ANEXO 9

FICHA DE SOLICITUD DE ACREDITACIÓN COMO ENTIDAD DE REGISTRO O VERIFICACIÓN (ER)

PARA SER LLENADO POR LA DGI
Ficha de Solicitud Nº
Expediente Nº
Fecha de Ingreso al INDECOPI

Ficha de Solicitud de Acreditación como Entidad de Registro o Verificación (ER)

Antes de llenar esta solicitud consulte los documentos que establecen los criterios de acreditación generales, específicos y complementarios [1] (legislación y guías de acreditación) que correspondan a la modalidad de Entidad de Registro que desea acreditar.

Mayores precisiones se pueden encontrar en la Cartilla de Instrucciones que se encuentra en la parte final del presente documento.

SEÑOR DIRECTOR DE LA DIRECCIÓN DE LA GESTIÓN DE LA INFRAESTRUCTURA OFICIAL DE LA FIRMA ELECTRÓNICA (DGI) DEL INDECOPI:

Yo, _____
(Nombres y apellidos)

Identificado con _____ en representación legal de la
(DNI, pasaporte, C. de extranjería u otro)

empresa / entidad pública
_____
(Nombre de la empresa / entidad pública)

con domicilio sito en _____

con correo electrónico _____

con teléfono fijo / móvil _____

y domicilio procesal en _____

[1] *La acreditación es un procedimiento administrativo, por lo tanto, las reglas que lo rigen son parte de la legislación nacional y se encuentran disponibles mediante su publicación en el Diario Oficial. En tal sentido, la suscripción de la solicitud implica conforme a lo expuesto la aceptación de dichas condiciones y la intención de ser calificado en el marco de ellas.*

Solicito a la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica del INDECOPI el siguiente procedimiento:

I. TIPO DE PROCEDIMIENTO (Marcar donde corresponda)

1. Acreditación como ER – Persona jurídica (incluye a las EREP)	☐	3. Renovación de la acreditación	☐
2. Acreditación como ER – Persona natural (notarios)	☐		

Siendo el nivel de seguridad al que postulo el siguiente [2]:

II. TIPO DE NIVEL DE SEGURIDAD (Marcar donde corresponda)

Medio (M)	☐
Medio Alto (M+)	☐

III. SEDE E INSTALACIONES

Indique la dirección completa de cada uno de los sitios o instalaciones en las cuales efectúa actividades para desarrollar el alcance de la acreditación solicitada, señalando las actividades que se realizan en cada uno:

Sitio	Dirección completa y país de ubicación	Actividades en cada sitio
1	Oficina Principal:	
2	Sucursales:	
3	Centro de Datos Principal:	
4	Centro de Datos Alterno:	
5	Centro de custodia de información y documentación:	

[2] Mayor información sobre el particular se encuentra en la Cartilla de Instrucciones.

6	Otro (Cuál):	

IV. CONSULTORIA PARA LA IMPLEMENTACIÓN DE LOS REQUISITOS DE ACREDITACIÓN

Si hubiera utilizado consultores externos para la implementación de los requisitos de acreditación, por favor indique el nombre del (los) consultor (es) y de la organización a la que pertenecen:

Nombre (s) del (los) consultor (es):	
Nombre de la organización de consultoría, si aplica:	

V. DOCUMENTOS QUE SE ACOMPAÑAN [3]

Se adjuntan los documentos siguientes [4] (marcar donde corresponda):

1. Copia del documento de identidad del solicitante.	☐	*11. Documentos que acrediten vinculación con un tercero que administre los servicios de almacenamiento de datos u otros.*	☐
2. Documentos que acrediten la existencia y vigencia de la persona jurídica solicitante.	☐	*12. Política de Registro.*	☐
3. Documentos que acrediten los poderes en virtud de los cuales los representantes legales se encuentran facultados para solicitar la acreditación.	☐	*13. Contrato con la Entidad de Certificación emisora de los certificados digitales.*	☐
4. Memoria descriptiva y organigrama estructural y funcional.	☐	*14. Política de Seguridad.*	☐
5. Documentos que acrediten domicilio en el país.	☐	*15. Política y Plan de Privacidad.*	☐
6. Declaración jurada de contar con infraestructura e instalaciones necesarias para la prestación del servicio.	☐	*16. Declaración jurada del cumplimiento de las obligaciones y los requisitos señalados en los artículos 30° y 31° del Reglamento de la Ley de Firmas y Certificados Digitales.*	☐

