Guía de Acreditación de Entidades de Certificación EC

Versión 4.0

Guía de Acreditación de Entidad de Certificación

ÍNDICE GENERAL

1. PREÁMBULO

Objetivo

El presente documento establece los procedimientos y criterios que deben cumplir las Entidades de Certificación (EC) para lograr:

1. Acreditación de la EC.
2. Certificación cruzada con una EC acreditada conducente al permiso para operar en la IOFE.

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 Certificación (EC) 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

Se pretende que el presente documento sea empleado por las Entidades de Certificación a través de sus delegados: oficiales de TI (Information Technology Officials), Gerentes de Certificación Digital, etc.; a efectos que estos prestadores de servicios de certificación digital puedan identificar los requisitos necesarios que deben cumplir.

2. DEFINICIONES/TERMINOLOGÍA

- Acreditación: Acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, en su Reglamento y en las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.
- Agente automatizado: procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana.

- 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. Este rango puede dividirse en tres partes: (a) Aplicaciones libres, destinadas a miembros comunes de una comunidad. (b) Aplicaciones restringidas a un grupo selecto dentro de la comunidad. (c) Aplicaciones prohibidas para cualquier miembro de la 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 (AAC): organismo público responsable de acreditar a los Prestadores de Servicios de Certificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura y las otras funciones señaladas en el 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.
- Certificación cruzada: acto por el cual una certificadora 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: documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.
- Clave privada: es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un mensaje de datos 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 mensaje de datos para verificar la firma digital puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.
- Código de verificación (hash o resumen): secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) El mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo. (2) Sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo. (3) Sea improbable que, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.
- Criptografía asimétrica: rama de las matemáticas aplicadas que se ocupa de transformar mensajes 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 mensaje a su forma original (clave pública). Las claves están matemáticamente relacionadas de tal modo que cualquier 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): 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.
- Depósito de certificados: sistema de almacenamiento y recuperación de certificados, así como de la información relativa a éstos, disponible por medios telemáticos.
- Destinatario: persona designada por el iniciador para recibir un mensaje de datos o un documento electrónico siempre y cuando no actúe a título de intermediario.
- Documento: 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.
- Entidad de certificación (EC): persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.
- Entidad de certificación extranjera: la que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos del Perú, conforme a la legislación de la materia.
- Usuario final: suscriptor o titular de un certificado digital.
- Entidad de Registro o Verificación (ER): persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, comprobación de éstos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de

mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.

- Estándares técnicos internacionales: requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.
- 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.
- 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, CPSs, etc.). Referencia: http://www.oid-info.com/index.htm.
- 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 electrónicas y proporcionar diversos niveles de seguridad respecto a: 1) la integridad de los mensajes de datos y documentos electrónicos; 2) la identidad de su autor, lo que es regulado conforme a la Ley. El sistema incluye la generación de firmas electrónicas, 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 (ECERNEP), las Entidades de Certificación para el Estado Peruano (ECEP) y las Entidades de Registro o Verificación para el Estado Peruano (EREP).
- Integridad: característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
- Lista de Certificados Digitales Revocados (CRL o LCR): es aquella en la que se deberán incorporar todos los certificados revocados por la entidad de certificación de acuerdo con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales.

- Mecanismos de Firma Electrónica: un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma. Dichos mecanismos varían según el nivel de seguridad que se les aplique.
- Medios telemáticos: 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.
- Middleware: es un software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de múltiples procesos sobre máquinas diferentes que deben interactuar. Proporciona las librerías que implementan todas las funcionalidades que permiten la comunicación.
- Neutralidad tecnológica: principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente, asimismo 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 electrónicas, 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.
- Nombre Diferenciado X.501: es un sistema estándar diseñado para consignar en el campo Sujeto de un certificado digital los datos identificativos 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 EC. En inglés se denomina “Distinguished Name”, DN X.501.
- Operadores de registro: Personal de la ER que tiene autorización y responsabilidad para realizar los procesos de verificación de identidad de los solicitantes y transferir las autorizaciones a las Entidades de Certificación.
- Par de claves: en un sistema de criptografía asimétrica, comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.
- Política: Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

