

Guía de Acreditación de Aplicaciones de Software

Requerimientos para acreditar una aplicación (SW) de Clave Pública (PK)

Versión 4.0

**Guía de Acreditación de
Aplicaciones de Software**

ÍNDICE GENERAL

1. INTRODUCCIÓN	4
1.1 PROPÓSITO.....	4
1.2 APLICACIONES (SOFTWARE) DE FIRMA DIGITAL.....	5
1.3 PÚBLICO AL QUE VA DIRIGIDO	5
1.4 VISIÓN GENERAL	5
1.6 DEFINICIONES/TERMINOLOGÍA	6
1.7. ACRÓNIMOS	16
1.8. ARQUITECTURA JERÁRQUICA DE CERTIFICACIÓN DEL ESTADO PERUANO Y MECANISMO DE INTEROPERABILIDAD	17
2.0 ANTECEDENTES.....	18
3.0 DOCUMENTOS APLICABLES Y ALCANCES	28
3.1 DOCUMENTOS APLICABLES	28
3.2 NIVELES DE SEGURIDAD DE PKI.....	29
3.3 LISTA DE SERVICIOS DE CONFIANZA – TSL.....	30
3.4 CLASIFICACIÓN DE APLICACIONES	30
3.5 CLASIFICACIÓN DE REQUERIMIENTOS.....	30
3.6 ESTRUCTURA DE DOCUMENTO	31
4.0 REQUERIMIENTOS.....	32
4.1 SOFTWARE DE FIRMA DIGITAL DE USUARIO FINAL.....	32
4.1.1 Requerimiento 1: Verificación del estado de revocación.....	34
4.1.2 Requerimiento 2: Verificación de no expiración del certificado	36
4.1.3 Requerimiento 3: Verificación del propósito.....	36
4.1.4 Requerimiento 4: Comprobaciones para aplicaciones Web:	38
4.1.5 Requerimiento 5: Las funciones criptográficas deben realizarse en el módulo criptográfico.....	38
4.1.6 Requerimiento 6: No se deben utilizar funciones criptográficas obsoletas ..	40
4.1.7 Requerimiento 7: Se debe proteger la autenticidad del código de firma	41
4.1.8 Requerimiento 8: Se debe proporcionar el visor para la verificación de la firma	41
4.1.9 Requerimiento 9: Se deben generar registros de validación de la firma	42
4.1.10 Requerimiento 10: Se deben implementar los manuales de administración y usuario.....	43
4.2 SOFTWARE DE FIRMA POR PARTE DE AGENTES AUTOMATIZADOS.....	43
4.2.1 Requerimiento 11: Verificación del estado de revocación	45
4.2.2 Requerimiento 12: Verificación de no expiración del certificado	47
4.2.3 Requerimiento 13: Verificación del propósito.....	48
4.2.4 Requerimiento 14: Control de acceso a las funciones de administración y configuración.	49
4.2.5 Requerimiento 15: Las funciones criptográficas deben realizarse en el módulo criptográfico.....	50
4.2.6 Requerimiento 16: No se deben utilizar funciones criptográficas obsoletas	52
4.2.7 Requerimiento 17: Se debe proteger la autenticidad del código de firma	52
4.2.8 Requerimiento 18: Se debe proporcionar el visor para la verificación de la firma 53	53
4.2.9 Requerimiento 19: Se deben generar registros de validación de la firma	54
4.2.10 Requerimiento 20: Se deben implementar los manuales de administración y usuario.....	54
4.3 SOFTWARE DE VERIFICACION POR PARTE DE AGENTES AUTOMATIZADOS	55

4.3.1	Requerimiento 21: Verificación del estado de revocación	58
4.3.2	Requerimiento 22: Verificación de no expiración del certificado	60
4.3.3	Requerimiento 23: Verificación del propósito	61
4.3.4	Requerimiento 24: Control de acceso a las funciones de administración y configuración.	62
4.3.5	Requerimiento 25: En caso que se firmen los documentos recibidos, las funciones criptográficas deben realizarse en el módulo criptográfico	63
4.3.6	Requerimiento 26: No se deben utilizar funciones criptográficas obsoletas	64
4.3.7	Requerimiento 27: Se debe proteger la autenticidad del código de firma	65
4.3.8	Requerimiento 28: En caso que el sistema automatizado realice la firma digital del documento recibido, se debe proporcionar un visor para verificar la firma del documento	66
4.3.9	Requerimiento 29: En caso de firmar los documentos recibidos, se deben generar registros de validación de la firma	66
4.3.10	Requerimiento 30: Se deben implementar los manuales de administración y usuario	67
4.4	FUNCIONALIDAD DE SOLICITUD DE SELLOS DE TIEMPO	68
4.4.1	Requerimiento 30: Verificación de sello de tiempo	68
5.0	CONFIGURACIÓN DE SEGURIDAD	68
6.0	PROCEDIMIENTOS DE EVALUACIÓN	69
6.1	PROCEDIMIENTO DE LA EVALUACION DE SEGUIMIENTO	69
6.1.1	Paso 1: Notificación	70
6.1.2	Paso 2: Evaluación	70
6.1.3	Paso 3: Resultado	70
6.2	PROCEDIMIENTO DE LA ACTUALIZACIÓN	70
6.2.1	Paso 1: Solicitud	70
6.2.2	Paso 2: Evaluación	71
6.2.3	Paso 3: Resultado	71
6.3	RESPONSABILIDAD EN CASOS DE INCUMPLIMIENTO	71
	SOFTWARE DE FIRMA DIGITAL DE USUARIO FINAL	79
	SOFTWARE DE FIRMA POR PARTE DE AGENTES AUTOMATIZADOS	86
	SOFTWARE DE VERIFICACIÓN POR PARTE DE AGENTES AUTOMATIZADOS	94
	FUNCIONALIDAD DE SOLICITUD DE SELLOS DE TIEMPO (OPCIONAL)	101

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

1. INTRODUCCIÓN

En conformidad con el artículo 4° del D.S. 052-2008-PCM - Reglamento de la Ley de Firmas y Certificados Digitales, el presente es un documento técnico – operativo, que regula los requisitos que las aplicaciones de software de firma digital deben cumplir para ser consideradas al amparo de la Infraestructura Oficial de la Firma Electrónica. La Infraestructura Oficial de la Firma Electrónica está compuesta por los siguientes actores, los cuales son el soporte de la confiabilidad de las transacciones electrónicas con firma electrónica:

- Entidades de Certificación Digital (EC)
- Entidades de Registro o Verificación (ER)
- Prestadores de Servicios de Valor Añadido (SVA)
- Aplicaciones de Software (SW)

Las Entidades de Certificación Digital, tienen como tarea principal dar fe y respaldo a la identidad de los usuarios de los certificados digitales y a su correspondencia con sus respectivas claves públicas.

Las Entidades de Registro o Verificación, tienen como principal tarea verificar la identidad de los titulares y suscriptores de los certificados digitales conforme a su propósito. En algunos casos las Entidades de Certificación asumen las funciones de registro internamente, y en otros, se utilizan Entidades de Registro externas e independientes. Los procedimientos de registro deben ser realizados conforme a la Política de Certificación emitida por la EC correspondiente.

Los Prestadores de Servicios de Valor Añadido, utilizan los servicios de certificación digital o son una parte componente de los mismos, que permiten fortalecer la confiabilidad y funcionalidad de los servicios soportados por la Infraestructura Oficial de la Firma Electrónica (IOFE).

Las Aplicaciones de Software de Firma Digital, son herramientas de software que permiten verificar el estado de validez de un certificado digital, respecto de su vigencia, estado de revocación y confiabilidad del certificado Raíz correspondiente.

1.1 Propósito

El presente documento contiene los requerimientos que los prestadores de aplicaciones de software de firma digital deben cumplir para poder gozar del amparo jurídico de la IOFE.

	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

1.2 Aplicaciones (software) de Firma Digital

El principio básico para el no repudio de los documentos digitales es que estos se encuentren firmados digitalmente “bajo el marco de la IOFE”¹. Todo documento firmado digitalmente es considerado no repudiable de manera individual, es decir, el principio del no repudio es aplicable al documento cuya firma digital le corresponde.

Es necesario hacer esta redundante aclaración pues, en casos como los documentos previamente comprimidos y cuyo archivo resultado de la compresión es firmado digitalmente, el principio del no repudio es únicamente aplicable al archivo comprimido firmado, más no a cada uno de los archivos en él contenidos. Del mismo modo, si un correo digital que contiene archivos adjuntos es firmado digitalmente – formato s-mime– se debe observar que adicionalmente cada archivo adjunto sea firmado digitalmente de modo individual. En caso contrario, el principio del no repudio es aplicable al correo y los adjuntos en conjunto, empero si alguno de los archivos adjuntos es individualmente extraído y no se encuentra firmado digitalmente de modo individual, el principio del no repudio no le es aplicable.

Las aplicaciones de firma digital deben permitir la realización de múltiples firmas digitales (*cosign*) en el mismo documento digital, de manera recurrente. Deben de cumplir con las normas establecidas por la IOFE, los estándares

1.3 Público al que va dirigido

Desarrolladores y proveedores de aplicaciones de software. El documento asume que los lectores ya se encuentran familiarizados con los fundamentos de Clave Pública y los fundamentos de la PKI.

1.4 Visión General

Este documento empieza con los antecedentes e información contextual previa a la descripción de los requerimientos. Las secciones 2 y 3 contienen estos antecedentes e información contextual.

La sección 2 provee información sobre los antecedentes. El propósito de la sección de antecedentes es el establecer los términos usados en el resto del documento.

La sección 3 establece los alcances de este documento. Esta sección lista los documentos que moldean y complementan los requerimientos encontrados en este documento. Esta sección también identifica los tipos de aplicaciones a las cuales se aplican los requerimientos.

La sección 4 contiene los requerimientos técnicos actuales que las aplicaciones deben satisfacer.

El anexo b establece la lista de Verificación de Auditoría.

¹ Artículo 3º y ss. del DS 052-2008-PCM.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

1.6 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 fin, 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

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

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.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

- 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.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

- 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

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

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:

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

- 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 N° 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley N° 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

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

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”.
- **Norma Marco sobre Privacidad.-** Es la norma basada en la normativa aprobada en la 16ª Reunión Ministerial del APEC, que fuera llevada a cabo en Santiago de Chile el 17 y 18 de noviembre de 2004, la cual forma parte integrante de las Guías de Acreditación aprobadas por la Autoridad Administrativa Competente.
- **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.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

- **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 electrónico, 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 presente documento, denominado Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley N° 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 electrónico 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.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

- Sistema de Intermediación Digital: Es el sistema WEB que permite la transmisión y 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 de Intermediación Electrónico: Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma electrónica, 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 hipervínculos.
- 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

	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

- 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.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

1.7. ACRÓNIMOS

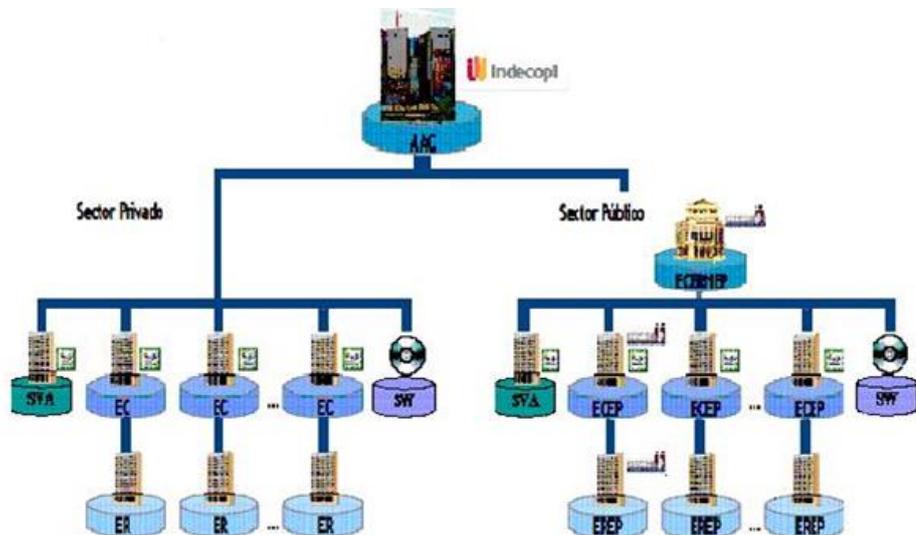
AAC	Autoridad Administrativa Competente (CNB del INDECOPI)
CC	Common Criteria
CEN	Comité Europeo de Normalización
CP	Políticas de Certificación
CPS	Declaración de Prácticas de Certificación de una EC
CRL o LCR	<i>Certificate Revocation List</i> (Lista de Certificados Revocados)
CFE	Comisión Transitoria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

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

Por mandato del artículo 57° del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por el Decreto Supremo N° 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.

TSL

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

	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

(PSCs) acreditados y supervisados por INDECOPÍ –y por tanto autorizados a operar en el marco de la IOFE– es la TSL, Lista de Estado de Servicio de Confianza.

La TSL 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 INDECOPÍ a efectos de asegurar su integridad y estará disponible para que las aplicaciones de software puedan procesarla.

2.0 ANTECEDENTES

El propósito es establecer la terminología a ser usada en la descripción de los requerimientos de aplicación.

La **criptografía simétrica** porque ambas partes de una comunicación requieren compartir la misma clave, tanto para cifrar como para descifrar los datos de dicha comunicación. En este sentido, para garantizar el secreto de sus comunicaciones es necesario lo siguiente:

- Un método fiable y seguro para distribuir la clave a las partes.
- Que las partes mantengan la clave en secreto y que no la hagan pública a terceros sin la aprobación y conocimientos de la contraparte.

A diferencia de la criptografía simétrica, la **criptografía asimétrica** utiliza distintas claves para el cifrado y descifrado² de datos dentro duna comunicación. Desde su generación, el **par de claves** tiene una relación particular: los datos que son cifrados con una de las claves solo pueden ser descifrados con la otra clave, a fin de acceder a los datos originales (**texto en claro**).

La criptografía de clave pública usa claves asimétricas en lugar de las claves simétricas tradicionales. El **propietario** del par de claves designa a una clave como **clave privada** y la otra como **clave pública**. Es su deber mantener la clave privada en secreto y hacer pública la otra clave, la cual puede ser publicada en repositorios accesibles a terceros.

Las claves asimétricas pueden ser usadas para **firmar** o **cifrar** información.

Durante el proceso de firma, el propietario utiliza su clave privada para cifrar un **resumen o hash**³ del documento. El resumen cifrado viene a ser la firma digital del

² Cuando se discute la criptografía asimétrica, el cifrado se refiere a la operación efectuada en datos limpios (texto en claro) o no cifrados, para producir información cifrada, mientras que el descifrado se refiere a la operación de transformar información cifrada a su forma original.

³ Los algoritmos hash y los algoritmos simétricos son usados para reducir la sobrecarga computacional de la clave pública para procesos de firma y cifrado, respectivamente. Los algoritmos hash son funciones criptográficas que convierten un mensaje de longitud variable en un mensaje resumen (digest) o hash de longitud fija.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

documento, la cual es adjuntada al documento original dando como resultado el **documento firmado**.

Para verificar la autenticidad de la firma y la integridad del documento firmado, el receptor realiza el proceso de verificación siguiente:

- a. Separa la firma digital del documento original.
- b. Descifra la firma digital, utilizando la clave pública perteneciente del remitente.
- c. Obtiene un resumen o hash del documento original recibido como parte del documento firmado.
- d. Compara el resumen obtenido de descifrar la firma digital (b) con el resumen obtenido del documento original (c). Si los valores son iguales, el receptor puede tener la certeza de que el documento firmado no ha sido alterado. Puesto que cada clave pública puede descifrar solamente datos cifrados con la correspondiente clave privada, el receptor tiene la seguridad de la identidad del remitente de dicho documento firmado. Si los valores no son iguales, esto implica que el mensaje fue alterado, o que la clave pública usada no es el par de la clave privada usada para firmar el documento.

Durante el proceso de cifrado, el remitente cifra los datos utilizando la clave pública del receptor. Puesto que sólo el propietario posee la clave privada correspondiente, solo él puede descifrar la información cifrada y acceder a los datos originales (texto en claro).

Para reducir densas operaciones relativas al cifrado asimétrico, el remitente de un mensaje puede realizar lo siguiente:

- Generar una clave simétrica, la **clave de sesión (session key)**.
- Cifra el documento usando la clave de sesión.
- Cifra la clave de sesión usando la clave pública del destinatario.
- Transmitir el documento cifrado junto con la clave de sesión cifrada.

La combinación del contenido cifrado y una clave de sesión cifrada para un determinado destinatario, se denomina **sobre digital (digital envelope)** para aquel destinatario. El documento puede ser enviado a múltiples destinatarios cifrando la clave de sesión y usando la clave pública de cada destinatario e incluyendo las claves de sesión cifradas en el sobre.