[3] Los documentos que se acompañen deberán encontrarse en idioma español. Si las fuentes originales provinieran de otro idioma, estas deberán ser traducidas de manera oficial. La relación de documentos antes señalada no es taxativa. En tal sentido, la DGI podrá considerar y solicitar cualquier documentación adicional que sea necesaria a efectos de poder tomar una decisión informada sobre la acreditación o no del solicitante.

[4] Relación de documentos establecida en base a la Ley de firmas y certificados digitales, su Reglamento, el TUPA del INDECOPI y la Guía de Acreditación de Entidad de Registro o Verificación (ER).

7. Declaración jurada de aceptación de visitas de auditoría cuando la Autoridad Administrativa Competente lo requiera.	☐	*17. Convenio con el RENIEC.*	☐
8. Declaración de Prácticas de Registro o Verificación (RPS).	☐	*18. Documento que acredite la contratación de seguros o garantías bancarias.*	☐
9. Declaración jurada del cumplimiento de los requisitos señalados en los artículos 16° y 17° del Reglamento de la Ley de Firmas y Certificados Digitales.	☐	*19. Certificado de Inspección Técnica de Seguridad en Edificaciones (ITSE).*	☐
10. Constancia que acredite pago de derechos administrativos.	☐		

VI. DATOS TÉCNICOS (Completar)

Especificando los siguientes datos técnicos:

Módulo Criptográfico (HSM) [5]: Nº de serie _____
Proveedor _____
Nº de factura _____
Certificación [6] FIPS 140-2 ☐ Common Criteria EAL4+ ☐

Tarjetas Inteligentes:

Proveedor _____
Nº de factura _____
Certificación HW [7] FIPS 140-2
Certificación FW [8] FIPS 140-2 ☐ Common Criteria EAL4+ ☐

Adjunto las constancias y/o certificaciones que sustentan lo anteriormente declarado.

Sobre este punto es necesario que la entidad/empresa postulante nos remita los siguientes documentos:

- Declaración jurada firmada por el representante en donde la entidad solicitante indique de manera detallada el o los HSM que utilice la Entidad de Registro que se está acreditando. Con respecto al HSM se debe describir la marca, número

[5] La información a consignar debe corresponder a cada raíz intermedia que se implemente.
HSM (*Hardware Security Module*): Dispositivo que almacena la clave privada.
[6] Tanto el hardware como el firmware.
[7] Hardware.
[8] Firmware ("Sistema Operativo").

de serie, folleto, propietario del equipo y la ubicación. Asimismo, debe diferenciarse si cuenta con un HSM principal y uno alterno.

- La entidad solicitante debe remitir la documentación sustentatoria sobre el acta de instalación de el o los HSM que utilice la Entidad de Registro que se está acreditando.

- En caso de que el Centro de Datos donde estuviera el HSM contara con certificaciones deben remitirse con el expediente.

DECLARACIÓN JURADA

POR TANTO:

***Declaro bajo juramento*:**

1. Conocer los criterios, requisitos y condiciones de acreditación establecidos por la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica; así como las obligaciones y derechos que involucra obtener la correspondiente acreditación.
2. Que la información indicada en la presente solicitud es verdadera.
3. Contar con la infraestructura e instalaciones necesarias para prestar los servicios de entidad de registro cuya acreditación se solicita.
4. Tener operativo software, hardware y demás componentes adecuados para las prácticas de los servicios de entidad de registro y las condiciones de seguridad adicionales basadas en estándares internacionales o compatibles a los internacionalmente vigentes que aseguren interoperabilidad.
5. Aceptar la visita comprobatoria que efectuará la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica o las personas o institución que esta designe para tales efectos. Asimismo, brindar las facilidades necesarias en todas las instalaciones en donde se lleven a cabo las evaluaciones para verificar el cumplimento de los requisitos necesarios para la acreditación.
6. Aceptar la programación de cinco (05) auditorías anuales que, en caso de otorgar la acreditación, la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica aplicará por mandato del artículo 69 del Reglamento de la Ley de Firmas y Certificados Digitales.
7. Contar con convenios o acuerdos de colaboración con las entidades encargadas de las bases de datos nacionales de Identificación y Registro Civil y de Registros Públicos, para efectos de la verificación de la información proporcionada por los solicitantes.
8. Contar con los documentos correspondientes a la Política y al Plan de Privacidad, y a la Política de Seguridad, de acuerdo a lo establecido por el Indecopi. Esta exigencia será verificada y evaluada durante la Fase II, Evaluación Técnica del proceso de acreditación.
9. Aceptar que en el manejo de datos personales de mis clientes o de terceros me encuentro obligado a gestionarlos con arreglo a la Ley Nº 29733, Ley de Protección de Datos Personales, incurriendo en responsabilidad administrativa en caso de omitir dicha obligación legal.

