DECLARACIÓN DE PRÁCTICAS DE ENTIDAD DE REGISTRO

Versión:	1.1	
Código:	ENRV-0008	
Fecha de la creación:	31/05/2019	
Creado por:	Jadimar Castillo	Cargo: Operador de Registro
Aprobado por:	Rocío Huamán	Cargo: Responsable de la Entidad de Registro
Nivel de confidencialidad:	Público	

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
07/06/2019	1.1	Jadimar Castillo	Cambio de código de documento, Actualización de punto 22 Suspensión de certificado de persona jurídica, Actualización de términos contractuales legalizado.

Índice

1. Introducción

INNOVA DIGITAL SOLUTIONS SAC en adelante INDIGITAL, es una empresa Peruana con impecable trayectoria; dedicada a innovar, desarrollar y generar soluciones integrales en tecnología en el ámbito empresarial. Contamos con amplia experiencia y trayectoria trabajando con tecnología PKI de Firma Digital y Gestión Documental.

La clave de nuestro crecimiento, lo debemos principalmente al equipo humano honesto, profesional y con un gran talento y experiencia en esta tecnología. Un equipo que ayuda a crecer diariamente con ideas e innovaciones pensadas para nuestros clientes.

El presente documento se elabora con el fin de establecer el marco normativo y legal definido en la Guía de Acreditación de Entidad de Registro del INDECOPI, para optar como Entidad de Registro vinculada a la Entidad de Certificación CAMERFIRMA PERÚ.

2. Visión General

La ER – INDIGITAL está vinculada a la EC – CAMERFIRMA PERU, la cual se encuentra amparada bajo el marco de la IOFE del INDECOPI. La entidad de registro brinda los servicios de emisión, revocación, reemisión y suspensión de Certificados Digitales.

La emisión del Certificado Digital se realiza de manera presencial o remota de acuerdo con lo definido en el presente documento.

Se emiten Certificados Digitales de persona natural y persona jurídica para peruanos y extranjeros, bajo el cumplimiento de los requisitos por tipo de certificados solicitados.

3. Nombre e identificación del documento

- Nombre: Declaración de Prácticas de Entidad de Registro de INDIGITAL
- Versión: 1.0
- Website: www.indigitalsolutions.com
- Fecha de edición: 31/05/2019
- Fecha de última modificación: 31/05/2019
- Lugar: Lima, Perú

4. Participantes

4.1. Entidad de Certificación

La EC vinculada a la ER es CAMERFIRMA PERU, la función principal de la EC es emitir, reemitir, revocar y suspender los Certificados Digitales, de acuerdo con lo especificado en su correspondiente Declaración de Prácticas de Certificación (CPS).

4.2. Entidad de Registro o Verificación

La función principal de una ER es la verificación de la identidad de los solicitantes de Certificados Digitales. La ER debe realizar el levantamiento de datos y la comprobación de la información suministrada por el solicitante. Asimismo, debe aprobar o rechazar las solicitudes de emisión, revocación o suspensión de Certificados Digitales, comunicando a la respectiva EC vinculada de acuerdo con lo estipulado a su Declaración de Prácticas de Registro (en adelante RPS).

4.3. Titulares y suscriptores

Las Entidades Finales pueden ser personas naturales o personas jurídicas. Las personas naturales se constituyen siempre en Titulares del Certificado Digital, mientras que las personas jurídicas, dependiendo del tipo de Certificado Digital, se constituyen en Titular o en Titular y suscriptor.

4.4. Terceros que confían

Los terceros que confían pueden ser personas naturales, jurídicas, equipos, servicios o cualquier otro ente diferente al suscriptor que decide aceptar y confiar en un Certificado Digital emitido por las EC vinculada y, por lo tanto, en las firmas digitales correspondientes.

4.5. Otros participantes

Se considera como otros participantes a aquellas entidades que proveen servicios de soporte a las operaciones del proceso de certificación digital. En la eventualidad que una ER requiera la tercerización de algún servicio debe suscribirse un acuerdo de tercerización que cuente con las cláusulas específicas relacionadas con la seguridad de la información y la protección de los datos personales de acuerdo con la normativa y legislación del Estado Peruano.

5. Organización que administra el documento

La organización encargada de la administración (elaboración, registro, mantenimiento y actualización) de este documento es:

- Nombre: Innova Digital Solutions - INDIGITAL S.A.C.
- Dirección de correo: indigital@indigitalsolutions.com
- Dirección: Av. República de Panamá N° 3535 Oficina N° 1204 Torre A. San Isidro
- Número de teléfono: 01- 7195537

6. Persona de contacto

- Contacto: Responsable de la Entidad de Registro
- Dirección de correo electrónico: rhuaman@indigitalsolutions.com
- Dirección: Av. República de Panamá N° 3535 Oficina N° 1204 Torre A. San Isidro
- Número de teléfono: 01- 7195537

7. Definiciones y Acrónimos

a) AAC: Autoridad Administrativa Competente (CFE del INDECOPI)
b) CRL o LCR: Certificate Revocation List (Lista de Certificados Revocados)
c) CFE: Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica
d) EC: Entidad de Certificación
e) ER: Entidad de Registro o Verificación
f) IOFE: Infraestructura Oficial de Firma Electrónica
g) ISO: International Organization for Standardization
h) OCSP: Online Certificate Status Protocol (Protocolo del estado en línea del certificado)
i) PKI: Public Key Infrastructure (Infraestructura de Clave Pública)
j) PSC: Prestador de Servicios de Certificación Digital
k) RPS: Declaración de Prácticas de Registro o Verificación de una ER
l) SHA: Secure Hash Algorithm
m) TSL: Trust Services List
n) CPS: Declaración de Prácticas de Certificación
o) CP: Políticas de Certificación

8. Publicación y difusión del documento

La RPS es publicada en la página web de INDIGITAL (www.indigitalsolutions.com), su difusión se realiza a través del correo electrónico indicado por el Titular/suscriptor.

Todas las modificaciones relevantes en la documentación de la ER, serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en la página web de INDIGITAL.

La RPS será firmada digitalmente por el Responsable de la Entidad de Registro de INDIGITAL, garantizando la integridad de mismo, la cual podrá ser verificada, tal como lo estipula la guía de entidad de registro vigente.

Asimismo, la Declaración de Prácticas y Políticas de Certificación de la EC vinculada son publicadas en la página web de CAMERFIRMA (www.camerfirma.com).

9. Revisión y Frecuencia de publicación

La ER - INDIGITAL revisa los documentos normativos al menos una vez al año, gestiona y actualiza sus repositorios conforme a la siguiente frecuencia:

- Declaración de Prácticas de Registro (RPS) de INDIGITAL: Actualizado cada vez que la ER aprueba una nueva versión.
- Política y Plan de Privacidad: Actualizado cada vez que la ER aprueba una nueva versión.
- Política de Seguridad: Actualizado cada vez que la ER aprueba una nueva versión.

10. Responsabilidades del suscriptor

Los suscriptores o titulares de los certificados digitales provistos por la ER-INDIGITAL, son responsables y están obligados a revisar el presente documento, la CPS y las Políticas de Certificación de la EC vinculada, a fin de tener conocimiento del servicio, infraestructura y procedimientos empleados para la gestión del ciclo de vida de los certificados digitales, así como las obligaciones de cada parte.

11. Responsabilidades de los terceros que confían

Un tercero que confía puede ser requerido a cumplir con las obligaciones establecidas en la CPS de la EC vinculada y la RPS de la ER.

El tercero que confía verifica la información de la ER, a través de la documentación publicada en la página web de INDIGITAL, la cual está basada en las normativas peruanas y es parte de la IOFE, debiendo cumplir con las obligaciones mencionadas en dichos documentos.

12. Terceros contratistas

No aplica a la ER.

13. Certificados Digitales

La ER proporcionará Certificados Digitales para persona natural y persona jurídica:

a) Certificados de Persona Natural, caracterizados por el hecho de que pertenecen a una Persona Física, que actúa a nombre propio y representación (siendo en este caso el Titular y suscriptor del certificado la misma persona).

b) Certificados de Persona Jurídica, la cual puede ser:

- Certificado de Atributos, caracterizados por el hecho que el Titular del certificado es una persona jurídica, que faculta a una persona natural de atributos que le permiten actuar en nombre de la persona jurídica. Dichos atributos pueden ser limitados como el caso de certificados de funcionarios o empleados, o plenos como es el caso del representante legal de la persona jurídica.

- Certificados de Agente Automatizado, cuando el poseedor de la clave privada es un dispositivo informático perteneciente a una persona jurídica que realiza las operaciones de firma y descifrado de forma automática, y cuyas acciones se encuentran bajo la responsabilidad de una Persona Física que es el suscriptor del certificado.