Las secciones previas han descrito las funciones primarias de la criptografía de Clave Pública: cifrado y firma digital. Estas dos funciones básicas soportan cuatro servicios distintos de seguridad:

Autenticación: La autenticación es el proceso de verificación y aseguramiento de la identidad de una persona natural o jurídica.

Confidencialidad: La confidencialidad de los datos es la protección de la información frente a una divulgación no autorizada.

Integridad: La integridad de los datos es la protección de la información frente a una modificación no autorizada y no detectada.

No repudio: El no repudio asocia a una persona natural o jurídica con los datos, de tal manera que la entidad no puede negar su asociación con ellos ni reclamar eventuales modificaciones de los mismos (falsificación).

La firma digital garantiza la autenticación, integridad y no repudio de un documento firmado. El cifrado permite la confidencialidad de los documentos cifrados. Los servicios basados en las firmas digitales asumen que el propietario de la clave privada controla la misma y asegura su secreto; es decir, sólo dicho propietario de la clave privada puede emplearla. La verificación de un documento firmado con una clave pública asegura que su propietario firmó el documento. La Tabla 1 resume las operaciones de clave pública que proveen los servicios.

Tabla 1. Métodos de clave pública usados para proporcionar servicios de seguridad.

Servicio de Seguridad	Métodos de Clave Pública
Autenticación	Firma
Confidencialidad	Cifrado
Integridad	Firma
No repudio	Firma

El proceso de verificación de una firma directamente soporta los servicios de integridad porque puede detectar (pero no prevenir ni corregir) la modificación no autorizada realizada con posterioridad a la firma.

La asociación de la clave privada con su propietario evita que éste deniegue la autoría del documento firmado. Así, las firmas soportan los servicios técnicos de no repudio. Técnicamente las firmas no pueden ser negadas. Una firma que se verifica con una clave pública particular tuvo que ser firmada con la clave privada asociada. La verificación puede ser realizada por cualquier otra persona (terceros que confían) en cualquier momento⁴. Sin embargo, el no repudio técnico por sí mismo puede no ser suficiente para un no repudio legal, en el cual una persona pueda ser legalmente reconocida como autor de la firma digital.

Existen circunstancias bajo las cuales un documento firmado digitalmente puede ser repudiado como:

- Cuando una persona, diferente al suscriptor. Ha tenido acceso a la clave privada a pesar de que este último haya sido precavido al proteger la clave.
- Cuando un suscriptor es estafado, forzado o coaccionado en el momento de efectuar la firma.

⁴ Puede haber un límite para el período durante el cual la verificación puede darse, como se discutirá posteriormente.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

Para garantizar la confiable asignación del par de claves a una persona natural o jurídica y evitar la usurpación de identidad o estafa es necesaria la presencia de una tercera parte confiable (*Trusted Third Party, TTP*), que en una PKI es la **Entidad de Certificación (EC)**, la cual relaciona al par de claves con la un **certificado digital (certificado de clave pública o certificado)**, el cual a su vez es un documento firmado digitalmente por la EC que lo emite, que incluye el nombre del **suscriptor y/o el titular del certificado digital**. En el caso de una persona natural, el suscriptor es el responsable de la posesión del par de claves, titular del certificado digital y **titular de la firma digital**. En el caso de una persona jurídica, el suscriptor es una persona natural responsable de la posesión del par de claves y titular de la firma digital, el cual es asignado por la persona jurídica, siendo ésta el **titular del certificado digital**. El certificado incluye información adicional relativa a la PKI, y los usos que la EC pretende para el certificado.

Las EC utilizan los servicios de una Entidad de Registro o Verificación (ER), para la verificación de la identidad de los solicitantes de los certificados digitales.

Cuando un certificado digital es emitido, el par de claves es generado primero, luego la clave pública es enviada a la EC. A continuación, la EC genera el certificado digital (y podría publicarlo en su **Repositorio**), lo firma digitalmente y lo envía para el correspondiente proceso de verificación. El Repositorio permite que los usuarios puedan obtener copias de los certificados que pertenecen a un individuo y, por consiguiente, puedan obtener la clave pública del suscriptor a partir del certificado.

Un usuario que obtiene una clave pública de un certificado y depende de la asociación entre el nombre del propietario y la clave pública y de alguna otra información contenida en el certificado, es un tercero que confía (*relying party*) o tercer usuario. La tabla 2 muestra cuál es el rol del suscriptor y del tercero que confía (tercer usuario) cuando se usan los métodos de clave pública.

Tabla 2. Operaciones del Suscriptor y la Tercera que confía.

Función	Suscriptor	Tercera Parte
Cifrado	Descifra los datos recibidos usando la clave privada.	Cifra los datos usando la clave pública del suscriptor receptor.
Firma Digital	Cifra (firma) datos usando la clave privada.	Descifra los datos usando la clave pública del suscriptor firmante para verificar la integridad del documento y la autenticidad de la firma digital.

A fin de garantizar una correcta verificación de la identidad de la persona natural o jurídica que solicita un certificado digital, como parte de la Infraestructura PKI, existen las Entidades de Registro o Verificación (ER), las cuales garantizan que el propietario

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

del par de calves sea correctamente identificado, y trabajan conjuntamente con las EC.

La EC se encarga de emitir y administrar el ciclo de vida de los certificados digitales y, además, proporciona información sobre el estado actual de un certificado a través de una **Lista de Certificados Revocados-LCR- (Certificate Revocation List, CRL)** o de una verificación en línea del estado del certificado (**Online Certificate Status Protocol, OCSP**). Como resultado de ciertas circunstancias adversas, algunos certificados pueden dejar de ser confiables. La EC revocará un certificado cuando sea informada de circunstancias que ya no garanticen la confianza del mismo.

El certificado revocado será incluido en las próximas CRLs que la EC emita. Luego que un **Respondedor OCSP (OCSP Responder, OCSPR)** recibe una CRL u otra notificación de la EC con relación al certificado revocado, éste responderá con una indicación de revocación para subsecuentes consultas relativas a dicho certificado.

La CRL es el más antiguo de los dos métodos de verificación de estado. La CRL tiene un encabezado que proporciona información general que incluye:

- El nombre del emisor de la CRL que usualmente es el mismo que el de la EC que emitió los certificados revocados.
- La **fecha**⁵ en que fue producida la CRL.
- La próxima fecha de actualización. La EC se compromete a producir una nueva CRL a más tardar en la fecha que figura en la CRL. La EC puede producir una nueva CRL antes de la fecha indicada. La CRL expira en la fecha de la próxima actualización.

La CRL lista los certificados revocados de manera individual mediante su número de serie junto con la fecha en que cada certificado fue revocado y, además, puede incluir un código con el que se indica la razón de dicha revocación.

Los certificados **expiran** al final de su período de validez y, si fuera el caso, son removidos de las CRLs emitidas después de su fecha de expiración. La EC firma digitalmente la CRL. Con la firma de la EC, las CRLs pueden ser transmitidas a través de enlaces de comunicación inseguros puesto que cualquier cambio subsiguiente será detectado a través del proceso de verificación de la firma.

La EC periódicamente emite las CRLs. La EC puede emitir las CRLs a intervalos dados de tiempo o en respuesta a un evento como la revocación de un certificado debido a la sospecha que la clave privada ha sido comprometida. La EC distribuye la CRL en un lugar donde los terceros que confían (terceros usuarios) pueden obtener la CRL más actualizada. Dicho lugar es conocido como **Punto de Distribución de CRL (CRL Distribution Point, CDP)** y usualmente especificado en términos de un Indicador Uniforme de Recursos (*Uniform Resource Indicator, URI*).

⁵ En este documento el término fecha denota un valor que tiene dos componentes: un día calendario y un tiempo dentro del día.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

El OCSP es el otro método para verificar la validez de un certificado.

El OCSP es el servicio que puede ser proporcionado por la EC o algún otro TTP. Un tercero que confía (tercer usuario) envía una solicitud al servicio OCSP con un certificado, éste responde con una respuesta firmada digitalmente que incluye fecha y hora, la identificación del certificado, y el estado del certificado sobre cuya validez el tercero que confía (tercer usuario) realizó la consulta. Las posibles respuestas incluyen "desconocimiento" ("*unknown*") la cual puede ser la respuesta a una consulta sobre un certificado expirado.

Los terceros que confían (terceros usuarios) deben efectuar la consulta del estado del certificado sin importar si se usa CRLs u OCSPRs para verificar el estado del certificado. El propósito de una revisión del estado del certificado es asegurar que el certificado continúa siendo confiable. Los terceros que confían (terceros usuarios) son responsables de verificar el estado del certificado, dado que se debe evitar perjuicios generados como resultado de utilizar un certificado revocado.

Las ECs pueden existir en **jerarquías**. Una EC puede delegar responsabilidades a otra EC. Una EC delega responsabilidad a otra, a través de la emisión de un certificado para una EC intermedia. El contenido de este certificado puede establecer las restricciones en las facultades delegadas a las ECs intermedias para emitir los subsiguientes certificados. La EC que se encuentra en la cima de la jerarquía es la **EC Raíz (Root CA)**. El certificado de una EC raíz ha sido **firmado por sí misma (self-signed)**. Las ECs intermedias emiten certificados a individuos que no pueden actuar como ECs y que no pueden emitir certificados. Un individuo que no puede emitir certificados es conocido como una **entidad final**⁶ (**end-entity**).

A fin de tener certeza de la confiabilidad de un certificado digital y de la entidad emisora, el tercero que confía (tercer usuario) debe verificar uno o más **puntos de confianza (trust points)**, que son las claves públicas (o certificados que las contienen) de los Prestadores de Servicios de Certificación Digital (EC, ER, SVA, SW) que son designados como confiables y fidedignos por la IOFE. Los terceros que confían (terceros usuarios) deben obtener las claves públicas (o los certificados) a través de algún método de distribución masiva confiable.

Los puntos de confianza son usualmente la lista de Proveedores de Servicios de Certificación (EC, ER, SVA, SW) de confianza –TSL- y los Certificados Raíz⁷ contenidos en aquélla. La confianza es transmisible, si la IOFE declara como confiable a una EC raíz, se entiende que son también confiables las ECs intermedias a las cuales la EC raíz ha delegado sus responsabilidades.

El tercero que confía (tercer usuario) puede fiarse del certificado de una entidad final si es que existe una secuencia de certificados que conectan el certificado de la entidad final a alguno de los puntos de confianza verificables por el tercero que

⁶ Suscriptor o titular de un certificado digital.

⁷ En determinadas circunstancias una parte confiada puede decidir confiar en una CA intermedia o incluso en una entidad final.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

confía. La secuencia es conocida como **ruta** o **cadena de certificación**. La construcción de la ruta es conocida como **desarrollo de la ruta (path development)**, y la verificación de que la ruta proporciona una cadena de confianza es conocida como **procesamiento de la ruta (path processing)**. El desarrollo y procesamiento de la ruta pueden sucederse secuencialmente o en paralelo. La ruta empieza con certificado digital de una EC raiz (el cual debe estar incluido en la lista TSL) prosigue con los certificados de las EC intermedias y finaliza con el certificado de la entidad final⁸.

El procesamiento de la ruta incluye:

- Verificación de las firmas en los certificados.
- Verificación de la cadena de certificados. Si el titular (*subject*) en un certificado es el emisor (*issuer*) del siguiente.
- Aseguramiento que el uso específico del certificado es consistente con el uso propuesto para dicho certificado como se indica en el contenido del mismo.
- Aseguramiento que ninguno de los certificados incluidos en la ruta han sido revocados, ni han expirado.
- Aseguramiento que la EC emisora se encuentre contenida en la lista TSL; es decir, que sea una Entidad de Certificación acreditada por el INDECOPI, en su calidad de AAC.

Podría haber un retraso entre el tiempo en que un certificado es revocado y el tiempo en que, o bien la CRL es actualizada o bien el OCSPR es informado de dicha revocación. Como resultado, existe la posibilidad de que un tercero que confía (tercer usuario) pueda confiar en un certificado después de que ha sido revocado pero antes de que ocurriera la actualización de la CRL o la notificación al OCSPR. Algunos terceros que confían podrían ser afectados en este tipo de situaciones. Dos enfoques para evitar esto son:

- Mantener suspendido durante un lapso especificado de tiempo el procedimiento de verificación de la CRL. Según el documento del APEC⁹, el tiempo máximo que debe existir entre la notificación de la solicitud de revocación de certificado y emitir una CRL que incluya dicho certificado como revocado es de 24 horas. Este acercamiento puede prevenir el que se acepte una firma inválida pero involucra retrasos en el procesamiento, lo que no es práctico en situaciones como la autenticación cercana al acceso en tiempo real de los sistemas o medios.
- Revisar las CRLs con posterioridad al tiempo máximo establecido –24 horas– para determinar si un certificado recientemente agregado a la CRL fue procesado luego de su revocación e identificar dichos certificados para un procesamiento especial. Esta aproximación puede contribuir a prevenir el que se acepten firmas inválidas pero con un tiempo posterior de 24 horas, facilita

⁸ La elección de la orientación de la cadena es discrecional. La cadena podría ser ordenada desde la entidad final hasta un punto de confianza. El orden no es importante siempre y cuando la ruta de procesamiento resultante sea la misma.

⁹ Guidelines for the Certificate Policy and Certificate Practices Framework for issuing certificates capable of being used Cross Jurisdiction e-Commerce.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

el descubrimiento de una firma con un certificado revocado, pero después de sucedido el hecho.

Los certificados tienen un tiempo de vida¹⁰. El período en que los certificados son válidos es determinado por el contenido en su campo de validez. Los certificados para usuarios generalmente tienen uno o tres años de tiempo de vida. Los certificados de la EC tienen un tiempo de vida más largo. El tiempo de vida de un certificado de EC tiene que abarcar el tiempo de vida de todos los certificados que ésta emite. Esta anidación de tiempos de vida de certificados es necesaria para el procesamiento de la ruta.

La vida limitada de los certificados puede impactar sobre algunas aplicaciones. Los certificados que pertenecen a ECs y a otras entidades expiran y tienen que ser reemplazados. Las ECs pueden tener múltiples certificados. La necesidad de anidar los tiempos de vida de certificados significa que las ECs no pueden emitir certificados cuando el período de validez de un nuevo certificado excede el período de validez de su propio certificado. Por ejemplo, si una EC tiene un certificado con tiempo de vida de cinco años y otorga certificados para usuarios con tiempos de vida máximos de tres años, la EC sólo puede usar su certificado para crear nuevos certificados de usuarios durante sus dos primeros años y así periódicamente. La EC debe obtener un nuevo certificado cuando ésta ya no pueda emitir nuevos certificados relativos a su antiguo certificado.

Las aplicaciones que procesan los certificados emitidos por una EC podrían tener que encontrar un certificado particular entre varios emitidos a una EC. Por ejemplo, considere el caso de dos usuarios que han recibido, por parte de la EC del ejemplo antes mencionado, certificados por un período de validez de tres años. Si los usuarios tramitaron sus certificados con una diferencia de más de dos años, la aplicación de software utilizará un certificado de EC diferente para verificar sus firmas digitales.

Tanto las entidades como los individuos que no son ECs también pueden tener múltiples certificados. Los individuos deben tener diferentes certificados para propósitos distintos: un certificado para firmar y/o autenticación, otro para cifrado, e incluso cada uno de estos podría ser para fines aún más específicos. Las aplicaciones deberán estar capacitadas para seleccionar un certificado apropiado desde los múltiples certificados existentes. Esta situación puede darse en aplicaciones que deben guardar información durante un largo período y deberían haber almacenado los resultados de la verificación de las firmas, el estado del certificado de la EC en la TSL, así como toda la cadena confiable de certificados que en su momento los validaron, pudiendo ser en el presente estos certificados ya expirados desde hace algún tiempo¹¹.

¹⁰ Las razones para limitar el tiempo de vida incluyen el control del tamaño de la CRL y el riesgo de que la clave privada pueda ser descubierta.

¹¹ La presunción aquí es que la información cifrada no tendrá que ser retenida por largos períodos o será cifrada nuevamente con una nueva clave debido al incremento de riesgos de que la clave del cifrado original sea descubierta.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

Cuando el periodo de vida de certificado esta pronto a expirar en un tiempo menor a un año, los suscriptores pueden solicitar el proceso de **re-emisión**. Este proceso implica la emisión de un certificado con un nuevo par de claves manteniendo los mismos datos correspondientes al certificado anterior, a excepción del número de serie, el periodo de validez y la clave pública.