10. Cumplir con los requisitos señalados en los artículos 30° y 31° del Reglamento de la Ley de firmas y certificados digitales, los mismos que se transcriben a continuación:

Artículo 30°. - De las obligaciones

Las Entidades de Registro o Verificación acreditadas tienen las siguientes obligaciones:

a) Cumplir con los requerimientos de la Autoridad Administrativa Competente respecto de la Política de Registro o Verificación, Declaración de Prácticas de Registro o Verificación, Política de Seguridad y Política y Plan de Privacidad. Estos documentos deberán ser aprobados por la Autoridad Administrativa Competente dentro del procedimiento de acreditación.

b) Determinar objetivamente y en forma directa la veracidad de la información proporcionada por los solicitantes del certificado digital, bajo su responsabilidad.

c) Mantener la confidencialidad de la información relativa a los suscriptores y titulares de certificados digitales, limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido del titular o suscriptor del certificado digital, según sea el caso, realizado mediante un mecanismo que garantice el no repudio, debiendo respetar para tales efectos los lineamientos establecidos por la Autoridad Administrativa Competente en la Norma Marco sobre Privacidad.

d) Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.

e) Acreditar domicilio en el Perú.

f) Cumplir con las disposiciones de la Autoridad Administrativa Competente a que se refiere el artículo 31 del presente Reglamento.

g) Brindar todas las facilidades al personal autorizado por la Autoridad Administrativa Competente para efectos de supervisión y auditoría.

Estas obligaciones podrán ser precisadas por la Autoridad Administrativa Competente, a excepción de las que señale expresamente la Ley.

Artículo 31°. - De la responsabilidad por riesgos

Para operar en el marco de la Infraestructura Oficial de la Firma Electrónica y afrontar los riesgos que puedan surgir como resultado de sus actividades de registro o verificación, las Entidades de Registro o Verificación acreditadas, de acuerdo a los niveles de seguridad establecidos, deberán cumplir con:

I. *Nivel de seguridad Medio: Mantener vigente la contratación de seguros o garantías bancarias y emplear para efectos de la verificación de la identidad de los ciudadanos:*

- *De nacionalidad peruana, la base de datos del Registro Nacional de Identificación y Estado Civil (RENIEC).*
- *Extranjeros, carné de extranjería actualizado (residentes) o pasaporte (no residentes); o*

II. *Nivel de seguridad Medio Alto: Mantener vigente la contratación de seguros o garantías bancarias y emplear para efectos de la verificación de la identidad de los ciudadanos:*

- *De nacionalidad peruana, el sistema de identificación biométrica AFIS del Registro Nacional de Identificación y Estado Civil (RENIEC).*
- *Extranjeros, carné de extranjería actualizado (residentes) o pasaporte (no residentes).*

La Autoridad Administrativa Competente establecerá la cuantía mínima de las pólizas de seguros o garantías bancarias. Asimismo, la Autoridad Administrativa Competente determinará los criterios para evaluar el cumplimiento de este requisito.

