Guía de Acreditación de Entidad de Registro

Versión 4.0

Guía de Acreditación de
Entidad de Registro

ÍNDICE GENERAL

1. PREÁMBULO 4

2. DEFINICIONES/TERMINOLOGÍA 5

3. ACRÓNIMOS 16

4. ARQUITECTURA JERÁRQUICA DE CERTIFICACIÓN DEL ESTADO PERUANO Y MECANISMO DE INTEROPERABILIDAD 18

5. LINEAMIENTOS DE LA POLITICA DE SEGURIDAD DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA - IOFE 19

I. MARCO LEGISLATIVO/LEGAL 20

II: MARCO DE POLÍTICAS 21

III: MARCO OPERACIONAL (RELATIVOS A LAS OPERACIONES DE ER) 21

IV: NIVELES DE SEGURIDAD DE PKI 24

6. REGISTRO OFICIAL DE PRESTADORES DE SERVICIO DE CERTIFICACIÓN DIGITAL – ROPS (TSL) 25

7. MODALIDAD DE REGISTRO O VERIFICACIÓN ..... ¡ERROR! MARCADOR NO DEFINIDO.

8. CLASIFICACIÓN DEL REQUERIMIENTO 25

9. PROCEDIMIENTO DE ACREDITACIÓN 25

9.1. PASO 1: SOLICITUD INICIAL 26

9.2. PASO 2 : EVALUACIÓN DE CONTENIDO LEGAL 29

9.3. PASO 3: EVALUACIÓN DE LA IMPLEMENTACIÓN DE LA DECLARACIÓN EN LOS DOCUMENTOS RPS, LA POLÍTICA Y PLAN DE PRIVACIDAD Y LA POLÍTICA DE SEGURIDAD 30

9.4. PASO 4: RESOLUCIÓN 32

9.5. PASO 5: PUBLICIDAD DE RESULTADOS: 32

10. PROCEDIMIENTO DE LA EVALUACIÓN DE SEGUIMIENTO 33

11. PROCEDIMIENTO DE ACTUALIZACIÓN 34

1. PREÁMBULO

Objetivo

El presente documento establece los procedimientos y criterios que deben cumplir las Entidades de Registro (ER) para lograr su acreditación ante INDECOPI.

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, designado como la Autoridad Administrativa Competente (AAC) por la legislación vigente, establece en el presente documento los requisitos y pautas que buscan asegurar que la Entidad de Registro (ER) que pretenda operar dentro de la Infraestructura Oficial de Firma Electrónica (IOFE) cumpla determinados niveles de seguridad e interoperabilidad a efectos de poder obtener la correspondiente acreditación.

Público al que va dirigido

El presente documento, emitido bajo la autoridad del INDECOPI en calidad de AAC, pretende ser empleado por las Entidades de Registro a través de sus delegados: Oficiales de TI (*Information Technology Officials*), Gerentes de Registro, Responsable de Privacidad, etc.; a efectos que estos prestadores de servicios de certificación digital puedan identificar los requisitos necesarios que deben cumplir.

2. DEFINICIONES/TERMINOLOGÍA

- Acreditación: Es el acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, el Reglamento y las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el presente Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.
- Acuse de Recibo. - Son los procedimientos que registran la recepción y validación de la Notificación Electrónica Personal recibida en el domicilio electrónico, de modo tal que impide rechazar el envío y da certeza al remitente de que el envío y la recepción han tenido lugar en una fecha y hora determinada a través del sello de tiempo electrónico.
- Agente automatizado: Son los procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.
- Ancho de banda. - Especifica la cantidad de información que se puede enviar a través de una conexión de red en un período de tiempo dado (generalmente un segundo). El ancho de banda se indica generalmente en bites por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps). Cuánto más elevado el ancho de la banda de una red, mayor es su aptitud para transmitir un mayor caudal de información.
- Archivo. - Es el conjunto organizado de documentos producidos o recibidos por una entidad en el ejercicio de las funciones propias de su fi n, y que están destinados al servicio.
- Archivo Electrónico. - Es el conjunto de registros que guardan relación. También es la organización de dichos registros.
- Aplicabilidad o propósito de un certificado: se refiere al rango de aplicaciones en las que se puede utilizar un certificado digital dentro de una comunidad.
- Autenticación: proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste y al cual se le vincula. Este proceso no otorga certificación notarial ni fe pública.
- Autoridad Administrativa Competente. - Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el presente Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha

responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI.

- Canal seguro. - Es el conducto virtual o físicamente independiente a través del cual se pueden transferir datos garantizando una transmisión confidencial y confiable, protegiéndolos de ser interceptados o manipulados por terceros.
- Certificación Cruzada. - Es el acto por el cual una Entidad de Certificación acreditada reconoce la validez de un certificado emitido por otra, sea nacional, extranjera o internacional, previa autorización de la Autoridad Administrativa Competente; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.
- Certificado Digital. - Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad. El ciclo de vida de un certificado digital podría comprender:
    - La suspensión consiste en inhabilitar la validez de un certificado digital por un periodo de tiempo establecido en el momento de la solicitud de suspensión, dicho periodo no puede superar la fecha de expiración del certificado digital.
    - La modificación de la información contenida en un certificado sin la re-emisión de sus claves.
    - La re-emisión consiste en generar un nuevo par de claves y un nuevo certificado, correspondiente a una nueva clave pública pero manteniendo la mayor parte de la información del suscriptor contenida en el certificado a expirar.
- Clave privada: Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.
- Clave pública: Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.
- Código de verificación o resumen (hash).- Es la secuencia de bits de longitud fija obtenida como resultado de procesar un documento electrónico con un algoritmo, de tal manera que:
    - El documento electrónico produzca siempre el mismo código de verificación (resumen) cada vez que se le aplique dicho algoritmo.
    - Sea improbable a través de medios técnicos, que el documento electrónico pueda ser derivado o reconstruido a partir del código de verificación (resumen) producido por el algoritmo.

- Sea improbable por medios técnicos, se pueda encontrar dos documentos electrónicos que produzcan el mismo código de verificación (resumen) al usar el mismo algoritmo.