Los suscriptores no deben usar la clave privada asociada con un certificado expirado para realizar firmas digitales y deben destruir la clave privada incluyendo cualquier copia. Aunque los terceros que confían en realidad no deben usar certificados expirados para verificar las firmas, pues el software de firma debe de almacenar (firmado digitalmente) los resultados del proceso de validación previo a la realización de la firma, durante la primera validación podrían necesitar los certificados para confirmar de manera independiente la verosimilitud (por ejemplo, reconfirmar) de las firmas verificadas previamente.

Los suscriptores deben mantener acceso a las claves privadas como requisito para descifrar cualquier información retenida en formato cifrado. Por ejemplo, el suscriptor podría necesitar la clave privada para descifrar y ver cualquier documento recibido previamente y aún mantenido en formato cifrado¹². La Tabla 3 resume el manejo de claves y certificados cuando los certificados expiran.

¹² La clave privada también puede ser necesitada para ver mensajes que el suscriptor envió cifrado, porque los clientes del correo a menudo mantienen los mensajes como texto cifrado en lugar de texto en claro por razones de seguridad. Efectivamente, los clientes incluyen al suscriptor como un destinatario para mensajes cifrados que el suscriptor envía.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

Tabla 3. Disposición de Clave y Certificado frente a la Expiración del Certificado.

Aplicación	Clave Privada	Clave Pública y Certificado
Firma Digital (Autenticación, integridad, no repudio)	Dstrucción, prevenir cualquier uso posterior	El cese en el uso de cualquier nueva firma. Retener para aplicaciones de no repudio tanto tiempo como se almacenen datos firmados, previamente verificados, y permanezcan sujetos a verificación. Se debe considerar la provisión de medidas para probar la recepción previa a la expiración del certificado (o revocación) y no modificaciones posteriores.
Cifrado (Confidencialidad)	Retener copia personal y de recuperación de datos de la clave, mientras se mantengan guardados los datos cifrados. Considerar el volver a cifrar con otra clave si el periodo de almacenamiento excede el tiempo de vida de la clave.	Dstrucción; cese del uso.

Dentro de la IOFE las ECs acreditadas pueden contar con políticas de recuperación de claves de descifrado (no está permitida la recuperación de claves para los certificados de firma digital ni autenticación) para asegurar que la información cifrada pueda recuperarse en casos legalmente establecidos y para la continuidad operacional. Los certificados utilizados para el cifrado no deben ser utilizados para los procesos de firma y/o autenticación, y viceversa.

Las aplicaciones de software en el curso de provisión de los servicios de seguridad a sus usuarios se sostienen en las necesidades tanto del suscriptor como del tercero que confía (tercer usuario). Las aplicaciones deben realizar las funciones descritas anteriormente como apropiadas en el dominio de la aplicación empleada.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ	Rev: 2016
		Aprobado:

3.0 DOCUMENTOS APLICABLES Y ALCANCES

Esta sección establece el contexto de los requisitos técnicos para habilitar aplicaciones dentro del marco de la IOFE. Las aplicaciones deben cumplir y deben ser consistentes con la política global de la IOFE para los niveles de aseguramiento de las aplicaciones y el uso de la PKI. Las siguientes subsecciones identifican los documentos que proporcionan la política y los requerimientos técnicos de las aplicaciones y los tipos de aplicaciones que pueden usar la PKI de la IOFE.

3.1 Documentos Aplicables

En esta subsección se referencian las normas y estándares que proveen una política global y guía para el desarrollo de aplicaciones en la IOFE. Los desarrolladores de aplicaciones deben cumplir tanto con los requisitos de estas referencias, así como los señalados en el presente documento. El acrónimo dentro de los corchetes - [] - que aparece antes de que cada referencia se usará en el resto del documento para referirse al correspondiente documento aplicable al que se asocia:

[Ley 27269 y anexos]	Ley de Firmas y Certificados Digitales, su Reglamento y Disposiciones Complementarias
[APEC]	Guidelines for the Certificate Policy and Certificate Practices Framework for issuing certificates capable of being used in Cross Jurisdiction e-Commerce
[DS NRO. 052-2008]	Reglamento de la Ley 27269, Ley de Firmas y Certificados Digitales
[DS NRO. 070-2011]	Decreto Supremo que modifica el Reglamento de la Ley 27269 y establece normas aplicables al Procedimiento Registral en virtud del Decreto Legislativo N° 681 y ampliatorias.
[DS NRO. 105-2012]	Decreto Supremo que establece disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo N° 052-2008-PCM.
[ETSI TS102.231]	Electronic Signatures and Infrastructures (ESI); Provision of Harmonized Trust service Provider Satus Information
[ETSI TS101 733]	Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures
[ETSI TS101 903]	Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures

[ETSI TS102 778 1]	Electronic Signatures and Infraestructures (ESI); PDF Advanced Electronic Signatures
[RFC 3161]	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
[RFC 5280]	Certificate and Certificate Revocation List (CRL) Profile
[RFC 5560]	Online Certificate Status Protocol - OCSP
[FIPS 140-2]	Security Requirements for Cryptographic Modules
[Common Criteria EAL4+]	Information Technology Security Evaluation

3.2 Niveles de Seguridad de PKI

El nivel de seguridad asociado con un certificado de clave pública es una aseveración por parte de una EC 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, por lo que definen múltiples niveles de seguridad.

Es de conocimiento general que no basta un único nivel de seguridad para todas las aplicaciones de PKI. Algunas aplicaciones que son menos críticas o que implican alguna transacción de bajo valor monetario pueden resistir un riesgo mayor comparado con otras aplicaciones que requieren de un mayor nivel de seguridad.

La PKI de la IOFE recoge estas tendencias y presenta los niveles de seguridad Medio, Medio Alto y Alto, descritos en el siguiente cuadro:

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.

Requerimientos de acreditación	Auditoría por parte de la AAC	<ul style="list-style-type: none"> - CMMI nivel 1 (mínimo), ISO 9001 u otra certificación ISO referida a la calidad en el Ciclo de Vida del Desarrollo de Software. - Consulta de estado de revocación vía OCSP - Common Criteria EAL 1 	<ul style="list-style-type: none"> - CMMI nivel 2 (mínimo), ISO 9001 u otra certificación ISO referida a la calidad en el Ciclo de Vida del Desarrollo de Software. - Common Criteria EAL 2
---------------------------------------	-------------------------------	--	---

3.3 Lista de servicios de confianza – TSL

La TSL 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.

3.4 Clasificación de Aplicaciones

Las aplicaciones deben cumplir los requisitos expresados en el presente documento de acuerdo a su clasificación:

- Software de firma de usuario final
- Software de verificación por parte de agentes automatizados
- Software de firma por parte de agente automatizado

3.5 Clasificación de Requerimientos

Los requerimientos están clasificados de acuerdo a los siguientes objetivos de control:

- Verificación de estado de validez del certificado
- Controles de seguridad
- Algoritmos criptográficos
- Protección de integridad de la aplicación
- Datos de verificación de la firma digital

	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

3.6 Estructura de documento

- Aplicación: Tipo de aplicación correspondiente a la clasificación definida en la sección 6 del presente documento.
 - Clasificación del requerimiento: Tipo de requerimiento correspondiente a la clasificación definida en la sección 7 del presente documento.
 - Requerimiento: Objeto del requisito técnico que debe cumplir la aplicación.
 - Definición del concepto: Concepto técnico relacionado al requerimiento.
 - Importancia: Razón por la cual es importante el cumplimiento del requerimiento, en función de reducir las posibilidades de suplantación de identidad de los titulares de certificados, y colaborar con la interoperabilidad de las herramientas.
 - Objeto de evaluación: Detalle del requerimiento.
 - Ejemplo de evidencia: Tipos de evidencia que puede ser presentada por el solicitante de la acreditación para demostrar el cumplimiento del requerimiento.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

4.0 REQUERIMIENTOS

El solicitante debe identificar el tipo de software que desea presentar en el proceso de acreditación y de acuerdo a ello, determinar los requerimientos que son de cumplimiento obligatorio. Los requerimientos son expresados en los campos denominados Objeto de Evaluación, el resto de información expresada en el presente documento es solamente informativa. Todos los requerimientos son de cumplimiento obligatorio, solamente el punto que define la verificación de la confiabilidad de un certificado no es obligatorio por lo que no es etiquetado como requerimiento.

4.1 SOFTWARE DE FIRMA DIGITAL DE USUARIO FINAL

El software de firma digital de usuario final presenta las siguientes características:

- Es aquel que puede ser utilizado por una persona natural para realizar procesos de firma
- El usuario final utiliza su propio módulo criptográfico, por lo que no se encuentra dentro del alcance de la presente evaluación.
- Este tipo de aplicación puede ser instalada en los sistemas cliente, en sistemas Web, así como en modelos cliente – servidor.
- La infraestructura de servidores es propia de los usuarios de la aplicación por lo que no se encuentra dentro del alcance de esta evaluación.

VERIFICACIÓN DE ESTADO DE VALIDEZ DEL CERTIFICADO

Antes de realizar la firma de un documento o información, la aplicación de software deberá verificar el estado de validez del certificado mediante los siguientes requerimientos:

Requerimiento OPCIONAL (A petición del auditado): Verificación de la confiabilidad del certificado:

Definición del Concepto:

Puede decirse que un certificado digital es confiable si proviene de una Entidad de Certificación Raíz reconocida por la regulación de la IOFE, cuya clave privada no haya sido comprometida o mal utilizada para realizar transacciones dolosas.

Los mecanismos para validar si una Entidad de Certificación Raíz es confiable son:

- Consulta a la Lista de Servicios de Confianza (TSL) de la Autoridad Administrativa Competente ó
- Consulta manual, instalando los certificados en los repositorios de los sistemas operativos o navegadores de

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

los usuarios finales. En este último caso, la verificación se realiza contra el certificado raíz instalado.

La TSL es la lista administrada por el INDECOPI donde se encuentran listadas las Entidades de Certificación que han pasado por un proceso de acreditación bajo los requisitos descritos en la Guía de Acreditación de Entidades de Certificación. Estas entidades son auditadas de manera periódica y se reciben reportes en caso de vulnerabilidad o mal uso de sus servicios de certificación digital.

Estándares y marcos de referencia: Webtrust for Certificate Authorities, ETSI TS 101 456, ISO 21188:2006, ETSI TR 102 040.

Importancia: La verificación de la confiabilidad de un certificado permite al firmante determinar si la Entidad de Certificación Raíz se encuentra dentro del reconocimiento legal, y que su clave raíz no ha sido comprometida o mal utilizada para realizar transacciones dolosas.

Objeto de evaluación:

Verificación por TSL

- La aplicación deberá verificar la firma de la AAC en la TSL y corroborar que corresponde a la raíz de la AAC.
- La aplicación deberá verificar que la fecha de vigencia de la TSL no ha expirado.
- La aplicación deberá verificar que la clave pública de la EC raíz correspondiente al certificado que se desea utilizar para realizar la firma, se encuentra listado en la TSL.
- La descarga de la TSL puede ser periódica conforme a su periodo de vigencia

Ejemplo de evidencia:

El solicitante de la acreditación puede evidenciar el cumplimiento de este requisito, mostrando que la aplicación no permita realizar la firma con certificados que no se encuentran en la TSL, o en los repositorios de los sistemas operativos o navegadores reconocidos por la IOFE.

La firma de la TSL puede ser verificada direccionando la aplicación a una TSL falsa, e intentar firmar un certificado contenido en dicha TSL.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

4.1.1 Requerimiento 1: Verificación del estado de revocación

Definición del concepto:

Cuando la clave privada de un certificado es comprometida, es decir, se encuentra en poder de terceros no autorizados, el titular o suscriptor del certificado tiene la capacidad de cancelar el certificado digital de modo que nadie pueda utilizar su clave privada en su nombre. A este proceso de cancelación se le llama revocación.

Antes de firmar un documento es necesario verificar que el certificado empleado no se encuentre revocado, a fin de evitar casos de suplantación de identidad.

El proceso de verificación del estado de revocación de un certificado se puede realizar de dos modos:

- Mediante la consulta a la lista de revocación de certificados – CRL, emitida por la EC que emitió el certificado a consultar (RFC 5280)
- Mediante la consulta en línea al directorio de certificados, según el protocolo OCSP (RFC 2560)

La CRL es generada por la propia EC que emitió el certificado y se encuentra firmada por su certificado digital, por lo que puede verificarse su autenticidad e integridad. Asimismo, la CRL tiene un periodo de vigencia, y es necesario determinar si ha expirado para poder confiar que la información se encuentra actualizada. En este sentido, la CRL requiere de una actualización periódica conforme al periodo de vigencia establecido por cada Entidad de Certificación. Debido a este periodo de actualización se dice que existe un tiempo en el que no se puede evitar que ocurran actos de suplantación de identidad, el cual es el tiempo que dura la actualización de la CRL luego de haber sido reportado un caso de compromiso de una clave.

La consulta en línea OCSP permite consultar el estado del certificado en el directorio, tomando los datos en tiempo real sin depender de un periodo de actualización. Esta es considerada una solución de mayor seguridad, ya que el certificado puede ser verificado en el tiempo oportuno.

Estándares y marcos de referencia: RFC 5280, RFC 3647, RFC 2560

Importancia: La verificación de los estados de revocación de los certificados permite reducir los casos de suplantación de identidad protegiendo a los titulares y suscriptores.

Objeto de evaluación:

	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Verificación por consulta a la CRL

- La aplicación deberá poder realizar el proceso de consulta de CRL mediante protocolos HTTP, LDAP o HTTPS, según sea el caso.
- La aplicación deberá verificar que la CRL esté firmada por la EC autorizada para realizar su emisión.
- La aplicación deberá verificar que la CRL se encuentre vigente, es decir que no se haya cumplido su fecha de expiración
- Antes de realizar la firma de un documento o información, se debe realizar la consulta a la CRL respectiva para verificar que el certificado no se encuentre revocado
- Se debe verificar que cada uno de los certificados que formen parte de la cadena de certificación no se encuentren revocados.

Verificación por consulta OCSP

- La aplicación deberá realizar la verificación del estado de revocación de un certificado y su respectiva cadena de certificación realizando la consulta OCSP conforme al protocolo definido en la RFC 2560.

Ejemplo de evidencia:

Para evidenciar el cumplimiento de la consulta CRL, el solicitante puede presentar lo siguiente:

- El resultado fallido de un intento de firma utilizando un certificado revocado
- El resultado fallido de un intento de firma utilizando un certificado, cuya CRL no ha sido actualizada pese a que se encuentra conectada a Internet y que la publicación en el Punto de Distribución de la EC sí se encuentra actualizado.
- El resultado fallido de un intento de firma utilizando un certificado, cuya CRL no ha sido actualizada pese a que se encuentra conectada a Internet y que la publicación en el Punto de Distribución de la EC sí se encuentra actualizado.

Para evidenciar el cumplimiento de la consulta OCSP, el solicitante puede mostrar el resultado fallido de un intento de firma utilizando un certificado revocado cuyo punto de distribución esté direccionado a un servicio OCSP.

4.1.2 Requerimiento 2: Verificación de no expiración del certificado

Definición del concepto:

Los certificados tienen un tiempo de vigencia establecido por la EC que los emitió. Por lo general este tiempo es definido en función de la fortaleza de los algoritmos criptográficos empleados en la generación del certificado.

Un certificado cuyo periodo de vigencia haya expirado no debería poder ser utilizado para realizar firmas, ya que podría prestarse a actos de suplantación de identidad, para evitar esto las aplicaciones de software deben verificar que la fecha de expiración aún no se ha cumplido.

Estándares y marcos de referencia: RFC 5280

Importancia: La verificación de los estados de vigencia de un certificado permite reducir los casos de suplantación de identidad protegiendo a los titulares y suscriptores.

Objeto de evaluación:

- La aplicación deberá realizar la verificación del estado de no expiración de un certificado, y su respectiva cadena de certificación.

Ejemplo de evidencia:

Para evidenciar el cumplimiento de este requerimiento, el solicitante puede demostrar que su aplicación impide la realización de la firma digital con un certificado no vigente.

4.1.3 Requerimiento 3: Verificación del propósito

Definición del concepto:

La estructura o perfil del contenido del certificado está definida en la RFC 5280. Uno de los campos importantes que las aplicaciones de software deben reconocer es el campo Key Usage el cual define los propósitos o aplicabilidad que puede tener la clave privada de un certificado:

Propósito	Bit	Uso
DigitalSignature	0	Utilizado para verificar la firma digital en procesos de autenticación de entidades,

		autenticación de datos y de integridad.
NonRepudiation	1	Utilizado para proporcionar un servicio de no repudio que proteja la firma contra la denegación por parte del firmante.
KeyEncipherment	2	Utilizado para cifrar claves privadas o secretas, como por ejemplo las claves simétricas de los canales cifrados SSL.
DataEncipherment	3	Utilizado para cifrar datos
Key Agreement	4	Utilizado cuando la clave pública es requerida para el intercambio seguro de claves
KeyCertSign	5	Utilizado para verificar la firma en certificados
CRLsign	6	Utilizado para verificar la firma en listas de revocación
EncipherOnly	7	Junto con el bit KeyAgreement puede ser utilizado para cifrar datos mientras se realiza el acuerdo de clave.
DecipherOnly	8	Junto con el bit KeyAgreement puede ser utilizado para descifrar datos mientras se realiza el acuerdo de clave.