- 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 EC Raíz, la CP incluye las directrices para la gestión del Sistema de Certificación de las EC vinculadas.
- Práctica: Modo o método que particularmente observa alguien en sus operaciones.
- Prácticas de Certificación: prácticas utilizadas para aplicar las directrices de la política establecida en la CP respectiva.
- Prácticas específicas de Certificación: prácticas que completan todos los aspectos específicos para un tipo de certificado que no están definidos en la CPS respectiva.
- Prácticas de Registro o Verificación: prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una SVA.
- Reconocimiento de servicios de certificación prestados en el extranjero: proceso a través del cual la Autoridad Administrativa Competente acredita, equipara y reconoce oficialmente a las entidades de certificación extranjeras.
- Reglamento de la Ley de Firmas y Certificados Digitales: el Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley N° 27310, aprobado por Decreto Supremo N° 052-2008-PCM.
- Revocación de Certificados: aquel cambio en el estado del certificado que ocasiona la pérdida de validez del mismo, por alguna circunstancia distinta a la de su caducidad. Cualquier firma digital realizada con un certificado revocado no tendrá validez.
- Sistema de Intermediación Digital: servicio de valor añadido complementario de la firma digital brindado dentro o fuera de la Infraestructura Oficial de Firma Electrónica que permiten grabar, almacenar, conservar cualquier información remitida por medios electrónicos que permiten certificar los datos de envío y recepción, su fecha y hora, el no repudio en el origen y de recepción. El sistema de intermediación digital dentro de la Infraestructura Oficial de Firma Electrónica es brindado por persona jurídica acreditada ante la Autoridad Administrativa Competente.
- Servicio OCSP (Protocolo del estado en línea del certificado, por sus siglas en inglés): permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la Autoridad de Certificación sobre el estado de un certificado.
- Software: palabra de origen ánglico que hace referencia a todos los componentes intangibles de una computadora, es decir, al conjunto de

programas y procedimientos necesarios para hacer posible la realización de una tarea específica. Probablemente la definición más formal de software es la atribuida a la IEEE, en su estándar 729: “la suma total de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de cómputo”.

- Suscriptor o titular de la firma digital: persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado sea una persona natural, sobre la misma recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado, 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 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.
- 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 de certificado digital: persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.
- TSL (Lista de Estado de Servicio de Confianza, por sus siglas en inglés) : lista de confianza que incluye a los PSC acreditados, autorizados a operar en el marco de la IOFE. El propósito de la TSL es proveer de modo ordenado información del estado de los proveedores de servicios, teniendo un rol preponderante en los servicios considerados confiables (acreditados) y los proveedores supervisados por la Autoridad Administrativa Competente.
- Usabilidad: es un término proveniente del inglés "usability", usado para denotar la forma en la que una persona puede emplear una herramienta particular de manera efectiva, eficiente y satisfactoria, en función de lograr una meta específica. A esta idea van asociadas la facilidad de aprendizaje (en la medida en que éste sea lo más amplio y profundo posible), la tasa de errores del sistema y la capacidad del sistema para ser recordado (que no se olviden las funcionalidades ni sus procedimientos).
- WebTrust for CA.- 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*
DPSVA	Declaración de Prácticas de Servicios Valor Añadido
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
ICC	Tarjeta de Circuitos Integrados
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)

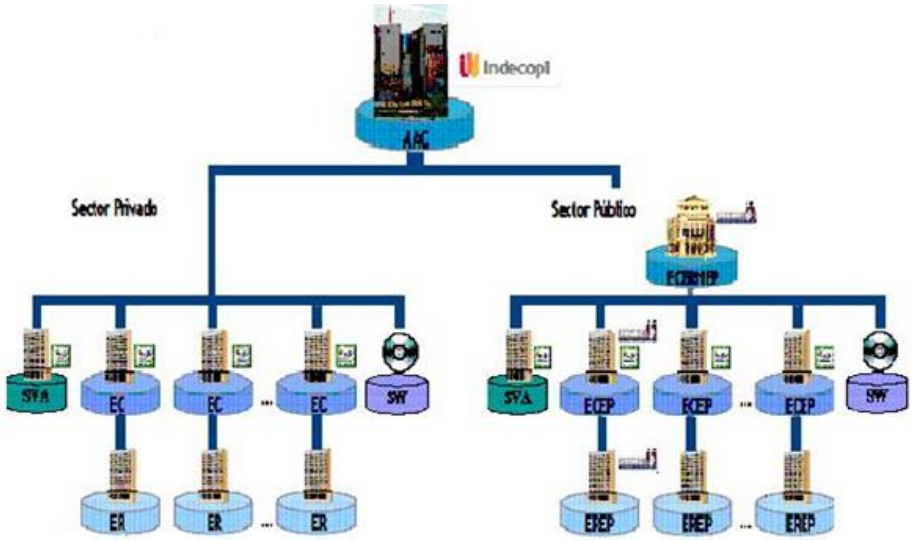
PSC	Prestador de Servicios de Certificación Digital Prestador de Servicios de Criptográficos
ROPS	Registro Oficial de Prestadores de Servicio de Certificación Digital
RFC	*Request for Comment*
RPS	Declaración de Prácticas de Registro o Verificación de una ER
SHA	*Secure Hash Algorithm*
PSVA	Prestador de Servicios de Valor Añadido
PSVAEP	Prestados de Servicios de Valor Añadido para el Estado Peruano
SVA	Servicios de Valor Añadido (*Sellado de Tiempo o Sistema de Intermediación Digital*)
TSL	Lista de Estado de Servicio de Confianza
UTC	Tiempo universal coordinado

