ANEXO I:

MARCO DE LA POLÍTICA DE EMISIÓN DE CERTIFICADOS DIGITALES

1. Declaración e implementación de las Prácticas

1.1. Introducción

Las Entidades de Certificación Digital deben elaborar y establecer como documento normativo su respectiva Declaración de Prácticas –CPS, mediante el cual la entidad deberá declarar los procedimientos y controles que adopta en cada etapa de los servicios y sistemas que brinda a sus clientes.

Los controles establecidos en el documento CPS y su contenido, deben estar de acuerdo con lo establecido por la Autoridad Administrativa Competente, en el presente documento. Las evaluaciones realizadas por la Autoridad Administrativa Competente velarán porque los controles implementados por la entidad que solicita la acreditación sean conformes a los requerimientos expresados en el presente documento, y a lo declarado por la entidad en su respectiva CPS.

En las siguientes secciones se describen los requerimientos que deben ser implementados en los procedimientos y operación de las Entidades de Certificación Digital, según el tipo de servicio que brindan, y que deben ser declarados en su documento CPS u otro documento normativo, o deben ser implementados en sus procesos de producción o como parte de su infraestructura. Estos requerimientos están basados en la RFC 3647, el documento “Guidelines for Schemes to issue certificates capable of being used in cross jurisdiction eCommerce”1 emitido por la secretaría de la Cooperación Económica Asia-Pacífico en el año 2005 y por los Principios de la certificación Webtrust para promover su interoperabilidad y reconocimiento por parte de los miembros del CAB Forum.

[1]Ver: http://publications.apec.org/publication-detail.php?pub_id=411

1.2. Provisiones

1.2.1. Introducción y alcance del servicio

Introducción y alcance			
Explicación preliminar: Puesto que el documento Declaración de Prácticas de Certificación es un documento normativo, que implica una obligación frente a los clientes de la EC, este documento debe ser adecuadamente gestionado a fin de mantener su autenticidad, vigencia, actualización y publicación.			
No	Provisiones		Referencia
1	Introducción	En esta sección la EC puede identificar e introducir el conjunto de disposiciones que serán descritas en su CPS, e indicar los tipos de entidades y aplicaciones para las que el documento está dirigido. La EC puede seguir estructuras estándar para la elaboración de su CPS, asegurándose que cumpla con los requerimientos establecidos por la AAC.	RFC 3647 sección 4.1: Introducción
2	Visión general	En esta sección la EC puede ofrecer una introducción general al documento CPS. También se puede proporcionar una sinopsis de la PKI a los que se aplica el CP o CPS.	RFC 3647 sección 4.1.1: Visión general
3	Nombre e identificación del documento	El documento de declaración deberá tener un código identificador aplicable, incluyendo identificadores de objeto ASN.1, el cual deberá ser colocado de manera visible en la	RFC 3647 sección 4.1.2: Nombre del documento e identificación

		carátula del documento	
4	Control de versiones	El documento deberá mostrar en la carátula, el control de versiones respectivo.	
5	Participantes	La EC deberá definir el campo de participantes o usuarios de los servicios que brinda, describiendo los tipos de titulares y terceros que son afectos al presente documento, es decir: - Autoridades de certificación - Autoridades de registro - Suscriptores - Terceras partes que confían - Otros participantes Por ejemplo: Pueden definirse limitaciones territoriales, profesionales, etc., como limitar el campo de usuarios a ciudadanos peruanos, al departamento de lima, o a un grupo profesional específico como los asociados al colegio de ingenieros, o los exportadores afiliados a la VUCE, etc. La comunidad de los terceros que confían de una EC puede ser más restringida que aquella establecida bajo el marco de la IOFE. La CPS de la EC debe detallar los requerimientos que se deben cumplir para ser considerados como terceros	RFC 3647 sección 4.1.3: Participantes PKI

		que confían dentro del ámbito de dicha EC	
6	Administración de la política	Se debe indicar el nombre o razón social de la entidad o empresa que administra y es autora bajo responsabilidad ante el proceso de acreditación de la AAC, de la redacción, registro, mantenimiento y actualización de esta CP o CPS. También incluye el nombre, dirección electrónica de correo, número de teléfono y número de fax de un Persona de contacto. Como una alternativa a nombrar una persona real, el documento puede nombrar a un título o un papel, un alias de correo electrónico, y otra información de contacto generalizada. En algunos casos, la organización puede expresar que su persona de contacto, sola o en combinación con otros, esté disponible para responder preguntas sobre el documento.	RFC 3647 sección 4.1.5: Administración de la Política
7	Definiciones y Acrónimos	Esta sección debe contener una lista de definiciones de términos utilizados en el documento, así como una lista de siglas en el documento y sus significados.	RFC 3647 sección 4.1.6: Definiciones y Acrónimos
8	Publicación y Responsabilidades del Repositorio	Las EC o Proveedores de servicios de repositorio acreditados, deben establecer repositorios que permitan a los titulares de certificados,	RFC 3647 sección 4.2: Publicación y Responsabilidades del Repositorio

		suscriptores y terceros que confían tener certeza respecto del estado de un certificado emitido por una EC dentro del marco de la IOFE. Todo procedimiento de interacción entre una EC y un Proveedor del servicio de repositorio debe ser especificado en la CPS o en otro documento relevante de estas entidades. Los repositorios deben ser capaces de inter-operar con otros repositorios establecidos bajo la IOFE, así como con otros repositorios de infraestructuras que hubieren sido reconocidos por INDECOPI y bajo la cual éstas operan. Los repositorios deben ser accesibles empleando los protocolos y tecnologías comúnmente disponibles: CRL y OCSP. Se deben identificar la entidad o entidades que operan repositorios dentro de la PKI, como la EC o en caso de existir alguna autoridad de fabricación de certificados, o servicio de depósito de proveedor independiente. En caso se requiera la tercerización de los servicios de directorio o repositorio y/o servicios de producción de certificados; entre otros, esto deberá estar claramente establecido en la CPS u otra documentación relevante y debe ser comunicado a INDECOPI para su	