- Criptografía asimétrica: Es la rama de las matemáticas aplicadas que se ocupa de transformar documentos electrónicos en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos “claves” diferentes, pero matemáticamente relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada), y la otra para verificar una firma numérica o devolver el documento electrónico a su forma original (clave pública). Las claves están matemáticamente relacionadas, de tal modo que cualquiera de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima.
- Declaración de prácticas de certificación (CPS): Es el documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.
- Declaración de prácticas de registro o verificación (RPS): Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación.
- Declaración de Prácticas de Valor Añadido. - Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define las prácticas y procedimientos que emplea en la prestación de sus servicios.
- Depósito de certificados: Es el sistema de almacenamiento y recuperación de certificados, así como de la información relativa a éstos, disponible por medios telemáticos.
- Destinatario: Es la persona designada por el iniciador para recibir un documento electrónico, siempre y cuando no actúe a título de intermediario.
- Dirección de correo electrónico. - Es el conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.
- Dirección oficial de correo electrónico. - Es la dirección de correo electrónico del ciudadano, reconocido por el Gobierno Peruano para la realización confiable y segura de las notificaciones electrónicas personales requeridas en los procesos públicos.
- Esta dirección recibirá los mensajes de correo electrónico que sirvan para informar al usuario acerca de cada notificación o acuse de recibo que haya sido remitida a cualquiera de sus domicilios electrónicos. A diferencia del domicilio electrónico, esta dirección centraliza todas las comunicaciones que

sirven para informar al usuario que se ha realizado una actualización de los documentos almacenados en sus domicilios electrónicos. Su lectura es de uso obligatorio.

- Documento: Es cualquier escrito público o privado, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o su resultado.
  Los documentos pueden ser archivados a través de medios electrónicos, ópticos o cualquier otro similar.
- Documento electrónico. - Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.
- Documento oficial de identidad. - Es el documento oficial que sirve para acreditar la identidad de una persona natural, que puede ser:
  - Documento Nacional de Identidad (DNI);
  - Carné de extranjería actualizado, para las personas naturales extranjeras domiciliadas en el país; o,
  - Pasaporte, si se trata de personas naturales extranjeras no residentes.
- Domicilio electrónico. - Está conformado por la dirección electrónica que constituye la residencia habitual de una persona dentro de un Sistema de Intermediación Digital, para la tramitación confiable y segura de las notificaciones, acuses de recibo y demás documentos requeridos en sus procedimientos. En el caso de una persona jurídica el domicilio electrónico se asocia a sus integrantes.

  Para estos efectos, se empleará el domicilio electrónico como equivalente funcional del domicilio habitual de las personas naturales o jurídicas. En este domicilio se almacenarán los documentos y expedientes electrónicos correspondientes a los procedimientos y trámites realizados en el respectivo Sistema de Intermediación Digital. El acceso a este domicilio se realiza empleando un certificado digital de autenticación.
- Entidad de certificación (EC): Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

- Entidad de certificación extranjera: Es la Entidad de Certificación que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos del Perú, conforme a la legislación de la materia.
- Entidades de la Administración Pública: Es el organismo público que ha recibido del poder político la competencia y los medios necesarios para la satisfacción de los intereses generales de los ciudadanos y la industria.
- Entidad de Registro o Verificación (ER): Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
- Entidad final. - Es el suscriptor de un certificado digital.
- Estándares técnicos internacionales: Son los requisitos de orden técnico y de uso internacional que deben observarse en la emisión de certificados digitales y en las prácticas de certificación.
- Estándares técnicos nacionales: Son los estándares técnicos aprobados mediante Normas Técnicas Peruanas por la Comisión de Normalización y Fiscalización de Barreras Comerciales no Arancelarias del INDECOPI, en su calidad de Organismo Nacional de Normalización.
- Equivalencia funcional. - Principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndolos sustituir para todos los efectos legales. De conformidad con lo establecido en la Ley y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.
- Expediente electrónico. - El expediente electrónico se constituye en los trámites o procedimientos administrativos en la entidad que agrupa una serie de documentos o anexos identificados como archivos, sobre los cuales interactúan los usuarios internos o externos a la entidad que tengan los perfiles de accesos o permisos autorizados.
- Firmware: es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria tipo ROM, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Funcionalmente, el firmware es la interfaz entre las órdenes externas que recibe el dispositivo y su electrónica, ya que es el encargado de controlar a ésta última para ejecutar correctamente dichas órdenes externas.

- Gobierno Electrónico. - Es el uso de las Tecnologías de Información y Comunicación para redefinir la relación del gobierno con los ciudadanos y la industria, mejorar la gestión y los servicios, garantizar la transparencia y la participación, y facilitar el acceso seguro a la información pública, apoyando la integración y el desarrollo de los distintos sectores.
- Hardware: es un neologismo proveniente del inglés, definido por la RAE como el conjunto de los componentes que integran la parte material de una computadora; sin embargo, es utilizado en una forma más amplia, generalmente para describir componentes físicos de una tecnología.
- Identificador de objeto OID. - Es una cadena de números, formalmente definida usando el estándar ASN.1 (ITU-T Rec. X.660 | ISO/IEC 9834 series), que identifica de forma única a un objeto. En el caso de la certificación digital, los OIDs se utilizan para identificar a los distintos objetos en los que ésta se enmarca (por ejemplo, componentes de los Nombres Diferenciados, CPS, etc.).
- Infraestructura Oficial de Firma Electrónica (IOFE): Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de:
    1. La integridad de los documentos electrónicos;
    2. La identidad de su autor, lo que es regulado conforme a Ley.

  El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.
- Integridad: Es la característica que indica que un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
- Interoperabilidad. - Según el OASIS Forum Group la interoperabilidad puede definirse en tres áreas:
    - Interoperabilidad a nivel de componentes: consiste en la interacción entre sistemas que soportan o consumen directamente servicios relacionados con PKI.
    - Interoperabilidad a nivel de aplicación: consiste en la compatibilidad entre aplicaciones que se comunican entre sí.
    - Interoperabilidad entre dominios o infraestructuras PKI: consiste en la interacción de distintos sistemas de certificación PKI (dominios,

infraestructuras), estableciendo relaciones de confianza que permiten el reconocimiento indistinto de los certificados digitales por parte de los terceros que confían.

- Ley. - Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.
- Lista de Certificados Digitales Cancelados. - Es aquella en la que se deberá incorporar todos los certificados cancelados por la entidad de certificación de acuerdo con lo establecido en el presente Reglamento.
- Mecanismos de firma digital. - Es un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma digital.
  Dichos mecanismos varían según el nivel de seguridad que se les aplique.
- Medios electrónicos. - Son los sistemas informáticos o computacionales a través de los cuales se puede generar, procesar, transmitir y archivar de documentos electrónicos.
- Medios electrónicos seguros. - Son los medios electrónicos que emplean firmas y certificados digitales emitidos por Prestadores de Servicios de Certificación Digital acreditados, donde el intercambio de información se realiza a través de canales seguros.
- Medios telemáticos: Es el conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.
- Mensaje de datos: es la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI por sus siglas en inglés), el correo electrónico, el telegrama, el télex o el telefax entre otros.
- Neutralidad tecnológica: Es el principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente; asimismo, implica la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.
- Niveles de seguridad: Son los diversos niveles de garantía que ofrecen las variedades de firmas digitales, cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma digital para enviar o recibir documentos electrónicos.
- No repudio. - Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de

Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil.