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 se tiene la Quinta Disposición Complementaria Final de la Ley 30224, Ley que crea el Sistema Nacional para la Calidad y el Instituto Nacional de Calidad, la misma 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

El mecanismo de interoperabilidad utilizado con el propósito de proveer, de modo ordenado, la información del estado de los Proveedores de Servicios de Certificación (PSC) 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 PSC 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],

[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:

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 ECs que facilitan la aceptación transnacional 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 tanto por ECs nacionales como extranjeras, y facilita la predictibilidad legal a nivel transnacional.
- El referido marco no determina el empleo de ningún tipo de tecnología en particular. Propugna más bien la neutralidad tecnológica, la adopción permanente de los estándares del mercado, el desarrollo de la tecnología existente y la introducción de nueva tecnología.

"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.

II: MARCO DE POLÍTICAS

- Los requerimientos para el establecimiento de ECs sirven para generar la confianza pública y la confidencialidad y facilitan el reconocimiento transnacional de los certificados emitidos por dichas entidades.
- 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 11– y de gestión en esquemas PKI permiten la adecuada implementación de las ECs 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 ECs)

General

- El empleo del estándar X.509 y el RFC 3647 para las Políticas de Certificación (CP) y la Declaración de Prácticas de Certificación (CPS) propugna el proceso de reconocimiento transnacional.

Registro y Validación de la Identidad

- El establecimiento de procedimientos para el registro y validación de la identidad del usuario que toman en consideración los procedimientos usados para tales efectos en otras jurisdicciones, propugnan el reconocimiento transnacional de certificados[3].
- Cada vez que un certificado expire (vencimiento del tiempo de vigencia) o sea revocado, el usuario debe repetir el mismo ciclo inicial de verificación de su identidad ante una ER acreditada a fin de adquirir un nuevo certificado digital.

[3] Se refiere a la interoperabilidad legal y técnica dentro de la Infraestructura de Clave Pública (PKI) por parte de los países miembros del APEC en función al cumplimiento de disposiciones y estándares internacionales. Esto implica el reconocimiento mutuo de documentos electrónicos firmados digitalmente.

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 11).
- 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[4] 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.

[4] 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 privada 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[5].

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 administrativas.	Intercambio de documentos resolutivos o normativos y transacciones monetarias. Transacciones internacionales.	Intercambio de información crítica clasificada o de seguridad nacional.
Dispositivos Criptográficos	Los dispositivos criptográficos físicos –hardware y firmware– que almacenen las claves privadas de la entidad final–usuarios– deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 2 (mínimo) o Common Criteria EAL4+.	Los dispositivos criptográficos físicos –hardware y firmware– que almacenen las claves privadas de la entidad final–usuarios– deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 2 (mínimo) o Common Criteria EAL4+.	Los dispositivos criptográficos físicos –hardware y firmware– que almacenen las claves privadas de la entidad final–usuarios– deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 3 (mínimo) o Common Criteria EAL4+.
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.
Generación de la Clave Privada	Los certificados a nivel de entidad final –usuarios– deben ser generados de manera individual y separados	Los certificados a nivel de entidad final –usuarios– deben ser generados en los dispositivos criptográficos de manera	Los certificados a nivel de entidad final –usuarios– deben ser generados en los dispositivos