		evaluación dentro del proceso de acreditación. La CPS u otro documento normativo de las EC acreditadas en la IOFE, debe detallar los convenios tanto para servicios de repositorio y registro, así como para producción de certificados, en caso fuere aplicable. La EC y el Proveedor del servicio Repositorio se encuentran sujetos a obligaciones legales tanto en la jurisdicción en la cual la IOFE, la EC o el mismo Repositorio se encuentren, cuando tiene lugar una transacción que utiliza un certificado emitido bajo el esquema de la IOFE. La EC es responsable de publicar información con respecto a sus prácticas, los certificados y el estado actual de dichos certificados. Se debe indicar cuándo la información debe ser publicada y la frecuencia de publicación. Control de acceso para proteger contra modificación no autorizada de los objetos de información publicados incluyendo, CP, CPS, certificados, estado de los certificados y CRL. Los documentos CP y CPS deben ser firmados digitalmente por la EC. El acceso a	

		los repositorios debe de ser restringido únicamente para el uso de los titulares y suscriptores legítimos, así como a los terceros que confían. La EC debe emplear sistemas fiables para el Repositorio, de modo tal que: • Únicamente las personas autorizadas puedan hacer anotaciones y modificaciones. • Pueda comprobarse la autenticidad de la información y la autenticidad de los certificados. • Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad. Las responsabilidades correspondientes al repositorio deben ser registradas en la CPS de la EC. • Si el Repositorio es operado por una entidad separada de la EC, sus responsabilidades también deberán ser registradas en la documentación del repositorio. Para minimizar la posibilidad de manipulación del Repositorio, el contenido de estos documentos debe ser firmado digitalmente por la EC. En caso de ocurrir un cambio significativo en los servicios, como la generación de nuevas claves, la generación de una EC Subordinada,	

		la pérdida de una certificación de seguridad declarada (por ejemplo: ISO 27001), debe ser comunicada al INDECOPI. El servicio de Repositorio debe incluir la Lista de Certificados Revocados de la EC. La cual debe tener una disponibilidad mínima de 99% anual, con un tiempo programado de inactividad máximo de 0.5% anual, y una frecuencia mínima de actualización de 24 horas. La latencia máxima entre la generación de las CRL y su publicación en el repositorio no debe ser mayor a una hora desde la generación de la CRL. Pueden establecerse Delta CRL y Puntos de Distribución CRL.	
9	Responsabilidades del suscriptor	Un suscriptor o titular debe estar obligado a cumplir las obligaciones de suscriptor establecidas en la CPS de la EC. Se debe requerir al suscriptor la firma de un acuerdo de cumplimiento de sus obligaciones, incluyendo las concernientes de eventuales incumplimientos. El acuerdo del suscriptor debe contemplar las obligaciones cuando	

		la legislación las establezca a los suscriptores o titulares a fin de asegurar los efectos legales de las transacciones realizadas utilizando certificados emitidos por la EC. Cuando una jurisdicción establece obligaciones a los suscriptores o titulares que se encuentran fuera de dicha jurisdicción, estas obligaciones deben de estar disponibles para los suscriptores o titulares. Se incluirá que el suscriptor o el titular son responsables por la exactitud de la información brindada para la emisión de sus certificados digitales, además de cumplir con el uso y aplicaciones previstas para los mismos bajo el alcance de la IOFE, debiendo brindar su protección a las claves y certificados frente a malos usos. Cuando un suscriptor celebra un acuerdo en representación de un número de titulares, sus responsabilidades en relación a las acciones de dichos titulares, también deben estar claramente establecidas.	
10	Responsabilidades de los terceros que confían	Un tercero que confía puede ser requerido a cumplir con las obligaciones establecidas en la CPS	

		de la EC. Se le debe notificar al tercero que confía dichas obligaciones por intermedio de la publicación de un documento accesible para el tercero que confía. La declaración o documento debe incluir las consecuencias derivadas del incumplimiento del acuerdo. Cuando la legislación establezca determinadas obligaciones a los terceros que confían para asegurar efecto legal a las transacciones realizadas utilizando certificados en los cuales esta parte confía, la documentación debe de establecer dichas obligaciones. Las obligaciones del tercero que confía deben incluir la necesidad de verificación del estado de los certificados y el acuerdo de no usar los certificados fuera de los términos establecidos en el marco de la IOFE. Los potenciales terceros que confían deben conocer sus obligaciones para establecer la validez de un certificado al momento de la realización de una transacción, y de las consecuencias de eventuales omisiones. Las EC deben notificar a los terceros que confían sobre la revocación de un certificado, esta puede efectuarse a	

		través de la publicación de un documento accesible para todos los terceros que confían debe advertirse respecto a la forma de dicha publicación y las implicancias de la misma	
11	Responsabilidades de otros participantes	El repositorio y otros participantes no específicamente mencionados anteriormente, deben establecer en su respectiva declaración de prácticas u otra documentación, provisiones sobre garantías y responsabilidades, incluyendo limitaciones y exclusiones de las mismas. Asimismo, deben asegurar que dichas provisiones se incluyan en todo contrato de suscriptor o tercero que confía. La EC debe establecer en su CPS su responsabilidad en relación a las operaciones que realiza el repositorio y cualquier otro participante no mencionado anteriormente. En particular, la EC y el repositorio deben establecer responsabilidad en relación a errores u omisiones en el procesamiento y mantenimiento de directorios y CRL y en la disponibilidad de dichos repositorios.	
12	Entidades de	Para ser acreditadas por INDECOPI,	

	Registro	las EC intermedias deben operar vinculadas por lo menos a una ER acreditada. La RPS de la ER debe ser compatible con la de dicha EC. Para demostrar dicha vinculación, la EC debe hacer referencia en sus documentos públicos o en su sitio web, la lista de ER autorizadas para emitir sus servicios de certificación digital y las limitaciones de responsabilidad entre ambas entidades.	

1.2.2. Requisitos operacionales del ciclo de vida de los certificados

Certificados digitales			
Explicación preliminar: Existen diversos tipos de certificados digitales que una EC puede proporcionar, según su aplicación o propósito, etc. Es necesario, que cada tipo de certificado relacionado a los servicios de registro de la EC sea descrito en el presente documento.			
No	Requerimiento		Referencia
13	Certificados digitales	La EC deberá indicar los tipos de certificados digitales que ofrecerá, según su propósito. Los certificados digitales se distinguen también por el tipo de proceso de verificación a seguir, si un certificado de un mismo tipo de propósito requiere de una validación de identidad mediante dos procedimientos diferentes, estos tipos de certificados deberán ser indicados como distintos.	