En el ámbito del artículo 2º de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).

- Nombre Diferenciado X.501: Es un sistema estándar diseñado para consignar en el campo sujeto de un certificado digital los datos de identificación del titular del certificado, de manera que éstos se asocien de forma inequívoca con ese titular dentro del conjunto de todos los certificados en vigor que ha emitido la Entidad de Certificación. En inglés se denomina “Distinguished Name”.
- Notificación electrónica personal. - En virtud del principio de equivalencia funcional, la notificación electrónica personal de los actos administrativos se realizará en el domicilio electrónico o en la dirección oficial de correo electrónico de las personas por cualquier medio electrónico, siempre que permita confirmar la recepción, integridad, fecha y hora en que se produce. Si la notificación fuera recibida en día u hora inhábil, ésta surtirá efectos al primer día hábil siguiente a dicha recepción.
- Par de claves: Es un sistema de criptografía asimétrica, comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.
- Políticas de Certificación (CP): Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual establece, entre otras cosas, los tipos de certificados digitales que podrán ser emitidos, cómo se deben emitir y gestionar los certificados, y los respectivos derechos y responsabilidades de las Entidades de Certificación. Para el caso de una Entidad de Certificación Raíz, la Política de Certificación incluye las directrices para la gestión del Sistema de Certificación de las Entidades de Certificación vinculadas.
- Práctica: Es el modo o método que particularmente observa alguien en sus operaciones.
- Prácticas de Certificación: Son las prácticas utilizadas para aplicar las directrices de la política establecida en la Política de Certificación respectiva.
- Prácticas específicas de Certificación: Son las prácticas que completan todos los aspectos específicos para un tipo de certificado que no están definidos en la Declaración de Prácticas de Certificación respectiva.

- Prácticas de Registro o Verificación: Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.
- Prestador de Servicios de Certificación: Es toda entidad pública o privada que indistintamente brinda servicios en la modalidad de Entidad de Certificación, Entidad de Registro o Verificación o Prestador de Servicios de Valor Añadido.
- Prestador de Servicios de Valor Añadido: Es la entidad pública o privada que brinda servicios que incluyen la firma digital y el uso de los certificados digitales. El presente Reglamento presenta dos modalidades:
    - Prestadores de Servicio de Valor Añadido que realizan procedimientos sin firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido, como Sellado de Tiempo que no requieren en ninguna etapa de la firma digital del usuario final en documento alguno.
    - Prestadores de Servicio de Valor Añadido que realizan procedimientos con firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido como el sistema de intermediación digital, en donde se requiere en determinada etapa de operación del procedimiento la firma digital por parte del usuario final en algún tipo de documento.
- Prestador de Servicios de Valor Añadido para el Estado Peruano. - Es la Entidad pública que brinda servicios de valor añadido, con el fin de permitir la realización de las transacciones públicas de los ciudadanos a través de medios electrónicos que garantizan la integridad y el no repudio de la información (Sistema de Intermediación Digital) y/o registran la fecha y hora cierta (Sello de Tiempo).
- Reconocimiento de Servicios de Certificación Prestados en el Extranjero: Es el proceso a través del cual la Autoridad Administrativa Competente, acredita, equipara y reconoce oficialmente a las entidades de certificación extranjeras.
- Registro. - En términos informáticos, es un conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos.
- Reglamento. - El documento, denominado Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.
- Servicio de Valor Añadido: Son los servicios complementarios de la firma digital brindados dentro o fuera de la Infraestructura Oficial de Firma Electrónica que permiten grabar, almacenar, conservar cualquier información remitida por medios electrónicos que certifican los datos de envío y recepción, su fecha y hora, el no repudio en origen y de recepción. El servicio de intermediación digital dentro de la Infraestructura Oficial de Firma Electrónica es brindado por persona natural o jurídica acreditada ante la Autoridad Administrativa Competente.

- Servicio OCSP (Protocolo del estado en línea del certificado, por sus siglas en inglés): Es el servicio que permite utilizar un protocolo estándar para realizar consultas en línea (on line) al servidor de la Autoridad de Certificación sobre el estado de un certificado.
- Sistema de Intermediación Digital: Es el sistema que permite la transmisión o almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma digital, autenticación y canales seguros.
- Sistema Web ("World Wide Web"): Sistema de documentos electrónicos enlazados y accesibles a través de Internet. Mediante un navegador Web, un usuario visualiza páginas Web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.
- Suscriptor: Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.
- Tercero que confía o tercer usuario. - Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.
- Titular. - Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.
- Usabilidad. - En el contexto de la certificación digital, el término Usabilidad se aplica a todos los documentos, información y sistemas de ayuda necesarios que deben ponerse a disposición de los usuarios para asegurar la aceptación y comprensión de las tecnologías, aplicaciones informáticas, sistemas y servicios de certificación digital de manera efectiva, eficiente y satisfactoria.
- Usuario final. - En líneas generales, es toda persona que solicita cualquier tipo de servicio por parte de un Prestador de Servicios de Certificación Digital acreditado.
- Voto electrónico. - Sistema de votación que utiliza una combinación de procedimientos, componentes de hardware y software, y red de comunicaciones que permiten automatizar los procesos de identificación del

elector, emisión del voto, conteo de votos, emisión de reportes y/o presentación de resultados de un proceso electoral, referéndum y otras consultas populares. El voto electrónico se puede clasificar en:

a) Presencial: cuando los procesos de votación se dan en ambientes o lugares debidamente supervisados por las autoridades electorales; y

b) No presencial: cuando los procesos de identificación del elector y emisión del voto se dan desde cualquier ubicación geográfica o ambiente que el elector elija y disponga de los accesos apropiados.

- WebTrust.- Certificación otorgada a prestadores de servicios de certificación digital - PSC, específicamente a las Entidades Certificadoras - EC, que de manera consistente cumplen con estándares establecidos por el Instituto Canadiense de Contadores Colegiados (CICA por sus siglas en inglés - ver Cica.ca) y el Instituto Americano de Contadores Públicos Colegiados (AICPA).

  Los estándares mencionados se refieren a áreas como privacidad, seguridad, integridad de las transacciones, disponibilidad, confidencialidad y no repudio.