13.1. Uso apropiado de los Certificados Digitales

La ER ofrecerá los tipos de Certificados Digitales que forman parte de los servicios de la EC, según su propósito, los cuales se distinguen por el tipo de proceso de verificación.

Para persona natural, será la persona natural quien asuma los roles de Titular, procediéndose de la misma manera al registro o verificación de su identidad y asumiendo las obligaciones como suscriptor del Certificado Digital en aplicación del Art. 14° del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por D.S 052-2008-PCM.

Las obligaciones del Titular son:

1) Entregar información veraz bajo su responsabilidad.
2) Actualizar la información proporcionada a la ER cuando estos ya no resulten exactos o son incorrectos.
3) Custodiar su contraseña o clave de identificación personal (PIN) de acceso a su clave privada de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
4) Observar las condiciones establecidas por la ER para la utilización del Certificado Digital y la generación de firmas digitales.
5) Realizar un uso debido y correcto del Certificado Digital.
6) Notificar de inmediato a la ER en caso detecte que se ha incluido información incorrecta o inexacta en el Certificado Digital.
7) Solicitar inmediatamente a la ER la revocación de su Certificado Digital en caso de tener conocimiento o sospecha de la ocurrencia de alguna de las siguientes circunstancias:
    a) Exposición, puesta en peligro o uso indebido de la llave privada o de la contraseña o PIN de acceso a su llave privada. El compromiso de la clave privada puede darse, entre otras causas, por pérdida, robo o conocimiento por terceros de la clave personal de acceso.
    b) Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada o la contraseña o PIN de acceso a su llave privada.
8) Solicitar de inmediato a la ER la revocación del certificado cuando:
    a) La información contenida en el Certificado Digital ya no resulte correcta.
    b) El Titular y suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la ER.

Asimismo, el Titular del certificado asumirá las responsabilidades, por los daños y perjuicios que pudiese causar por aportar datos falsos, incompletos o inexactos, así como, es de su exclusiva responsabilidad el uso indebido, incorrecto o no acorde a los fines para el que fue extendido el certificado. A tal efecto, la ER está excluida de toda responsabilidad.

Para los certificados digitales de atributos y para agentes automatizados la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER la documentación legal que acredite sus facultades como representante.

14. Solicitud de certificados digitales de persona natural

En el caso de personas naturales, la solicitud deberá ser hecha por la misma persona quién es también el titular del certificado digital.

14.1. Descripción de procedimientos

Para proporcionar el Certificado Digital de personal natural (Titular), se debe:

- El solicitante a través de la página web www.certificados.pe o www.indigitalsolutions.com, solicita la cotización y brinda los siguientes datos: número de RUC, teléfono y correo electrónico. El correo electrónico asociado al Certificado Digital es de su uso exclusivo, ya que a través de este se le notificara sobre los procesos y ciclos de vida de su certificado digital.
- El Operador de Registro de la ER vía correo electrónico envía la cotización con la información de los requerimientos para la emisión de los Certificados y los requisitos mínimos de compatibilidad de los módulos criptográficos homologados por la RENIEC.
- El solicitante debe enviar por correo electrónico el Voucher de pago y los documentos correspondientes a la cuenta de correo del operador de registro y posterior a ello se le envía el enlace para el registro de la pre-solicitud.
- El Solicitante recibirá en su correo electrónico la confirmación de la pre-solicitud y la aceptación de los términos de uso del Certificado Digital, a su vez se le informa que deberá presentarse en la ER para realizar la verificación presencial física y la entrega de los documentos correspondientes. Si existe alguna duda en cuanto al proceso de la verificación presencial el solicitante puede comunicarse con el Operador de Registro de la ER vía correo electrónico o a los números telefónicos que están publicados en las páginas web www.certificados.pe o www.indigitalsolutions.com.
- El Operador de Registro y Validación será el encargado de validar la identidad del solicitante.
- Una vez el Solicitante realiza la confirmación de la pre-solicitud, los operadores de registro de la ER reciben un correo con el enlace a la plataforma de la EC vinculada para su validación y gestión (visualizar datos, modificar, validar o eliminar).
- Una vez que el operador de registro valide la solicitud se procede a la descarga o inserción del certificado en el módulo criptográfico y se le enviara al solicitante a su correo el pin de revocación del certificado.
- Si la ER provee el modulo criptográfico éste debe tener la certificación FIPS 140 – 2 Nivel 2 y ser compatible con la plataforma de la EC.
- Si los Certificados Digitales son solicitados en algún departamento o ciudad distinta a las oficinas de la ER, y la misma es quién provee el módulo criptográfico, la inserción de los Certificados Digitales en el módulo criptográfico se realiza en las instalaciones de la ER y se envía a través de un proveedor de Courier.

- Si el cliente provee su mismo módulo criptográfico el operador de registro debe comprobar la vigencia (vida útil), los requisitos mínimos y la compatibilidad con la plataforma EC, en este caso la descarga o inserción del certificado digital será en las instalaciones de la ER.

14.2. Verificación presencial

En el caso que el Certificado Digital sea solicitado en la ciudad donde se encuentra la oficina de la ER es necesario consignar el siguiente documento (DNI del solicitante del Certificado Digital), el cual se verificará para corroborar que los datos sean correctos, luego se realizará el trámite de Verificación Presencial física del Solicitante ante el Operador de Registro y Validación de la ER para una correcta identificación de este, la cual se realizará en las instalaciones de la ER o del cliente previa cita.

Si el Certificado Digital es solicitado en algún departamento o ciudad distinta a las oficinas de la ER se solicita la verificación de identidad por parte de un notario y el documento contractual de la ER, los documentos se envían a través de un proveedor de Courier hasta las instalaciones de la ER.

14.3. Verificación mediante consulta de bases nacionales

La identidad del solicitante se verifica a través de medios no repudiables, los cuales son:

- En el caso de ciudadanos peruanos, por las bases de datos del RENIEC (Validación de DNI).
- En el caso de extranjeros, por las bases de datos de Migraciones (Validación de Carné de Extranjería).

14.4. Verificación de los datos de la solicitud

Para validar los datos de la solicitud, que serán consignados a la EC vinculada es necesario que se hayan realizado las siguientes obligaciones:

- Trámite de Verificación Presencial Física del solicitante ante el Operador de Registro y Validación de la ER para una correcta identificación de este.
- Comprobación de la validez y vigencia de los datos en la documentación consignada por el solicitante.

14.5. No repudio de la solicitud

Los datos de la solicitud para la emisión de Certificados Digitales son validados por los Operadores de Registro de la ER a través de la plataforma de la EC vinculada, la cual permite garantizar su autenticidad y no repudio. La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS#10, a través de un canal seguro SSL, el cual es administrado por la EC vinculada.

14.6. Aprobación o rechazo de la solicitud

La ER debe comunicar a la EC vinculada la aprobación de la solicitud para la emisión del Certificado Digital debiendo contar previamente con el documento contractual de la ER legalizado y firmado por el solicitante donde constan las responsabilidades de la Entidad de Registro, de la Entidad de Certificación y del Titular de los Certificados Digitales.

La ER tiene la potestad y obligación de rechazar la solicitud de emisión del Certificado Digital en los siguientes casos:

- Si el solicitante no tiene plena capacidad de ejercicio de sus derechos civiles.
- Si el resultado de la verificación de identidad del Titular fue negativo.

14.7. No repudio a la invitación de generación de claves e instalación del certificado

La solicitud de la ER a la EC vinculada con los datos validados del solicitante se realiza en PKCS#10, a través de un canal seguro SSL el cual es administrado por la EC vinculada.

14.8. Contrato del titular

El titular debe firmar el documento contractual legalizado de la ER en señal de conformidad de las cláusulas de este, donde se indica las responsabilidades y todo lo inherente al Certificado Digital.

14.9. Tiempo de procesamiento

El máximo tiempo de respuesta para la emisión del certificado digital será de 2 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo por el servicio brindado.

15. Re-emisión de certificados de persona natural

La plataforma dispuesta por la EC permite realizar la re-emisión de Certificados Digitales, cuando la fecha de expiración de este sea próxima o haya expirado. Una vez realizados todos los procesos y validaciones correspondientes a la solicitud, se obtendrá un nuevo par de claves y un nuevo Certificado Digital.

15.1. Descripción de procedimientos

Para la re-emisión de Certificados Digitales de persona natural el operador de registro informa con anticipación a través del correo electrónico al titular del certificado digital sobre la re-emisión del mismo; a su vez envía todas las especificaciones para la gestión. En este caso el titular del certificado digital debe validar su identidad a través de la verificación de identidad por parte de un notario y el documento contractual de la ER legalizado, también puede realizar la validación de identidad a través de la verificacion presencial física en las instalaciones de la ER o en las instalaciones de la empresa para ello deberá seguir el procedimiento inicial de verificación de identidad.

