documentos digitales para el envío del ROS.	- Carta de solicitud del Notario - Designación de Oficial de cumplimiento	- Consulta biométrica IDENTIFICA - Consulta En Línea del RENIEC
	Personal de notaría	Usuario interno que utiliza los certificados para el acceso al SISGEN para el envío a la SUNAT/UIF, y emitir respuestas de las Alertas Notariales al Poder Judicial/otros. Este usuario no firma ni se auténtica.	- Carta de solicitud del Notario - Designación de cargo	- Consulta biométrica IDENTIFICA - Consulta En Línea del RENIEC
	Personal de entidades externas	Usuario externo del CNL que utiliza los certificados para el acceso al SISGEN y para realizar la solicitud de personas investigadas. Este usuario no firma ni se auténtica	- Convenio - Nombramiento del representante legal o autoridad - Norma legal - Carta de solicitud del responsable operativo	- Consulta biométrica IDENTIFICA - Consulta En Línea del RENIEC

- El Operador de Registro verificará la validez del documento de identidad presentado.
  - En caso se trate de un ciudadano peruano, su identidad será verificada mediante dos modalidades: Mediante el Sistema de Consulta en Línea de la base de datos del RENIEC o por medio de la Consulta Biométrica IDENTIFICA. Se necesitará la verificación de identidad en al menos una de las modalidades antes mencionadas.

El OR validará el parecido con la fotografía, los datos de fecha de nacimiento y número de DNI.

- En caso se trate de un ciudadano extranjero, su identidad será verificada mediante la presentación de su Carné de Extranjería. Donde el OR validará la información brindada consultando la Base de datos de Migraciones.

- El Operador registrará los datos proporcionados por el RENIEC o por Migraciones en el expediente junto a las evidencias impresas de los resultados de la verificación de identidad y las fotocopias de los documentos físicos.
- En caso que todos los requisitos de validación hayan sido cumplidos, la solicitud de emisión será aprobada por el OR, registrando su autorización con su firma digital en el sistema de registro de la EC que emitió el certificado.
- El Operador de Registro hará firmar al solicitante el contrato respectivo, explicando sus responsabilidades respecto de la protección de las claves.
- Luego, el contrato y los documentos sustentatorios, así como la impresión del resultado de la consulta al Sistema de Consulta en Línea de la base de datos del RENIEC, la Consulta Biométrica IDENTIFICA o por la Base de datos de Migraciones; será registrado y almacenado en el archivo físico, siendo responsabilidad del Responsable de la ER su custodia. La EC almacenará los sustentos digitalizados y la autorización firmada digitalmente por el OR.
- En caso de no aprobarse dicha solicitud, el OR documentará las razones que generaron el rechazo.
- En caso de aprobarse, el OR realizará la confirmación por llamada telefónica al emisor de la solicitud para que, posteriormente, sea registrado de forma adecuada.

13.2.7 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA NATURAL

La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER del CNL a través de un mecanismo de consulta a las bases de datos del RENIEC.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante carnet de extranjería por medio de consulta con la base de datos de Migraciones.

De manera general, no se incluirá en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER del CNL no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

14 PROCESAMIENTO DE LA SOLICITUD DE EMISIÓN

14.1 RECHAZO DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER del CNL.

14.2 APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

En caso que una solicitud sea aprobada por la ER del CNL realizará lo siguiente:

a) Comunicar a la EC su aprobación para la emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por cada EC.

b) Se requerirá la firma del contrato del suscriptor.

14.3 REGISTRO DE DOCUMENTOS

Con respecto a los registros físicos, la ER del CNL registrará y archivará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

Asimismo, se realizará la fedatación de documentos físicos de forma anual.

14.4 MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor.

Los módulos criptográficos distribuidos por el CNL cuentan con la certificación FIPS 140-2 o equivalente.

Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Luego, se realizará la petición segura del certificado a la respectiva EC en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

14.5 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER del CNL enviará a la respectiva EC la autorización de la emisión del certificado de manera inmediata.

El máximo tiempo de respuesta para la emisión del certificado será de 05 días, luego de haber sido aprobada la validación de identidad y del pago respectivo.

14.6 EMISIÓN DEL CERTIFICADO

La emisión del certificado será realizada mediante el correo electrónico del suscriptor, registrado en su solicitud.

15 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DIGITALES

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

16 PROCESAMIENTO DE LA SOLICITUD DE RE-EMISIÓN

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

17 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

17.1 CIRCUNSTANCIAS PARA REALIZAR LA SOLICITUD

El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

a) Por exposición, puesta en peligro o uso indebido de la clave privada.

b) Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.

c) Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica

d) Cuando la información contenida en el certificado ya no resulte correcta.

e) Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.

f) 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.

g) Por decisión de la legislación respectiva.

No obstante, la revocación del certificado digital se llevará a cabo sin necesidad de una solicitud en los siguientes casos:

- Cuando la ER finaliza sus servicios.
- Cuando el Notario sale de la Notaría, dejando su cargo.

17.2 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

17.2.1 SERVICIOS BRINDADOS

La ER del CNL brinda los siguientes servicios a personas jurídicas y naturales:

h) Atención de solicitudes de revocación de certificados para personas naturales de nacionalidad peruana.

i) Atención de solicitudes de revocación de certificados de atributos para personas naturales de nacionalidad extranjera.

j) Atención de solicitudes de revocación de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

Los certificados corresponden a las Entidades de Certificación acreditadas que se encuentran publicadas en la siguiente dirección: www.notarios.org.pe

17.2.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

De acuerdo a lo estipulado por la Ley, el tipo de personas que pueden solicitar la revocación de un certificado son:

k) El titular del certificado

l) El suscriptor del certificado.

m) La EC o ER que emitió el certificado.

n) Un juez que de acuerdo a la Ley decida revocar el certificado.

o) 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.

Si como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER del CNL, bastará con presentar su solicitud firmada de manera manuscrita o con firma digital al Operador de Registro. En el caso de que la solicitud sea firmada de manera manuscrita, el solicitante deberá presentar su documento oficial de identidad.

17.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS SOLICITANTES

En los casos de que la solicitud sea presencial:

p) Los suscriptores deben presentar en la ER como mínimo su documento oficial de identidad.

q) El representante asignado por la persona jurídica debe presentar documentos que acrediten dicha representación y la voluntad de dicha persona jurídica.

r) Los terceros (diferentes de la EC, el suscriptor y el titular) deberán presentar en la ER pruebas fehacientes del uso indebido del certificado de acuerdo a la ley vigente, junto a la orden judicial respectiva.

17.2.4 MODALIDADES DE ATENCIÓN

La solicitud puede ser realizada por los titulares y suscriptores mediante de manera presencial en las instalaciones de la ER del CNL.

Los solicitantes deberán completar el formulario brindado por el OR, el cual formará parte del registro.

En caso se necesite revocar un certificado digital fuera del horario de atención del CNL, el solicitante deberá comunicarse con el OR por vía telefónica o por correo electrónico, para poder realizar la revocación de manera remota. No obstante, el solicitante tendrá que regularizar presencialmente la documentación necesaria o electrónicamente a través de un certificado digital.

La EC no requerirá realizar la solicitud a la ER en los casos que el suscriptor haya infringido las obligaciones descritas en su contrato o en caso sea necesario por revocación del certificado de la EC. Una EC puede revocar los certificados que ha emitido, siempre y cuando los motivos de revocación estén claramente especificados en su CPS y se encuentren de acuerdo con la legislación vigente.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER del CNL, utilizando un certificado digital reconocido por el INDECOPI.