Estándares y marcos de referencia: RFC 5280

Importancia: La verificación del propósito del certificado permite que este no sea utilizado para un uso indebido.

Objeto de evaluación:

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- La aplicación deberá verificar que los bit Non Repudiation y/o DigitalSignature se encuentran activos cuando se realiza el proceso de firma.

Ejemplo de evidencia:

Para evidenciar el cumplimiento de este requerimiento, el solicitante puede demostrar que su aplicación impide la realización de la firma digital con un certificado de propósito distinto a la firma digital.

CONTROLES DE SEGURIDAD

4.1.4 Requerimiento 4: Comprobaciones para aplicaciones Web:

Definición del concepto:

Las aplicaciones que remitan contenido al usuario para que éste lo firme haciendo uso del “cliente de firma” deben verificar la integridad de la firma realizada y que los datos firmados sean coincidentes con los remitidos originalmente para su firma.

De no realizarse esta verificación, un usuario malicioso podría reemplazar los datos a firmar por otros distintos, y remitir el resultado de la firma de los datos alterados. La aplicación que no realizara la comprobación, aceptaría la firma en una situación en la cual no podría garantizarse el no repudio por parte del usuario final ya que lo firmado no coincide con lo establecido por la aplicación.

Estándares y marcos de referencia: OWASP Top Ten, OWASP Testing Project.

Importancia: La comprobación de la firma luego de ser efectuada limita los casos de suplantación de datos a firmar.

Objeto de evaluación:

Los procesos de firma electrónica realizados en el equipo cliente del usuario de la aplicación, con el cliente de firma, deben ser validados en el servidor una vez que recibe el resultado de la firma, para verificar la validez del certificado electrónico empleado y que los datos firmados son coincidentes con los remitidos por la aplicación.

4.1.5 Requerimiento 5: Las funciones criptográficas deben realizarse en el módulo criptográfico

Definición del concepto:

El proceso de firma digital se compone principalmente de dos etapas:

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- La generación del resumen característico del documento a firmar, realizado mediante un algoritmo HASH
- El cifrado del resumen usando la clave privada del suscriptor

La función de cifrado de la clave privada debe realizarse en el módulo criptográfico certificado del suscriptor y no en las librerías criptográficas de la aplicación. Esto es necesario para garantizar que nunca la clave privada es copiada en el computador, sino que se mantiene protegida en el módulo criptográfico.

Estándares y marcos de referencia: FIPS 140-2, Common Criteria EAL 4+

Importancia: La protección de la clave privada es la base para evitar la suplantación de identidad de los suscriptores y titulares.

Objeto de evaluación:

- En caso que la aplicación firme los documentos recibidos, la función de firma con la clave privada debe realizarse solamente en el módulo criptográfico certificado y no en las librerías criptográficas de la aplicación.
- No deben generarse copias automatizadas de la clave privada en el computador durante el proceso de firma.
- En caso que el módulo criptográfico sea parte de la solución a acreditar, el módulo utilizado debe cumplir con la certificación FIPS 140 -2 o Common Criteria EAL 4+
- En caso que la clave privada sea parte de la solución a acreditar, desde su generación, el acceso a la clave privada de firma debe ser protegido por al menos dos personas a la vez.
- En caso que la clave privada sea parte de la solución a acreditar, desde su generación, el acceso a las copias de la clave privada deben ser protegidas por al menos dos personas por vez.
- En caso que la clave privada sea parte de la solución a acreditar, la importación y exportación de claves debe realizarse con la clave privada cifrada, por una clave protegida por dos personas a la vez.
- En caso que la clave privada sea parte de la solución a acreditar, deben generarse registros de auditoría de la generación, exportación, transporte, revocación, expiración y eliminación de la clave privada de firma.
- En caso que la clave privada sea parte de la solución a acreditar, el módulo criptográfico debe ser protegido contra acceso físico

no autorizado, mediante un control de al menos dos personas. Todos los movimientos del módulo criptográfico deben ser registrados y su administración debe ser asignada a roles específicos bajo responsabilidad contractual.

- En caso que la clave privada sea parte de la solución a acreditar, todos los movimientos de los respaldos de las claves deben ser registrados (por ejemplo, mediante actas firmadas y dispositivos biométricos y cámaras) y su administración debe ser asignada a roles específicos bajo responsabilidad contractual.
- En caso que la clave privada sea parte de la solución a acreditar, la petición para la instalación del certificado debe ser conforme al estándar PKCS #10.
- En caso que la clave privada sea parte de la solución a acreditar, en caso de compromiso se deberá solicitar la revocación inmediata del certificado.

ALGORITMOS CRIPTOGRÁFICOS

4.1.6 Requerimiento 6: No se deben utilizar funciones criptográficas obsoletas

Definición del concepto:

Conforme transcurre el tiempo, se encuentran vulnerabilidades a las funciones criptográficas que hacen que puedan ser manipuladas por atacantes malicioso para actos de suplantación de identidad, tal es el caso del algoritmo HASH MD5, SHA-1 y las claves RSA 1024. A estas funciones se les denomina funciones criptográficas obsoletas.

Estándares y marcos de referencia: ETSI TS 102 176

Importancia: El uso de funciones criptográficas obsoletas favorece los casos de suplantación de identidad, por lo tanto en caso se utilice los algoritmos SHA; se recomienda sean a partir del SHA-2.

Objeto de evaluación:

La aplicación debe utilizar algoritmos criptográficos vigentes, no vulnerados o no obsoletos:

- La lista de estándares criptográficos recomendados se lista en el anexo 1.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

PROTECCIÓN DE INTEGRIDAD DE LA APLICACIÓN

4.1.7 Requerimiento 7: Se debe proteger la autenticidad del código de firma

Definición del concepto:

Para ser diferenciadas de código malicioso, los sistemas operativos verifican la autenticidad de la aplicación mediante la firma digital del archivo ejecutable o el instalador. Esta firma debe ser realizada utilizando un certificado digital de firma de código, apropiado para el entorno en el que se instalará la aplicación.

Importancia: La firma de código permite diferenciar las aplicaciones seguras de las aplicaciones maliciosas.

Objeto de evaluación:

La autenticidad de la aplicación debe estar protegida por firma digital mediante un certificado de firma de código, emitido por una Entidad de Certificación reconocida por los sistemas operativos, plataformas de desarrollo y proveedores de red móvil.

Ejemplo de evidencia:

Los registros de instalación permiten observar la firma y el certificado digital utilizado.

DATOS DE VERIFICACIÓN DE LA FIRMA DIGITAL

4.1.8 Requerimiento 8: Se debe proporcionar el visor para la verificación de la firma

Definición del concepto:

Luego de ser firmado el documento, este debe poder ser verificado por cualquier tercero que requiera confiar en la firma. Las aplicaciones de firma digital deben brindar al firmante y al receptor visores para verificar el estado de integridad del documento firmado, la fecha de realización de la firma, la clave pública y los datos contenidos en el certificado.

Importancia: Los visores permiten verificar si un documento ha sido modificado o si se mantiene íntegro. Asimismo, permiten verificar si un documento fue firmado antes de que un certificado haya expirado o haya sido revocado.

Objeto de evaluación:

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Las aplicaciones de firma digital deben brindar al firmante y al receptor visores para verificar el estado de integridad del documento firmado, la fecha de realización de la firma, la clave pública y los datos contenidos en el certificado.

Ejemplo de evidencia:

Estos datos se pueden observar en los formatos de verificación de la firma.

4.1.9 Requerimiento 9: Se deben generar registros de validación de la firma

Definición del concepto:

Los documentos firmados digitalmente deben poder ser verificados a lo largo del tiempo, incluso luego de la expiración o revocación de un certificado. Para ello, es necesario guardar datos que permitan recuperar el estado de validez del certificado en el momento en el que se realizó la firma.

Estándares y marcos de referencia: ETSI TS 102 778 -1, XADES: ETSI TS 101 903, CADES: ETSI TS 101 733.

Importancia: Los documentos firmados podrán ser protegidos por la firma digital a lo largo del tiempo, incluso luego de haber sido expirado o revocado el certificado.

Objeto de evaluación:

La aplicación debe adjuntar a la firma los siguientes datos de verificación de la firma, los cuales deben ser protegidos por la firma del suscriptor:

- Fecha y hora de realizada la firma
- Clave pública de los certificados de la cadena de certificación
- Como equivalencia funcional a este requerimiento se reconocen los estándares:
 - PADES: ETSI TS 102 778 -1 desde el nivel de equivalencia a CAdES-EPES.
 - XADES: ETSI TS 101 903 desde el nivel de equivalencia a CAdES-EPES.
 - CADES: ETSI TS 101 733 desde el nivel CAdES-EPES.

Ejemplo de evidencia:

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Estos datos se pueden observar en los formatos de generación de la firma.

4.1.10 Requerimiento 10: Se deben implementar los manuales de administración y usuario

Definición del concepto:

Las aplicaciones deben ser respaldadas por documentos que sirvan de guía para su adecuada configuración, administración y uso.

Importancia: Los manuales de usuario y administración sirven de guía a los usuarios para realizar la administración y uso adecuado de las herramientas de firma digital.

Objeto de evaluación:

Se deben implementar manuales de administración y usuario e incluir la siguiente información:

- Políticas o requerimientos de seguridad, respecto de la configuración y uso del software.
- Capacidades de configuración en los manuales de administración y de usuario.
- En caso que la aplicación a evaluar sea una librería criptográfica, se deberá presentar la información referida al "manual de programador" o información sobre el funcionamiento y configuración adecuada de la librería.

Ejemplo de evidencia:

Presentar los manuales de usuario y administración.

4.2 SOFTWARE DE FIRMA POR PARTE DE AGENTES AUTOMATIZADOS

El software de firma por parte de agentes automatizados presenta las siguientes características:

- Es aquel que puede ser utilizado por una persona jurídica para realizar procesos automatizados de firma desatendida

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- La firma es realizada por una sola clave privada administrada por el agente automatizado
- La persona jurídica provee el módulo criptográfico, por lo que sí se encuentra dentro del alcance de la acreditación

VERIFICACIÓN DE ESTADO DE VALIDEZ DEL CERTIFICADO

Antes de realizar la firma de un documento o información, la aplicación de software deberá verificar el estado de validez del certificado mediante los siguientes requerimientos:

Requerimiento OPCIONAL (A petición del auditado): Verificación de la confiabilidad del certificado:

Definición del Concepto:

Puede decirse que un certificado digital es confiable si proviene de una Entidad de Certificación Raíz reconocida por la regulación de la IOFE, cuya clave privada no haya sido comprometida o mal utilizada para realizar transacciones dolosas.

Los mecanismos para validar si una Entidad de Certificación Raíz es confiable son:

- Consulta a la Lista de Servicios de Confianza (TSL) de la Autoridad Administrativa Competente ó
- Consulta manual, instalando los certificados en los repositorios de los sistemas operativos o navegadores de los usuarios finales. En este último caso, la verificación se realiza contra el certificado raíz instalado.

La TSL es la lista administrada por el INDECOPI donde se encuentran listadas las Entidades de Certificación que han pasado por un proceso de acreditación bajo los requisitos descritos en la Guía de Acreditación de Entidades de Certificación. Estas entidades son auditadas de manera periódica y se reciben reportes en caso de vulnerabilidad o mal uso de sus servicios de certificación digital.

Estándares y marcos de referencia: Webtrust for Certificate Authorities, ETSI TS 101 456, ISO 21188:2006, ETSI TR 102 040

Importancia: La verificación de la confiabilidad de un certificado permite al firmante determinar si la Entidad de Certificación Raíz se encuentra dentro del reconocimiento legal, y que su clave raíz no ha sido comprometida o mal utilizada para realizar transacciones dolosas.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Objeto de evaluación:

Verificación por TSL

- La aplicación deberá verificar la firma de la AAC en la TSL y corroborar que corresponde a la raíz de la AAC.
- La aplicación deberá verificar que la fecha de vigencia de la TSL no ha expirado.
- La aplicación deberá verificar que la clave pública de la EC raíz correspondiente al certificado que se desea utilizar para realizar la firma, se encuentra listado en la TSL.
- La descarga de la TSL puede ser periódica conforme a su periodo de vigencia

Ejemplo de evidencia:

El solicitante de la acreditación puede evidenciar el cumplimiento de este requisito, mostrando que la aplicación no permita realizar la firma con certificados que no se encuentran en la TSL, o en los repositorios de los sistemas operativos o navegadores reconocidos por la IOFE.

La firma de la TSL puede ser verificada direccionando la aplicación a una TSL falsa, e intentar firmar un certificado contenido en dicha TSL.

4.2.1 Requerimiento 11: Verificación del estado de revocación

Definición del concepto:

Cuando la clave privada de un certificado es comprometida, es decir, se encuentra en poder de terceros no autorizados, el titular o suscriptor del certificado tiene la capacidad de cancelar el certificado digital de modo que nadie pueda utilizar su clave privada en su nombre. A este proceso de cancelación se le llama revocación.

Antes de firmar un documento es necesario verificar que el certificado empleado no se encuentre revocado, a fin de evitar casos de suplantación de identidad.

El proceso de verificación del estado de revocación de un certificado se puede realizar de dos modos:

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- Mediante la consulta a la lista de revocación de certificados – CRL, emitida por la EC que emitió el certificado a consultar (RFC 5280)
- Mediante la consulta en línea al directorio de certificados, según el protocolo OCSP (RFC 2560)

La CRL es generada por la propia EC que emitió el certificado y se encuentra firmada por su certificado digital, por lo que puede verificarse su autenticidad e integridad. Asimismo, la CRL tiene un periodo de vigencia, y es necesario determinar si ha expirado para poder confiar que la información se encuentra actualizada. En este sentido, la CRL requiere de una actualización periódica conforme al periodo de vigencia establecido por cada Entidad de Certificación. Debido a este periodo de actualización se dice que existe un tiempo en el que no se puede evitar que ocurran actos de suplantación de identidad, el cual es el tiempo que dura la actualización de la CRL luego de haber sido reportado un caso de compromiso de una clave.

La consulta en línea OCSP permite consultar el estado del certificado en el directorio, tomando los datos en tiempo real sin depender de un periodo de actualización. Esta es considerada una solución de mayor seguridad, ya que el certificado puede ser verificado en el tiempo oportuno.

Estándares y marcos de referencia: RFC 5280, RFC 3647, RFC 2560

Importancia: La verificación de los estados de revocación de los certificados permite reducir los casos de suplantación de identidad protegiendo a los titulares y suscriptores.

Objeto de evaluación:

Verificación por consulta a la CRL

- La aplicación deberá poder realizar el proceso de consulta de CRL mediante protocolos HTTP, LDAP o HTTPS, según sea el caso.
- La aplicación deberá verificar que la CRL esté firmada por la EC autorizada para realizar su emisión.
- La aplicación deberá verificar que la CRL se encuentre vigente, es decir que no se haya cumplido su fecha de expiración
- Antes de realizar la firma de un documento o información, se debe realizar la consulta a la CRL respectiva para verificar que el certificado no se encuentre revocado
- Se debe verificar que cada uno de los certificados que formen parte de la cadena de certificación no se encuentren revocados.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Verificación por consulta OCSP

- La aplicación deberá realizar la verificación del estado de revocación de un certificado y su respectiva cadena de certificación realizando la consulta OCSP conforme al protocolo definido en la RFC 2560.

Ejemplo de evidencia:

Para evidenciar el cumplimiento de la consulta CRL, el solicitante puede presentar lo siguiente:

- El resultado fallido de un intento de firma utilizando un certificado revocado
- El resultado fallido de un intento de firma utilizando un certificado, cuya CRL no ha sido actualizada pese a que se encuentra conectada a Internet y que la publicación en el Punto de Distribución de la EC sí se encuentra actualizado.
- El resultado fallido de un intento de firma utilizando un certificado, cuya CRL no ha sido actualizada pese a que se encuentra conectada a Internet y que la publicación en el Punto de Distribución de la EC sí se encuentra actualizado.

Para evidenciar el cumplimiento de la consulta OCSP, el solicitante puede mostrar el resultado fallido de un intento de firma utilizando un certificado revocado cuyo punto de distribución esté direccionado a un servicio OCSP.

4.2.2 Requerimiento 12: Verificación de no expiración del certificado

Definición del concepto:

Los certificados tienen un tiempo de vigencia establecido por la EC que los emitió. Por lo general este tiempo es definido en función de la fortaleza de los algoritmos criptográficos empleados en la generación del certificado.