15.2. Frecuencia de re-emisión

La re-emisión solo se realizara una vez, para certificados cuya fecha de expiración es menor o igual a un año, antes de cumplirse el periodo de vigencia. El certificado re-emitido debe tener un periodo de vigencia máximo de un año.

En el caso de certificados revocados o expirados se seguirá el procedimiento inicial de verificación de identidad.

15.3. Solicitantes

Sólo los Titulares de Certificados Digitales pueden solicitar la re-emisión de certificados.

15.4. No repudio de la solicitud

Los datos de la solicitud para la re-emisión de Certificados Digitales son validados por los Operadores de Registro de la ER, a través de la plataforma de la EC, la cual permite garantizar su autenticidad y no repudio. La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS10, a través de un canal seguro SSL el cual es administrado por la EC vinculada.

15.5. Verificación de los datos de la solicitud

Para la verificación de identidad remota se validara los datos a través del documento de verificación de identidad por un notario y el documento contractual legalizado, los cuales deben ser enviados a la ER por un Courier. La comprobación de la validez y vigencia de los datos en la documentación consignada se realizara a través de los instrumentos públicos.

En el caso que el titular solicite realizar verificación presencial física en las instalaciones de la ER o en las instalaciones de la empresa deberá seguir el procedimiento inicial de verificación de identidad. La ER realiza la verificación de identidad del solicitante en el caso de ciudadanos peruanos, por las bases de datos del RENIEC mediante la comprobación de su Documento Nacional de Identidad vigente (Validación de DNI). En el caso de tratarse de solicitantes extranjeros, la ER realiza la verificación con el carné de extranjería.

15.6. Aprobación o rechazo de la solicitud

La ER debe comunicar a la EC vinculada la aprobación de la solicitud para la re-emisión del Certificado Digital debiendo contar previamente con el documento contractual de la ER legalizado y firmado por el solicitante donde constan las responsabilidades de la Entidad de Registro, de la Entidad de Certificación y del Titular de los Certificados Digitales.

La ER tiene la potestad y obligación de rechazar la solicitud de reemisión del Certificado Digital en los siguientes casos:

- Si el solicitante no tiene plena capacidad de ejercicio de sus derechos civiles.
- Si el resultado de la verificación de identidad del Titular fue negativo.

15.7. No repudio de la invitación de generación de claves e instalación del certificado

La solicitud de la ER a la EC vinculada con los datos validados del solicitante se realiza en PKCS#10, a través de un canal seguro SSL el cual es administrado por la EC vinculada.

15.8. Contrato del titular

El titular debe firmar el documento contractual legalizado de la ER en señal de conformidad de las cláusulas de este donde se indica las responsabilidades y todo lo inherente a los Certificados Digitales.

15.9. Tiempo de procesamiento

El máximo tiempo de respuesta para la emisión del certificado digital será de 2 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo por el servicio brindado.

16. Solicitud de certificados de persona jurídica de atributos

En el caso de Certificados Digitales de atributos, la persona jurídica se considera como Titular del certificado y los empleados vienen a ser los suscriptores. El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado digital, 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.

La solicitud debe ser realizada por un representante legal designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, la documentación legal que acredite sus facultades como representante.

16.1. Descripción de procedimientos

Los certificados se emitirán en módulos criptográficos, cuando el certificado sea para facturación electrónica se emitirá en formato p.12:

- El solicitante a través de la página web www.certificados.pe o www.indigitalsolutions.com, solicita la cotización y brinda los siguientes datos: número de RUC, teléfono y correo electrónico.

El correo electrónico asociado al Certificado Digital es de su uso exclusivo, ya que a través de este se le notificara sobre los procesos y ciclos de vida de su certificado digital.

- El Operador de Registro de la ER vía correo electrónico envía la cotización con la información de los requerimientos para la emisión de los Certificados.
- El solicitante debe enviar por correo electrónico el Voucher de pago y los documentos correspondientes a la cuenta de correo del operador de registro y posterior a ello se le envía el enlace para el registro de la pre-solicitud.
- El Solicitante recibirá en su correo electrónico la confirmación de la pre-solicitud y la aceptación de los términos de uso del Certificado Digital, a su vez se le informa que deberá presentarse en la ER para realizar la verificación presencial física y la entrega de los documentos correspondientes. Si existe alguna duda en cuanto al proceso de la verificación presencial física el solicitante puede comunicarse con el Operador de Registro de la ER vía correo electrónico o a los números telefónicos que están publicados en las páginas web www.certificados.pe o www.indigitalsolutions.com.
- El Operador de Registro y Validación será el encargado de validar la identificación del solicitante.
- Una vez el Solicitante realiza la confirmación de la pre-solicitud debe guardar el código de descarga en un lugar seguro ya que lo utilizara para la descarga del certificado digital; los operadores de registro de la ER reciben un correo con el enlace a la plataforma de Camerfirma para su validación y gestión (visualizar datos, modificar, validar o eliminar).Al solicitante le llegará un correo con el enlace para la generación del Certificado Digital en formato p.12

Para la emisión de Certificados Digitales de persona jurídica de atributos en módulo criptográfico se debe:

- El solicitante a través de la página web www.certificados.pe o www.indigitalsolutions.com, solicita la cotización y brinda los siguientes datos: número de RUC, teléfono y correo electrónico. El correo electrónico asociado al Certificado Digital es de su uso exclusivo, ya que a través de este se le notificara sobre los procesos y ciclos de vida de su certificado digital.
- El Operador de Registro de la ER vía correo electrónico envía la cotización con la información de los requerimientos para la emisión de los Certificados y los requisitos mínimos de compatibilidad de los módulos criptográficos homologados por la RENIEC.
- El solicitante debe enviar por correo electrónico el Voucher de pago y los documentos correspondientes a la cuenta de correo del operador de registro y posterior a ello se le envía el enlace para el registro de la pre-solicitud.
- El Solicitante recibirá en su correo electrónico la confirmación de la pre-solicitud y la aceptación de los términos de uso del Certificado Digital, a su vez se le informa que deberá presentarse en la ER para realizar la verificación presencial física y la entrega de los documentos correspondientes. Si existe alguna duda en cuanto al proceso de la verificación presencial física el solicitante puede comunicarse con el Operador de Registro de la ER vía correo electrónico o a los números telefónicos que están publicados en las páginas web www.certificados.pe o www.indigitalsolutions.com.

- El Operador de Registro y Validación será el encargado de validar la identificación del solicitante.
- Una vez el Solicitante realiza la confirmación de la pre-solicitud, los operadores de registro de la ER reciben un correo con el enlace a la plataforma de Camerfirma para su validación y gestión (visualizar datos, modificar, validar o eliminar).
- Una vez que el operador de registro valide la solicitud se procede a la descarga o inserción del certificado en el módulo criptográfico y se le enviara al solicitante a su correo el pin de revocación del certificado.
- Si la ER provee el modulo criptográfico éste debe tener la certificación FIPS 140 – 2 Nivel 2 y ser compatible con la plataforma de la EC.
- Si los Certificados Digitales son solicitados en algún departamento o ciudad distinta a las oficinas de la ER, y la misma es quién provee el módulo criptográfico, la inserción de los Certificados Digitales en el módulo criptográfico se realiza en las instalaciones de la ER y se envía a través de un proveedor de Courier.

  Si el cliente provee su mismo módulo criptográfico el operador de registro debe comprobar la vigencia (vida útil), los requisitos mínimos y la compatibilidad con la plataforma EC, en este caso la descarga o inserción del certificado digital será en las instalaciones de la ER.

16.2. Acreditar la existencia de la persona jurídica

Este proceso se valida a través de la vigencia de poder, la autenticidad del mismo se verifica en línea a través de la plataforma de la SUNARP con un tiempo menor que 90 días.

16.3. Reconocimiento de nombres y marcas registradas

La ER solicitará la documentación o información necesaria con la finalidad de garantizar que un nombre o marca pertenece al Titular del Certificado Digital solicitante. En el caso de la validación para personas jurídicas, no se podrá volver asignar un nombre de Titular que ya haya sido asignado a un Titular diferente. La documentación por presentar para la verificación es la vigencia de poder y la ficha RUC en la cual el estado del contribuyente debe estar activo y la condición del domicilio fiscal debe estar habido. La ER no se hace responsable ante alguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

16.4. Acreditar facultades de solicitantes

El solicitante de los certificados digitales deberá acreditar, a través de la vigencia de poder expedida por la SUNARP sus facultades como representante legal.