		Por ejemplo: certificados de firma para personas naturales, certificados de autenticación, certificados de firma para sistemas automatizados, etc.	
14	Uso del certificado	Una EC puede brindar distintos tipos de servicios de certificación, sin embargo, los certificados de firma digital reconocidos por la IOFE se clasifican de la siguiente manera: • Certificados de Persona Natural, caracterizados por el hecho de que pertenecen a una persona física, que actúa a nombre propio y representación (siendo en este caso el suscriptor y titular del certificado la misma persona). • Certificados de Persona Jurídica, la cual puede ser: a. Certificado de Atributos, caracterizados por el hecho que el titular del certificado es una persona jurídica, que faculta a una persona natural de atributos que le permiten actuar en nombre de la persona jurídica. Dichos atributos pueden ser limitados como el caso de certificados de funcionarios o empleados, o plenos como es el caso del representante legal de la persona jurídica. b. Certificados de agente automatizado, – Cuando el poseedor de la clave privada es un dispositivo informático perteneciente a una	RFC 3647 sección 4.1.4: Uso del certificado Reglamento de la Ley de Firmas y Certificados Digitales – D.S. 052-2008 – PCM.

		persona jurídica que realiza las operaciones de firma y descifrado de forma automática, y cuyas acciones se encuentran bajo la responsabilidad de una persona física que es el suscriptor del certificado (Puede ser el caso de un sistema SID, PSC, Time Stamping, etc.). Nota: Si se requiere definir la aplicabilidad de los certificados para un fin específico, por ejemplo, emitir comprobantes de pago electrónicos, boletas de pago para trabajadores u otros, el uso del certificado debe estar definido dentro de la CP. Esta sección debe describir lo siguiente: - Una lista o los tipos de uso apropiado para los certificados, así como las limitaciones técnicas y normativas en de su uso, de conformidad con la RFC 3647. En particular, debe establecerse un uso apropiado de los mismos para las transacciones de comercio y gobierno electrónico. Un certificado digital es utilizado apropiadamente si ha sido emitido a una persona adecuada conforme a la clasificación descrita en el presente documento y si esta persona utiliza el certificado para realizar cualquiera de las acciones mencionadas en su respectiva política de certificación. En algunos casos, el uso apropiado de certificados de las EC acreditadas por el marco de la IOFE puede ser más	

		restringido que el establecido bajo el mismo marco. - Una lista o los tipos de usos para los que el uso de los certificados está prohibido. INDECOPI prohíbe el uso del certificado digital de cualquier modo que contravenga la legislación de la materia, la presente Guía de Acreditación o sus anexos. En algunos casos, el uso prohibido del certificado de una EC y ER acreditadas bajo el marco de la IOFE puede ser más restringido que aquél establecido para el esquema en sí mismo. En el caso de una CP o CPS describa diferentes niveles de seguridad, esta sección puede describir aplicaciones o tipos de aplicaciones que son apropiadas o inapropiadas para los diferentes niveles de seguridad. La comunidad de usuarios y la aplicabilidad de los certificados pueden ser de índole pública, gubernamental, sectorial o una organización expresamente especificada en el RFC 3647.	
15	Titulares de certificados digitales	En el certificado del representante legal quedarán registrados sus atributos, los cuales le permitirán utilizar el certificado para realizar transacciones en nombre de la persona jurídica. Tratándose de certificados digitales solicitados por	

		personas jurídicas para su utilización a través de agentes automatizados, la titularidad de certificados y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.	
	Identificación y autenticación		
16	Denominación	Se deben describir los siguientes elementos en relación a los nombres y la identificación de los suscriptores: - Tipos de nombres asignados al subscriptor, como X.500 nombres distinguidos; Nombres RFC-822; y nombres X.400; - Las restricciones de nombre deben de estar soportados tal como se establece en el RFC 5280. - Si los nombres deben tener significado o no; - Los certificados correspondientes a máquinas autónomas o agentes automatizados pueden ser anónimos o bajo seudónimo, y si pueden, qué nombres se asignan o se pueden utilizar por suscriptores anónimos; - Reglas para la interpretación de diversas formas de nombre, como el X.500 estándar y RFC-822;	RFC 3647 sección 4.3.1: Denominación

		- Los nombres tienen que ser únicos, Para evitar conflictos de nombres en certificados correspondientes a personas físicas la identificación del titular debe estar formada por su nombre y apellidos, más su documento oficial de identidad. En certificados en que aparezcan datos de personas jurídicas, esta identificación se debe realizar por medio de su denominación o razón social y su RUC. Además del nombre y apellidos del suscriptor, más su documento oficial de identidad. - Reconocimiento, autenticación y el papel de las marcas comerciales. Se prohíbe a los solicitantes de certificados de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros. En el caso de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente. No le corresponde a la ER determinar si un solicitante de certificados le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado. La ER tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombres. El certificado de firma digital de una persona natural debe contener lo siguiente: - Nombre completo	

		- Número de documento oficial de identidad - Tipo de documento - El certificado de firma digital de una persona jurídica debe contener lo siguiente: - Razón social - Número del Registro Único de Contribuyentes (RUC) - Tipo de documento del suscriptor	
17	Validación inicial de identidad	La Entidad de Certificación deberá estar vinculada a una Entidad de Registro acreditada en Perú, a través de la cual deberá realizar todos los procedimientos de verificación de identidad, en particular la verificación presencial de identidad de los solicitantes de emisión inicial de certificados digitales. Este requisito puede ser precisado en el documento CPS, a través de un acuerdo o contrato celebrado entre la ER y la EC en caso de pertenecer a organizaciones distintas, o un documento que muestre la constitución de la ER como parte de la misma organización, o publicados en su sitio web. Los procedimientos de validación de identidad deberán estar descritos en el documento RPS de la ER y deberán guardar conformidad con la CPS o CP. La EC debe hacer referencia en sus CPS o en su sitio web u otro	

		documento relevante los procedimientos descritos en la RPS de la ER.	
18	Identificación y Autenticación para solicitudes de re-emisión de claves	Las solicitudes de re-emisión pueden ser realizadas a través de la ER o directamente a la EC. La EC debe indicar en su CPS u otro documento normativo los siguientes elementos para los procedimientos de identificación y autenticación para la re-emisión de claves para cada tipo de sujeto (EC, ER, de suscriptores, y otros participantes): – Los requisitos de identificación y autenticación para re-emisión de claves, tales como una solicitud de renovación del par de claves y está firmado utilizando la clave vigente; y – Los requisitos de identificación y autenticación para re-emisión de clave después de la expiración de certificados. – Los requisitos de identificación y autenticación para re-emisión de clave después de la revocación de certificados. La EC debe hacer referencia en sus CPS o en su sitio web u otro documento relevante los procedimientos descritos en la RPS de la ER.	RFC 3647 sección 4.3.3: Identificación y Autenticación para solicitudes de re-emisión de claves
19	Identificación y Autenticación	Las solicitudes de revocación pueden ser realizadas a través de la ER o	RFC 3647 sección 4.3.4: Identificación y Autenticación