Un certificado cuyo periodo de vigencia haya expirado no debería poder ser utilizado para realizar firmas, ya que podría prestarse a actos de suplantación de identidad, para evitar esto las aplicaciones de software deben verificar que la fecha de expiración aún no se ha cumplido.

Estándares y marcos de referencia: RFC 5280

Importancia: La verificación de los estados de vigencia de un certificado permite reducir los casos de suplantación de identidad protegiendo a los titulares y suscriptores.

Objeto de evaluación:

- La aplicación deberá realizar la verificación del estado de no expiración de un certificado, y su respectiva cadena de certificación.

Ejemplo de evidencia:

Para evidenciar el cumplimiento de este requerimiento, el solicitante puede demostrar que su aplicación impide la realización de la firma digital con un certificado no vigente.

4.2.3 Requerimiento 13: Verificación del propósito

Definición del concepto:

La estructura o perfil del contenido del certificado está definida en la RFC 5280. Uno de los campos importantes que las aplicaciones de software deben reconocer es el campo Key Usage el cual define los propósitos o aplicabilidad que puede tener la clave privada de un certificado:

Propósito	Bit	Uso
DigitalSignature	0	Utilizado para verificar la firma digital en procesos de autenticación de entidades, autenticación de datos y de integridad.
NonRepudiation	1	Utilizado para proporcionar un servicio de no repudio que proteja la firma contra la denegación por parte del firmante.
KeyEncipherment	2	Utilizado para cifrar claves privadas o secretas, como por ejemplo las claves simétricas de los canales cifrados SSL.
DataEncipherment	3	Utilizado para cifrar datos

Key Agreement	4	Utilizado cuando la clave pública es requerida para el intercambio seguro de claves
KeyCertSign	5	Utilizado para verificar la firma en certificados
CRLsign	6	Utilizado para verificar la firma en listas de revocación
EncipherOnly	7	Junto con el bit KeyAgreement puede ser utilizado para cifrar datos mientras se realiza el acuerdo de clave.
DecipherOnly	8	Junto con el bit KeyAgreement puede ser utilizado para descifrar datos mientras se realiza el acuerdo de clave.

Estándares y marcos de referencia: RFC 5280

Importancia: La verificación del propósito del certificado permite que este no sea utilizado para un uso indebido.

Objeto de evaluación:

- La aplicación deberá verificar que los bit Non Repudiation y/o DigitalSignature se encuentran activos cuando se realiza el proceso de firma.

Ejemplo de evidencia:

Para evidenciar el cumplimiento de este requerimiento, el solicitante puede demostrar que su aplicación impide la realización de la firma digital con un certificado de propósito distinto a la firma digital.

CONTROLES DE SEGURIDAD

4.2.4 Requerimiento 14: Control de acceso a las funciones de administración y configuración.

Definición del concepto:

Las aplicaciones y los sistemas operativos que las soportan deben ser protegidos de acceso no autorizado y manipulación, en particular

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

respecto de las funciones de verificación, así como de la actualización de las Listas Raíces de Confianza.

Estándares y marcos de referencia: WebTrust for Certification Authorities, ISO 27002.

Importancia: La seguridad de la aplicación reduce la posibilidad de permitir el ingreso de documentos generados en actos de suplantación de identidad.

Objeto de evaluación:

- Las aplicaciones deben estar protegidos contra acceso no autorizado.
- Las funciones de verificación del estado de validez de los certificados deben estar siempre activadas a menos que exista un caso de contingencia y se haya operado conforme a un procedimiento aprobado por la AAC.
- Registros de auditoría de las firmas generadas, según el tipo de transacción.
- Los derechos de administración no debe permitir la generación de firmas fuera de la realización de la transacción definida para la firma desatendida.

4.2.5 Requerimiento 15: Las funciones criptográficas deben realizarse en el módulo criptográfico.

Definición del concepto:

El proceso de firma digital se compone principalmente de dos etapas:

- La generación del resumen característico del documento a firmar, realizado mediante un algoritmo HASH
- El cifrado del resumen usando la clave privada del suscriptor

La función de cifrado de la clave privada debe realizarse en el módulo criptográfico certificado del suscriptor y no en las librerías criptográficas de la aplicación. Esto es necesario para garantizar que nunca la clave privada es copiada en el computador, sino que se mantiene protegida en el módulo criptográfico.

Estándares y marcos de referencia: FIPS 140-2, Common Criteria EAL 4+

Importancia: La protección de la clave privada es la base para evitar la suplantación de identidad de los suscriptores y titulares.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Objeto de evaluación:

- En caso que la aplicación firme los documentos recibidos, la función de firma con la clave privada debe realizarse solamente en el módulo criptográfico certificado y no en las librerías criptográficas de la aplicación.
- No deben generarse copias automatizadas de la clave privada en el computador durante el proceso de firma.
- En caso que el módulo criptográfico sea parte de la solución a acreditar, el módulo utilizado debe cumplir con la certificación FIPS 140 -2 o Common Criteria EAL 4+
- En caso que la clave privada sea parte de la solución a acreditar, desde su generación, el acceso a la clave privada de firma debe ser protegido por al menos dos personas a la vez.
- En caso que la clave privada sea parte de la solución a acreditar, desde su generación, el acceso a las copias de la clave privada deben ser protegidas por al menos dos personas por vez.
- En caso que la clave privada sea parte de la solución a acreditar, la importación y exportación de claves debe realizarse con la clave privada cifrada, por una clave protegida por dos personas a la vez.
- En caso que la clave privada sea parte de la solución a acreditar, deben generarse registros de auditoría de la generación, exportación, transporte, revocación, expiración y eliminación de la clave privada de firma.
- En caso que la clave privada sea parte de la solución a acreditar, el módulo criptográfico debe ser protegido contra acceso físico no autorizado, mediante un control de al menos dos personas. Todos los movimientos del módulo criptográfico deben ser registrados y su administración debe ser asignada a roles específicos bajo responsabilidad contractual.
- En caso que la clave privada sea parte de la solución a acreditar, todos los movimientos de los respaldos de las claves deben ser registrados (por ejemplo, mediante actas firmadas y dispositivos biométricos y cámaras) y su administración debe ser asignada a roles específicos bajo responsabilidad contractual.
- En caso que la clave privada sea parte de la solución a acreditar, la petición para la instalación del certificado debe ser conforme al estándar PKCS #10.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- En caso que la clave privada sea parte de la solución a acreditar, en caso de compromiso se deberá solicitar la revocación inmediata del certificado.

ALGORITMOS CRIPTOGRÁFICOS

4.2.6 Requerimiento 16: No se deben utilizar funciones criptográficas obsoletas

Definición del concepto:

Conforme transcurre el tiempo, se encuentran vulnerabilidades a las funciones criptográficas que hacen que puedan ser manipuladas por atacantes malicioso para actos de suplantación de identidad, tal es el caso del algoritmo HASH MD5, SHA-1 y las claves RSA 1024. A estas funciones se les denomina funciones criptográficas obsoletas.

Estándares y marcos de referencia: ETSI TS 102 176

Importancia: El uso de funciones criptográficas obsoletas favorece los casos de suplantación de identidad, por lo tanto en caso se utilice los algoritmos SHA; se recomienda sean a partir del SHA-2.

Objeto de evaluación:

La aplicación debe utilizar algoritmos criptográficos vigentes, no vulnerados o no obsoletos:

- La lista de estándares criptográficos recomendados se lista en el anexo 1.

PROTECCIÓN DE INTEGRIDAD DE LA APLICACIÓN

4.2.7 Requerimiento 17: Se debe proteger la autenticidad del código de firma

Definición del concepto:

Para ser diferenciadas de código malicioso, los sistemas operativos verifican la autenticidad de la aplicación mediante la firma digital del archivo ejecutable o el instalador. Esta firma debe ser realizada utilizando un certificado digital de firma de código, apropiado para el entorno en el que se instalará la aplicación.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Importancia: La firma de código permite diferenciar las aplicaciones seguras de las aplicaciones maliciosas.

Objeto de evaluación:

La autenticidad de la aplicación debe estar protegida por firma digital mediante un certificado de firma de código, emitido por una Entidad de Certificación reconocida por los sistemas operativos, plataformas de desarrollo y proveedores de red móvil.

Ejemplo de evidencia:

Los registros de instalación permiten observar la firma y el certificado digital utilizado.

DATOS DE VERIFICACIÓN DE LA FIRMA DIGITAL

4.2.8 Requerimiento 18: Se debe proporcionar el visor para la verificación de la firma

Definición del concepto:

Luego de ser firmado el documento, este debe poder ser verificado por cualquier tercero que requiera confiar en la firma. Las aplicaciones de firma digital deben brindar al firmante y al receptor visores para verificar el estado de integridad del documento firmado, la fecha de realización de la firma, la clave pública y los datos contenidos en el certificado.

Importancia: Los visores permiten verificar si un documento ha sido modificado o si se mantiene íntegro. Asimismo, permiten verificar si un documento fue firmado antes de que un certificado haya expirado o haya sido revocado.

Objeto de evaluación:

Las aplicaciones de firma digital deben brindar al firmante y al receptor visores para verificar el estado de integridad del documento firmado, la fecha de realización de la firma, la clave pública y los datos contenidos en el certificado.

Ejemplo de evidencia:

Estos datos se pueden observar en los formatos de verificación de la firma.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

4.2.9 Requerimiento 19: Se deben generar registros de validación de la firma

Definición del concepto:

Los documentos firmados digitalmente deben poder ser verificados a lo largo del tiempo, incluso luego de la expiración o revocación de un certificado. Para ello, es necesario guardar datos que permitan recuperar el estado de validez del certificado en el momento en el que se realizó la firma.

Estándares y marcos de referencia: ETSI TS 102 778 -1, XADES: ETSI TS 101 903, CADES: ETSI TS 101 733

Importancia: Los documentos firmados podrán ser protegidos por la firma digital a lo largo del tiempo, incluso luego de haber sido expirado o revocado el certificado.

Objeto de evaluación:

La aplicación debe adjuntar a la firma los siguientes datos de verificación de la firma, los cuales deben ser protegidos por la firma del suscriptor:

- Fecha y hora de realizada la firma
- Clave pública de los certificados de la cadena de certificación
- Como equivalencia funcional a este requerimiento se reconocen los estándares:
 - PADES: ETSI TS 102 778 -1 desde el nivel de equivalencia a CAdES-EPES.
 - XADES: ETSI TS 101 903 desde el nivel de equivalencia a CAdES-EPES.
 - CADES: ETSI TS 101 733 desde el nivel CAdES-EPES.

Ejemplo de evidencia:

Estos datos se pueden observar en los formatos de generación de la firma.

4.2.10 Requerimiento 20: Se deben implementar los manuales de administración y usuario

Definición del concepto:

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Las aplicaciones deben ser respaldadas por documentos que sirvan de guía para su adecuada configuración, administración y uso.

Importancia: Los manuales de usuario y administración sirven de guía a los usuarios para realizar la administración y uso adecuado de las herramientas de firma digital.

Objeto de evaluación:

Se deben implementar manuales de administración y usuario e incluir la siguiente información:

- Políticas o requerimientos de seguridad, respecto de la configuración y uso del software.
- Capacidades de configuración en los manuales de administración y de usuario.
- En caso que la aplicación a evaluar sea una librería criptográfica, se deberá presentar la información referida al "manual de programador" o información sobre el funcionamiento y configuración adecuada de la librería.

Ejemplo de evidencia:

Presentar los manuales de usuario y administración.

4.3 SOFTWARE DE VERIFICACION POR PARTE DE AGENTES AUTOMATIZADOS

El software de verificación por parte de agentes automatizados presenta las siguientes características:

- Es aquel que recibe documentos electrónicos con firma digital y realiza las verificaciones de estado de validez del certificado de manera automatizada.
- Realiza la verificación de los certificados correspondientes a cada firma contenida en el documento recibido
- La verificación se realiza de manera automática sin intervención de administradores u operadores de la aplicación
- Existe un documento que evidencie un acuerdo o declaración previa, donde el solicitante de la acreditación declara el campo de usuarios de los cuales recibirá los documentos y las cláusulas de responsabilidad sobre la verificación de las firmas contenidas en los documentos.

VERIFICACIÓN DE ESTADO DE VALIDEZ DEL CERTIFICADO

	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Al recibir un documento firmado, la aplicación de software deberá verificar de manera automatizada el estado de validez de los certificados correspondientes a cada firma contenida en dicho documento, mediante los requerimientos listados a continuación, en caso de no ser válido alguno de los certificados, la aplicación deberá devolver un comunicado al emisor o emisores del documento:

Requerimiento OPCIONAL (A petición del auditado): Verificación de la confiabilidad del certificado:

Definición del Concepto:

Puede decirse que un certificado digital es confiable si proviene de una Entidad de Certificación Raíz reconocida por la regulación de la IOFE, cuya clave privada no haya sido comprometida o mal utilizada para realizar transacciones dolosas.

Los mecanismos para validar si una Entidad de Certificación Raíz es confiable son:

- Consulta a la Lista de Servicios de Confianza (TSL) de la Autoridad Administrativa Competente ó
- Consulta a los repositorios de los sistemas operativos y navegadores que administran certificados de Webtrust y sus equivalentes, debidamente reconocidos por la Autoridad Administrativa Competente.
- Consulta manual, instalando los certificados en los repositorios de los sistemas operativos o navegadores de los usuarios finales. En este último caso, la verificación se realiza contra el certificado raíz instalado.

La TSL es la lista administrada por el INDECOPI donde se encuentran listadas las Entidades de Certificación que han pasado por un proceso de acreditación bajo los requisitos descritos en la Guía de Acreditación de Entidades de Certificación. Estas entidades son auditadas de manera periódica y se reciben reportes en caso de vulnerabilidad o mal uso de sus servicios de certificación digital.

Los repositorios de Certificados Raíz de Confianza de los navegadores y sistemas operativos reconocidos por la IOFE, son aquellos que han sido generados por programas de certificación análogos a la IOFE y que cumplen con los siguientes requisitos:

- Mantener un programa de acreditación que exija el cumplimiento de los requerimientos del Estándar WebTrust, ETSI TS 101456, un estándar, regulación o auditoría que pueda evidenciar requerimientos equivalentes.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- Exigir evaluaciones realizadas por auditores licenciados por WebTrust o un organismo equivalente o gubernamental, independientes a la entidad auditada.
- Mantener una lista actualizada de Entidades Confiables en los sistemas operativos o navegadores de Internet.
- Mantener un canal de detección o atención de reportes de vulnerabilidades de seguridad informáticas que permita detectar los casos de compromiso o mal uso de las claves de las Entidades de Certificación.
- Emitir mensajes informativos a los usuarios cuando se estén utilizando certificados que no pertenecen a la Lista de Confianza.
- Contar con procedimientos de contingencia para el caso en el que el Estado peruano desee retirar o incluir una Entidad de Certificación Raíz de manera manual.
- Haber sido reconocido por la AAC .

Estándares y marcos de referencia: Webtrust for Certificate Authorities, ETSI TS 101 456, ISO 21188:2006, ETSI TR 102 040

Importancia: La verificación de la confiabilidad de un certificado permite al firmante determinar si la Entidad de Certificación Raíz se encuentra dentro del reconocimiento legal, y que su clave raíz no ha sido comprometida o mal utilizada para realizar transacciones dolosas.

Objeto de evaluación:

Verificación por TSL

- La aplicación deberá verificar la firma de la AAC en la TSL y corroborar que corresponde a la raíz de la AAC.
- La aplicación deberá verificar que la fecha de vigencia de la TSL no ha expirado.
- La aplicación deberá verificar que la clave pública de la EC raíz correspondiente al certificado que se desea utilizar para realizar la firma, se encuentra listado en la TSL.
- La descarga de la TSL puede ser periódica conforme a su periodo de vigencia

Verificación por repositorios reconocidos por la IOFE

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- La aplicación deberá verificar que la clave pública de la EC raíz correspondiente al certificado que se desea utilizar para realizar la firma, se encuentra listado en el repositorio reconocido por la AAC.
- La configuración del sistema debe permitir la actualización automática de la lista de Raíces de Confianza en los repositorios.

Ejemplo de evidencia:

El solicitante de la acreditación puede evidenciar el cumplimiento de este requisito, mostrando que la aplicación no permita realizar la firma con certificados que no se encuentran en la TSL, o en los repositorios de los sistemas operativos o navegadores reconocidos por la IOFE. La firma de la TSL puede ser verificada direccionando la aplicación a una TSL falsa, e intentar firmar un certificado contenido en dicha TSL.

4.3.1 Requerimiento 21: Verificación del estado de revocación

Definición del concepto:

Cuando la clave privada de un certificado es comprometida, es decir, se encuentra en poder de terceros no autorizados, el titular o suscriptor del certificado tiene la capacidad de cancelar el certificado digital de modo que nadie pueda utilizar su clave privada en su nombre. A este proceso de cancelación se le llama revocación.