3. ACRÓNIMOS

AAC	Autoridad Administrativa Competente (CFE del INDECOPI)
CC	Common Criteria
CEN	Comité Europeo de Normalización
CP	Políticas de Certificación
CPS	Declaración de Prácticas de Certificación de una EC
CRL o LCR	*Certificate Revocation List* (Lista de Certificados Revocados)
CFE	Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica
CWA	*CEN Workshop Agreements*
EAL	*Evaluation Assurance Level*
EC	Entidad de Certificación
ECEP	Entidad de Certificación para el Estado Peruano
ECERNEP	Entidad de Certificación Nacional para el Estado Peruano
ER	Entidad de Registro o Verificación
EREP	Entidad de Registro para el Estado Peruano
ETSI	*European Telecommunications Standards Institute*
FBCA	Federal Bridge Certification Authority
FIPS	*Federal Information Processing Standards*
IEC	*International Electrotechnical Commission*
IETF	*Internet Engineering Task Force*
IOFE	Infraestructura Oficial de Firma Electrónica
ISO	*International Organization for Standardization*
NTP	Norma Técnica Peruana
OCSP	*Online Certificate Status Protocol* (Protocolo del estado en línea del certificado)
OID	Identificador de Objeto
PKI	*Public Key Infrastructure* (Infraestructura de Clave Pública)
PSC	Prestador de Servicios de Certificación Digital Prestador de Servicios de Criptográficos
PSVA	Prestador Servicios de Valor Añadido
ROPS	Registro Oficial de Prestadores de Servicio de Certificación Digital
RFC	Request for Comment
RPS	Declaración de Prácticas de Registro o Verificación de una ER
SHA	Secure Hash Algorithm

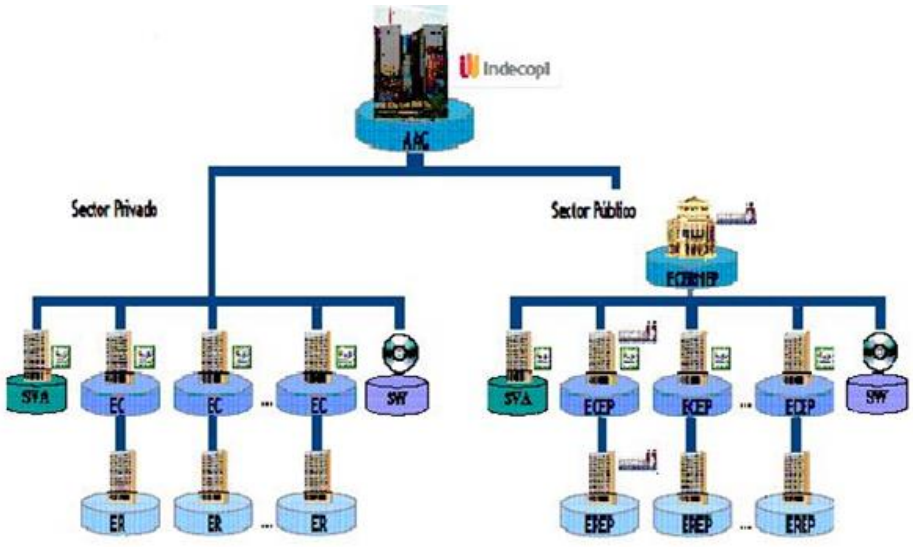
SID	Sistema de Intermediación Digital
SVA	Servicios de Valor Añadido (por ejemplo *Sellado de Tiempo*)
TSL	Lista de Estado de Servicio de Confianza
DPSVA	Declaración de Prácticas de Valor Añadido

4. ARQUITECTURA JERÁRQUICA DE CERTIFICACIÓN DEL ESTADO PERUANO Y MECANISMO DE INTEROPERABILIDAD

Por mandato del artículo 57º del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por el Decreto Supremo Nº 052-2008-PCM, el Instituto de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) ha sido designado como Autoridad Administrativa Competente (AAC) teniendo como principal función la implantación y buen funcionamiento de la Infraestructura Oficial de Firma Electrónica (IOFE) para lograr eficiencia, eficacia y transparencia en la gestión pública y para promover su uso en el comercio electrónico.

En esta misma línea, en la Quinta Disposición Complementaria Final de la Ley 30224, Ley que crea el Sistema Nacional para la Calidad y el Instituto Nacional de Calidad que asigna al Indecopi la función de administrar la Infraestructura Oficial de Firma Electrónica (IOFE), conforme a la normativa de la materia.

En base a lo anteriormente dicho se presenta el siguiente esquema:



ECERNEP: Entidad De Certificación Nacional para el Estado Peruano
ECEP: Entidad de Certificación para el Estado Peruano
EREP: Entidad de Registro o Verificación para el Estado Peruano
EC: Entidad de Certificación
ER: Entidad de Registro o Verificación
SVA: Prestadora de Servicio de Valor Añadido
SW: Aplicación de Software.

Registro Oficial de Prestadores de Servicio de Certificación Digital (ROPS)

El mecanismo de interoperabilidad utilizado con el propósito de proveer, de modo ordenado, la información del estado de los Proveedores de Servicios de Certificación (PSCs) acreditados y supervisados por INDECOPI –y por tanto autorizados a operar en el marco de la IOFE– es el ROPS.

El ROPS consiste en una lista "blanca" que contiene la relación de los PSCs acreditados y es elaborada siguiendo el estándar ETSI TS102 231. Dicha lista es firmada digitalmente por INDECOPI a efectos de asegurar su integridad y estará disponible para que las aplicaciones de software puedan procesarla.

5. LINEAMIENTOS DE LA POLITICA DE SEGURIDAD DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA - IOFE

Estos lineamientos se estructuran conforme al marco legislativo peruano que comprende: la Ley N° 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley N° 27310 y su Reglamento (aprobado por Decreto Supremo N° 052-2008-PCM).

Asimismo incorporan los lineamientos establecidos por los "Principios rectores para esquemas de autenticación electrónica basados en PKI", que fueran suscritos por el Perú en su condición de economía miembro del APEC (*Asia-Pacific Economic Cooperation*, en español Cooperación Económica del Asia-Pacífico) mediante la denominada Declaración de Lima, siendo la intención de estas políticas, "facilitar la aceptación transnacional de Entidades de Certificación (EC) extranjeras y el establecimiento de acuerdos de reconocimiento transnacional para tales efectos".

Igualmente, se toman en consideración los principios establecidos en la Norma Marco sobre Privacidad del APEC, los mismos que tiene como objeto principal el reconocimiento de "… *la importancia del desarrollo de protecciones a la privacidad efectivas que eviten las barreras para el flujo de información, aseguren el intercambio comercial continuo y el crecimiento económico de la región del APEC*".

Por otro lado, se tomó en consideración para efectos del presente documento, el

hecho que es de consenso general y además es recogido por la legislación vigente[1], que no basta un único nivel de seguridad[2] para todas las aplicaciones de PKI.

Ciertas transacciones son menos críticas o implican alguna operación de bajo valor monetario y pueden soportar un nivel de mayor riesgo comparado con otras que requieren de un mayor nivel de seguridad.

En tal sentido, se recogen estas diferencias y se presentan tres niveles: Medio (M), Medio Alto (M+) y Alto (A) de seguridad, descritos en las sub-secciones siguientes. La presente Guía de Acreditación sólo se refiere a los dos primeros niveles de seguridad para certificados de usuario finales.