16.5. Verificación mediante consulta de base de datos nacionales

La identidad del solicitante se verifica a través de medios no repudiables, los cuales son:

- En el caso de ciudadanos peruanos, por las bases de datos del RENIEC (Validación de DNI).

- En el caso de extranjeros, por las bases de datos de Migraciones (Validación de Carné de Extranjería).

16.6. Verificación de los datos de la solicitud

Para validar los datos de la solicitud, que serán consignados a la EC es necesario que se hayan realizado las siguientes obligaciones:

- Trámite de Verificación Presencial Física del solicitante ante el Operador de Registro y Validación de la ER para una correcta identificación de este.
- Comprobación de la validez y vigencia de los datos en la documentación consignada por el solicitante.

16.7. Aprobación o rechazo de la solicitud

La ER debe comunicar a la EC vinculada la aprobación de la solicitud para la emisión del Certificado Digital debiendo contar previamente con el documento contractual de la ER legalizado y firmado por el solicitante donde constan las responsabilidades de la Entidad de Registro, de la Entidad de Certificación y del Titular de los Certificados Digitales.

La ER tiene la potestad y obligación de rechazar la solicitud de emisión del Certificado Digital en los siguientes casos:

- Si el solicitante no tiene plena capacidad de ejercicio de sus derechos civiles.
- Si el resultado de la verificación de identidad del Titular fue negativo.

16.8. Contrato del titular

El suscriptor debe firmar el documento contractual legalizado de la ER en señal de conformidad de las cláusulas de este donde se indica las responsabilidades y todo lo inherente a los Certificados Digitales.

16.9. No repudio de la solicitud

Los datos de la solicitud para la emisión de Certificados Digitales son validados por los operadores de registro de la ER, a través de la plataforma de la EC vinculada, la cual permite garantizar su autenticidad y no repudio. La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS10, a través de un canal seguro SSL el cual es administrado por la EC vinculada.

16.10. Asignación de suscriptores

La persona jurídica adopta el papel de titular del certificado digital y las personas naturales (sus empleados) vienen a ser los suscriptores de los certificados. Los suscriptores deben estar de acuerdo

con la responsabilidad que implica el obtener el certificado digital, por lo que el operador de registro de la ER verificara que el suscriptor declarado por la persona jurídica está de acuerdo, y es quien recibe el certificado digital, y que no se trata de una suplantación de identidad de suscriptores.

16.11. Verificación de la identidad de los suscriptores

La identidad del suscriptor será verificada:

- En el caso de ciudadanos peruanos, por las bases de datos del RENIEC.
- En el caso de extranjeros, por las bases de datos de Migraciones.

En cualquiera de las siguientes formas:

- De manera presencial en las instalaciones de la ER.
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER.

El suscriptor está en la obligación de presentar el original de su Documento Nacional de Identidad, en caso de Nacionalidad Peruana; o Carné de Extranjería en caso de extranjeros.

16.12. Verificación de las facultades laborales de los suscriptores

El operador de la ER verificará la documentación legal (vigencia de poder) en la cual se evidencia y acredita el ejercicio del cargo en concreto, incluyendo las limitaciones y facultades de actuar como empleado de la persona jurídica correspondientes a dicho cargo.

16.13. Verificación de los datos de la solicitud

Para validar los datos de la solicitud, que serán consignados a la EC es necesario que se hayan realizado las siguientes obligaciones:

- Trámite de Verificación Presencial Física del solicitante ante el Operador de Registro y Validación de la ER para una correcta identificación de este.
- Comprobación de la validez y vigencia de los datos en la documentación consignada por el solicitante.

16.14. Información no verificada del suscriptor o titular

De manera general no debe incluirse 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 debe comprobar que la dirección de correo electrónico que se incluye en

el certificado es la que efectivamente desea incluir el solicitante. Pero, la ER no tiene que comprobar ni la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, toda la responsabilidad recae en el solicitante.

16.15. No repudio de la invitación de generación de claves e instalación del certificado

La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS#10; a través de un canal seguro SSL. En caso de realizarse la generación de clave fuera de las instalaciones de la ER la petición PKCS#10 se realiza a través de medios de comunicación no repudiables con canal seguro SSL para prever posibles suplantaciones de identidad digital.

16.16. Tiempo de procesamiento

El máximo tiempo de respuesta para la emisión del certificado digital será de 2 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo por el servicio brindado.

17. Re-emisión de certificados de persona jurídica de atributos

La plataforma dispuesta por la EC vinculada permite realizar la re-emisión de Certificados Digitales, cuando la fecha de expiración del mismo sea próxima o haya expirado. Una vez realizados todos los procesos y validaciones correspondientes a la solicitud, se obtendrá un nuevo par de claves y un nuevo Certificado Digital.

17.1. Descripción de procedimientos

Para la re-emisión de Certificados Digitales de persona jurídica de atributos el operador de registro informa con anticipación a través del correo electrónico al titular del certificado digital sobre la reemisión del mismo; a su vez envía todas las especificaciones para la gestión. En este caso el titular del certificado digital debe validar su identidad a través de la verificación de identidad por parte de un notario y el documento contractual de la ER legalizado, también puede realizar la validación de identidad a través de la verificación presencial física en las instalaciones de la ER o en las instalaciones de la empresa para ello deberá seguir el procedimiento inicial de verificación de identidad.

17.2. Autorizado para realizar la solicitud

Solo el titular y/o suscriptor designado como representante legal por la persona jurídica ante la ER a través de la documentación legal (vigencia de poder) que acredite sus facultades como representante legal puede realizar la solicitud de la re-emisión del Certificado Digital.

17.3. Frecuencia de re-emisión

En el caso de certificados expirados la re-emisión solo puede ser realizada una vez, para certificados cuya fecha de expiración es menor o igual a dos años. El certificado re-emitido tendrá un periodo de vigencia máximo de un año.

En el caso de certificados revocados, la re-emisión requiere de una validación inicial de identidad.

17.4. No repudio de la solicitud

Los datos de la solicitud para la re-emisión de Certificados Digitales son validados por los operadores de registro de la ER a través de la plataforma de la EC vinculada, la cual permite garantizar su autenticidad y no repudio. La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS#10 a través de un canal seguro SSL el cual es administrado por la EC vinculada.

17.5. Verificación de los datos de la solicitud

Para la verificación de identidad remota se validara los datos a través del documento de verificación de identidad por un notario y el documento contractual legalizado, los cuales deben ser enviados a la ER por un Courier. La comprobación de la validez y vigencia de los datos en la documentación consignada se realizara a través de los instrumentos públicos.

En el caso que el titular solicite realizar verificación presencial física en las instalaciones de la ER o en las instalaciones de la empresa deberá seguir el procedimiento inicial de verificación de identidad. La ER realiza la verificación de identidad del solicitante en el caso de ciudadanos peruanos, por las bases de datos del RENIEC mediante la comprobación de su Documento Nacional de Identidad vigente (Validación de DNI). En el caso de tratarse de solicitantes extranjeros, la ER realiza la verificación con el carné de extranjería.

17.6. Aprobación o rechazo de la solicitud

La ER debe comunicar a la EC vinculada la aprobación de la solicitud para la re-emisión del Certificado Digital debiendo contar previamente con el documento contractual de la ER legalizado y firmado por el solicitante donde constan las responsabilidades de la Entidad de Registro, de la Entidad de Certificación y del Titular de los Certificados Digitales.

La ER tiene la potestad y obligación de rechazar la solicitud de re-emisión del Certificado Digital en los siguientes casos:

- Si el solicitante no tiene plena capacidad de ejercicio de sus derechos civiles.
- Si el resultado de la verificación de identidad del Titular fue negativo.

17.7. No repudio de la invitación de generación de claves e instalación del certificado

La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS#10 a través de un canal seguro SSL. En caso de realizarse la generación de clave fuera de las instalaciones de la ER la petición PKCS#10 se realiza a través de medios de comunicación no repudiables con canal seguro SSL el cual es administrado por la EC vinculada.

17.8. Conformidad de los suscriptores

Los suscriptores deberán expresar su conformidad respecto a la re-emisión de los Certificados Digitales a través del documento contractual de la ER legalizado y firmado por el solicitante donde constan las responsabilidades de la Entidad de Registro, de la Entidad de Certificación y del Titular de los Certificados Digitales, aceptando las responsabilidades implicadas, así como las consecuencias de no cumplir con lo estipulado.

17.9. Tiempo de procesamiento

El máximo tiempo de respuesta para la emisión del certificado digital será de 2 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo por el servicio brindado.

18. Solicitud de certificados de persona jurídica - agente automatizado

Si el Certificado Digital esta designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica, la cual deberá ser dueña del agente automatizado. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el Certificado Digital.