Antes de firmar un documento es necesario verificar que el certificado empleado no se encuentre revocado, a fin de evitar casos de suplantación de identidad.

El proceso de verificación del estado de revocación de un certificado se puede realizar de dos modos:

- Mediante la consulta a la lista de revocación de certificados – CRL, emitida por la EC que emitió el certificado a consultar (RFC 5280)
- Mediante la consulta en línea al directorio de certificados, según el protocolo OCSP (RFC 2560)

La CRL es generada por la propia EC que emitió el certificado y se encuentra firmada por su certificado digital, por lo que puede verificarse su autenticidad e integridad. Asimismo, la CRL tiene un periodo de vigencia, y es necesario determinar si ha expirado para poder confiar que la información se encuentra actualizada. En este sentido, la CRL requiere de una actualización periódica conforme al periodo de vigencia

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

establecido por cada Entidad de Certificación. Debido a este periodo de actualización se dice que existe un tiempo en el que no se puede evitar que ocurran actos de suplantación de identidad, el cual es el tiempo que dura la actualización de la CRL luego de haber sido reportado un caso de compromiso de una clave.

La consulta en línea OCSP permite consultar el estado del certificado en el directorio, tomando los datos en tiempo real sin depender de un periodo de actualización. Esta es considerada una solución de mayor seguridad, ya que el certificado puede ser verificado en el tiempo oportuno.

Estándares y marcos de referencia: RFC 5280, RFC 3647, RFC 2560

Importancia: La verificación de los estados de revocación de los certificados permite reducir los casos de suplantación de identidad protegiendo a los titulares y suscriptores.

Objeto de evaluación:

Verificación por consulta a la CRL

- La aplicación deberá poder realizar el proceso de consulta de CRL mediante protocolos HTTP, LDAP o HTTPS, según sea el caso.
- La aplicación deberá verificar que la CRL esté firmada por la EC autorizada para realizar su emisión.
- La aplicación deberá verificar que la CRL se encuentre vigente, es decir que no se haya cumplido su fecha de expiración
- Antes de realizar la firma de un documento o información, se debe realizar la consulta a la CRL respectiva para verificar que el certificado no se encuentre revocado
- Se debe verificar que cada uno de los certificados que formen parte de la cadena de certificación no se encuentren revocados.

Verificación por consulta OCSP

- La aplicación deberá realizar la verificación del estado de revocación de un certificado y su respectiva cadena de certificación realizando la consulta OCSP conforme al protocolo definido en la RFC 2560.

Ejemplo de evidencia:

Para evidenciar el cumplimiento de la consulta CRL, el solicitante puede presentar lo siguiente:

- El resultado fallido de un intento de firma utilizando un certificado revocado

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- El resultado fallido de un intento de firma utilizando un certificado, cuya CRL se encuentra expirada
- El resultado fallido de un intento de firma utilizando un certificado, cuya CRL se encuentra modificada

Para evidenciar el cumplimiento de la consulta OCSP, el solicitante puede mostrar el resultado fallido de un intento de firma utilizando un certificado revocado cuyo punto de distribución esté direccionado a un servicio OCSP.

4.3.2 Requerimiento 22: Verificación de no expiración del certificado

Definición del concepto:

Los certificados tienen un tiempo de vigencia establecido por la EC que los emitió. Por lo general este tiempo es definido en función de la fortaleza de los algoritmos criptográficos empleados en la generación del certificado. El tiempo máximo de vigencia de un certificado a ser empleado por una persona natural, recomendado por la RFC 3647 es de 3 años, ya que se considera que luego de ese plazo podrían descubrirse vulnerabilidades a la tecnología que pueden ser empleadas para realizar actos de suplantación de identidad.

Un certificado cuyo periodo de vigencia haya expirado no debería poder ser utilizado para realizar firmas, ya que podría prestarse a actos de suplantación de identidad, para evitar esto las aplicaciones de software deben verificar que la fecha de expiración aún no se ha cumplido.

Estándares y marcos de referencia: RFC 5280

Importancia: La verificación de los estados de vigencia de un certificado permite reducir los casos de suplantación de identidad protegiendo a los titulares y suscriptores.

Objeto de evaluación:

- La aplicación deberá realizar la verificación del estado de no expiración de un certificado, y su respectiva cadena de certificación.

Ejemplo de evidencia:

Para evidenciar el cumplimiento de este requerimiento, el solicitante puede demostrar que su aplicación impide la realización de la firma digital con un certificado no vigente.

4.3.3 Requerimiento 23: Verificación del propósito

Definición del concepto:

La estructura o perfil del contenido del certificado está definida en la RFC 5280. Uno de los campos importantes que las aplicaciones de software deben reconocer es el campo Key Usage el cual define los propósitos o aplicabilidad que puede tener la clave privada de un certificado:

Propósito	Bit	Uso
DigitalSignature	0	Utilizado para verificar la firma digital en procesos de autenticación de entidades, autenticación de datos y de integridad.
NonRepudiation	1	Utilizado para proporcionar un servicio de no repudio que proteja la firma contra la denegación por parte del firmante.
KeyEncipherment	2	Utilizado para cifrar claves privadas o secretas, como por ejemplo las claves simétricas de los canales cifrados SSL.
DataEncipherment	3	Utilizado para cifrar datos
Key Agreement	4	Utilizado cuando la clave pública es requerida para el intercambio seguro de claves
KeyCertSign	5	Utilizado para verificar la firma en certificados
CRLsign	6	Utilizado para verificar la firma en listas de revocación
EncipherOnly	7	Junto con el bit KeyAgreement puede ser utilizado para cifrar

		datos mientras se realiza el acuerdo de clave.
DecipherOnly	8	Junto con el bit KeyAgreement puede ser utilizado para descifrar datos mientras se realiza el acuerdo de clave.

Estándares y marcos de referencia: RFC 5280

Importancia: La verificación del propósito del certificado permite que este no sea utilizado para un uso indebido.

Objeto de evaluación:

- La aplicación deberá verificar que los bit Non Repudiation del perfil de certificado se encuentran activos cuando se realiza el proceso de firma.

Ejemplo de evidencia:

Para evidenciar el cumplimiento de este requerimiento, el solicitante puede demostrar que su aplicación impide la realización de la firma digital con un certificado de propósito distinto a la firma digital.

CONROLES DE SEGURIDAD

4.3.4 Requerimiento 24: Control de acceso a las funciones de administración y configuración.

Definición del concepto:

Las aplicaciones y los sistemas operativos que las soportan deben ser protegidos de acceso no autorizado y manipulación, en particular respecto de las funciones de verificación, así como de la actualización de las Listas Raíces de Confianza.

Estándares y marcos de referencia: OWASP Top Ten, OWASP Testing Project.

Importancia: La seguridad de la aplicación reduce la posibilidad de permitir el ingreso de documentos generados en actos de suplantación de identidad.

Objeto de evaluación:

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- Las aplicaciones deben estar protegidos contra acceso no autorizado.
- Las funciones de verificación del estado de validez de los certificados deben estar siempre activadas a menos que exista un caso de contingencia y se haya operado conforme a un procedimiento aprobado por la AAC.
- Registros de auditoría de las firmas generadas, según el tipo de transacción.
- Los derechos de administración no debe permitir la generación de firmas fuera de la realización de la transacción definida para la firma desatendida.

4.3.5 Requerimiento 25: En caso que se firmen los documentos recibidos, las funciones criptográficas deben realizarse en el módulo criptográfico

Definición del concepto:

El proceso de firma digital se compone principalmente de dos etapas:

- La generación del resumen característico del documento a firmar, realizado mediante un algoritmo HASH
- El cifrado del resumen usando la clave privada del suscriptor

La función de cifrado de la clave privada debe realizarse en el módulo criptográfico certificado del suscriptor y no en las librerías criptográficas de la aplicación. Esto es necesario para garantizar que nunca la clave privada es copiada en el computador, sino que se mantiene protegida en el módulo criptográfico.

Estándares y marcos de referencia: FIPS 140-2, Common Criteria EAL 4+

Importancia: La protección de la clave privada es la base para evitar la suplantación de identidad de los suscriptores y titulares.

Objeto de evaluación:

- En caso que la aplicación firme los documentos recibidos, la función de firma con la clave privada debe realizarse solamente en el módulo criptográfico certificado y no en las librerías criptográficas de la aplicación.
- No deben generarse copias automatizadas de la clave privada en el computador durante el proceso de firma.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- En caso que el módulo criptográfico sea parte de la solución a acreditar, el módulo criptográfico utilizado debe cumplir con la certificación FIPS 140 -2 o Common Criteria EAL 4+
- En caso que el módulo criptográfico sea parte de la solución a acreditar, desde su generación, el acceso a la clave privada de firma debe ser protegido por al menos personas a la vez.
- En caso que el módulo criptográfico sea parte de la solución a acreditar, el acceso a las copias de la clave privada deben ser protegidas por al menos dos personas por vez.
- En caso que el módulo criptográfico sea parte de la solución a acreditar, la importación y exportación de claves debe realizarse con la clave privada cifrada, por una clave protegida por dos personas a la vez
- En caso que el módulo criptográfico sea parte de la solución a acreditar, deben generarse registros de auditoría de la generación, exportación, transporte, revocación, expiración y eliminación de la clave privada de firma.
- En caso que el módulo criptográfico sea parte de la solución a acreditar, el módulo criptográfico debe ser protegido contra acceso físico no autorizado, mediante un control de al menos dos personas. Todos los movimientos del módulo criptográfico deben ser registrados y su administración debe ser asignada a roles específicos bajo responsabilidad contractual
- En caso que el módulo criptográfico sea parte de la solución a acreditar, todos los movimientos de los respaldos de las claves deben ser registrados (por ejemplo, mediante actas firmadas y dispositivos biométricos y cámaras) y su administración debe ser asignada a roles específicos bajo responsabilidad contractual
- En caso que el módulo criptográfico sea parte de la solución a acreditar, la petición para la instalación del certificado debe ser conforme al estándar PKCS #10
- En caso que el módulo criptográfico sea parte de la solución a acreditar, en caso de compromiso se deberá solicitar la revocación inmediata del certificado.

ALGORITMOS CRIPTOGRÁFICOS

4.3.6 Requerimiento 26: No se deben utilizar funciones criptográficas obsoletas

Definición del concepto:

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Conforme transcurre el tiempo, se encuentran vulnerabilidades a las funciones criptográficas que hacen que puedan ser manipuladas por atacantes malicioso para actos de suplantación de identidad, tal es el caso del algoritmo HASH MD5, SHA-1 y las claves RSA 1024. A estas funciones se les denomina funciones criptográficas obsoletas.

Estándares y marcos de referencia: ETSI TS 102 176 -1

Importancia: El uso de funciones criptográficas obsoletas favorece los casos de suplantación de identidad, por lo tanto en caso se utilice los algoritmos SHA; se recomienda sean a partir del SHA-2.

Objeto de evaluación:

La aplicación debe utilizar algoritmos criptográficos vigentes, no vulnerados o no obsoletos:

- La lista de estándares criptográficos recomendados se lista en el anexo 1.

PROTECCIÓN DE INTEGRIDAD DE LA APLICACIÓN

4.3.7 Requerimiento 27: Se debe proteger la autenticidad del código de firma

Definición del concepto:

Para ser diferenciadas de código malicioso, los sistemas operativos verifican la autenticidad de la aplicación mediante la firma digital del archivo ejecutable o el instalador. Esta firma debe ser realizada utilizando un certificado digital de firma de código, apropiado para el entorno en el que se instalará la aplicación.

Importancia: La firma de código permite diferenciar las aplicaciones seguras de las aplicaciones maliciosas.

Objeto de evaluación:

La autenticidad de la aplicación debe estar protegida por firma digital mediante un certificado de firma de código, emitido por una Entidad de Certificación reconocida por los sistemas operativos, plataformas de desarrollo y proveedores de red móvil.

Ejemplo de evidencia:

Los registros de instalación permiten observar la firma y el certificado digital utilizado.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

DATOS DE VERIFICACIÓN DE LA FIRMA DIGITAL

4.3.8 Requerimiento 28: En caso que el sistema automatizado realice la firma digital del documento recibido, se debe proporcionar un visor para verificar la firma del documento

Definición del concepto:

Luego de ser firmado el documento, este debe poder ser verificado por cualquier tercero que requiera confiar en las firmas realizadas.

Importancia: Los visores y las firmas permiten verificar si un documento ha sido aprobado luego de realizadas las tareas de verificación, si ha sido modificado o si se mantiene íntegro. Asimismo, permiten verificar si un documento era válido antes de que un certificado haya expirado o haya sido revocado.

Objeto de evaluación:

En caso que la aplicación realice la firma digital de documentos firmados, se debe brindar de ser aplicable, a los terceros que confían, visores para verificar el estado de aprobación de los documentos, la integridad del documento firmado, la fecha de realización de la verificación, las claves públicas y los datos contenidos en los certificados, o firmar los documentos recibidos en un formato estándar aprobado por la AAC, que pueda ser verificado por los terceros que confían.

4.3.9 Requerimiento 29: En caso de firmar los documentos recibidos, se deben generar registros de validación de la firma

Definición del concepto:

Los documentos firmados digitalmente deben poder ser verificados a lo largo del tiempo, incluso luego de la expiración o revocación de un certificado. Para ello, es necesario guardar datos que permitan recuperar el estado de validez del certificado en el momento en el que se realizó la firma.

Estándares y marcos de referencia: ETSI TS 102 778 -1, XADES:
ETSI TS 101 903, CADES: ETSI TS 101 733

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Importancia: Los documentos firmados podrán ser protegidos por la firma digital a lo largo del tiempo, incluso luego de haber sido expirado o revocado el certificado.

Objeto de evaluación:

La aplicación debe adjuntar a la firma los siguientes datos de verificación de la firma, los cuales deben ser protegidos por la firma del suscriptor:

- Fecha y hora de realizada la firma
- Clave pública de los certificados de la cadena de certificación
- Una referencia al estado de no revocación de la cadena de certificación
- Como equivalencia funcional a este requerimiento se reconocen los estándares:
 - PADES: ETSI TS 102 778 -1
 - XADES: ETSI TS 101 903
 - CADES: ETSI TS 101 733 en su equivalencia al nivel CADES.EPES.

Ejemplo de evidencia:

Estos datos se pueden observar en los formatos de generación de la firma.

4.3.10 Requerimiento 30: Se deben implementar los manuales de administración y usuario

Definición del concepto:

Las aplicaciones deben ser respaldadas por documentos que sirvan de guía para su adecuada configuración, administración y uso.

Importancia: Los manuales de usuario y administración sirven de guía a los usuarios para realizar la administración y uso adecuado de las herramientas de firma digital.

Objeto de evaluación:

Se deben implementar manuales de administración y usuario e incluir la siguiente información:

- Políticas seguridad, respecto de la configuración y uso del software.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

- Capacidades de configuración en los manuales de administración y de usuario.

Ejemplo de evidencia:

Presentar los manuales se de usuario y administración.

4.4 FUNCIONALIDAD DE SOLICITUD DE SELLOS DE TIEMPO

4.4.1 Requerimiento 30: Verificación de sello de tiempo

Definición del concepto:

A fin de asegurar que las transacciones de sello de tiempo son correctas y auténticas, las aplicaciones de software deben verificar la confiabilidad de su procedencia, es decir verificar que el sello de tiempo corresponde a la Autoridad solicitada y que el certificado digital empleado para firmar los sellos de tiempo, no se encuentra expirado o revocado.

Estándares y marcos de referencia: RFC 3161

Importancia: La verificación de los sellos de tiempo evita la suplantación de los mismos.

Objeto de evaluación:

Conforme a la RFC 3161, la aplicación de software que realiza solicitudes de sello de tiempo debe realizar lo siguiente:

- Verificar que el sello de tiempo contiene el identificador del certificado de la Autoridad de Sello de tiempo que fue consultada
- Verificar la firma del sello de tiempo para corroborar que los datos son íntegros.
- Verificar que el certificado de la Autoridad de sello de tiempo no ha sido revocado
- Verificar que la vigencia del certificado de la Autoridad de sello de tiempo no ha expirado.

5.0 CONFIGURACIÓN DE SEGURIDAD

En caso que la aplicación requiera una determinada configuración para cumplir con todos los requerimientos expresados en el presente documento, el solicitante de la aplicación deberá comunicar por un medio masivo, a todos los

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

usuarios de su aplicación de ámbito nacional, los detalles y procedimiento de la configuración que debe implementarse.

Los usuarios de las aplicaciones serán responsables de ejecutar y actualizar la referida configuración.