Asimismo, me comprometo formalmente a:

1. Cumplir con los requisitos de acreditación establecidos por la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica.
2. Respetar el procedimiento de acreditación establecido por la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica.
3. Abonar todos los gastos administrativos y de evaluación que se originen.
4. Facilitar el acceso a la información, los documentos y los registros que sean necesarios para la evaluación sobre la procedencia o no de la acreditación solicitada.
5. En caso de obtener la acreditación, declarar frente a terceros estar acreditado sólo respecto al alcance de la acreditación que me sea otorgada, distinguiéndola permanentemente de otras actividades que preste fuera de dicho alcance.
6. No usar la acreditación de manera que afecte la reputación de la Infraestructura Oficial de la Firma Electrónica y/o la competencia del Indecopi en su condición de Autoridad Administrativa Competente.

7. En caso de que la acreditación sea cancelada, suspendida o reducida, interrumpiré inmediatamente el uso del logotipo o declaración de acreditación en todos los documentos y material publicitario relacionados con la acreditación afectada.
8. Cumplir con mantener confidencialidad de la información relativa a los solicitantes o titulares de los servicios de entidad de registro, limitando su empleo a las necesidades propias de los mismos, salvo orden judicial o pedido expreso de los solicitantes; quedando expresamente impedido de comercializar de cualquier forma las bases de datos o archivos digitales con información personal de los solicitantes o titulares que emplean los servicios de entidad de registro. Asimismo, me comprometo expresamente a respetar los principios de privacidad contenidos en la Ley de Protección de Datos Personales Nº 29733 y su respectivo Reglamento.

_____

Firma

_____

Nombre del Representante Legal

Fecha de la Solicitud:

CARTILLA DE INSTRUCCIONES

Acreditación: Acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, en el Reglamento y en las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de la Firma Electrónica.

Marco legislativo: El procedimiento de acreditación de un prestador de Servicios de Valor Añadido, se rige por la Ley de Firmas y Certificados digitales –Ley 27269–, su Reglamento aprobado por Decreto Supremo Nº 052-2008-PCM y sus respectivas normas modificatorias, el TUPA del Indecopi, así como la Guía de Acreditación de Prestadores de Servicios de Valor Añadido, aprobada por la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica del Indecopi.

Presentación de la solicitud: La solicitud de acreditación deberá ser presentada ante la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica del Indecopi que es la primera instancia administrativa ante la cual debe tramitarse la solicitud de acreditación. El plazo total del procedimiento es de ciento veinte (120) días hábiles. La solicitud deberá ser suscrita por el representante legal con facultades de representación suficientes. Los datos de identidad de esta persona deberán ser consignados en la parte introductoria de la ficha de solicitud.

I. Tipo de procedimiento: Deberá marcarse sólo un recuadro dependiendo del tipo de acreditación que se solicita. Para tales efectos debe tenerse presente lo siguiente:

a) La acreditación como ER – Persona Jurídica, será solicitada por todas las personas jurídicas privadas y las EREP.
b) La acreditación como ER – Persona Natural, sólo podrá ser solicitada por Notarios en ejercicio de sus funciones.
c) La renovación de la acreditación deberá cuando menos realizarse dentro de los ciento veinte (120) días hábiles anteriores al vencimiento de la acreditación conferida.

II. Tipo de nivel de seguridad: Según el punto IV de la Guía de Acreditación de Entidad de Registro o Verificación (ER), existen dos niveles de seguridad aplicables, cuyas características se describen a continuación:

- Nivel de Seguridad Medio (M): Los certificados digitales de nivel de seguridad medio son concebidos para:

1. Trámites con el Estado en las transacciones económicas de monto bajo o medio y para el intercambio de documentos de riesgo bajo o medio.
2. Información crítica y de seguridad nacional en redes cifradas.
3. Acceso a información clasificada o información de acceso especial en redes protegidas.
4. Aplicaciones de valor financiero medio o de comercio electrónico, tales como las planillas, contratos, compra de vehículos, etc.

Condiciones técnicas:
Aplicable todo el documento "Marco de la Política de Registro para la emisión de certificados digitales" [9] con las siguientes especificaciones:

5. Los dispositivos criptográficos físicos –hardware y firmware (sistema operativo)– que almacenan las claves privadas de la entidad final (usuarios) deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 1 (mínimo) o Common Criteria EAL4.
6. La longitud de clave privada mínima debe ser de 1024 bits y el certificado debe ser renovado como máximo anualmente.
7. Los certificados a nivel de entidad final (usuarios) deben ser generados de manera individual y separados para las siguientes funciones: cifrado y firma (no repudio) o autenticación. Las funciones de firma y autenticación son compatibles y pueden ser realizadas con un mismo certificado.