18.1. Descripción de procedimientos

Para la emisión de Certificados Digitales de agente automatizado solo para facturación electrónica se emitirá en formato p.12 se debe:

- El solicitante a través de la página web www.certificados.pe o www.indigitalsolutions.com, solicita la cotización y brinda los siguientes datos: número de RUC, teléfono y correo electrónico. El correo electrónico asociado al Certificado Digital es de su uso exclusivo, ya que a través de este se le notificara sobre los procesos y ciclos de vida de su certificado digital.
- El Operador de Registro de la ER vía correo electrónico envía la cotización con la información de los requerimientos para la emisión de los Certificados.
- El solicitante debe enviar por correo electrónico el Voucher de pago y los documentos correspondientes a la cuenta de correo del operador de registro y posterior a ello se le envía el enlace para el registro de la pre-solicitud.
- El Solicitante recibirá en su correo electrónico la confirmación de la pre-solicitud y la aceptación de los términos de uso del Certificado Digital, a su vez se le informa que deberá presentarse en

la ER para realizar la verificación presencial física y la entrega de los documentos correspondientes. Si existe alguna duda en cuanto al proceso de la verificación presencial física el solicitante puede comunicarse con el Operador de Registro de la ER vía correo electrónico o a los números telefónicos que están publicados en las páginas web www.certificados.pe o www.indigitalsolutions.com.

- El Operador de Registro y Validación será el encargado de validar la identificación del solicitante.
- Una vez el Solicitante realiza la confirmación de la pre-solicitud debe guardar el código de descarga en un lugar seguro ya que lo utilizara para la descarga del certificado digital; los operadores de registro de la ER reciben un correo con el enlace a la plataforma de Camerfirma para su validación y gestión (visualizar datos, modificar, validar o eliminar).Al solicitante le llegará un correo con el enlace para la generación del Certificado Digital en formato p.12

18.2. Acreditar la existencia de la persona jurídica

Este proceso se valida a través de la vigencia de poder, la autenticidad del mismo se verifica en línea a través de la plataforma de la SUNARP en un tiempo menor a 90 días.

18.3. Acreditar las facultades del solicitante

El solicitante de los certificados digitales deberá acreditar, a través de la vigencia de poder expedida por la SUNARP sus facultades como representante legal.

18.4. Verificación mediante consulta de base de datos nacionales

La identidad del solicitante se verifica a través de medios no repudiables, los cuales son:

- En el caso de ciudadanos peruanos, por las bases de datos del RENIEC (Validación de DNI).
- En el caso de extranjeros, por las bases de datos de Migraciones (Validación de Carné de Extranjería).

18.5. Reconocimientos de nombres y marcas registrados

La ER solicitará la documentación o información necesaria con la finalidad de garantizar que un nombre o marca pertenece al Titular del Certificado Digital solicitante. En el caso de la validación para personas jurídicas, no se podrá volver asignar un nombre de Titular que ya haya sido asignado a un Titular diferente. La documentación a presentar para la verificación es la vigencia de poder y la ficha RUC en la cual el estado del contribuyente debe estar activo y la condición del domicilio fiscal debe estar habido. La ER no se hace responsable ante alguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

18.6. Verificación de los datos de la solicitud

Para validar los datos de la solicitud, que serán consignados a la EC es necesario que se hayan realizado las siguientes obligaciones:

- Trámite de Verificación Presencial Física del solicitante ante el Operador de Registro y Validación de la ER para una correcta identificación del mismo.
- Comprobación de la validez y vigencia de los datos en la documentación consignada por el solicitante.

18.7. Aprobación o rechazo de la solicitud

La ER debe comunicar a la EC vinculada la aprobación de la solicitud para la emisión del Certificado Digital debiendo contar previamente con los términos y condiciones legalizado y firmado por el solicitante donde constan las responsabilidades de la Entidad de Registro, de la Entidad de Certificación y del Titular de los Certificados Digitales.

La ER tiene la potestad y obligación de rechazar la solicitud de emisión del Certificado Digital en los siguientes casos:

- Si el solicitante no tiene plena capacidad de ejercicio de sus derechos civiles.
- Si el resultado de la verificación de identidad del Titular fue negativo.

18.8. Contrato del titular

El suscriptor debe firmar el documento contractual legalizado de la ER en señal de conformidad de las cláusulas de este donde se indica las responsabilidades y todo lo inherente a los Certificados Digitales.

18.9. No repudio de la solicitud

Los datos de la solicitud para la emisión de Certificados Digitales son validados por los operadores de registro de la ER, a través de la plataforma de la EC, la cual permite garantizar su autenticidad y no repudio. La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS#10, a través de un canal seguro SSL el cual es administrado por la EC vinculada.

18.10. No repudio de la petición del certificado

La solicitud de los Certificados Digitales se realiza a través de la plataforma de la EC, la cual cuenta con todos los medios no repudiables. Cada uno de los procesos para obtener el Certificado Digital asegura que proviene de la entidad validada y por las personas autorizadas. La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS#10 a través de un canal seguro SSL. En caso de realizarse la generación de clave fuera de las instalaciones de la ER la petición PKCS#10 se realiza a través de medios de comunicación no repudiables con canal seguro SSL el cual es administrado por la EC vinculada.

18.11. Tiempo de procesamiento

El máximo tiempo de respuesta para la emisión del certificado digital será de 2 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo por el servicio brindado.

19. Re-emisión de certificados de persona jurídica – agente automatizado

La re-emisión de certificados digitales para agentes automatizados solo puede ser realizada una vez, cuando haya sido revocado un certificado digital antes de ser cumplido su periodo de vigencia

19.1. Descripción de procedimientos

Para la re-emisión de Certificados Digitales de agentes automatizados el operador de registro informa con anticipación a través del correo electrónico al titular del certificado digital sobre la re-emisión del mismo; a su vez envía todas las especificaciones para la gestión. En este caso el titular del certificado digital debe validar su identidad a través de la verificación de identidad por parte de un notario y el documento contractual de la ER legalizado, también puede realizar la validación de identidad a través de la verificación presencial física en las instalaciones de la ER o en las instalaciones de la empresa para ello deberá seguir el procedimiento inicial de verificación de identidad.

19.2. Autorizado para realizar la solicitud

Solo el titular y/o suscriptor designado como representante legal por la persona jurídica ante la ER a través de la documentación legal (vigencia de poder) que acredite sus facultades como representante legal puede realizar la solicitud de la re-emisión del Certificado Digital.

19.3. Frecuencia de re-emisión

La re-emisión sólo puede ser realizada una vez, cuando haya sido revocado un certificado digital antes de ser cumplido su periodo de vigencia.

19.4. No repudio de la solicitud

Los datos de la solicitud para la re-emisión de Certificados Digitales son validados por los operadores de registro de la ER a través de la plataforma de la EC vinculada, la cual permite garantizar su autenticidad y no repudio. La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS#10 a través de un canal seguro SSL el cual es administrado por la EC vinculada.

19.5. Verificación de los datos de la solicitud

Para la verificación de identidad remota se validara los datos a través del documento de verificación de identidad por un notario y el documento contractual legalizado, los cuales deben ser enviados a la ER

por un Courier. La comprobación de la validez y vigencia de los datos en la documentación consignada se realizara a través de los instrumentos públicos.

En el caso que el titular solicite realizar verificación presencial física en las instalaciones de la ER o en las instalaciones de la empresa deberá seguir el procedimiento inicial de verificación de identidad. La ER realiza la verificación de identidad del solicitante en el caso de ciudadanos peruanos, por las bases de datos del RENIEC mediante la comprobación de su Documento Nacional de Identidad vigente (Validación de DNI). En el caso de tratarse de solicitantes extranjeros, la ER realiza la verificación con el carné de extranjería.

19.6. Aprobación o rechazo de la solicitud

La ER debe comunicar a la EC vinculada la aprobación de la solicitud para la re-emisión del Certificado Digital debiendo contar previamente con los términos y condiciones legalizado y firmado por el solicitante donde constan las responsabilidades de la Entidad de Registro, de la Entidad de Certificación y del Titular de los Certificados Digitales.

La ER tiene la potestad y obligación de rechazar la solicitud de re-emisión del Certificado Digital en los siguientes casos:

- Si el solicitante no tiene plena capacidad de ejercicio de sus derechos civiles.
- Si el resultado de la verificación de identidad del Titular fue negativo.

19.7. No repudio de la invitación de generación de claves e instalación del certificado

La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS#10 a través de un canal seguro SSL. En caso de realizarse la generación de clave fuera de las instalaciones de la ER la petición PKCS#10 se realiza a través de medios de comunicación no repudiables con canal seguro SSL el cual es administrado por la EC vinculada.