6.0 PROCEDIMIENTOS DE EVALUACIÓN

Las evaluaciones deberán seguir el siguiente procedimiento:

1. Luego de haber sido seleccionado el auditor, este deberá proporcionar al auditado una lista de requerimientos, conforme a los objetos de evaluación del presente documento según el tipo de software que será evaluado.
2. El auditado deberá sustentar el alcance de la acreditación, y justificar la no aplicabilidad del documento en caso existiera.
3. La sesión de auditoría deberá realizarse en presencia del auditor y el auditado, el cual deberá presentar todas las evidencias correspondientes a cada objeto de evaluación correspondiente a su tipo de aplicación.
4. El auditor presentará un informe al auditado y a la CNB respecto de la evaluación realizada, el cual deberá contener las observaciones encontradas o recomendaciones. Ninguna recomendación será de cumplimiento obligatorio.
5. El auditor expondrá las evidencias a la CNB para su revisión.
6. En caso de ser aprobado por la CNB el logro de la acreditación, el auditado expondrá las funciones de su aplicación acreditada ante los Comisionados de la CNB antes de ser emitida la Resolución de Acreditación
7. De estar conformes, los Comisionados emitirán la Resolución de Acreditación.

6.1 PROCEDIMIENTO DE LA EVALUACION 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.

Las evaluaciones serán realizadas en ambientes de producción reales donde hayan sido implantados. La selección de estos ambientes será a criterio de la Autoridad Administrativa Competente.

	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

6.1.1 Paso 1: Notificación

Se 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.

6.1.2 Paso 2: Evaluación

El PSC tendrá un plazo de 30 días para tramitar la evaluación por parte de un auditor independiente seleccionado 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 confianza del certificado antes de permitir la firma
- La verificación del estado de no revocación del certificado antes de permitir la firma
- La verificación de no expiración del certificado antes de permitir la firma.

6.1.3 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 1 año.
- Una investigación para determinar el impacto del incumplimiento sobre los suscriptores y terceros que confían.
- La suspensión del estado de acreditación será levantada al finalizar el plazo establecido y luego de ser efectuada una nueva evaluación que incluya la verificación de la subsanación del incumplimiento.
- Otras medidas que determine la AAC.

6.2 PROCEDIMIENTO DE LA 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 del estado de acreditación.

6.2.1 Paso 1: Solicitud

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

	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

6.2.2 Paso 2: Evaluación

El PSC tendrá un plazo de 60 días para tramitar la evaluación por parte de un auditor independiente seleccionado por el INDECOPI.

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

6.2.3 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.

6.3 RESPONSABILIDAD EN CASOS DE INCUMPLIMIENTO

Es responsabilidad de los acreditados mantener el cumplimiento de los requerimientos expresados en el presente documento, conforme al alcance declarado en la acreditación y cualquier incumplimiento que permita el uso indebido de las claves privadas, ameritará una sanción a favor de los usuarios de las herramientas.

Luego de haber sido acreditada una aplicación, en caso de ser detectado o denunciado el incumplimiento de alguno de estos requerimientos, el INDECOPI procederá a levantar el estado de acreditación y asimismo establecerá la sanción pertinente a favor de los afectados.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

**ANEXO A:
ESTÁNDARES RECONOCIDOS (*)**

Estándar	Propósito
EC/PKI	
RFC 3280, RFC 3279	Certificados de firma
RFC 5280, RFC 3279, RFC 4325, RFC 4630, RFC 4055, RFC 4491, RFC 5480, RFC 5758	Lista de Certificados Revocados
RFC 2560	Respuesta OCSP
RFC 3280, RFC 3279	Certificados de Entidad de Certificación
RFC 3161, TS 101 861	Peticiones de Sellos de tiempo
RFC 3161, TS 101 861, RFC 5816	Certificados de Unidades de Sellado de tiempo
RFC 3280, RFC 3279	Certificados auto-firmados para certificados de TSU (unidades de sellado de tiempo)
RFC 3280, RFC 3279	Certificado de atributos
RFC 3281	Certificado de autoridad de atributos
SHA 224 SHA 384 SHA 512 SHA 256	Algoritmos de resumen, para la identificación de documentos firmados.
RSA 2048, RSA 4096, DSA, ECDSA	Generación de claves asimétricas.
ETSI TS 102 778	Formato de firma electrónica avanzada en PDF - PAdES

ETSI TS 101 733	Formato de firma electrónica avanzada - CADES
ETSI TS 101 903	Formato de firma electrónica avanzada en XML - XAdES
DSA, FIPS 186-4	Algoritmo de firma digital
RSA, FIPS 186-3	Algoritmo de firma digital RSA
ECDSA, FIPS 186-3	Algoritmo de firma digital de Curvas Elípticas
ETSI TS 102 918	Associated Signature Containers
EN 419211-2-2014	Perfiles de protección para dispositivos de creación de firma segura – Parte 2: Dispositivos con generación de clave
EN 419211-3-2014	Perfiles de protección para dispositivos de creación de firma segura – Parte 3: Dispositivos con importación de clave
EN 419211-4-2014	Perfiles de protección para dispositivos de creación de firma segura – Parte 4: Extensión para dispositivos con generación de claves y canal seguro para la aplicación de creación de firma
ETSI TS 102 176-1	Algoritmos y parámetros para firmas electrónicas seguras Parte 1: Funciones de Hash y algoritmos asimétricos
ETSI TS 102 023	Requerimientos de política para autoridades de sellado de tiempo
ETSI TS 101 861	Perfil del sello de tiempo
ETSI TR 102 038	Formato XML para políticas de firma
ETSI TR 102 041	Reporte de políticas de firma
ETSI TR 102 045	Política de firma para modelo de negocio extendido

ETSI TR 102 272	Formato ASN.1 para políticas de firma
IETF RFC 2560, X.509	Protocolo de Estado de Certificado en Línea - OCSP
IETF RFC 3125	Políticas de firma electrónica
RFC 5652, RFC 4853, RFC 3852	Sintaxis del mensaje criptográfico (CMS)
ITU-T Recommendation X.680	Abstract Syntax Notation ONE (ASN.1).
ETSI TS 101862, IETF RFC 3739, RFC 3279, RFC 5756	Perfil de certificados cualificados
ETSI TS 102280 x.509 v.3	Perfil de certificados emitidos para personas naturales
IETF RFC 4055	Algoritmos e identificadores adicionales para Criptografía RSA para el uso en la Internet X.509 Certificado de Infraestructura de la Clave pública y Perfil de Lista de Certificados Revocados (CRL)
SP 800-102	Recomendación para las líneas de tiempo de la firma digital
RFC 3647	Sistema básico de Política de Certificados y Prácticas de Certificación X.509 para PKI
PKCS#1	Estándar criptográfico RSA
PKCS#3	Estándar Diffie-Hellman para el acuerdo de claves
PKCS#6	Estándar de sintaxis de extensiones de certificado
PKCS#7	Estándar de sintaxis de mensaje criptográfico
PKCS#8	Estándar de sintaxis de información de clave privada

PKCS#9	Tipo de atributos seleccionados
PKCS#10	Estándar de petición de certificado
PKCS#11	Interface de token criptográfico
PKCS#12	Estándar de sintaxis de intercambio de información personal
PKCS#13	Estándar de criptografía de curvas elípticas
PKCS#15	Estándar de formato de información de token criptográfico
TSL	
ETSI TS 102 231	Proveedor de información sobre confianza de servicios
ETSI TS 101 456	Políticas para AC que expiden certificados reconocidos
ETSI TR 102 040	Armonización internacional de políticas para las AC que expiden certificados
Tarjetas Inteligentes	
EN 14890-2:2009, ISO/IEC 15946 series, ISO/IEC 7816-4:2005, 7816-8:2004, 7816- 9:2004	Interface para tarjetas inteligentes como dispositivos de creación segura de firma digital
Certificaciones	
ISO 20000	Gestión de tecnología
Webtrust	Certificación de evaluación de Entidades de Certificación
CMMI	Estándar que define procesos de calidad en el ciclo de vida de desarrollo de software

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

Common Criteria EAL	Seguridad de las aplicaciones de software
ISO 27001	Sistemas de gestión de seguridad de la información
ISO 21188	Infraestructura de llave pública para servicios financieros - Estructura de prácticas y políticas
ISO 27002	Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información
ISO 9000	Estándar que define procesos de calidad
HSM	
FIPS 140-2	Seguridad de módulos criptográficos
Aplicaciones Web	
OWASP Top Ten, OWASP Testing Project	Seguridad de Aplicaciones Web

(*) A efectos de los procedimientos de acreditación y seguimiento; debe tomarse en cuenta que las últimas versiones de los estándares utilizados serán los vigentes.

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

**ANEXO B:
LISTA DE VERIFICACIÓN DE AUDITORÍA**

 Indecopi <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	Infraestructura Oficial de Firma Electrónica-IOFE/PERÚ	Rev:
		Aprobado:

SOFTWARE DE FIRMA DIGITAL DE USUARIO FINAL

A continuación se presentan los requerimientos que el evaluador revisará como parte del proceso de acreditación, respecto de las aplicaciones de firma digital de usuario final. En cada caso el auditado deberá indicar si el requerimiento es aplicable a su aplicación de software sustentando debidamente cada caso de no aplicabilidad.

El evaluador deberá adjuntar una evidencia visual (pantalla capturada) respecto del cumplimiento de cada requerimiento.

En el caso que sea utilizado un certificado digital para efectuar una prueba, el evaluador deberá registrar el certificado, adjuntando a la evidencia la imagen de los detalles del perfil del certificado utilizado en la prueba.

Datos que deben ser registrados en el informe de auditoría respecto del alcance de la acreditación:

- a. Nombre de la Aplicación: (Incluye nombre comercial y versión del producto)
- b. Funcionalidades PKI: (realiza funciones de firma, autenticación o cifrado)
- c. Consulta de estado de revocación: (CRL, OCSP o ambos)
- d. Tipo de Operación: (Web, desktop, etc.)
- e. Sistemas operativos donde funciona la aplicación: (Windows versión __, Linux versión __, Java u otros)
- f. Formato del documento firmado: (resultado en formato PDF, XML, etc.)
- g. ¿Realiza funciones de módulo criptográfico?: (se incluye la evaluación de la seguridad de las claves)
- h. ¿Genera copias de la clave privada?: (se incluye la evaluación de la seguridad de las claves)
- i. Formato de documento a firmar: (formato original del documento)
- j. Herramientas: (herramientas empleadas en el entorno de pruebas).
- k. ¿Realiza consultas de sello de tiempo?:

Lista de verificación que debe ser incluida en el informe de auditoría respecto del alcance de la acreditación:

No	Requerimiento	¿Aplica?	Evidencia	Observaciones
Requerimiento Opcional: Verificación de consulta automatizada de la TSL (de cumplimiento opcional a petición del auditado)				
1	La aplicación deberá verificar la firma de la AAC en la TSL y corroborar que	Opcional		

	corresponde a la raíz de la AAC			
2	La aplicación deberá verificar que la fecha de vigencia de la TSL no ha expirado			
3	La aplicación deberá verificar que la clave pública de la EC raíz correspondiente al certificado que se desea utilizar para realizar la firma, se encuentra listado en la TSL.			
4	La descarga de la TSL puede ser periódica conforme a su periodo de vigencia			
<p>Requerimiento 1: Verificación del estado de revocación (el auditado podrá elegir el mecanismo CRL u OCSP)</p>				
<p>Verificación por consulta de la CRL</p>				
5	La aplicación deberá poder realizar el proceso de consulta de CRL mediante protocolos HTTP, LDAP o HTTPS, según sea el caso.			
6	La aplicación deberá verificar que la CRL esté firmada por la EC autorizada para realizar su emisión.			
7	La aplicación deberá verificar que la CRL se encuentre vigente, es decir que no se haya cumplido su fecha de expiración			

8	<p>Antes de realizar la firma de un documento o información, se debe realizar la consulta a la CRL respectiva para verificar que el certificado no se encuentre revocado. Se debe verificar que cada uno de los certificados que formen parte de la cadena de certificación no se encuentren revocados.</p>			
<p>Verificación por consulta OCSP</p>				
9	<p>La aplicación deberá realizar la verificación del estado de revocación de un certificado y su respectiva cadena de certificación realizando la consulta OCSP conforme al protocolo definido en la RFC 2560.</p>			
<p>Requerimiento 2: Verificación de no expiración del certificado</p>				
10	<p>La aplicación deberá realizar la verificación del estado de no expiración de un certificado, y su respectiva cadena de certificación.</p>			
<p>Requerimiento 3: Verificación del propósito</p>				
11	<p>La aplicación deberá verificar que los bit Non Repudiation y/o DigitalSignature se</p>			

	encuentran activos cuando se realiza el proceso de firma.			
Requerimiento 4: Comprobaciones para aplicaciones Web				
12	Los procesos de firma electrónica realizados en el equipo cliente del usuario de la aplicación, con el cliente de firma, deben ser validados en el servidor una vez que recibe el resultado de la firma, para verificar la validez del certificado electrónico empleado y que los datos firmados son coincidentes con los remitidos por la aplicación.			
Requerimiento 5: Las funciones criptográficas deben realizarse en el módulo criptográfico:				
13	La función de cifrado de la clave privada debe realizarse solamente en el módulo criptográfico certificado del suscriptor y no en las librerías criptográficas de la aplicación.			
14	No deben generarse copias automatizadas de la clave privada en el computador durante el proceso de firma.			
Requerimiento 6: No se deben utilizar funciones criptográficas obsoletas				

15	La aplicación debe utilizar algoritmos criptográficos vigentes, no vulnerados o no obsoletos			
Requerimiento 7: Se debe proteger la autenticidad del código de firma				
16	La autenticidad de la aplicación debe estar protegida por firma digital mediante un certificado de firma de código, emitido por una Entidad de Certificación reconocida por los sistemas operativos, plataformas de desarrollo y proveedores de red móvil.			
Requerimiento 8: Se debe proporcionar el visor para la verificación de la firma				
17	Las aplicaciones de firma digital deben brindar al firmante y al receptor visores para verificar el estado de integridad del documento firmado, la fecha de realización de la firma, la clave pública y los datos contenidos en el certificado.			
Requerimiento 9: Se deben generar registros de validación de la firma				
18	La aplicación debe adjuntar a la firma los siguientes datos de verificación de la firma, los cuales deben ser protegidos			

	<p>por la firma del suscriptor:</p> <ul style="list-style-type: none"> - Fecha y hora de realizada la firma - Clave pública de los certificados de la cadena de certificación - Como equivalencia funcional a este requerimiento se reconocen los estándares: <ul style="list-style-type: none"> ○ PADES: ETSI TS 102 778 -1 desde el nivel de equivalencia a CAdES-EPES. ○ XADES: ETSI TS 101 903 desde el nivel de equivalencia a CAdES-EPES. ○ CADES: ETSI TS 101 733 v2.2.1 desde el nivel CAdES-EPES. 			
<p>Requerimiento 10: Se deben implementar los manuales de administración y usuario</p>				
<p>19</p>	<p>Se deben implementar manuales de administración y usuario e incluir la siguiente información:</p> <ul style="list-style-type: none"> • Políticas o requerimientos de seguridad, respecto de la configuración y uso del software. • Capacidades de configuración en los manuales de administración y de usuario. <p>En caso que la aplicación a evaluar sea una librería criptográfica, se</p>			

	<p>deberá presentar la información referida al "manual de programador" o información sobre el funcionamiento y configuración adecuada de la librería.</p>			
--	---	--	--	--

SOFTWARE DE FIRMA POR PARTE DE AGENTES AUTOMATIZADOS

A continuación se presentan los requerimientos que el evaluador revisará como parte del proceso de acreditación, respecto de las aplicaciones de firma digital masiva realizada por parte de agentes automatizados. En cada caso el auditado deberá indicar si el requerimiento es aplicable a su aplicación de software sustentando debidamente cada caso de no aplicabilidad.

El evaluador deberá adjuntar una evidencia visual (pantalla capturada) respecto del cumplimiento de cada requerimiento.

En el caso que sea utilizado un certificado digital para efectuar una prueba, el evaluador deberá registrar el certificado, adjuntando a la evidencia la imagen de los detalles del perfil del certificado utilizado en la prueba.