[9] El documento (ver anexo 1 de la Guía de Acreditación de Entidad de Registro o Verificación – ER) establece los lineamientos para la elaboración de la RPS. Está basado en los "Lineamientos para el marco de la política de emisión de certificados que pueden ser usados en comercio electrónico transnacional", emitido por el *APEC Telecommunications & Information Working Group - APEC eSecurity Task Group*: Draft Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction E-Commerce, Marzo 2004. Información disponible en: http://www.apectel29.gov.hk/download/estg_20.doc.

Adicionalmente, este nivel de seguridad se aplica a los Prestadores de Servicios de Certificación Digital (PSC) sin certificación; que sólo cuentan con la aprobación de las auditorías correspondientes para la acreditación o implementación de las normas correspondientes.

- Nivel de Seguridad Medio Alto (M+): Los certificados digitales de nivel de seguridad medio son concebidos para:

1. Todas las aplicaciones apropiadas para certificados de Nivel de Seguridad Medio (M).
2. Intercambio de documentos y transacciones monetarias de alto riesgo y trámites con el Estado en las transacciones económicas de alto monto y alto riesgo.
3. Información crítica no clasificada o de seguridad nacional en una red no cifrada.
4. Acceso a información clasificada o información de acceso especial en redes no protegidas.
5. Aplicaciones de valor financiero de riesgo y monto medio alto o de comercio electrónico.

Condiciones técnicas:
Aplicable todo el documento "Marco de la Política de Registro para la emisión de certificados digitales" con las siguientes especificaciones:

6. Los dispositivos criptográficos físicos –hardware y firmware (sistema operativo), que almacenan las claves privadas de la entidad final (usuarios), deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 2 (mínimo) o Common Criteria EAL4+.
7. La longitud de clave privada mínima debe ser de 2048 bits y el certificado debe ser renovado como máximo cada dos (2) años.
8. Los certificados a nivel de entidad final (usuarios) deben ser generados de manera individual y separados para las siguientes funciones: Cifrado y firma (no repudio) o autenticación. Las funciones de firma y autenticación son compatibles y pueden ser realizadas con un mismo certificado.

Adicionalmente, este nivel de seguridad se aplica a los Prestadores de Servicios de Certificación Digital (PSC) con las siguientes certificaciones:

- ER: ISO 9001:2000.
- EC: ISO 27001.
- SVA: ISO 9001:2000 o ISO 27001, y SW con ISO 9001:2000 o CMMI nivel 2 (mínimo).

III. Documentos que se acompañan: Toda la documentación que se acompañe a la solicitud deberá estar en idioma español. Si las fuentes originales provinieran de otro idioma, éstas deberán ser traducidas de manera oficial. Las especificaciones de cada uno de los documentos se señalan a continuación:

1. Copia del documento de identidad del solicitante: En el caso que el solicitante sea un nacional deberá acompañar su Documento Nacional de Identidad. En el caso de solicitantes extranjeros, deberán acompañar su Carné de Extranjería o Pasaporte con el visado correspondiente.
2. Documentos que acrediten la existencia y vigencia de la persona jurídica: Deberá acreditarse este hecho con el documento de vigencia de persona jurídica expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen. Adicionalmente, en el caso de las instituciones del Estado, deberán acreditar la existencia de una Oficina, Gerencia o dependencia interna a la cual se le otorgan funciones como prestador de servicios de certificación digital.
3. Documentos que acrediten los poderes en virtud de los cuales los representantes legales se encuentran facultados para solicitar la acreditación: En donde se deberá acreditar contar con las facultades suficientes para solicitar la acreditación o autorización solicitada. Adicionalmente, debe tenerse en cuenta que:
   - En el caso de personas jurídicas constituidas en el país: En el documento que acredite la representación, deberán constar las facultades conferidas al representante, bastando para tales efectos la presentación de la copia del poder respectivo.
   - En el caso de personas jurídicas constituidas en el extranjero: Los correspondientes poderes deberán ser legalizados por un funcionario consular peruano y de encontrarse redactados en idioma extranjero, será necesario que sean traducidos, debiendo el responsable de la traducción suscribir el correspondiente documento.
   - En el caso de instituciones del Estado: Deberá acreditarse el nombramiento de la persona encargada de dirigir la oficina, gerencia o dependencia interna encargada de la prestación de servicios de valor añadido. Debiéndose asimismo acreditarse las facultades de este funcionario.