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

	para las siguientes funciones: cifrado y firma (no repudio) o autenticación. Las funciones de firma y autenticación son compatibles y pueden ser realizadas con un mismo certificado.	individual y separados para las siguientes funciones: cifrado y firma (no repudio) o autenticación. Las funciones de firma y autenticación son compatibles y pueden ser realizadas con un mismo certificado.	criptográficos de manera individual y separados para las siguientes funciones: cifrado, firma (no repudio) y autenticación.
Requerimientos de acreditación	• Consulta de revocación mediante OCSP y CRL • Seguros o garantías bancarias equivalentes a $50 000.00 Dólares americanos.	• ISO 27001 • WebTrust for CA • Consulta de revocación mediante OCSP y CRL • Seguros o garantías bancarias equivalentes a $50 000.00 Dólares americanos.	• ISO 27001 • WebTrust for CA • Consulta de revocación mediante OCSP y CRL • Seguros o garantías bancarias equivalentes a $50 000.00 Dólares americanos. • Jurisdicción Peruana

Alcance

Los niveles de seguridad integran diversos aspectos relativos a la IOFE. Se exige que todos ellos ostenten un nivel de seguridad mínimo, de modo que en conjunto brinden una garantía sobre su uso.

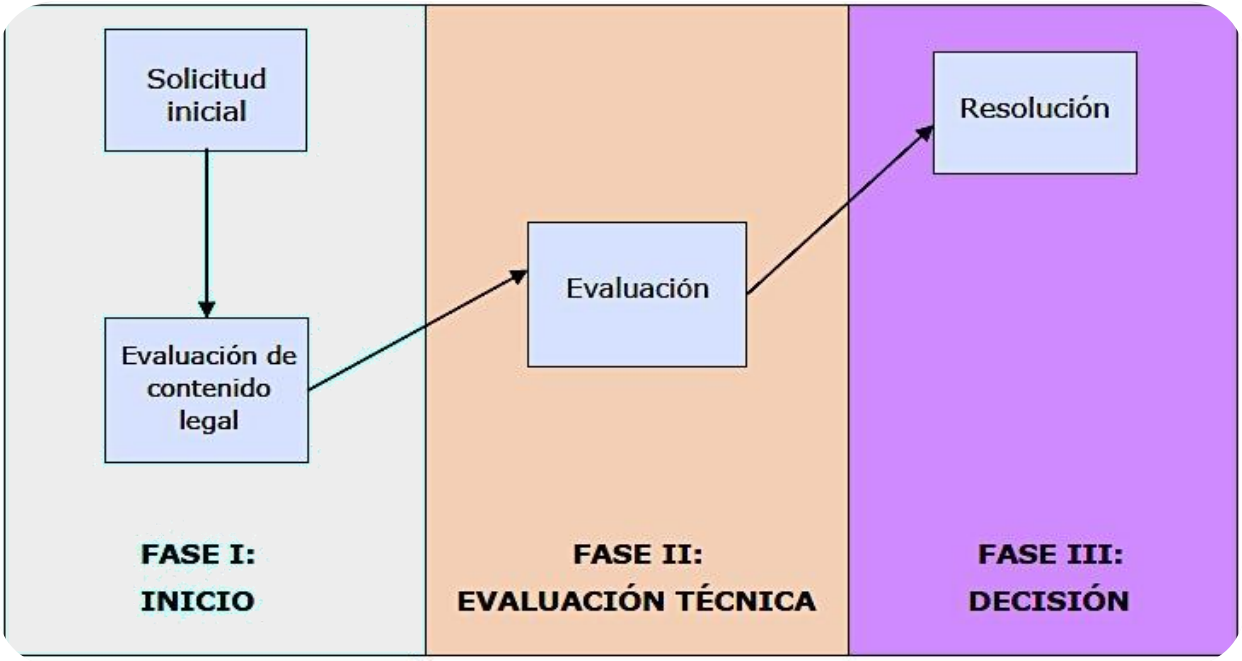
Dispositivos criptográficos: tanto el hardware (chip) como el firmware (sistema operativo) de la EC deben de cumplir con certificaciones de seguridad FIPS 140-2 Nivel de Seguridad 3 o Common Criteria EAL4+ como mínimo para todos los niveles de Seguridad.

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. 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.

7.1. Paso 1: Solicitud inicial

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

1. Solicitud dirigida al Secretario Técnico de Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica (CFE) del INDECOPI, mediante el formato adjunto en el Anexo 10.
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 empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro documento equivalente expedido por la autoridad competente en su país de origen.
   iii. 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 prestador de servicios de certificación digital.