19.8. Tiempo de procesamiento

El máximo tiempo de respuesta para la re-emisión del certificado digital será de 2 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo por el servicio brindado.

20. Entidades de certificación afiliadas a la ER

La ER – INDIGITAL se encuentra afiliada y/o vinculada a la EC – CAMERFIRMA PERÚ.

20.1. Publicación de Entidades

La información normativa de la EC vinculada se encuentra en la página web de INDIGITAL www.indigitalsolutions.com.

20.2. Publicación de CP y CPS

Los documentos de Política de Certificación (CP) y la Declaración de Prácticas de Certificación (CPS) de la EC vinculada, se publicarán en la página web www.camerfirma.com.pe.

20.3. Publicación de certificaciones

La EC vinculada cuenta con la acreditación web Webtrust for Certification Authorities Resolución de Acreditación o cualquiera de sus equivalentes reconocidos por la AAC, las cuales se encuentran publicadas en la página web www.camerfirma.com.pe.

20.4. Publicación de un documento que acredite la representación de la EC

El documento que acredita la vinculación con la EC se publicará en la página web www.indigitalsolutions.com.

20.5. Limitación de responsabilidades

La limitación de responsabilidades, por los temas de compensación y garantías con la EC vinculada se encuentra definida en los contratos firmados por ambas partes.

21. Revocación de certificados de persona natural o jurídica

A efectos de una solicitud de revocación, el Titular y suscriptor de un Certificado Digital, bajo su responsabilidad, pueden realizar la mencionada solicitud, al tener conocimiento de la ocurrencia de cualquiera de las siguientes situaciones:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica privada o pública.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la ER.
- 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 “Acuerdo del Suscriptor”.
- Por decisión de la legislación respectiva.
- Por resolución administrativa o judicial que lo ordene.
- Por suplantación de identidad.

21.1. Descripción de procedimientos

El solicitante podrá revocar su certificado digital; accediendo a la plataforma de la EC vinculada www.camerfirma.com en el menú de Área de Usuario y submenú de Revocar certificado o directamente a través del link:
https://status.camerfirma.com/certificados_2010/revocar_certificado.php haciendo uso del PIN de revocación que recibió en su correo electrónico al momento de confirmar la validación de la solicitud.

21.1.1. Registro de documentos

La ER 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 EC vinculada, sus suscriptores y los terceros que confían. En cumplimiento de la Política de Seguridad de la ER, toda la documentación será protegida contra acceso no autorizado y destrucción. En caso que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

21.2. Solicitantes

Conforme a lo establecido por la Ley, el tipo de personas que pueden solicitar la revocación de un Certificado Digital son las siguientes:

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

En el caso de personas jurídicas, los Titulares de los Certificados Digitales pueden solicitar la revocación de los mismos, por lo que la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.
En el supuesto que como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER, será suficiente con presentar su solicitud firmada de forma manuscrita (previa presentación de su documento de identidad) o con firma digital al operador de registro.

21.3. No repudio de la solicitud

Los datos de la solicitud para la revocación de los Certificados Digitales son validados por los operadores de registro de la ER a través de la plataforma de la EC, la cual permite garantizar su autenticidad y no repudio. La solicitud de la ER a la EC con los datos validados del solicitante se realiza en PKCS#10 a través de un canal seguro SSL el cual es administrado por la EC vinculada.

21.4. Aprobación o rechazo de la solicitud

La ER debe comunicar a la EC vinculada la aprobación de la solicitud para la revocación del Certificado Digital, a través de un medio de comunicación no repudiable con canal seguro SSL, el cual será brindado por la EC.
La ER tiene la potestad y obligación de rechazar la solicitud de revocación del Certificado Digital en los siguientes casos:

- Si el solicitante no tiene plena capacidad de ejercicio de sus derechos civiles.
- Si el resultado de la verificación de identidad del Titular fue negativo.

21.5. Ejecución de la revocación

La ER publicará los tiempos máximos que tardará la ejecución de la revocación de los Certificados Digitales, desde la solicitud de los Titulares o suscriptores. Una vez aceptada la solicitud este tiempo no debe ser mayor a 2 horas para la actualización de la base de datos de las consultas OCSP y de 24 horas para la actualización de la lista CRL.

21.6. Tiempo de procesamiento

La ER comunicará a la EC vinculada vía correo electrónico la revocación del Certificado Digital. El máximo tiempo de respuesta para la revocación del Certificado Digital dependerá de lo establecido en la CP y CPS de la EC vinculada.

22. Suspensión de certificados de persona jurídica

No aplica.

23. Protección de registros

Los documentos digitales serán almacenados en un gestor documental, el cual permitirá la asignación de controles de seguridad para salvaguardar la información confidencial de la ER, la misma que será accedida solo por personal autorizado.

En el caso de los documentos físicos, estos serán custodiados por un periodo mínimo de 10 años dentro de un armario corta fuego o ignifugo, su acceso será solo al personal que la ER designe.

23.1. Tipos de eventos registrados

- Información de contacto de los solicitantes de los servicios de la ER, incluyendo a suscriptores y Titulares.
- Solicitudes de emisión, re-emisión y revocación de Certificados Digitales, realizadas mediante la plataforma de la EC vinculada.
- Resultados y evidencias de cada proceso de validación de identidad de persona jurídica o natural, incluyendo procesos con resultados positivos como procesos fallidos en los que se denegó el servicio a un cliente.
- Contratos del suscriptor y/o Titular.
- Registros o evidencias de las solicitudes de emisión, reemisión y revocación de Certificados Digitales realizadas por parte de los operadores de registro a la EC, indicando el operador de registro que realizó la transacción.
- Registro de expediente de todos los involucrados en la ER.
- Registros de certificados emitidos y/o revocados.
- Designación de roles de la ER.
- Documentación normativa de la ER.

23.2. Protección de los registros

Los documentos digitales serán almacenados en un gestor documental en los servidores de la ER, el cual permitirá la asignación de permisos de lectura y escritura a la información confidencial, además permitirá visualizar un historial de los accesos y modificaciones por parte de todos los involucrados de la ER. Únicamente los operadores de registro tendrán acceso a la plataforma de la EC para realizar los procesos de emisión, re-emisión, revocación y/o suspensión de los Certificados Digitales.

En el caso de los documentos físicos, estos serán almacenados en las instalaciones de la ER y custodiados dentro de un armario corta fuego o ignifugo en un ambiente restringido, el control de acceso al ambiente restringido se gestionará a través de una lista de entrada y salida y por cámaras de seguridad. El acceso al armario que custodiará la información solo será permitido al personal que la ER designe. El traslado de los registros físicos solo se dará cuando la ER cambie su dirección social o fiscal, previa autorización de la autoridad competente.

23.3. Archivo de los registros

La información almacenada de las operaciones de la ER se encuentra en ambientes restringidos con controles físicos y ambientales para garantizar la duración de la información, incluyendo control anti incendio, acceso físico y aniego.

23.4. Tiempo de almacenamiento del archivo

Los registros físicos de información serán almacenados por un periodo mínimo de 10 años en las instalaciones de la ER. La destrucción de los registros de información solo se podrá llevar a cabo con la autorización del INDECOPI, siempre y cuando haya transcurrido su periodo de almacenamiento mínimo.

24. Seguridad en las comunicaciones con la EC

La comunicación entre la ER y la EC se realizara a través de la plataforma de la EC vinculada, la comunicación se realiza por SSL y usando los certificados digitales de los operadores de registros autorizados.

24.1. Uso de los canales seguros

La comunicación entre la ER y la EC se realizará usando un canal seguro SSL, para realizar los procesos de emisión, re-emisión, revocación y suspensión de Certificados Digitales.

24.2. Autenticación de operadores de registro

La autenticación de los operadores de registro de la ER con la plataforma de la EC se realiza mediante un Certificado Digital autorizado como operador de registro emitido en un módulo criptográfico que cumple la certificación FIPS 140 – 2 nivel 2 como mínimo.

24.3. Registros de auditoría

Los registros de auditoría sobre las solicitudes de emisión, re-emisión y revocación de certificados son gestionados por la plataforma de la EC vinculada.

Los registros generados de auditorías internas son gestionados a través del gestor documental.

24.4. Seguridad Computacional

Los computadores utilizados por los operadores de registro cuentan con una aplicación antivirus y los parches del sistema antivirus y sistema operativo actualizados.

24.5. Gestión de residuos

La información confidencial almacenada en soportes de almacenamiento digital es eliminada de forma segura siguiendo procedimientos de formateo del equipo principal. En el caso de la información física su destrucción se llevara a cabo utilizando un triturador de papel.