Finalmente, a través del presente documento, se establece la interoperabilidad y equivalencia de condiciones de seguridad entre los especificados por APEC –en la Declaración de Lima– y el nivel de seguridad medio (M) y medio alto (M+), para efectos de la implementación de la política de seguridad de la IOFE, los mismos que se consignan a continuación:

I. MARCO LEGISLATIVO/LEGAL

- Los presentes lineamientos son conformes al marco legal estipulado y establecen parámetros para la constitución y operación de ERs que facilitan la aceptación de los servicios que éstas proveen.
- Tal marco permite y propugna la aceptación de servicios generados en otras jurisdicciones.
- Dicho marco dota de efectos legales a los documentos y firmas electrónicas producidos por las ERs.
- El referido marco no determina el empleo de ningún tipo de tecnología en particular. Propugna más bien la neutralidad tecnológica, la adopción

[1] En el Glosario de Términos recogido en la Octava Disposición Final del Reglamento de la Ley de Firmas y certificados digitales, se establece la definición de Niveles de Seguridad que se transcribe a continuación:
"Octava Disposición Final.- Glosario de Términos (…)
Niveles de seguridad: son los diversos niveles de garantía que ofrecen las variables de firma electrónica cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos."

[2] El nivel de seguridad asociado con un certificado de clave pública es una aserción del grado de confianza que un usuario puede tener razonablemente en el vínculo de la clave pública de un suscriptor con el nombre y los atributos consignados en el certificado.

permanente de los estándares del mercado, el desarrollo de la tecnología existente y la introducción de nueva tecnología existente y la introducción de nueva tecnología.

II: MARCO DE POLÍTICAS

- Los requerimientos para el establecimiento de ERs sirven para generar la confianza pública y la confidencialidad y facilitan el reconocimiento transnacional de los certificados emitidos por las respectivas ECs vinculadas.
- Los esquemas de valoración que utilizan estándares reconocidos y buenas prácticas para asegurar la interoperabilidad técnica entre los usuarios, son óptimos para facilitar el reconocimiento transnacional de certificados.
- La implementación de estándares ampliamente aceptados –ver anexo 10– y de gestión en esquemas PKI permiten la adecuada implementación de las ERs y su reconocimiento.
- Las políticas y los procedimientos para el reconocimiento transnacional de la implementación de esquemas PKI facilitan la predictibilidad legal y certeza respecto a certificados emitidos bajo dichos esquemas.

III: MARCO OPERACIONAL (RELATIVOS A LAS OPERACIONES DE ER)

General

- El empleo del estándar X.509 y el RFC 3647 para la Declaración de Prácticas de Registro o Verificación (RPS) propugna el proceso de reconocimiento transnacional.

Registro y Validación del Certificado

- Los esquemas de valoración que utilizan estándares reconocidos y buenas prácticas para asegurar la interoperabilidad técnica entre los usuarios, son óptimos para facilitar el reconocimiento transnacional de certificados.
- La implementación de estándares ampliamente aceptados –ver anexo 10– y de gestión en esquemas PKI permiten la adecuada implementación de las ERs y su reconocimiento.
- Las políticas y los procedimientos para el reconocimiento transnacional de la implementación de esquemas PKI facilitan la predictibilidad legal y certeza respecto a certificados emitidos bajo dichos esquemas.

Manejo de claves

- No se permite el empleo de los depósitos de claves privadas de backup (Key Escrow) para las claves de firma digital pues minan la confianza en el uso del sistema e impiden el reconocimiento transnacional de certificados (ver anexo 10).
- Se propugna el reconocimiento transnacional de los certificados en la medida que se incorpore el uso de buenas prácticas para la generación de claves, las cuales sean derivadas de estándares y fuentes aceptadas internacionalmente.
- Se genera confianza en el sistema y se propugna el reconocimiento transnacional de los certificados cuando se adoptan las buenas prácticas internacionales referidas a la distinción entre los certificados asignados para procesos de cifrado (confidencialidad), de autenticación y de firma digital (no repudio).

Ingeniería criptográfica

- Se propugna la interoperabilidad y el reconocimiento transnacional de los certificados mediante el uso de algoritmos criptográficos de reconocimiento internacional de tamaño y seguridad criptográfica suficiente.
- Se incrementa la seguridad y se propugna el reconocimiento transnacional de certificados al asegurar que las claves criptográficas y los algoritmos sean lo suficientemente seguros para proteger de ataques el resultado criptográfico durante el tiempo de duración del certificado.
- Se propugna el reconocimiento transnacional de los certificados mediante la realización de los procesos criptográficos con dispositivos certificados de conformidad con el estándar FIPS 140-2[3] u otro equivalente.

Nombres distinguidos

- Se propugna la interoperabilidad mediante el uso de buenas prácticas para la estandarización de los contenidos de los componentes de Nombres diferenciados en el certificado.
- En particular, el uso del estándar X.509, así como la política OID para representar la aplicabilidad pretendida del certificado digital, propugnan el reconocimiento transnacional.

[3] Nivel de Seguridad 3 para el caso de los módulos criptográficos de las ECs y Nivel de Seguridad 2 para el caso de los módulos criptográficos de las ERs y los SVAs.

Estándares de Directorio

Se promueve la confianza del usuario y se propugna el reconocimiento transnacional de certificados mediante:

- El uso de estándares internacionales y más comúnmente aceptados, tales como el X.500 *Directory Service* o LDPA *(Lightweight Directory Access Protocol*) v3 que facilita la interoperabilidad de las aplicaciones, sistemas y operaciones de PKI.
- El uso de buenas prácticas internacionales para la seguridad del personal, seguridad de control y control de seguridad física de conformidad con el estándar NTP-ISO/IEC 27001 o ISO/IEC 27001.
- El uso de por lo menos controles duales para las operaciones de los servicios y procesos de las ECs (por ejemplo control y manejo de la clave pública de la EC) de conformidad con la RFC 3647.
- El uso de guías para los sistemas e integridad del software y control que cumplen con FIPS o estándares reconocidos equivalentes.
- El establecimiento de políticas de archivo que aseguren la retención del material relevante por una duración mínima suficiente (mínimo de 10 años).
- El uso del sellado de tiempo (estándares de Time Stamp RFC 3161 y RFC 3628) y mecanismos de seguridad para prevenir cualquier cambio intencional en los documentos archivados, tales como el uso de resúmenes (hashes).
- El aseguramiento que el propósito general del repositorio y de la lista de certificados revocados – Certificate Revocation List (CRL) – estén disponibles cuando sean requeridos.
- La garantía de la disponibilidad para la recepción y actuación frente a requerimientos de revocación de certificados cuando se produzcan.