3. Adjuntar los poderes en virtud a los cuales los representantes legales se encuentran facultados para solicitar la acreditación o autorización. Sobre el particular deberá tenerse en cuenta lo siguiente:
   i. En el caso de personas jurídicas constituidas en el país: 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 encargada de la certificación digital. Debiéndose asimismo acreditarse las facultades de este funcionario.
4. Memoria descriptiva de la empresa o entidad estatal.
5. Organigrama estructural y funcional de la EC.
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 en formato adjunto en el Anexo 9 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 10.
9. Declaración de Practicas de Certificación y Política de Certificación
10. En el caso que cualesquiera 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.

11. Declaración jurada declarando cumplir con tener operativo software, hardware y demás componentes adecuados para las prácticas de certificación, repositorio y las condiciones de seguridad adicionales basadas en estándares internacionales o compatibles a los internacionalmente vigentes que aseguren interoperabilidad –ver anexo 11–. Esta declaración jurada se encuentra incluida en el anexo 10.
12. Declaración jurada de aceptación de la visita comprobatoria del INDECOPI. Esta declaración jurada se encuentra incluida en el anexo 10.
13. Documento que acredite relación con al menos una ER acreditada. No será necesario este requisito en el caso que una misma persona jurídica desee asumir al mismo tiempo funciones de EC y ER, en cuyo supuesto deberá solicitar su acreditación de conformidad con la Guía de Acreditación de ER. En este caso, su acreditación como EC quedará condicionada a la obtención de la correspondiente acreditación como ER.
14. Informe favorable –cuando así lo solicite el INDECOPI–, de la entidad sectorial correspondiente, en el caso de personas jurídicas supervisadas, respecto de la legalidad y seguridad para el desempeño de actividades de certificación.
15. 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.
16. Documentación que acredite contar con respaldo económico. Para tales efectos la EC solicitante deberá presentar estados financieros (balance general, estado de ganancias y pérdidas y notas contables), con una antigüedad no mayor a dos meses del cierre contable del mes anterior a la presentación de la solicitud, acreditando solvencia económica.

    Nota: Los estados financieros antes señalados deberán ser individuales (no consolidados) y encontrarse auditados. Si una empresa presentara estados financieros con pérdidas acumuladas de ejercicios anteriores, para acreditar solvencia económica deberá capitalizar dicha pérdida o realizar nuevos aportes en cuantía que compense el desmedro y mostrar el nuevo capital suscrito y pagado e inscrito en Registros Públicos.
17. Constancia de pago de los derechos administrativos correspondientes. Este pago será efectuado en las oficinas del INDECOPI.
18. En el caso que el INDECOPI hubiera celebrado un acuerdo de reconocimiento mutuo con entidades similares a nivel mundial, bastará que la EC solicitante acompañe la homologación o acreditación otorgada en su país de origen, debiendo hacer referencia al instrumento en el que conste el acuerdo de reconocimiento mutuo antes señalado. Serán válidas las auditorías por terceras partes independientes realizadas en el extranjero, siempre y cuando

las mismas hayan sido elaboradas conforme a los lineamientos tecnológicos requeridos para tales efectos por el INDECOPI y contenidos en el documento del APEC.

Nota: Queda claro que dos o más EC no pueden compartir la misma jerarquía PKI (Entidad de Certificación subordinada o de nivel subsiguiente).

7.2. Paso 2: Evaluación de contenido legal

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

19. La CFE realizará una verificación preliminar de índole formal, con relación a la solicitud y los recaudos acompañados a la misma.
20. En caso se haya cumplido de manera defectuosa o se haya omitido alguno de los requisitos exigidos, otorgará un plazo máximo de cinco (5) 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.
21. 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 EC 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 Certificación Digital.
22. 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 los documentos CP y CPS, por cuanto la misma será materia de evolución en el Paso 3 referido a la evaluación técnica de la EC solicitante.
23. En caso existan observaciones a la documentación presentada, otorgará al solicitante un plazo de diez (10) días hábiles para el levantamiento de las mismas.
24. 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 EC solicitante a

efectos de realizar las coordinaciones necesarias para la etapa de evaluación técnica.

25. Si no se levantan las observaciones formuladas dentro del plazo establecido, se declarará la improcedencia de la solicitud y la conclusión del procedimiento.
26. En todos los supuestos antes señalados la CFE deberá fundamentar claramente su decisión. 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.

7.3. Paso 3: Evaluación de la implementación de la declaración en los documentos CP, CPS, la Política y Plan de Privacidad, la Política de seguridad y el cumplimiento de los criterios de usabilidad.

En esta etapa se examinarán los documentos CP, CPS, la Política y el Plan de Privacidad y la Política de Seguridad de la EC, y establecer su alineación con el Marco de la Política de emisión de certificados digitales (anexo 1), la Norma Marco sobre Privacidad (anexo 6), respectivamente.