25. Seguridad del personal

La ER implementa los siguientes controles y requisitos para el personal que participa en sus operaciones, estos son:

- Antecedentes policiales, penales y crediticios.
- Firma de Acuerdo de confidencialidad por ambas partes.
- Control de acciones realizadas en la plataforma de la EC vinculada.
- Capacitaciones.

25.1. Definición de roles

La ER ha definido y comunicado las funciones a su personal, los cuales se encuentran descritos en el documento de definición y/o asignación de roles.
Los roles que la ER ha designado son:

- Responsable de la ER
- Oficial de Privacidad de Datos
- Operador de Registro
- Operador de Registro y Validación
- Auditor Interno

25.2. Verificación de antecedentes

Los roles de la ER cuentan con antecedentes penales, policiales y crediticios, a fin de reducir las posibilidades de suplantación de identidad.

25.3. Cualidades, requisitos, experiencia y certificados

La ER establece los siguientes requisitos básicos de formación y conocimiento:

- Responsable de la ER: Como mínimo se requiere conocimientos en Certificados Digitales y firmas electrónicas.
- Operador de Registro y Validación: Como mínimo se requiere formación técnica y cocimientos básicos en administración o secretariado y conocimiento en Certificados Digitales.
- Oficial de Privacidad de Datos: Como mínimo se requiere conocimientos básicos en Seguridad de la Información y conocimiento en Certificados Digitales.
- Auditor Interno: Como mínimo se requiere conocimientos básicos de auditorías y conocimiento en Certificados Digitales y Firma Digital.

25.4. Compromiso contractual de confidencialidad

Se establece un acuerdo de confidencialidad entre la ER y el personal involucrado en sus operaciones respecto a la protección de la privacidad y confidencialidad de la información suministrada por los clientes, el mismo que es firmado por ambas partes en señal de conformidad.

25.5. Responsabilidades contractuales

Las responsabilidades contractuales entre la ER y sus participantes se definen en los contratos, de ocasionar algún compromiso estarán cubiertas por una póliza de seguro de responsabilidad civil contratada por la ER.

25.6. Compromiso de cumplir la política de seguridad

El oficial de privacidad de datos de la ER capacitara como mínimo dos veces al año al personal involucrado en las operaciones de la ER reforzando el cumplimiento de la Política de Seguridad, se firmara un documento de compromiso y cumplimiento de la Política.

25.7. Capacitación

El personal de la ER que tiene acceso a la plataforma de la EC vinculada para realizar las solicitudes de emisión, re-emisión y revocación de certificados digitales, debe recibir capacitaciones continuas respecto a:

- Certificados Digitales
- Firma digital
- Regulación de la IOFE
- Política de registro
- Políticas de seguridad y privacidad de la ER
- RPS
- Plan de contingencia
- Funciones respecto de su rol
- Seguridad de la Información
- La frecuencia de la capacitación deberá ser de al menos una vez antes de operar en la ER y luego de manera anual.

25.8. Sanciones por acciones no autorizadas

Las sanciones al personal involucrado en la ER están definidas en el documento contractual que vincula a la ER con los colaboradores.

25.9. Rotación en el trabajo

La ER en caso determine la conveniencia podrá implementar rotaciones de trabajo entre los distintos roles definidos, con el objeto de asegurar la continuidad de las operaciones e incrementar la seguridad. Las rotaciones serán comunicadas a los colaboradores con la documentación pertinente.

26. Auditoría

La ER, efectuará auditorías internas al menos una vez al año. Se someterá a auditorias por parte de la AAC cada vez que ésta lo requiera, respecto a las operaciones realizadas como Entidad de Registro.

26.1. Auditoría de registros

Los registros deben ser revisados como parte de la auditoría de la AAC, de manera anual.

26.2. Auditoría del archivo

El archivo debe ser revisado como parte de la auditoría de la AAC, de manera anual.

26.3. Auditoría de los procedimientos y controles

Los procedimientos y controles implementados deben ser auditados por la AAC anualmente.
Las auditorías internas deben llevarse a cabo, como mínimo, una vez al año en la ER.

26.4. Auditor

El auditor es seleccionado de la lista de auditores autorizados por la AAC.
El auditor no deberá haber laborado para la ER, ni deberá haber tenido ninguna relación comercial con la misma, ni de efectos de auditoría en el mismo alcance de evaluación, en los últimos 2 años calendario.

27. Medidas de contingencia

La ER cuenta con medidas de contingencia definidas en el plan de contingencia.

27.1. Protección contra compromisos de las claves del suscriptor

La protección en cuanto a los compromisos de las claves del titular y/o suscriptor está definida en los contratos del Titular.

27.2. Compromiso de las claves del operador de registro

La ER debe establecer procedimientos en caso de compromiso de las claves del operador de registro.

27.3. Contingencia en caso de indisponibilidad de servicios de recepción de solicitudes de revocación

La ER debe establecer canales alternos de recepción de solicitudes de revocación de certificados, en caso que estos no puedan ser recibidos por la ER. Entendiéndose que la recepción involucra los pasos de verificación de identidad y aprobación o negación de la solicitud.

27.4. Contingencia en caso de indisponibilidad de servicios de recepción de solicitudes de re-emisión

La ER debe establecer canales alternos de recepción de solicitudes de re-emisión de certificados, en caso que estos no puedan ser recibidos por la ER.
Entendiéndose que la recepción involucra los pasos de verificación de identidad y aprobación o negación de la solicitud.

28. Finalización de la ER

Antes de su finalización, la ER – INDIGITAL deberá informar al INDECOPI, a los titulares, suscriptores y terceros que confían sobre el cese de sus operaciones.

28.1. Procedimiento de finalización

La ER cesa en sus operaciones en los casos siguientes:

- Decisión adoptada por la Junta General de Accionista.
- Transferencia de la titularidad de la empresa.
- Sanción impuesta por INDECOPI.
- Decisión judicial.
- Disolución y liquidación de la empresa.

La ER – INDIGITAL informará al INDECOPI sobre el cese de sus operaciones con por lo menos 60 días calendario de anticipación y a los titulares, suscriptores y terceros que confían con por lo menos 30 días calendario de anticipación. Además se deberá publicar un comunicado en la página web de INDIGITAL (www.indigitalsolutions.com).

Todos los registros de solicitudes y contratos de titulares y suscriptores deberán ser transferidos al INDECOPI o a otro PSC designado por éste.

En caso de una transferencia de titularidad, los nuevos dueños o responsables de la ER deberán solicitar al INDECOPI una evaluación de cumplimiento para garantizar que se mantienen los requisitos de acreditación.

28.2. Transferencia de los registros de auditoría

Todos los registros de datos de la ER (solicitudes, contratos, etc.) se transferirán al INDECOPI o a otra ER acreditada por el INDECOPI, a fin de cumplir con la custodia de 10 años establecida por la AAC después de generado el registro.

28.3. Garantías y responsabilidades

Las garantías por los servicios prestados como entidad de registro (registro de datos, errores u omisiones de validación de identidad, procesamiento de las solicitudes de emisión, re-emisión o revocación y protección de datos personales) son definidos en los contratos.

Las responsabilidades de los titulares y suscriptores se definen en los respectivos términos y condiciones, en particular tienen la responsabilidad de solicitar ante la ER la revocación de sus certificados digitales en caso de compromiso de su clave privada. En caso de los terceros que confían, estos tienen la responsabilidad de verificar el estado de confiablidad de los certificados digitales dentro del marco normativo establecido por la IOFE.

La ER no se responsabiliza si el titular/suscriptor compromete su clave privada o si realiza cualquier solicitud fuera de los procedimientos descritos o definidos en el presente documento.

28.4. Transferencia de las operaciones de registro para las solicitudes de revocación y re-emisión

La ER en coordinación con el INDECOPI deberá transferir todos los registros de solicitudes de revocación y reemisión a otra Entidad de Registro acreditada por el INDECOPI.

29. Aspectos Legales de la Operación de la ER

29.1. Tarifas

Las tarifas para la emisión de los Certificados Digitales serán definidas en las cotizaciones enviadas a cada cliente, estás pueden incluir:

- Servicios de visita para verificación presencial de identidad
- Servicios por emisión de certificados
- Servicios por módulo criptográficos
- Servicios de envío
- Política de reembolso
- Otros que se consideren necesarios

Las tarifas de la ER son establecidas en coordinación con la EC vinculada, y la ER debe asumir las tarifas por participar en la IOFE, cumpliendo la legislación Peruana.

29.2. Política de reembolso

La ER cuenta con la siguiente política de reembolso para los siguientes casos:

- Por el registro de información errónea que se encuentra en el certificado
- Cuando el certificado no puede ser instalado correctamente en el módulo criptográfico proporcionado por la ER, debido a inconvenientes con la plataforma.
- Cuando se proporciona un certificado de propósitos o características tecnológicas diferentes al solicitado.
- Si se disuelve sin motivo por parte de la EC o ER.