	para solicitudes de revocación	directamente a la EC. La EC debe indicar en su CPS u otro documento normativo los procedimientos de identificación y autenticación para una solicitud de revocación por cada tipo de sujeto (EC, ER, suscriptor, y otro participante). Los ejemplos incluyen la solicitud de revocación firmada digitalmente con la clave privada correspondiente a un certificado digital distinto al que se quiere revocar, y una solicitud firmada digitalmente por la ER. La EC debe hacer referencia en sus CPS o en su sitio web u otro documento normativo los procedimientos descritos en la RPS de la ER con la que se encuentra vinculada.	para solicitudes de revocación
	Requerimientos operacionales del ciclo de vida del certificado		
20	Solicitud del certificado	La EC debe describir los siguientes requisitos respecto a la solicitud de cada certificado: – Quién puede presentar una solicitud de certificado, como un suscriptor de certificado o la ER; y – Proceso de solicitud utilizado por los suscriptores que presenten solicitudes de certificado y responsabilidades en relación con este proceso. Un ejemplo de este proceso es que el suscriptor genera el par de	RFC 3647 sección 4.4.1: Solicitud del certificado

		claves y envía una solicitud de certificado a la ER. Lo valida con la ER, firma la solicitud y la envía a la CA. La EC o ER son responsables de establecer un proceso de inscripción para recibir las solicitudes de certificados. Del mismo modo, los solicitantes del certificado pueden tener la responsabilidad de proporcionar información exacta sobre sus solicitudes de certificados. La EC debe informar a los suscriptores y titulares sobre los términos y limitaciones aplicables al certificado y las obligaciones que deben cumplir de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas empleando un certificado emitido por dicha EC. Dicha información puede ser entregada por la ER a los suscriptores y titulares como parte de su convenio con la EC. Estos procedimientos deberán estar en estricta observancia de la legislación en la materia, así como de los lineamientos establecidos por INDECOPI en las Guías de Acreditación y documentos anexos. Los procedimientos pueden estar descritos en la CPS. CP. RPS de la ER vinculada u en otro documento relevante de la EC.	

		En el caso de certificados de firma digital y no repudio para personas naturales y jurídicas, incluyendo agentes automatizados, los habilitados para presentar la solicitud de un certificado son: – La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado o por un representante que cuente con facultades expresas para tales efectos otorgadas mediante poder – En el caso de personas jurídicas, se pueden solicitar certificados de atributo para ser usados por funcionarios y personal específico, incluso por el Representante legal – Se debe permitir que un suscriptor pueda efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera. – Cada EC puede establecer limitaciones para la adquisición de sus certificados digitales	
21	Procesamiento de la solicitud del certificado	La EC puede describir el régimen de procesamiento de las solicitudes de certificados. La EC emitirá un certificado digital siempre que reciba una solicitud de una ER acreditada en un tiempo determinado por la EC. La solicitud deberá estar autorizada y validada. Siguiendo estos pasos, la	RFC 3647 sección 4.4.2: Procesamiento de la solicitud del certificado

		EC o ER pueden aprobar o rechazar la solicitud de certificado, tal vez por la aplicación de determinados criterios. Por último, se puede definir un límite de tiempo durante el cual una EC y / o la ER deben actuar en un proceso y solicitud de certificado de firma digital y no repudio de personas naturales, este tiempo no debe ser mayor a cinco (5) días útiles a partir de la entrevista presencial del solicitante en la ER, considerando el intercambio de información necesario entre la EC y la ER. La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE, sea el caso de una persona natural o jurídica o si el resultado de la validación realizada por la ER fue negativo. Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud.	
22	Contrato del suscriptor	Las EC deben establecer el contenido del contrato del suscriptor en coordinación con la ER, reflejando tanto las responsabilidades de la EC, la ER y la de los suscriptores y titulares; y los procedimientos a seguir para realizar la firma del mismo. Las EC deberán establecer, en	

		coordinación con la ER, en sus modelos de contratos de suscriptor y terceros que confían, cláusulas de supervivencia, de modo que ciertas reglas continúen vigentes después del término de validez de la CPS, RPS y de los contratos de los suscriptores y terceros que confían. Los requerimientos legalmente significativos deben de estar establecidos o referenciados en los contratos de suscriptores y terceros que confían.	
23	Emisión del certificado	La EC debe describir los siguientes elementos relacionados a la emisión del certificado: – Las acciones realizadas por la EC durante la emisión del certificado, por ejemplo, un procedimiento por el que la EC valida la firma y la autoridad de la ER y genera un certificado; La emisión del certificado implica la realización de las siguientes acciones: ○ Generación del par de claves de manera segura. ○ Asociación del par de claves que corresponde al certificado con un suscriptor. ○ Emisión del certificado asociada para su uso operativo, de acuerdo con el “Nombre Diferenciado” asociado con el	RFC 3647 sección 4.4.3: Emisión del certificado

		suscriptor y la Guía de Acreditación de EC – Mecanismos de notificación, en su caso, utilizado por la EC para notificar al suscriptor la emisión del certificado; Un ejemplo es un procedimiento por el que la EC envía el certificado por mensajes de correo electrónico al suscriptor o la ER envía por mensajes de correo electrónico que permite al suscriptor descargar el certificado de un sitio web. – Los certificados emitidos deben ser almacenados en un Repositorio acreditado por INDECOPI, con previo conocimiento de los suscriptores y titulares de los certificados, habiendo sido estipulado en el contrato del suscriptor. No almacenar las claves privadas de los usuarios finales a menos que correspondan a certificados cuyo uso se limite al cifrado de datos. – Una EC puede notificar a otras entidades acerca de la emisión de un certificado, mediante una notificación directa o a través de la publicación de la clave pública y datos que no comprometan la privacidad de los suscriptores y titulares en un repositorio al cual tengan acceso estas otras entidades. En los casos en que una ER procese las solicitudes de emisión de certificados en representación de una EC, debe notificarse a dicha EC la emisión y aceptación de ese certificado. Una EC puede publicar cualquier certificado relativo a su acreditación o certificados cruzados que	