Lineamientos de gestión

Se promueve la confianza del usuario y se propugna el reconocimiento transnacional de certificados mediante:

- El establecimiento de planes de continuidad en el negocio y recuperación de desastres.
- El establecimiento de provisiones o guías en la eventualidad que una EC o ER deje de funcionar.
- El empleo de auditorías/evaluaciones de conformidad realizadas por una

tercera parte independiente, como parte de una buena práctica de seguridad para la acreditación o licenciamiento [4].

IV: NIVELES DE SEGURIDAD DE PKI

La IOFE define los siguientes niveles de seguridad en los que pueden brindarse los servicios de certificación digital, respecto de las aplicaciones de software de firma digital:

Aspecto	Nivel de seguridad medio	Nivel de seguridad medio - alto	Nivel de Seguridad Alto
Tipo de información que se puede proteger	Trámites con el Estado en las transacciones económicas de monto bajo o medio y para el intercambio de documentos de riesgo bajo o medio.	Intercambio de documentos y transacciones monetarias de alto riesgo. Trámites con el Estado en las transacciones económicas de alto monto y alto riesgo.	Intercambio de información crítica clasificada o de seguridad nacional.
Longitud de la clave privada	La longitud de clave privada mínima debe ser de 2048 bits y el certificado debe ser renovado como máximo cada tres (3) años.	La longitud de clave privada mínima debe ser de 2048 bits y el certificado debe ser renovado como máximo cada dos (2) años.	La longitud de clave privada mínima debe ser de 2048 bits y el certificado debe ser renovado como máximo anualmente.
Requerimientos de acreditación	• Verificación de la identidad empleando la base de datos	• Verificación de la identidad empleando la base de datos	• ISO 27001 • Verificación de la identidad empleando el

[4] Documento disponible en inglés en: www.apectelwg.org/

	del RENIEC • Seguros o garantías bancarias equivalentes a $35 000.00 Dólares americanos	del AFIS del RENIEC • Seguros o garantías financiera equivalentes al menos a $35 000.00 Dólares Americanos	sistema de identificación biométrica AFIS del RENIEC • Seguros o garantías financiera equivalentes a $35 000.00 Dólares Americanos

6. REGISTRO OFICIAL DE PRESTADORES DE SERVICIO DE CERTIFICACIÓN DIGITAL – ROPS (TSL)

El ROPS consiste en una lista “blanca” que contiene la relación de los PSC acreditados y es elaborada siguiendo el estándar ETSI TS 102 231. Dicha lista es firmada digitalmente por el INDECOPI a efectos de asegurar su integridad y estará disponible para su consulta por parte de los terceros que confían.

7. CLASIFICACIÓN DEL REQUERIMIENTO

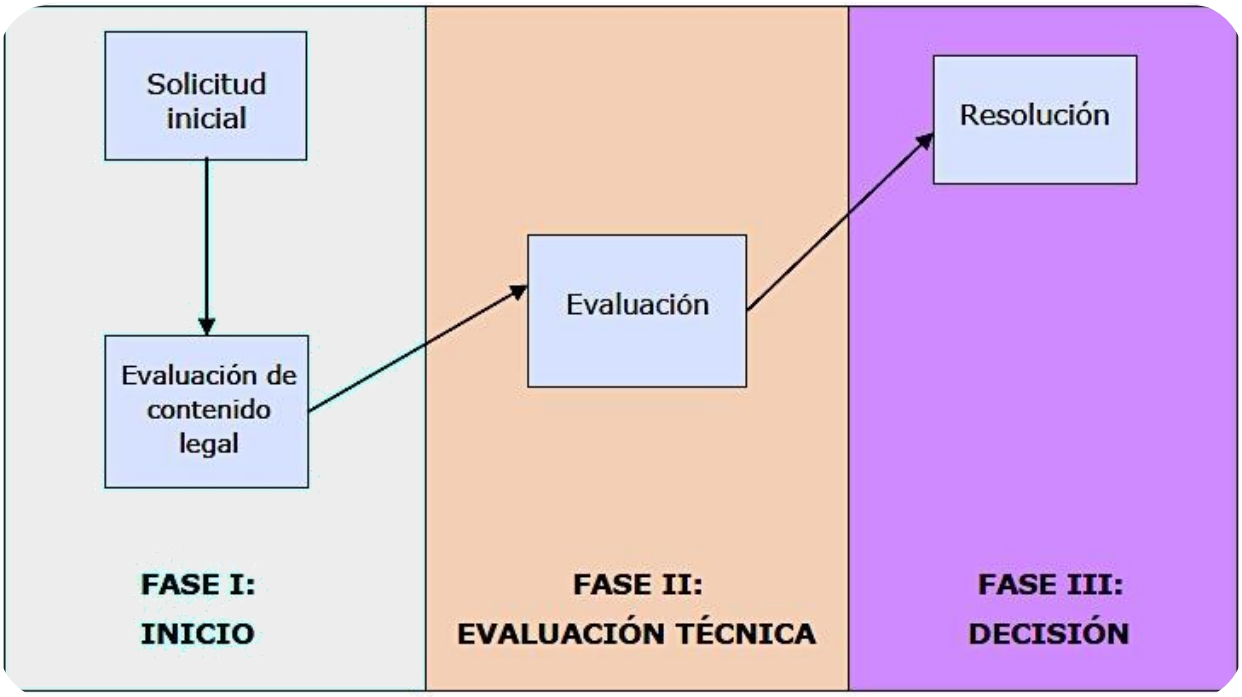
Conforme a su propósito, los requerimientos pueden ser clasificados de la siguiente manera:

1. Declaración de Prácticas de Registro.
2. Gestión de Prácticas de Registro.
3. Procesos de Registro o Verificación.
4. Controles técnicos de seguridad y del entorno.
5. Controles del ciclo de vida de la clave privada del titular y del suscriptor.
6. Auditorías.
7. Aspectos legales y de responsabilidad.

8. PROCEDIMIENTO DE ACREDITACIÓN

Para efectos de la presente Guía de Acreditación, el mencionado procedimiento está

compuesto de las fases que se resumen en la tabla siguiente:



El plazo total del procedimiento de acreditación será de 120 días hábiles.

8.1. Paso 1: Solicitud inicial

Presentación de la documentación requerida por la ER a efectos de obtener la correspondiente acreditación:

1. Solicitud dirigida al Secretario Técnico de la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica (CFE) del INDECOPI, mediante el formato adjunto en el Anexo X, solicitando lo siguiente:

Nota: La acreditación de una ER implica la evaluación de sus sucursales o agencias existentes al momento de realizar la solicitud inicial, las cuales deben de cumplir con lo establecido en la RPS y demás documentos relevantes de la ER. Debe entregarse un documento donde se especifique la localización de las agencias y sus respectivos certificados emitidos por el Instituto Nacional de Defensa Civil (INDECI), así como los nombres de los responsables de los procesos de registro en cada una de las mismas. En el trascurso de los 5 años de acreditación la ER puede poner en funcionamiento más sucursales, a condición que informen diez (10) días hábiles antes del funcionamiento a la autoridad administrativa competente, la cual evaluará dichas sucursales en un plazo de 60 días.

