Proyecto **Entidad de Registro**

Título **Plan de Privacidad**

Realizado por	**COLEGIO DE NOTARIOS DE LIMA**		
Dirigido a	**INDECOPI**		
Documento			
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 de protección de datos personales que utiliza el CNL en calidad de Entidad de Registro o Verificación – ER del CNL, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Registro o Verificación (ER)" establecida por el INDECOPI.

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 ER 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. PKI 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:

a) Garantizar la seguridad, disponibilidad y calidad de las operaciones de gestión de los certificados digitales de los usuarios finales.
b) Garantizar la seguridad de las claves de la EC Raíz del CNL y las EC Subordinadas durante todo su ciclo de vida.
c) Garantizar la disponibilidad y accesibilidad de los servicios de consulta de estado de revocación de los certificados digitales
d) Garantizar la protección de los datos personales de los usuarios finales.
e) 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 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.

6 ALCANCE

La presente política es de cumplimiento obligatorio para el personal contratado por el CNL que participan de las operaciones críticas de los servicios de registro descritos en la Declaración de Prácticas de Registro.

7 PLAN DE PRIVACIDAD

7.1 INFORMACIÓN RECOLECTADA Y PROTEGIDA

Como parte de las operaciones de registro, el CNL en calidad de ER recolecta información de los suscriptores y titulares del siguiente tipo:

- Datos de identificación personal, incluyendo la fotografía que aparece en su documento de identidad.

- Contrato de solicitud de servicios.

7.2 TRATAMIENTO DE LOS DATOS PERSONALES

- **Información considerada confidencial**

La ER del CNL mantiene de manera confidencial la siguiente información:

- Material comercialmente reservado de la ER: planes de negocio y diseños e información de propiedad intelectual, e información que pudiera perjudicar la normal realización de sus operaciones.

- Información de los suscriptores y titulares, incluyendo contratos, información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores y titulares;

- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores y titulares.

- **Información que puede ser publicada**

La siguiente información será considerada no confidencial:

- Información respecto de la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión, la publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

- Información de certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) y su estado.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

7.3 FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Los contratos de los suscriptores contendrán cláusulas que soliciten el consentimiento del suscriptor y titular de transferir los datos personales contenidos en los certificados digitales a las locaciones ANCERT, como prestador de servicios del CNL.

7.4 IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD

El presente documento adopta lo establecido por el APEC a través de la Norma Marco sobre Privacidad respecto de los principios que deben ser observados siempre que se realice algún tipo de labor o función que involucre la recolección, posesión, procesamiento, uso, transferencia o revelación de información personal.

- **Medidas preventivas**

a) Se restringirá el acceso a los datos personales a los Operadores de Registro.
b) Estos datos serán protegidos contra acceso no autorizado.
c) Se concientizará al personal para no divulgar o exponer de manera accidental datos personales de los usuarios.
d) Se implementarán procedimientos para documentar las prácticas en lo que respecta a la información personal que se recolecta durante las actividades de operación o comercialización de los servicios de sellado de tiempo, las mismas que deben informar sobre:
   - El hecho de que se está recolectando información personal;
   - Los propósitos para los cuales se recolecta dicha información personal;
   - Los tipos de personas u organizaciones a las que dicha información podría ser revelada;
   - La identidad y ubicación del responsable de la información personal, incluyendo información respecto a la forma de contactarlo en razón a sus prácticas y manejo de la información personal;
   - Las opciones y medios que ofrece el responsable de la información personal a los individuos para limitar el uso y revelación, así como los mecanismos para el acceso y corrección de su información.
   - Deben tomarse todos los pasos razonablemente necesarios, a fin de asegurar que se provee tal información, sea antes o en el mismo momento en que se está efectuando la recolección de la información personal. Caso contrario, deberá proveerse esta información tan pronto como sea factible.
e) Puede no resultar apropiado exigir que los responsables de la información personal provean información respecto a la recolección y uso de información que se encuentra públicamente disponible.

- **Limitaciones a la recolección**

La recolección de información personal debe encontrarse limitada a la información que es relevante para el propósito para el cual se está recolectando y esta información deberá ser obtenida de manera legal y apropiada, y, en la medida de lo posible, con la debida información o consentimiento del individuo al cual pertenece.

- **Uso de la información personal**

La información personal recolectada será usada en estricto cumplimiento de los propósitos de la recolección o aspectos relativos a los mismos, excepto:

- Que exista consentimiento del individuo al que pertenece la información personal recolectada;
- Que esta información fuera necesaria para la provisión de un servicio o producto solicitado por el individuo; o
- Que la recolección fuera permitida por mandato de ley u otros instrumentos legales o exista algún tipo de pronunciamiento con efectos legales que lo autorizara.

- **Elección**

Cuando sea apropiado, se proveerá a los individuos mecanismos claros, prominentes, fáciles de entender, accesibles y económicos a fin que puedan decidir respecto a la recolección, uso y revelación de su información personal. Puede no resultar necesario que los responsables de la información provean estos mecanismos en los casos de recolección de información que sea públicamente disponible.

- **Integridad de la información personal**

La información personal deberá ser exacta, completa y mantenerse actualizada en el extremo que fuere necesario para los propósitos de su empleo.

- **Salvaguardas a la seguridad**

Los responsables de la información personal deberán proteger la información personal que mantienen, a través de salvaguardas apropiadas contra riesgos tales como pérdida de la información o acceso indebido a la misma, así como contra la destrucción, uso, modificación o revelación no autorizada o cualquier otro abuso. Estas salvaguardas deberán ser proporcionales a la naturaleza y gravedad del daño potencial, la sensibilidad de la información y el contexto en que ésta es mantenida, y deberán ser sometidas a revisiones y reevaluaciones periódicas.

- **Acceso y corrección**

a) Los individuos deben ser capaces de:
   - Obtener del responsable de la información personal, la confirmación respecto a si mantiene o no información personal que les concierne.
   - Comunicar su información personal, luego de haber probado suficientemente su identidad, dentro de un periodo de tiempo razonable; por una tarifa, si es que la hubiera, la cual no debe ser excesiva; de una manera razonable; de un formato que sea razonablemente comprensible; y

- Cuestionar la exactitud de la información que les concierne y de ser posible y apropiado, hacer que la información sea rectificada, completada, enmendada o borrada.

b) Debe proveerse acceso y oportunidad para la corrección de la información, salvo cuando:
- La carga o costo de hacerlo sea indebido o desproporcional a los riesgos de la privacidad individual en el caso en cuestión;
- La información no pueda ser divulgada por razones legales o de seguridad o para proteger información comercial de carácter confidencial; o
- Se podría violar la privacidad de la información de personas diferentes al individuo.

Si una solicitud bajo el supuesto (a) o (b) es denegado, se debe informar al individuo las razones en las que se basa dicha denegatoria y se le debe informar respecto a los mecanismos para cuestionar dicha decisión.

8 RESPONSABLE DE PRIVACIDAD

El Responsable de Privacidad de Datos Personales del CNL gestiona la implementación y vela por el cumplimiento del presente plan, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

9 CONFORMIDAD

Este documento ha sido aprobado por el Responsable de la ER del CNL, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.