Datos que deben ser registrados en el informe de auditoría respecto del alcance de la acreditación:

- Nombre de la Aplicación: (Incluye nombre comercial y versión del producto)
- Funcionalidades PKI: (realiza funciones de firma, autenticación o cifrado)
- Consulta de estado de revocación: (CRL, OCSP o ambos)
- Tipo de Operación: (Web, desktop, etc.)
- Sistemas operativos donde funciona la aplicación: (Windows versión __, Linux versión __, Java u otros)
- Formato del documento firmado: (resultado en formato PDF, XML, etc.)
- ¿Realiza funciones de módulo criptográfico?: (se incluye la evaluación de la seguridad de las claves)
- ¿Genera copias de la clave privada?: (se incluye la evaluación de la seguridad de las claves)
- Formato de documento a firmar: (formato original del documento)
- Herramientas: (herramientas empleadas en el entorno de pruebas.
- ¿Realiza consultas de sello de tiempo?:

Lista de verificación que debe ser incluida en el informe de auditoría respecto del alcance de la acreditación:

No	Requerimiento	¿Aplica?	Evidencia	Observaciones
Requerimiento Opcional: Verificación de consulta automatizada de la TSL (de cumplimiento opcional a petición del auditado)				
1	La aplicación deberá verificar la firma de la AAC en la TSL y corroborar que corresponde a la raíz de la AAC			
2	La aplicación deberá verificar que la fecha de			

	vigencia de la TSL no ha expirado			
3	La aplicación deberá verificar que la clave pública de la EC raíz correspondiente al certificado que se desea utilizar para realizar la firma, se encuentra listado en la TSL.			
4	La descarga de la TSL puede ser periódica conforme a su periodo de vigencia			
<p>Requerimiento 11: Verificación del estado de revocación (el auditado podrá elegir el mecanismo CRL u OCSP)</p>				
<p>Verificación por consulta de la CRL</p>				
5	La aplicación deberá poder realizar el proceso de consulta de CRL mediante protocolos HTTP, LDAP o HTTPS, según sea el caso.			
6	La aplicación deberá verificar que la CRL esté firmada por la EC autorizada para realizar su emisión.			
7	La aplicación deberá verificar que la CRL se encuentre vigente, es decir que no se haya cumplido su fecha de expiración			
8	Antes de realizar la firma de un documento o información, se debe realizar la consulta a la CRL respectiva para verificar que el certificado no se encuentre revocado			

9	Se debe verificar que cada uno de los certificados que formen parte de la cadena de certificación no se encuentren revocados.			
Verificación por consulta OCSP				
10	La aplicación deberá realizar la verificación del estado de revocación de un certificado y su respectiva cadena de certificación realizando la consulta OCSP conforme al protocolo definido en la RFC 2560.			
Requerimiento 12: Verificación de no expiración del certificado				
11	Al expirar el periodo de vigencia del certificado, la aplicación no debe permitir su uso para generar la firma digital.			
Requerimiento 13: Verificación del propósito				
12	Al instalar el certificado, la aplicación deberá verificar que el bit Non Repudiation del perfil de certificado se encuentra activo cuando se realiza el proceso de firma.			
Requerimiento 14: Control de acceso a las funciones de administración y configuración				
13	Las aplicaciones deben estar protegidos contra acceso no autorizado.			
14	Las funciones de verificación del estado de validez de los certificados deben estar siempre activadas a menos que			

	exista un caso de contingencia y se haya operado conforme a un procedimiento aprobado por la AAC.			
15	Registros de auditoría de las firmas generadas, según el tipo de transacción.			
16	Los derechos de administración no debe permitir la generación de firmas fuera de la realización de la transacción definida para la firma desatendida.			
Requerimiento 15: Las funciones criptográficas deben realizarse en el módulo criptográfico:				
17	En caso que la aplicación firme los documentos recibidos, la función de firma con la clave privada debe realizarse solamente en el módulo criptográfico certificado y no en las librerías criptográficas de la aplicación.			
18	No deben generarse copias automatizadas de la clave privada en el computador durante el proceso de firma.			
19	En caso que el módulo criptográfico sea parte de la solución a acreditar, el módulo utilizado debe cumplir con la certificación FIPS 140 -2 o Common Criteria EAL 4+			
20	En caso que la clave privada sea parte de la solución a acreditar, desde su generación, el acceso a			

	la clave privada de firma debe ser protegido por al menos dos personas a la vez.			
21	En caso que la clave privada sea parte de la solución a acreditar, desde su generación, el acceso a las copias de la clave privada deben ser protegidas por al menos dos personas por vez.			
22	En caso que la clave privada sea parte de la solución a acreditar, la importación y exportación de claves debe realizarse con la clave privada cifrada, por una clave protegida por dos personas a la vez.			
23	En caso que la clave privada sea parte de la solución a acreditar, deben generarse registros de auditoría de la generación, exportación, transporte, revocación, expiración y eliminación de la clave privada de firma.			
24	En caso que la clave privada sea parte de la solución a acreditar, el módulo criptográfico debe ser protegido contra acceso físico no autorizado, mediante un control de al menos dos personas. Todos los movimientos del módulo criptográfico deben ser registrados y su administración debe ser asignada a roles			

	específicos bajo responsabilidad contractual.			
25	En caso que la clave privada sea parte de la solución a acreditar, todos los movimientos del de los respaldos de las claves deben ser registrados (por ejemplo, mediante actas firmadas y dispositivos biométricos y cámaras) y su administración debe ser asignada a roles específicos bajo responsabilidad contractual.			
26	En caso que la clave privada sea parte de la solución a acreditar, la petición para la instalación del certificado debe ser conforme al estándar PKCS #10.			
27	En caso que la clave privada sea parte de la solución a acreditar, en caso de compromiso se deberá solicitar la revocación inmediata del certificado.			
Requerimiento 16: No se deben utilizar funciones criptográficas obsoletas				
28	La aplicación debe utilizar algoritmos criptográficos vigentes, no vulnerados o no obsoletos			
Requerimiento 17: Se debe proteger la autenticidad del código de firma				
29	La autenticidad de la aplicación debe estar protegida por firma digital mediante un certificado de firma de código,			

	emitido por una Entidad de Certificación reconocida por los sistemas operativos, plataformas de desarrollo y proveedores de red móvil.			
Requerimiento 18: Se debe proporcionar el visor para la verificación de la firma				
30	Las aplicaciones de firma digital deben brindar al firmante y al receptor visores para verificar el estado de integridad del documento firmado, la fecha de realización de la firma, la clave pública y los datos contenidos en el certificado.			
Requerimiento 19: Se deben generar registros de validación de la firma				
31	<p>La aplicación debe adjuntar a la firma los siguientes datos de verificación de la firma, los cuales deben ser protegidos por la firma del suscriptor:</p> <ul style="list-style-type: none"> - Fecha y hora de realizada la firma - Clave pública de los certificados de la cadena de certificación - Como equivalencia funcional a este requerimiento se reconocen los estándares: <ul style="list-style-type: none"> ○ PADES: ETSI TS 102 778 -1 desde el nivel de equivalencia a CAdES-EPES. ○ XADES: ETSI TS 101 903 desde el nivel de equivalencia a CAdES-EPES. ○ CADES: ETSI TS 101 733 v2.2.1 desde el nivel CAdES-EPES 			

Requerimiento 20: Se deben implementar los manuales de administración y usuario

32	<p>Se deben implementar manuales de administración y usuario e incluir la siguiente información:</p> <ul style="list-style-type: none"> • Políticas o requerimientos de seguridad, respecto de la configuración y uso del software. • Capacidades de configuración en los manuales de administración y de usuario. 			
----	--	--	--	--

SOFTWARE DE VERIFICACIÓN POR PARTE DE AGENTES AUTOMATIZADOS

A continuación se presentan los requerimientos que el evaluador revisará como parte del proceso de acreditación, respecto de las aplicaciones de verificación de documentos firmados realizada por parte de agentes automatizados. En cada caso el auditado deberá indicar si el requerimiento es aplicable a su aplicación de software sustentando debidamente cada caso de no aplicabilidad.

El evaluador deberá adjuntar una evidencia visual (pantalla capturada) respecto del cumplimiento de cada requerimiento.

En el caso que sea utilizado un certificado digital para efectuar una prueba, el evaluador deberá registrar el certificado, adjuntando a la evidencia la imagen de los detalles del perfil del certificado utilizado en la prueba.

Datos que deben ser registrados en el informe de auditoría respecto del alcance de la acreditación:

- a. Nombre de la Aplicación: (Incluye nombre comercial y versión del producto)
- b. Funcionalidades PKI: (realiza funciones de firma, autenticación o cifrado)
- c. Consulta de estado de revocación: (CRL, OCSP o ambos)
- d. Tipo de Operación: (Web, desktop, etc.)
- e. Sistemas operativos donde funciona la aplicación: (Windows versión __, Linux versión __, Java u otros)
- f. Formato del documento firmado: (resultado en formato PDF, XML, etc.)
- g. ¿Realiza funciones de módulo criptográfico?: (se incluye la evaluación de la seguridad de las claves)
- h. ¿Genera copias de la clave privada?: (se incluye la evaluación de la seguridad de las claves)
- i. Formato de documento a firmar: (formato original del documento)
- j. Herramientas: (herramientas empleadas en el entorno de pruebas.
- k. ¿Realiza consultas de sello de tiempo?:

Lista de verificación que debe ser incluida en el informe de auditoría respecto del alcance de la acreditación:

No	Requerimiento	¿Aplica?	Evidencia	Observaciones
Requerimiento Opcional: Verificación de consulta automatizada de la TSL (de cumplimiento opcional a petición del auditado)				
1	La aplicación deberá verificar la firma de la AAC en la TSL y corroborar			

	que corresponde a la raíz de la AAC			
2	La aplicación deberá verificar que la fecha de vigencia de la TSL no ha expirado			
3	La aplicación deberá verificar que la clave pública de la EC raíz correspondiente al certificado que se desea utilizar para realizar la firma, se encuentra listado en la TSL.			
4	La descarga de la TSL puede ser periódica conforme a su periodo de vigencia			
Requerimiento 21: Verificación del estado de revocación (el auditado podrá elegir el mecanismo CRL u OCSP)				
Verificación por consulta de la CRL				
5	La aplicación deberá poder realizar el proceso de consulta de CRL mediante protocolos HTTP, LDAP o HTTPS, según sea el caso.			
6	La aplicación deberá verificar que la CRL esté firmada por la EC autorizada para realizar su emisión.			
7	La aplicación deberá verificar que la CRL se encuentre vigente, es decir que no se haya cumplido su fecha de expiración			
8	Antes de realizar la firma de un documento o información, se debe			

	realizar la consulta a la CRL respectiva para verificar que el certificado no se encuentre revocado			
9	Se debe verificar que cada uno de los certificados que formen parte de la cadena de certificación no se encuentren revocados.			
Verificación por consulta OCSP				
10	La aplicación deberá realizar la verificación del estado de revocación de un certificado y su respectiva cadena de certificación realizando la consulta OCSP conforme al protocolo definido en la RFC 2560.			
Requerimiento 22: Verificación de no expiración del certificado				
11	La aplicación deberá realizar la verificación del estado de no expiración de un certificado, y su respectiva cadena de certificación.			
Requerimiento 23: Verificación del propósito				
12	Al instalar el certificado, la aplicación deberá verificar que el bit Non Repudiation del perfil de certificado se encuentra activo cuando se realiza el proceso de firma.			
Requerimiento 24: Control de acceso a las funciones de administración y configuración				
13	Las aplicaciones deben estar protegidos contra acceso no autorizado.			

14	Las funciones de verificación del estado de validez de los certificados deben estar siempre activadas a menos que exista un caso de contingencia y se haya operado conforme a un procedimiento aprobado por la AAC.			
15	Registros de auditoría de las firmas generadas, según el tipo de transacción.			
16	Los derechos de administración no debe permitir la generación de firmas fuera de la realización de la transacción definida para la firma desatendida.			
<p>Requerimiento 25: Las funciones criptográficas deben realizarse en el módulo criptográfico:</p>				
17	En caso que la aplicación firme los documentos recibidos, la función de firma con la clave privada debe realizarse solamente en el módulo criptográfico certificado y no en las librerías criptográficas de la aplicación.			
18	No deben generarse copias automatizadas de la clave privada en el computador durante el proceso de firma.			
19	En caso que el módulo criptográfico sea parte de la solución a acreditar, el módulo utilizado debe cumplir con la certificación FIPS 140 -2 o Common Criteria EAL 4+			

20	En caso que la clave privada sea parte de la solución a acreditar, desde su generación, el acceso a la clave privada de firma debe ser protegido por al menos dos personas a la vez.			
21	En caso que la clave privada sea parte de la solución a acreditar, desde su generación, el acceso a las copias de la clave privada deben ser protegidas por al menos dos personas por vez.			
22	En caso que la clave privada sea parte de la solución a acreditar, la importación y exportación de claves debe realizarse con la clave privada cifrada, por una clave protegida por dos personas a la vez.			
23	En caso que la clave privada sea parte de la solución a acreditar, deben generarse registros de auditoría de la generación, exportación, transporte, revocación, expiración y eliminación de la clave privada de firma.			
24	En caso que la clave privada sea parte de la solución a acreditar, el módulo criptográfico debe ser protegido contra acceso físico no autorizado, mediante un control de al menos dos personas. Todos los movimientos del módulo			

	criptográfico deben ser registrados y su administración debe ser asignada a roles específicos bajo responsabilidad contractual.			
25	En caso que la clave privada sea parte de la solución a acreditar, todos los movimientos de los respaldos de las claves deben ser registrados (por ejemplo, mediante actas firmadas y dispositivos biométricos y cámaras) y su administración debe ser asignada a roles específicos bajo responsabilidad contractual.			
26	En caso que la clave privada sea parte de la solución a acreditar, la petición para la instalación del certificado debe ser conforme al estándar PKCS #10.			
27	En caso que la clave privada sea parte de la solución a acreditar, en caso de compromiso se deberá solicitar la revocación inmediata del certificado.			
Requerimiento 26: No se deben utilizar funciones criptográficas obsoletas				
28	La aplicación debe utilizar algoritmos criptográficos vigentes, no vulnerados o no obsoletos			
Requerimiento 27: Se debe proteger la autenticidad del código de firma				

29	La autenticidad de la aplicación debe estar protegida por firma digital mediante un certificado de firma de código, emitido por una Entidad de Certificación reconocida por los sistemas operativos, plataformas de desarrollo y proveedores de red móvil.			
<p>Requerimiento 28: En caso que el sistema automatizado realice la firma digital del documento recibido, se debe proporcionar un visor para verificar la firma del documento.</p>				
30	En caso que la aplicación realice la firma digital de documentos firmados, se debe brindar de ser aplicable, a los terceros que confían, visores para verificar el estado de aprobación de los documentos, la integridad del documento firmado, la fecha de realización de la verificación, las claves públicas y los datos contenidos en los certificados, o firmar los documentos recibidos en un formato estándar aprobado por la AAC, que pueda ser verificado por los terceros que confían.			
<p>Requerimiento 29: En caso de firmar los documentos recibidos, se deben generar registros de validación de la firma</p>				
31	La aplicación debe adjuntar a la firma los siguientes datos de verificación de la firma, los cuales deben ser protegidos por la firma del suscriptor:			

	<ul style="list-style-type: none"> - Fecha y hora de realizada la firma - Clave pública de los certificados de la cadena de certificación - Como equivalencia funcional a este requerimiento se reconocen los estándares: <ul style="list-style-type: none"> o PADES: ETSI TS 102 778 -1 desde el nivel de equivalencia a CAdES-EPES. o XADES: ETSI TS 101 903 desde el nivel de equivalencia a CAdES-EPES. o CADES: ETSI TS 101 733 v2.2.1 desde el nivel CAdES-EPES. 			
<p>Requerimiento 30: Se deben implementar los manuales de administración y usuario</p>				
32	<p>Se deben implementar manuales de administración y usuario e incluir la siguiente información:</p> <ul style="list-style-type: none"> • Políticas o requerimientos de seguridad, respecto de la configuración y uso del software. • Capacidades de configuración en los manuales de administración y de usuario. 			

FUNCIONALIDAD DE SOLICITUD DE SELLOS DE TIEMPO (OPCIONAL)

A continuación se presentan los requerimientos que el evaluador revisará como parte del proceso de acreditación, de la funcionalidad de la petición de sellado de tiempo.

La funcionalidad de petición de sellado de tiempo, puede ser evaluada como parte de las evaluaciones de cualquiera de las modalidades de software:

- Software de firma digital de usuario final
- Software de firma por parte de agentes automatizados
- Software de verificación por parte de agentes automatizados

El evaluador deberá adjuntar una evidencia visual (pantalla capturada) respecto del cumplimiento de cada requerimiento.

En el caso que sea utilizado un certificado digital para efectuar una prueba, el evaluador deberá registrar el certificado, adjuntando a la evidencia la imagen de los detalles del perfil del certificado utilizado en la prueba.

No	Requerimiento	¿Aplica?	Evidencia	Observaciones
Requerimiento 31: Verificación del sellado				
1	Verificar que el sello de tiempo contiene el identificador del certificado de la Autoridad de Sello de tiempo que fue consultada			
2	Verificar la firma del sello de tiempo para corroborar que los datos son íntegros.			
3	Verificar que el certificado de la Autoridad de sello de tiempo no ha sido revocado			
4	Verificar que la vigencia del certificado de la Autoridad de sello de tiempo no ha expirado			