17.2.5 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE ATRIBUTOS

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

17.2.6 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

17.2.7 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE PERSONA NATURAL

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

18 PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

18.1 RECHAZO DE LA SOLICITUD DE REVOCACIÓN EMISIÓN DE UN CERTIFICADO

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las modalidades de solicitud o que el solicitante no se encuentre debidamente autorizado conforme a lo descrito en el presente documento.

Adicionalmente, la solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER del CNL.

18.2 APROBACIÓN DE LA SOLICITUD DE REVOCACIÓN DE UN CERTIFICADO

En caso que una solicitud sea aprobada por la ER del CNL realizará lo siguiente:

a) Comunicar a la EC su aprobación para la revocación del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por cada EC.

b) Una copia de dicha solicitud firmada será enviada a la EC o almacenada en la ER del CNL conforme a los acuerdos celebrados con la EC.

18.3 REGISTRO DE DOCUMENTOS

La ER del CNL registrará y archivará la solicitud y los documentos de sustento presentados por el solicitante dejando constancia de la persona que efectúa la solicitud, la relación que tiene ésta con el titular, las razones de la solicitud, las acciones tomadas para la verificación de la veracidad de la solicitud, fecha y hora de la revocación y de la notificación de la misma a la EC, sus suscriptores y los terceros que confían.

Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad. Asimismo, se realizará la fedatación de documentos físicos de forma anual.

En caso que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

18.4 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER del CNL enviará a la respectiva EC la autorización de la revocación del certificado de manera inmediata.

El máximo tiempo de respuesta para la revocación del certificado dependerá de lo establecido en la CP y CPS de la EC del CNL.

18.5 REVOCACIÓN DEL CERTIFICADO

La revocación del certificado será comunicada al suscriptor y titular mediante el correo electrónico del suscriptor, registrado en su solicitud.

19 GESTIÓN DE LA SEGURIDAD

Las medidas de seguridad adoptadas para proteger los activos críticos que sostienen los servicios de registro son señaladas en la Política de Seguridad de la ER del CNL.

20 GESTIÓN DE OPERACIONES

20.1 MÓDULO CRIPTOGRÁFICO

La generación de claves de los suscriptores debe ser realizada en módulos criptográficos FIPS 140-2.

Los módulos criptográficos usados por los Operadores de Registro deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 como mínimo.

20.2 RESTRICCIONES DE LA GENERACIÓN DE CLAVES

Las claves pueden ser generadas solamente por los propios suscriptores.

20.3 ENTREGA DE LA CLAVE PÚBLICA

Cuando un suscriptor genera su propio par de claves o par de claves del titular, las claves públicas correspondientes deben ser entregadas al emisor del certificado de manera tal que se asegure la autenticidad de dicho suscriptor.

En los casos en que las ERs acepten las claves públicas en representación de los emisores de los certificados, éstas deberán ser entregadas a dicho emisor de manera tal que se asegure el mantenimiento de la asociación que debe existir entre el titular y la clave.

20.4 DEPÓSITO DE CLAVE PRIVADA

La ER del CNL no genera copias de las claves privadas de los suscriptores ni de los Operadores de Registro en ninguna modalidad.

20.5 DATOS DE ACTIVACIÓN

Los datos de activación del módulo criptográfico serán administrados por los suscriptores. En caso de obtener módulos criptográficos del CNL, se brindará la información correspondiente para realizar la asignación de los de activación por canales seguros.

21 CONTROLES DE SEGURIDAD COMPUTACIONAL

Los sistemas de registro utilizados por el CNL son provistos y administrados por EC reconocidas por el INDECOPI, con la certificación Webtrust. La ER sólo accede a estos sistemas vía web con acceso vía certificados digitales de los Operadores de Registro.

22 AUDITORÍAS

22.1 FRECUENCIAS DE AUDITORÍAS

Las evaluaciones técnicas del INDECOPI deberán llevarse a cabo una vez al año y cada vez que el INDECOPI lo requiera.