		pueda mantener con otras EC, siempre y cuando no comprometa la seguridad de la IOFE	
24	Método para probar la posesión de la clave privada	La EC debe requerir del suscriptor una demostración de la posesión de las claves generadas. Esto se puede realizar a través de la firma electrónica de un mensaje, datos que sean verificables con dicha clave pública, la petición PKCS#10 u otro método equivalente. No será necesario realizar este paso en los casos en que la clave sea provista al suscriptor por un medio seguro que permita que únicamente dicha persona tenga acceso y conocimiento sobre la recepción de la referida clave. Cuando el par de claves sea generado en las instalaciones de la ER, no es el solicitante quien debe demostrar la posesión de la clave privada, sino la ER, la cual debe hacerlo en virtud del procedimiento fiable de emisión, de entrega y de aceptación del dispositivo seguro, del correspondiente certificado y el par de claves almacenados en su interior. La EC debe establecer en su CPS el procedimiento para probar la posesión de la clave privada, el cual puede ser hecho por el suscriptor o por la ER. Además, en el caso de una persona jurídica (certificados de atributos), la EC o la ER deben	

		asegurarse de que únicamente el suscriptor de certificados es poseedor de la clave privada.	
25	Aceptación del certificado	La EC debe describir lo siguiente: – El comportamiento de un solicitante que se considerará como la aceptación del certificado. Dichas prácticas pueden incluir pasos afirmativos para indicar la aceptación, lo que implica acciones de aceptación, o la incapacidad de oponerse al certificado o su contenido. Por ejemplo, la aceptación puede considerarse que ocurra si la EC no recibe ninguna notificación del suscriptor dentro de un período de tiempo determinado; un suscriptor puede enviar un mensaje firmado para aceptar el certificado; o un suscriptor puede enviar un mensaje firmado rechazando el certificado donde el mensaje incluye el motivo del rechazo y se identifican los campos en el certificado que son incorrectos o incompletos. – Publicación del certificado por la EC. Por ejemplo, la EC puede publicar el certificado a un X.500 LDAP o repositorio. – Notificación de la emisión del certificado por la EC a otras entidades. A modo de ejemplo, la EC puede enviar el certificado a la ER.	RFC 3647 sección 4.4.4: Aceptación del certificado
26	Uso del par de	La EC debe describir las	RFC 3647 sección 4.4.5: Uso

	claves y del certificado	responsabilidades relacionadas al uso de claves y certificados, incluyendo: – Responsabilidades del suscriptor en relación con el uso de la clave privada y el certificado. Por ejemplo, el suscriptor debe utilizar una clave privada y el certificado sólo para su uso apropiado como se establece en la CPS y en coherencia con el contenido del certificado (por ejemplo, el campo de uso de clave). El uso de la clave privada y el certificado están sujetos a los términos del acuerdo del suscriptor, el uso de una clave privada sólo se permite después de que el suscriptor ha aceptado el certificado correspondiente, o el suscriptor debe suspender el uso de la clave privada después de la expiración o revocación del certificado. – Las responsabilidades del tercero que confía relativas a la utilización de la clave pública y certificado del suscriptor. Por ejemplo, un tercero que confía podrá ser obligado a confiar en los certificados sólo para aplicaciones apropiadas como se establece en las CPS o CP y en concordancia con el contenido de los certificados requeridos (por ejemplo, el campo de uso de clave), realizar con éxito operaciones de clave pública, como condición de confiar en un certificado, asumir la responsabilidad de comprobar el estado de un certificado mediante uno de los mecanismos requeridos o permitidos establecidos en la	del par de claves y del certificado

		CP/CPS y asentir a los términos del acuerdo de la parte que confía como condición para confiar en el certificado.	
27	Re-emisión del certificado	La EC debe describir los siguientes elementos relacionados a generar un nuevo par de claves para un suscriptor u otro participante y solicitar la emisión de un nuevo certificado que acredite la nueva clave pública: – Las circunstancias bajo las cuales la re-emisión de certificado pueden o deben tomar lugar, como después de que un certificado es revocado por razones de compromiso o después de que un certificado ha caducado y el período de uso del par de claves también ha expirado; – Quién puede solicitar la re-emisión de un certificado, por ejemplo, el suscriptor; – Procedimientos de una EC o ER para procesar las solicitudes de re-emisión para emitir el nuevo certificado, tales como los mismos procedimientos utilizados para la emisión inicial del certificado; – Notificación del nuevo certificado al suscriptor; – La conducta que constituye la aceptación del certificado; – Publicación del certificado por la EC; – Notificación de la emisión del certificado por la EC a otras entidades. En ningún caso se puede solicitar la	RFC 3647 sección 4.4.7: Re-emisión del certificado

		re-emisión mediante un mensaje firmado con un certificado revocado. La EC debe comunicar al suscriptor, con una anticipación de al menos 30 días antes de la expiración del certificado, para que pueda renovar a tiempo dicho certificado. Sólo el titular de un certificado o un representante legalmente acreditado, puede solicitar a la ER respectiva la re-emisión de su certificado. Las solicitudes de re-emisión serán recibidas directamente por la EC o por la ER.	
28	Suspensión del certificado	La EC debe describir en su CPS, CP, RPS de la ER vinculada o cualquier otro documento relevante, lo siguiente: – Las circunstancias bajo las cuales se puede suspender un certificado; Sólo se puede solicitar la suspensión para el caso de personas jurídicas, cuando el suscriptor se ve impedido temporalmente de cumplir con sus funciones. – Quién puede solicitar la suspensión de un certificado; Conforme a la IOFE sólo los titulares de certificados emitidos a personas jurídicas pueden solicitar la suspensión de los certificados de sus suscriptores. Los titulares de certificados emitidos a personas jurídicas, pueden solicitar la suspensión de su	RFC 3647 sección 4.4.9: Revocación y suspensión del certificado

		certificado a la ER, a través de un representante legalmente autorizado. – Procedimientos de solicitud de suspensión de un certificado, como un mensaje firmado digitalmente por el suscriptor o ER, o una llamada telefónica de la ER; El solicitante debe especificar las fechas de inicio y fin del periodo de suspensión. – Cuánto tiempo puede durar la suspensión. El tiempo máximo en el que un certificado puede ser suspendido está limitado por su periodo de expiración.	
29	Revocación del certificado	La EC debe describir lo siguiente: – Las circunstancias bajo las cuales se puede revocar un certificado, por ejemplo, en casos de terminación del empleo del suscriptor, la pérdida del módulo criptográfico o sospecha de compromiso de la clave privada. Las EC deben especificar en su CPS o CP o en su sitio web o la RPS de la ER a la que se encuentran vinculadas o en cualquier otro documento relevante, las circunstancias en las que los suscriptores, titulares o terceros pueden solicitar la revocación de un certificado, como mínimo, el titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias: o Por exposición, puesta en peligro o uso	RFC 3647 sección 4.4.9: Revocación y suspensión del certificado

		indebido de la clave privada. ○ Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada. ○ Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados. ○ Cuando la información contenida en el certificado ya no resulte correcta. ○ Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC. ○ Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular. ○ Cuando la información contenida en el certificado ya no resulte correcta. ○ Por decisión de la legislación respectiva. – Quién puede solicitar la revocación del certificado, conforme a la normatividad peruana, los habilitados son: ○ El titular o suscriptor del certificado. ○ La EC que emitió el certificado. ○ Un juez que de acuerdo a la Ley decida revocar el certificado.	