2. Documentos que evidencien la existencia y vigencia de la persona jurídica:
   i. Documento de vigencia emitido por los Registros Públicos o mediante la especificación de la norma legal de la creación de la persona jurídica.
   ii. En el caso de las entidades y empresas del Estado, deberán acreditar la existencia de una oficina, gerencia o dependencia interna a la cual se le otorgan las funciones como Entidad de Registro.
   iii. En el caso de los Notarios, se acreditará este hecho con una constancia expedida para tales efectos por su Colegio Profesional, así como con su correspondiente Resolución Ministerial de nombramiento en el cargo.

3. Adjuntar los poderes en virtud a los cuales los representantes legales se encuentran facultados para solicitar la acreditación. Sobre el particular deberá tenerse en cuenta lo siguiente:
   i. 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.
   ii. 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.
   iii. En el caso de instituciones del Estado, deberá acreditarse el nombramiento de la persona encargada de dirigir la oficina, gerencia o dependencia interna de la Entidad de Registro. Debiéndose asimismo acreditarse las facultades de este funcionario.
   iv. En el caso de los Notarios, se acreditará este hecho con una constancia expedida para tales efectos por su Colegio Profesional, así como con su correspondiente Resolución Ministerial de nombramiento en el cargo.

4. Memoria descriptiva de la empresa o entidad estatal.

5. Organigrama estructural y funcional de la ER.

6. Los documentos a que se refieren los puntos (4) y (5) serán elaborados en el formato denominado: Memoria descriptiva y organigrama estructural y funcional – Entidad de Registro o Verificación (ER), en el formato adjunto en el Anexo IX de la presente Guía de Acreditación.

7. Documentos que acrediten domicilio en el país. Este hecho quedará acreditado con el comprobante de inscripción de la persona jurídica en el Registro Único de Contribuyentes (R.U.C.), la misma que debe figurar 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 CFE.

8. Declaración jurada de contar con infraestructura e instalaciones necesarias, según el nivel de seguridad solicitado. Esta declaración jurada se encuentra incluida en el anexo IX.

9. Declaración de Prácticas de Registro o Verificación (RPS) conforme al Anexo I.
   - 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.
   - La Declaración de Prácticas de Registro o Verificación deberá estar elaborada según el documento "Marco de la Política de Registro para la emisión de certificados digitales" –ver anexo I–, así como de la Norma Marco sobre Privacidad –ver anexo VI–. Ambos documentos forman parte integrante de la presente Guía de Acreditación.

10. A efectos de realizar una óptima prestación de sus servicios, la ER solicitante deberá 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.

11. En el caso que cualquiera de los elementos que conforman el sistema de gestión señalado sean administrados por un tercero, la entidad solicitante, deberá demostrar su vinculación con aquél, asegurando la viabilidad de sus servicios bajo dichas condiciones y la disponibilidad de estos elementos para la evaluación y supervisión que el INDECOPI considere necesarias. En este caso, el INDECOPI tiene derecho a precisar los términos bajo los cuales se rigen este tipo de servicios de certificación digital. Esta vinculación podrá ser demostrada a través de contrato, acuerdo, convenio de outsourcing o

cualquier otro documento con valor legal dentro del ordenamiento jurídico peruano.

12. Declaración jurada de aceptación de la visita comprobatoria del INDECOPI. Esta declaración jurada se encuentra incluida en el Anexo X.

13. Declaración Jurada en la cual se señale que en caso se obtenga la acreditación por parte del INDECOPI, se procederá a la contratación del seguro o garantía bancaria correspondiente.

14. Constancia de pago de los derechos administrativos correspondientes.

8.2. Paso 2 : Evaluación de contenido legal

Establecer la idoneidad de la documentación presentada por la ER solicitante para efectos de la acreditación:

15. La CFE realizará una verificación preliminar de índole formal, con relación a la solicitud y los recaudos acompañados a la misma.

16. En caso se haya cumplido de manera defectuosa o se haya omitido alguno de los requisitos exigidos, otorgará un plazo máximo de cinco (05) días hábiles para la subsanación de estas observaciones. Transcurrido este plazo sin la subsanación correspondiente, se declarará la inadmisibilidad de la solicitud y la conclusión del procedimiento.

17. Una vez presentados los documentos necesarios para levantar las observaciones formuladas, la CFE luego de la evaluación correspondiente, emitirá la resolución de admisibilidad en la cual designará al Comité Evaluador encargado de la evaluación técnica a la solicitante. En caso la ER solicitante tuviera algún tipo de observación a los miembros designados del Comité, deberá proceder conforme a los lineamientos establecidos para tales efectos en el Reglamento General de Acreditación - Prestadores de Servicios de Entidad de Registro.

18. Luego de emitida la resolución de admisibilidad, la CFE procederá a realizar un análisis legal detallado de la documentación presentada y pronunciarse sobre su procedencia. El plazo para esta evaluación es de diez (10) días hábiles. En esta etapa no se evaluará la documentación técnica contenida en

el documento RPS por cuanto la misma será materia de evaluación en el Paso 3 referido a la evaluación técnica de la ER solicitante.

19. En caso existan observaciones a la documentación presentada, otorgará al solicitante un plazo de diez (10) días hábiles para el levantamiento de las mismas.

20. Si se cumple con subsanar las observaciones dentro del plazo establecido, la CFE declarará la conformidad de la documentación presentada y se procederá a la etapa siguiente del procedimiento de acreditación. En esta misma resolución se citará al designado representante técnico de la ER solicitante a efectos de realizar las coordinaciones necesarias para la etapa de evaluación técnica.

21. Si no se levantan las observaciones formuladas dentro del plazo establecido, se declarará la improcedencia de la solicitud y la conclusión del procedimiento.

22. En todos los supuestos antes señalados la CFE deberá fundamentar claramente su decisión.

23. En caso de no encontrarse conforme con la decisión emitida, el solicitante tiene un plazo de quince (15) días hábiles, para efectos de interponer los recursos impugnatorios que considere pertinentes. Con la resolución que se emita en esta segunda instancia, quedará agotada la vía administrativa.

8.3. Paso 3: Evaluación de la implementación de la declaración en los documentos RPS, la Política de Registro o Verificación, la Política y Plan de Privacidad y la Política de seguridad

En esta etapa se examinarán los documentos RPS, la Política de Registro o Verificación, Política y Plan de Privacidad y la Política de Seguridad de la ER, y establecer su equivalencia con el Marco de la Política de emisión de certificados digitales (anexo I), la Norma Marco sobre Privacidad (anexo VI), respectivamente.