22.2 CALIFICACIONES DE LOS AUDITORES

La selección de los auditores depende del INDECOPI.

22.3 RELACIÓN DEL AUDITOR CON LA ER

Los auditores o asesores deben ser independientes de la ER del CNL.

23 MATERIAS DE NEGOCIO Y LEGALES

23.1 TARIFAS

Las tarifas por los servicios de registro y certificación digital serán indicadas en los contratos de suscriptor/titular.

23.2 POLÍTICAS DE REEMBOLSO

Las políticas de reembolso por los servicios los servicios de registro serán indicadas en los contratos de suscriptor/titular.

23.3 COBERTURA DE SEGURO

El CNL proporciona a sus clientes servicios de registro amparados por la cobertura del Seguro de Responsabilidad Civil de la Entidad de Certificación.

23.4 PROVISIONES Y GARANTÍAS

Las garantías por los servicios de registro y certificación digital serán definidas en los contratos de suscriptor/titular, en relación a errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de certificado o de revocación y protección de datos personales provistos.

23.5 EXCEPCIONES DE GARANTÍAS

La ER del CNL no se responsabiliza en casos de compromiso de la clave en manos del suscriptor, o cualquier solicitud no realizada según los procedimientos definidos en el presente documento.

23.6 OBLIGACIONES DE LOS SUSCRIPTORES Y TITULARES

Las obligaciones de los suscriptores y titulares se definen en sus respectivos contratos.

En particular los suscriptores y titulares tienen la responsabilidad de solicitar la revocación de sus certificados en casos de compromiso de su clave privada.

23.7 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Las obligaciones del tercero que confía son verificar el estado de confiabilidad de los certificados dentro de los términos establecidos en el marco de la IOFE.

23.8 INDEMNIZACIÓN

Los casos de indemnización son definidos en los contratos de suscriptor/titular.

23.9 NOTIFICACIONES

Los medios de notificación serán definidos en los contratos de suscriptor/titular.

23.10 ENMENDADURAS Y CAMBIOS

Las enmendaduras y cambios serán comunicadas al INDECOPI y luego de su aprobación serán publicadas en el repositorio y notificadas a los titulares y suscriptores, conforme a los medios especificados en sus contratos.

23.11 RESOLUCIÓN DE DISPUTAS

El procedimiento de resolución de disputas será definido en los contratos de suscriptor/titular.

23.12 CONFORMIDAD CON LA LEY APLICABLE

La ER del CNL se compromete a cumplir la ley aplicable a las operaciones de registro: las Guías de Acreditación de Entidades de Registro o Verificación del INDECOPI, la Ley de Firmas y Certificados Digitales y su Reglamento.

23.13 SUBROGACIÓN

La ER del CNL no delega sus responsabilidades respecto de las operaciones de registro sobre terceros no autorizados por la IOFE. Todos los casos de responsabilidad de otros participantes como las EC son especificados en este documento.

23.14 FUERZA MAYOR

Las cláusulas de fuerza mayor serán definidas en los contratos de suscriptor/titular.

23.15 DERECHOS DE PROPIEDAD INTELECTUAL

La ER del CNL tiene derechos de propiedad intelectual sobre todos sus documentos normativos, planes, herramientas de software de firma digital y material comercial, y no podrán ser modificados o atribuidos a otra entidad de manera no autorizada.

24 FINALIZACIÓN DE LA ER DEL CNL

Antes de su finalización, la ER del CNL informará al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con un periodo de anticipación de al menos treinta (30) días calendario.

Todas las solicitudes y contratos de suscriptores y titulares serán transferidos al INDECOPI o a otro PSC designado por este.

En caso de una operación de transferencia de titularidad, los nuevos dueños u operadores solicitarán la evaluación de cumplimiento al INDECOPI para garantizar que se mantienen los requisitos de acreditación.

Se advertirá a todos los suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por una EC que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección: www.notarios.org.pe

25 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