		○ Un tercero que tenga pruebas fehacientes – Los procedimientos utilizados para la solicitud de revocación de certificados. Por ejemplo, un mensaje de la ER firmado digitalmente, un mensaje firmado digitalmente por parte del suscriptor, o una llamada telefónica de la ER; El suscriptor y el titular pueden solicitar a la EC o ER la revocación de su certificado utilizando un medio que garantice el no repudio o que sea aceptado por ambas partes. La EC debe establecer en su CPS, el procedimiento para realizar las solicitudes de revocación de los certificados de los suscriptores, emitidos por EC acreditadas. – Los terceros (incluyendo órdenes judiciales) deben presentarse personalmente o mediante un representante legalmente autorizado en las instalaciones de la ER... Dicha documentación y el proceso de validación de identidad del solicitante se encuentra especificado en la RPS de cada ER – El período de gracia disponible para el suscriptor, en el que el suscriptor debe hacer una solicitud de revocación; – El tiempo en el que la EC debe procesar la solicitud de revocación; La solicitud de revocación debe ser procesada dentro de las 24 horas siguientes a la realización de la solicitud en la ER o en la EC, o en caso de existir, a la expiración del periodo de gracia de la misma.	

		– Los mecanismos, en su caso, que un tercero que confía puede usar o debe utilizar con el fin de comprobar el estado de los certificados en los que desea confiar; – Si se utiliza un mecanismo de CRL, la frecuencia de emisión; – Si se utiliza un mecanismo de CRL, la latencia máxima entre la generación de CRL y publicación de las listas CRL en el repositorio (en otras palabras, el importe máximo de los retrasos Procesamiento y relacionadas con la comunicación en la publicación de las CRL en el repositorio después de que los laboratorios comunitarios de referencia se generan); – La disponibilidad On-line de comprobación de estado de revocación, por ejemplo, OCSP y un sitio web para consultas sobre el estado de los certificados; – Los requisitos de las partes de confianza para llevar a cabo verificaciones on-line de estado de revocación; – Otras formas disponibles de publicar el estado de revocación; – Cualquier variación de las estipulaciones anteriores para la revocación como resultado de un compromiso de clave privada (en contraposición a otras razones para revocación).	
30	Servicios de estado del certificado	La EC debe describir los servicios de comprobación de estado de los certificados a disposición de los	RFC 3647 sección 4.4.10: Servicios de estado del certificado

		terceros que confían, incluyendo: – Las características operativas de los servicios de verificación de estado de los certificados; – La disponibilidad de estos servicios, y cualquier política aplicable sobre la falta de disponibilidad; y – Cualquier característica opcional de este tipo de servicios. Cualquier información publicada por una EC respecto al estado de uno de sus certificados debe ser firmada digitalmente por la EC emisora. La hora y fecha deben ser consignadas por la entidad que genera esta información. En los casos en los que exista información sobre el estado del certificado, ésta deberá estar disponible con la misma confiabilidad que brinda una CRL o el directorio que reemplaza o con el cual opera de manera conjunta. Se reconoce el servicio OCSP (Online Certificate Status Protocol) como adicional al CRL y que puede ser empleado por las EC acreditadas previa declaración de su empleo y características operacionales.	Guidelines for the Certificate Policy and Certificate Practices Framework for issuing certificates capable of being used in Cross Jurisdiction eCommerce – APEC – Mayo 2005/ Sección 4.10 Certificate Status Services
31	Finalización de la suscripción	La EC debe describir los procedimientos que pueden ser	RFC 3647 sección 4.4.11: Finalización de la suscripción

		utilizados por el suscriptor para terminar la suscripción a los servicios de la EC, incluyendo: – La revocación de los certificados al final de la suscripción (que pueden ser diferentes, dependiendo de si el final de la suscripción se debió a la expiración del certificado o resolución del servicio). – La finalización de la suscripción puede darse cuando un suscriptor elija finalizar su suscripción como parte de la IOFE o la EC termine su suscripción al mismo, por fallecimiento del suscriptor o extinción de la persona jurídica que es titular del certificado	
32	Almacenamiento y recuperación de la clave (certificados de cifrado)	La EC debe describir los siguientes elementos para identificar las políticas y prácticas relativas al almacenamiento, y / o recuperación de claves privadas donde los servicios de custodia de claves privadas están disponibles (a través de la EC u otros terceros de confianza): – La identificación del documento que contiene políticas y prácticas de depósito de claves privadas y recuperación o una lista de este tipo de políticas y prácticas; y – La identificación del documento que contiene políticas y prácticas de encapsulamiento de la clave y recuperación o una lista de tales políticas y prácticas.	RFC 3647 sección 4.4.12: Almacenamiento de la clave y recuperación