- En el caso de los Notarios, se estará a lo establecido en el Decreto Ley Nº 26662, Ley del Notariado.

4. Memoria descriptiva y organigrama estructural y funcional: La misma que deberá ser realizada conforme al formato denominado: Memoria descriptiva y organigrama estructural y funcional de Entidad de Registro o Verificación (ER).
5. Documentos que acrediten domicilio en el país: Este hecho se acredita con el comprobante de inscripción de la persona jurídica en el Registro Único de Contribuyentes (RUC), donde debe constar con la condición de "habida". En su defecto, se podrá acompañar cualquier otra documentación que sirva para acreditar la condición de domiciliado en el país, la misma que será materia de evaluación por parte de la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica del INDECOPI.
6. Declaración jurada de contar con infraestructura e instalaciones necesarias para la prestación del servicio.
7. Declaración jurada de aceptación de visitas de auditoría cuando la Autoridad Administrativa Competente lo requiera.
8. Declaración de Prácticas de Registro o Verificación (RPS): La Declaración de Prácticas de Registro o Verificación, es el documento en el que constan de manera detallada las políticas y procedimientos que aplica la ER para la prestación de sus servicios. La Declaración de Prácticas de Registro o Verificación deberá establecer procedimientos detallados que garanticen el cumplimiento de las funciones legalmente establecidas para las ER. Asimismo, tendrá que asegurar la verificación presencial de la identidad del solicitante de un nuevo certificado digital.
9. Declaración jurada del cumplimiento de los requisitos señalados en los artículos 16° y 17° del Reglamento de la Ley de Firmas y Certificados Digitales.
10. Constancia que acredite pago de derechos administrativos: Los mismos que ascienden a S/. 3,111. 80 (Tres mil ciento once soles con ochenta céntimos).
11. Documentos que acrediten vinculación con un tercero que administre los servicios de almacenamiento de datos u otros: Los documentos presentados deben servir para acreditar de manera suficiente la viabilidad de la prestación de los servicios de certificación digital bajo estas condiciones y la disponibilidad de estos elementos para la evaluación y supervisión que la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica considere necesaria.
12. Política de Registro: Las evaluaciones realizadas por la Autoridad Administrativa Competente velarán porque los controles implementados por la entidad que solicita la acreditación sean conformes a los requerimientos expresados en el presente documento.
13. Contrato con la Entidad de Certificación emisora de los certificados digitales: La Entidad de Registro deberá demostrar un documento que acredite su vinculación con cada Entidad de Certificación con la que se va a vincular.
14. Política de Seguridad: Una política de seguridad es el resultado de la elaboración de un conjunto de documentos basados en el estudio de la estructura del negocio. Para el proceso de acreditación ante el INDECOPI deberá presentarse una Política de Seguridad basada en términos que garanticen la seguridad de los procesos de registro en la Entidad de Registro.
15. Política y Plan de Privacidad: Debe establecer el tipo de datos personales que pueden ser recolectados y cómo serán utilizados, protegidos, recuperados/corregidos de conformidad con la Ley de Protección de Datos Personales Nº 29733 y su respectivo Reglamento.
16. Declaración jurada del cumplimiento de las obligaciones y los requisitos señalados en los artículos 30° y 31° del Reglamento de la Ley de Firmas y Certificados Digitales.
17. Convenio con el RENIEC: En el convenio con el RENIEC se va a verificar la vigencia y que figure el acceso actualizado de los operadores de registro.
18. Documento que acredite la contratación de seguros o garantías bancarias: Revisar el monto que corresponde a la presente acreditación.
19. Certificado de Inspección Técnica de Seguridad en Edificaciones (ITSE): En el documento en mención se va a verificar la vigencia y la dirección del domicilio evaluado.