Actividades:

27. En esta etapa corresponde a la EC solicitante la presentación los documentos correspondientes a la CP, CPS, Política de Privacidad, al Plan de Privacidad y a la Política de Seguridad.

28. Los requerimientos de seguridad son aquellos comprendidos en la sección Controles de Seguridad descritos en el Anexo 1. En caso que exista una certificación de seguridad ISO 27001 o BS 7799-II vigente cuyo alcance cubra los requerimientos descritos en el Anexo 1, puede que no sea necesaria la presentación de evidencias de cumplimiento de dicha sección.

29. La EC podrá presentar como evidencia cualquiera de siguientes los informes de auditorías independientes:
    - Webtrust – Trust Service Principles and Criteria for Certification Authorities
    - ISO 21188 - “Public key infrastructure for financial services -- Practices and policy framework”
    - ETSI EN 319 411-1
    - ETSI EN 319 401

La EC deberá demostrar que el alcance de los controles evaluados en estas auditorías independientes cubre los requerimientos descritos en la presente guía y sus anexos, complementando las evidencias que sean necesarias para completar aquellos requerimientos que no hayan sido evaluados.

30. En caso que la EC solicitante subcontrate la totalidad de la infraestructura tecnológica (incluyendo todos los procesos del sistema de gestión) utilizada también por una EC acreditada, se deberá sustentar este hecho, pudiendo emplear la documentación de la Política de Seguridad –correspondiente a la infraestructura tecnológica referida– presentada por dicha EC acreditada. En caso de incorporar modificaciones, éstas deberán ser sustentadas mediante las auditorías correspondientes.

31. 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 anexo 6.

32. El Comité Evaluador procederá a la evaluación de cumplimiento en la implementación y operaciones de certificación conforme a los documentos CP y CPS, la Política de Privacidad, el Plan de Privacidad, la Política de Seguridad y los requerimientos de Usabilidad para la EC – conforme a los establecido en el anexo 12 de la presente Guía de Acreditación.

33. El Comité Evaluador, una vez realizada la correspondiente evaluación, emitirá un informe que 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.

34. 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 EC. Este hecho debidamente fundamentado, se pondrá en conocimiento de la EC solicitante y correrá por cuenta de la misma los gastos que puedan generarse por esta evaluación.

35. En caso de presentarse no conformidades, la EC solicitante tiene un plazo de cinco (5) 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.

36. 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 Certificación Digital.

37. La EC 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 Certificación digital.

7.4. Paso 4: Resolución

La CFE decidirá si se permite el ingreso a la IOFE de la EC 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 EC solicitante.
- Denegar la acreditación.

Una vez recibida la documentación a que se alude en el punto anterior, se entenderá que la EC acreditada ingresará a la IOFE, a través de su inscripción en el Registro de Prestadores de Servicios de Certificación Digital 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.

7.5. Paso 5: Publicidad de resultados:

INDECOPI publicará la acreditación y estado de una EC a través de un directorio en su página WEB, estableciendo un Repositorio de certificados o claves públicas de las entidades acreditadas para la emisión de certificados, incluyendo los certificados cruzados o la emisión de certificados para certificación cruzada.

Para efectos de estandarizar el formato de información confiable sobre el estado de acreditación del PSC (EC, ER o SVA), INDECOPI implementará el ROPS basada en el estándar ETSI TS 102 231, donde publicará el estado de todas las Entidades de Certificación acreditadas.

8. 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.

8.1. Paso 1: Notificación:

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

8.2. 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 los controles de seguridad para proteger la gestión del ciclo de vida de las claves de la EC.
- La verificación de los controles de seguridad para proteger la gestión del ciclo de vida de las claves del Suscriptor.
- La verificación de la disponibilidad de los servicios de CRL y OCSP.
- La verificación de la vigencia del seguro o garantía financiera.
- El mantenimiento de la certificación WebTrust, ISO 27001, etc. (si fuera aplicable)

8.3. 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 el 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.

9. 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 Software), 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.

9.1. Paso 1: Solicitud:

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

9.2. Paso 2: Evaluación:

El PSC tendrá un plazo de 120 días hábiles para tramitar y someterse a la evaluación por parte de un auditor independiente seleccionado de una lista presentada por el INDECOPI.
El auditor evaluará la actualización del documento CPS y su respectiva implementación. Todos los controles y documentos aplicables al nuevo alcance deberán ser verificados.

9.3. 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.