1.2.3. Seguridad en la Gestión del ciclo de vida de las claves de los Certificados de la Entidad de Certificación

Gestión del ciclo de vida de las claves			
Explicación preliminar: La EC debe mantener controles para proveer la razonable certeza que la gestión del par de claves es segura durante todo su ciclo de vida en concordancia con los controles descritos en la CPS			
No	Requerimiento		Referencia
33	Generación de las claves de la EC	PRÁCTICAS a) La Generación de las claves de la EC deberá ser realizada en un ambiente asegurado físicamente b) La generación de las claves de la EC deberá ser realizada por personal que pertenezca a la EC, bajo al menos, control de acceso de dos personas y separación de accesos. c) La generación de la clave de firma de la EC deberá ser realizada en un módulo criptográfico que: • Cumpla con los requerimientos FIPS 140-2 nivel 3 o superior d) La generación de las claves de la EC es atestiguada por partes independientes o registradas mediante videograbación e) Las actividades de la generación de las claves de la EC son registradas. DOCUMENTOS a) Definición de roles y responsabilidades de los participantes b) Aprobación para la realización de la ceremonia de generación de claves c) Materiales de activación y hardware criptográfico requerido para la ceremonia	RFC 3647 sección 4.6.1: Generación e instalación del par de claves

		d) Pasos específicos que deben ser ejecutados durante la ceremonia de generación e) Requerimientos de seguridad física para el lugar donde se realiza la ceremonia f) Procedimientos para asegurar el almacenamiento del hardware criptográfico y los materiales de activación, luego de la ceremonia de generación g) Firma de los participantes y testigos indicando si la ceremonia de generación ha sido ejecutada en concordancia con el procedimiento de generación de las claves h) Anotación de cualquier desviación en la ejecución del procedimiento durante la ceremonia.	
34	Almacenamiento, respaldo y recuperación de la clave privada de la EC	a) La EC debe mantener controles para asegurar que las claves privadas de la EC permanecen en confidencial y mantiene su integridad. b) Las claves privadas de la EC son respaldadas, almacenadas y recuperadas por personal autorizado en roles de confianza, usando controles de acceso de al menos dos personas en un ambiente asegurado físicamente. c) La clave privada es almacenada usando un dispositivo criptográfico que cumple la certificación Common Criteria EAL4 o FIPS 140-2 nivel 3 o superior. d) Si la clave privada de la EC no es exportada fuera del módulo criptográfico, entonces la clave debe ser generada, almacenada y usada dentro del mismo módulo criptográfico.	RFC 3647 sección 4.6.2: Controles de ingeniería de protección de la clave privada y del módulo criptográfico Conforme a los lineamientos del APEC: ***Guidelines for Schemes to Issue Certificate Capable of Being Used in Cross-Jurisdiction eCommerce 2005 - Guidelines for the certificate Policy and Certificate Practices Framework for issuin certificates capable of being used in cross jurisdiction eCommerce, secciones 6.2.4 Private***

		e) Si la clave privada de la EC es exportada desde el módulo criptográfico para un almacenamiento seguro para propósitos de procesamiento fuera de línea o respaldo y recuperación, luego ellos son exportados dentro de un esquema de gestión que debe cumplir lo siguiente: i. La clave debe ser exportada en un formato cifrado usando una clave lo suficientemente segura ii. La clave de cifrado debe ser fragmentada usando control de múltiple acceso (al menos 2 personas) y división de conocimiento o iii. En otro módulo criptográfico seguro del mismo nivel de seguridad que el utilizando en la generación, usando control de acceso múltiple (al menos 2 personas). f) Las copias de respaldo de las claves privadas de la EC deben ser protegidas con al menos los mismos controles de seguridad utilizados para proteger las claves que se encuentran en uso. La recuperación de las claves debe ser realizada de una manera segura similar al proceso de generación.	***Key Backup, 6.2.5 Private Key Archival*** contemplan controles para el almacenamiento, respaldo y recuperación de la clave privada de la EC.
35	Distribución de la clave pública	La EC debe mantener controles para garantizar la integridad y autenticidad de las claves públicas de la EC y cualquier parámetro asociado durante su generación y su subsecuente distribución para: a) Los certificados auto-firmados, como es el caso de las raíces, la EC debe proveer un mecanismo para verificar la autenticidad e integridad del certificado auto-firmado.	

		b) Los certificados de las EC intermedias deben ser firmados por los certificados raíz. c) La distribución de la clave pública de la EC es realizada en concordancia con las prácticas declaradas en la CPS.	
36	Uso de la clave de la EC	La EC debe mantener controles para proveer una protección razonable para que las claves de la EC sean usadas sólo para las funciones destinadas en sus locaciones predeterminadas: a) Las claves privadas de la EC que son utilizadas para generar certificados y emitir información de estado de revocación de certificados, no serán usadas para ningún otro propósito. b) Las claves no deberán ser utilizadas al terminar su periodo establecido de vida ni en caso de compromiso. c) Las claves no deben ser utilizadas cuando los algoritmos empleados o el tamaño de las claves sean vulnerados de modo que se permita la suplantación de las claves.	
37	Archivo y destrucción de las claves	La EC debe mantener controles para asegurar de manera razonable que: a) Las claves archivadas de la EC permanecen confidenciales y seguras y que jamás son vueltas a poner en producción y b) Las claves de la EC son completamente destruidas al final de su ciclo de vida en concordancia con las prácticas declaradas. c) Las claves públicas o los certificados que las contengan, deben ser archivadas de conformidad con las políticas de archivo de registro.	RFC 3647 sección 4.6.2: Controles de ingeniería de protección de la clave privada y del módulo criptográfico RFC 3647 sección 4.6.3: Otros aspectos de gestión del par de claves.

		d) Cuando legalmente se permita la destrucción de la clave privada usada sólo para la firma, deben destruirse tanto esta clave como las copias de seguridad que pudieran existir. Los procedimientos deben asegurar que las copias recuperables no se mantengan en la memoria, módulo o disco, incluyendo cualquier copia de seguridad. En términos generales la destrucción siempre debe ser precedida por una revocación del certificado asociado a la clave, si éste estuviese todavía vigente.	
38	Compromiso de la Clave de la EC y cambio de clave	La EC debe mantener controles para proveer una razonable certeza que la continuidad de las operaciones es mantenida en el caso del compromiso o cambio de las claves privadas y certificados: a) Impedir las firmas con claves comprometidas b) Asegurar que los certificados son revocados y re-emitidos c) El plan de continuidad debe contemplar los casos de compromisos de las claves de la EC como un desastre d) Los procedimientos de recuperación de desastres deben incluir la revocación y re-emisión de todos los certificados que han sido firmados por las claves de la EC luego de ser comprometidas. e) Los procedimientos de recuperación usados en caso de compromiso o cambio de las claves privadas de la EC deben contemplar las siguientes acciones: i. Cómo la clave que es usada en el ambiente de producción es re-establecida de manera segura ii. Cómo la antigua clave, comprometida, es revocada	RFC 3647 sección 4.5.7: Compromiso y recuperación de las claves

		iii. Cómo las partes afectadas son notificadas iv. Cómo las claves públicas nuevas son provistas a todos los usuarios finales y a los terceros que confían, considerando el mecanismo para verificar la autenticidad de estas claves v. Cómo las claves públicas de los certificados de los suscriptores son re-certificadas f) En caso de compromiso de la clave privada de una EC raíz se deberá contemplar lo siguiente: i. Se revocará el certificado correspondiente a la clave privada comprometida. ii. Se revocará todos los certificados emitidos por dicha raíz. iii. Los planes de continuidad para casos de compromiso o cambio de la clave de la EC, debe considerar quién es notificado y qué acciones se deben tomar con los sistemas de software y hardware, las claves simétricas y asimétricas, firmas generadas previamente y datos cifrados.	