El Titular/suscriptor debe enviar un correo a rhuaman@indigitalsolutions.com indicando el motivo del reembolso y las evidencias pertinentes para ser verificados por la ER y brindar una respuesta a la solicitud realizada.

Excepciones

La política de reembolso no cubre cuando:

- El módulo criptográfico del solicitante no se encuentre homologado con la plataforma de emisión de la ER
- El solicitante provee el módulo criptográfico que no cuente con la certificación FIPS 140 – 2 Nivel 2
- Si la EC hubiera emitido el Certificado Digital pero el Suscriptor/Titular no lo hubiera descargado en Software o recogido en el correspondiente dispositivo Hardware.
- Si se disuelve sin motivo por parte del Suscriptor/Titular, no se realizarán reembolsos del monto cancelado.
- En caso de disolución por parte de la EC o ER y con motivo (incumplimiento por partes el Suscriptor), no se realizarán reembolsos.

29.3. Responsabilidad Financiera

La EC dispone de una garantía de cobertura de su responsabilidad civil suficiente, bien mediante un seguro de responsabilidad civil profesional por errores y omisiones. En cualquier caso, la cuantía garantizada cubrirá la cuantía mínima establecida por la Autoridad Administrativa Competente en todo momento, que cubre las operaciones de la plataforma.

La ER cuenta con los recursos financieros para apoyar el desempeño de las responsabilidades operacionales que realizan, se cuenta con una póliza de responsabilidad civil que cubre las operaciones por errores y omisiones. En cualquier caso, la cuantía garantizada cubrirá la cuantía mínima establecida por la Autoridad Administrativa Competente en todo momento.

29.4. Información confidencial

Las disposiciones referentes a la información confidencial son descritas en el Plan de Privacidad de la ER.

29.5. Información privada

Las disposiciones referentes a la información privada son descritas en el Plan de Privacidad de la ER.

29.6. Información no privada

Las disposiciones referentes a la información no privada o no confidencial son descritas en el Plan de Privacidad de la ER.

29.7. Derechos de propiedad intelectual

Todos los derechos de propiedad intelectual de la presente Declaración de Prácticas, Políticas de Registro, Política de Seguridad, Política de Privacidad y Plan de Privacidad, así como cualquier otro documento, electrónico o de cualquier otro tipo, son de propiedad de INDIGITAL. Por lo tanto queda expresamente prohibido cualquier acto de reproducción, distribución, comunicación pública o transformación de cualquiera de los elementos que son de titularidad de INDIGITAL.

29.8. Representaciones y garantías

Las garantías por los servicios de la ER son definidas en el contrato, en relación a errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de los certificados digitales, revocación de los mismos y la protección de los datos personales suministrados.

29.9. Excepciones de responsabilidad de garantías

Las excepciones de garantías por los servicios de la ER son definidas en el contrato, de manera particular la ER no se responsabiliza en casos de compromiso de la clave privada en manos del cliente, o cualquier solicitud no realizada según los procedimientos definidos en la presente Declaración de Prácticas.

29.10. Notificaciones y comunicaciones entre participantes

La ER establecerá la comunicación con sus clientes y otros participantes a través de su página web www.indigitalsolutions.com y por correo electrónico. Con la finalidad de mantenerlos informados en cuanto a los cambios en las políticas y prácticas de los PSC acreditados a los suscriptores, terceros que confían y otras partes tales como otras infraestructuras cuando dichos cambios puedan afectarles. A su vez cualquier cambio en los términos y condiciones deberá ser notificado a los suscriptores y terceros que confían.

29.11. Correcciones o enmiendas

Las correcciones y enmendaduras serán comunicadas al INDECOPI y luego de su aprobación serán publicadas en la página web de INDIGITAL.

29.12. Procedimiento de resolución de disputas

El procedimiento de resolución de disputas está establecido en el documento de términos y condiciones.

29.13. Conformidad con la Ley aplicable

La ER declara que el presente documento está basado en conformidad con la Ley aplicable y su reglamento de acuerdo a la Ley N° 27269.

29.14. Cumplimiento de la Ley aplicable

La ER se compromete a cumplir la Ley aplicable a las operaciones de registro según lo estipulado en la Guía de Acreditación de Entidad de Registro del INDECOPI, la Ley de Firmas y Certificados Digitales y su Reglamento, y la protección de datos personales acorde a la Ley N° 29733.

29.15. Limitaciones de responsabilidad

La ER establece en los contratos del titular, suscriptor o tercero que confía, las limitaciones de responsabilidad que aplican.

29.16. Indemnizaciones

La ER establece en los contratos del titular, suscriptor o tercero que confía, los casos de indemnización que aplican.

29.17. Vigencia y conclusión

La documentación normativa es vigente en el periodo de acreditación.

29.18. Provisiones misceláneas

Las provisiones misceláneas serán definidas en los contratos de titulares, en relación con errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de los certificados o de revocación y protección de datos personales provistos.

29.19. Otras provisiones

La ER puede incluir en su RPS o en el contrato de términos y condiciones otras disposiciones donde las responsabilidades y los términos que no encajan perfectamente dentro de uno de las secciones anteriores pueden ser impuestas a los participantes de la PKI.

30. Seguridad de la gestión del ciclo de vida de las claves del suscriptor

30.1. Obtención de los módulos criptográficos

La ER mantendrá controles para garantizar de manera razonable que:

a) Las obtenciones del módulo son controladas por la EC o ER
b) El uso del módulo es habilitado por la ER antes de emitir el módulo
c) Los módulos son almacenados y distribuidos de manera segura por la ER
d) Si la ER contrata a un tercero encargado de gestionar y proteger los módulos, debe existir un contrato formal entre ambas partes. La ER mantiene la responsabilidad y obligaciones de garantizar la protección de los módulos.
e) Los módulos deben ser lógicamente protegidos durante su transporte desde su fabricación hasta su emisión mediante una clave de transporte o una frase de paso.
f) Los módulos cumplen los estándares FIPS 140-2 nivel 2 o Common Criteria EAL 4+ como mínimo.

30.2. Preparación y personalización

a) En caso que la personalización y generación de las claves sea gestionada por la ER debe garantizar la seguridad y autenticidad de los procesos de personalización del módulo, los cuales incluyen lo siguiente:
    i. La carga de la información de identificación dentro del módulo.
    ii. La generación de las claves del suscriptor
    iii. La carga del certificado del suscriptor en el módulo garantizando que no existen generación de copias ni uso no autorizado de la clave, y que solamente el suscriptor tiene acceso y control sobre la misma.
    iv. Protección lógica del módulo de acceso no autorizado.
b) La ER debe generar registros de auditoría de los procesos de preparación y personalización
c) El módulo no puede ser emitido sino ha sido personalizado por la ER.
d) Un módulo no puede ser utilizado sino se encuentra en estado de activación o reactivación

30.3. Almacenamiento y distribución del módulo criptográfico

a) El operador de registro de la ER llevara un control de los módulos criptográficos donde se visualizara el listado con toda la información de distribución y recepción del módulo por parte del suscriptor.
b) Los datos de activación del módulo (PIN y PUK) son comunicados de manera segura al suscriptor garantizando que sólo él suscriptor tiene acceso a los mismos.

30.4. Uso del módulo criptográfico

a) El suscriptor debe ser provisto de un mecanismo que protege el acceso a los datos del módulo incluyendo el almacenamiento de las claves privadas.
b) Las claves del suscriptor no deben poder ser exportadas por una aplicación para realizar funciones criptográficas
c) El suscriptor debe ser requerido para usar mecanismos de autenticación para aplicaciones criptográficas y funciones del módulo

d) La aplicación del módulo del suscriptor debe generar registros de auditoría, incluyendo casos de intentos de acceso en el proceso de verificación del Titular del módulo.

30.5. Desactivación y reactivación

La activación y desactivación del módulo criptográfico será administrado por los suscriptores. En caso de obtener los módulos criptográficos de la ER se brindará la información correspondiente para realizar la asignación de los datos de activación correspondientes.

30.6. Reemplazo del módulo criptográfico

a) En caso de pérdida o daño del módulo, las claves y certificados del suscriptor serán revocados y reemitidos.
b) El reemplazo del módulo será registrado para efectos de auditoría de la ER.

30.7. Terminación del módulo criptográfico

a) Los módulos criptográficos no serán retornados a la ER para ser desactivados o destruidos.
b) No deberán ser archivadas las claves privadas empleadas para la firma y autenticación de los usuarios finales, ni de los archivos electrónicos que los contengan (por ejemplo, los archivos con extensión PFX para facturación electrónica).