Actividades:

a) En esta etapa corresponde a la ER solicitante la presentación los documentos correspondientes a la Política de Registro o Verificación, RPS, Política de Privacidad, Plan de Privacidad y Política de Seguridad.
b) Los requerimientos de seguridad son aquellos comprendidos en la sección Gestión de Seguridad descritos en el Anexo I.
c) La Política de Privacidad y el 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 Norma Marco sobre Privacidad presentada en el VI.
d) El Comité Evaluador procederá a la evaluación de cumplimiento de los documentos RPS, el anexo I, la Política de Registro o Verificación, la Política de Privacidad, el Plan de Privacidad, la Política de Seguridad.
e) El Comité Evaluador, una vez realizada la correspondiente evaluación, emitirá un informe que cuando menos contendrá lo siguiente:
    - Grado de cumplimiento de los requisitos técnicos requeridos para la acreditación.
    - Reporte de las no conformidades y observaciones detectadas durante la evaluación.
    - Otra información que el Comité considere importante consignar.

f) En todos los supuestos antes señalados el Comité Evaluador deberá fundamentar claramente su informe. De considerarlo pertinente, el Comité podrá determinar dentro del plazo de evaluación, la necesidad de realizar una visita comprobatoria a la ER. Este hecho debidamente fundamentado, se pondrá en conocimiento de la ER solicitante y correrá por cuenta de la misma los gastos que puedan generarse por esta evaluación.
g) En caso de presentarse no conformidades, la ER solicitante tiene un plazo de cinco (05) días hábiles de culminada la evaluación técnica para presentar a la CFE las propuestas de acciones correctivas que considere pertinentes y los plazos para su ejecución, los cuales no pueden ser superiores a 30 días calendario.
h) La verificación del levantamiento de no conformidades se realizará mediante una evaluación complementaria dentro de los términos establecidos por el Reglamento General de Acreditación – Prestadores de Servicios de Entidad de Registro.
i) La ER solicitante podrá solicitar la suspensión del procedimiento a efectos de implementar las medidas técnicas necesarias para superar las observaciones formuladas. En este caso, el procedimiento se reactivará con la presentación de la documentación que acredite la subsanación de las observaciones formuladas y se procederá a la evaluación

complementaria a que se refiere el Reglamento General de Acreditación – Prestadores de Servicios de Entidad de Registro.

8.4. Paso 4: Resolución

La CFE decidirá si se permite el ingreso a la IOFE de la ER solicitante, por medio de la correspondiente resolución de acreditación.

Actividades:

El INDECOPI con los resultados obtenidos en las dos fases anteriores, procederá a resolver en cualquiera de los sentidos siguientes:

- Otorgar la acreditación a la ER solicitante.
- Denegar la acreditación.

Una vez recibida la documentación a que se alude en el punto anterior, se entenderá que la ER acreditada ingresará a la IOFE, a través de su inscripción en el Registro de Prestadores de Servicios de Entidad de Registro que mantiene para tales efectos la CFE y se encontrará obligada al pago del aporte por supervisión y control anual.

En caso de no encontrarse conforme con la decisión emitida, el solicitante tiene un plazo de cinco (05) días hábiles posteriores a la recepción de la decisión, para efectos de interponer los recursos impugnatorios que considere pertinentes. Con la resolución que se emita en esta segunda instancia quedará agotada la vía administrativa.

8.5. Paso 5: Publicidad de resultados:

INDECOPI publicará la acreditación y estado de una ER a través de un directorio en su página WEB.
Para efectos de estandarizar el formato de información confiable sobre el estado de acreditación del PSC, INDECOPI implementará el ROPS basado en el estándar ETSI TS 102 231, donde publicará el estado de todas las Entidades de Certificación acreditadas.

9. PROCEDIMIENTO DE LA EVALUACIÓN DE SEGUIMIENTO

Cada año, dentro del plazo de vigencia de la acreditación, el Prestador de Servicios de Certificación Digital deberá someterse a una evaluación de seguimiento.

9.1. Paso 1: Notificación:

La AAC notificará a los Prestadores de Servicios de Entidad de Registro acreditados acerca del cumplimiento de un nuevo año de vigencia y la necesidad de efectuar el proceso de evaluación de seguimiento.

9.2. Paso 2: Evaluación:

El PSC tendrá los plazos establecidos en el Procedimiento para la Auditoria Anual de los Prestadores de Servicios de Certificación Digital (PE-CFE-01) para tramitar la evaluación por parte de un auditor independiente seleccionado de una lista presentada por el INDECOPI.
El auditor no deberá haber laborado para el PSC, ni deberá haber tenido ninguna relación comercial con el mismo, ni de efectos de auditoría en el mismo alcance de evaluación, en los últimos 2 años calendario.

El alcance de la evaluación debe comprender:

- La verificación de la identidad de los suscriptores, contra las bases de datos nacionales.
- La verificación de la identidad de la persona jurídica contra las bases de datos nacionales.
- Verificación de los controles de seguridad.
- Verificación de la vigencia del seguro o garantía financiera.
- Mantener las certificaciones y requisitos declarados en el proceso de acreditación correspondientes al nivel de seguridad.

9.3. Paso 3: Resultado:

En caso que la evaluación no sea realizada en el plazo establecido, el PSC será suspendido y retirado del registro público que mantiene el Indecopi, hasta que sea efectuada la evaluación.
En el caso que el resultado de la evaluación refleje el incumplimiento por parte del PSC, este perderá el estado de acreditado y deberá ser sometido a:

- Una suspensión del proceso de acreditación por un plazo establecido por la AAC.
- Una investigación para determinar el impacto del incumplimiento sobre los suscriptores y terceros que confían.
- Otras medidas que determine la AAC.

10. PROCEDIMIENTO DE ACTUALIZACIÓN

Si un PSC acreditado desea extender el alcance de los servicios que brinda, dentro de la clasificación determinada (EC, ER, SVA o SW), podrá solicitar al Indecopi una evaluación de actualización del alcance de la acreditación, la cual no deberá exceder el plazo máximo de 120 días hábiles.

10.1. Paso 1: Solicitud:

El PSC debe enviar al INDECOPI su correspondiente solicitud indicando el alcance a actualizar.

10.2. Paso 2: Evaluación:

El PSC tendrá un plazo de 120 días hábiles para tramitar y someterá a la evaluación por parte de un auditor independiente seleccionado de una lista presentada por el INDECOPI.

El auditor evaluará la actualización del documento RPS y su respectiva implementación. Todos los controles y documentos aplicables al nuevo alcance deberán ser verificados.

10.3. Paso 3: Resultado:

En el caso que el resultado de la evaluación refleje el cumplimiento de lo declarado por parte del PSC, la AAC emitirá la resolución correspondiente.