1.2.4. Ciclo de vida del módulo criptográfico de la EC

Ciclo de vida del módulo criptográfico		
Explicación preliminar: La EC debe proteger el módulo criptográfico donde se almacena su clave privada, a fin de evitar su compromiso.		
No	Requerimiento	Referencia

39	Gestión del ciclo de vida del módulo criptográfico	a) El hardware del módulo criptográfico no debe ser manipulado durante su transporte b) El hardware del módulo criptográfico no debe ser manipulado durante su almacenamiento c) Procedimientos y controles deben proteger para restringir el acceso físico a sólo personal autorizado d) La instalación, activación y duplicación de la clave de firma de la EC en el hardware del módulo criptográfico deberá ser realizado solo por personal que ocupa roles de confianza, usando al menos un control de acceso de dos personas en un ambiente físico seguro. e) El hardware del módulo criptográfico debe funcionar correctamente f) Las claves de firma de la EC que son almacenadas en un módulo criptográfico deben ser borradas antes de que el dispositivo sea retirado.	RFC 3647 sección 4.6.2: Controles de ingeniería de protección de la clave privada y del módulo criptográfico.

1.2.5. Repositorio de claves privadas (si fuera aplicable)

Repositorio de claves privadas			
Explicación preliminar: La EC debe asegurar de manera razonable que la clave privada de la EC permanece confidencial, aunque se encuentre en un repositorio de claves			
No	Requerimiento		
40	Almacenamiento de claves privadas de la EC	a) Si un tercero provee los servicios de almacenamiento o repositorio de claves, debe ser definido un contrato que delimite las responsabilidades y compensaciones entre las partes b) Si la clave privada de la EC es almacenada en un repositorio, las copias almacenadas deben ser protegidas en un nivel de	

		controles seguridad igual o mayor que la protección implementada para las claves que se encuentran en producción	

1.2.6. Seguridad en la Gestión del ciclo de vida de las claves de los Certificados del suscriptor

Controles de gestión del ciclo de vida de las claves del suscriptor			
Explicación preliminar: La Entidad de Certificación debe mantener controles efectivos para asegurar de manera razonable que la integridad de las claves del suscriptor es protegida durante todo su ciclo de vida.			
No	Requerimiento		Referencia
41	Servicios de generación y distribución de claves privadas (si se brinda el servicio)	Si la EC brinda servicios de gestión de claves privadas del suscriptor, entonces debe proveer controles de seguridad suficientes para garantizar que: a) Las claves del suscriptor, cuando sean generadas por la EC o ER, deberán ser generadas dentro de un módulo criptográfico seguro, certificado con FIPS 140-2 nivel 2 como mínimo, en concordancia con las prácticas declaradas. b) Las claves del suscriptor cuando sean generadas por la EC o ER, deberán ser distribuidas al suscriptor de una manera segura, garantizando la protección contra la suplantación de identidad de los suscriptores. c) El algoritmo de generación de claves debe ser reconocido por la IOFE. Se reconoce la lista de estándares criptográficos	ANSI X9.30 [ANS97] es el estándar de la industria financiera de Estados Unidos para la firma digital basada en la firma digital federal Algoritmo (DSA), y ANSI X9.31 [ANS98] es el estándar de contrapartida para la firma digital basada en el algoritmo RSA. Ver http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/ansi-x9-standards.htm

		recomendados se lista en el estándar ETSI TS 119 312. d) La generación de las claves es realizada usando un algoritmo de generación especificado en ANSI X9 o ISO/IEC 18032 e) La generación de claves es realizada usando un tamaño de clave en concordancia con la Política de Certificación o CPS. En caso que se utilice el algoritmo de generación RSA, debe utilizar un tamaño mínimo de 2048 bits. f) La generación de claves es realizada por personal autorizado. g) La distribución de las claves debe ser realizada conforme a lo declarado en la CPS o en la Política de Certificación, asegurando que la clave privada no sea revelada a ninguna otra entidad o persona que no sea el suscriptor correspondiente h) La EC no debe mantener una copia de la clave privada de firma, bajo ningún motivo.	
42	Periodos operacionales del certificado y periodo de uso de las claves	El periodo máximo de uso de una clave privada debe estar determinado por el riesgo de compromiso que pudiera existir para una clave de tal tamaño y este periodo puede necesitar ser variado dependiendo de los avances tecnológicos. En este punto, una clave de 2048 bit debe tener el periodo máximo de uso establecido de conformidad con el ciclo de vida del certificado o un plazo máximo de tres (3) años, cualquiera que fuera el menor.	

1.2.7. Requerimientos para la gestión de claves por parte del suscriptor

Requerimientos para el suscriptor			
Explicación preliminar: La EC debe establecer requerimientos que deben ser cumplidos por los suscriptores para proteger sus claves privadas.			
No	Requerimiento		Referencia
43	Requerimientos al suscriptor	La EC debe mantener controles que aseguren que: a) Los requerimientos para la protección de las claves del suscriptor son comunicados a los suscriptores b) La EC debe brindar al suscriptor mecanismos para el acceso, gestión y control del uso de sus claves privadas, de modo que pueda cumplir con lo declarado en la CPS. c) La EC debe requerir el uso aceptable de las claves.	

1.2.8. Gestión de certificados del suscriptor

Gestión de certificados del suscriptor		
Explicación preliminar: La EC debe establecer y mantener controles efectivos para asegurar que la información del suscriptor fue autenticada de manera apropiada.		
No	Requerimiento	Referencia

44	Solicitudes de certificados	La EC debe mantener controles que aseguren de manera razonable que: a) Los suscriptores son identificados de manera exacta en concordancia con lo declarado en la CPS y RPS de sus respectivas ER autorizadas. b) Las solicitudes de certificados son exactas, autorizadas y completas	RFC 3647 sección 4.4: Requerimientos operacionales del ciclo de vida del certificado
45	Re-emisión del certificado	c) La EC debe asegurar de una manera razonable que las solicitudes de re-emisión de certificados, incluyendo las solicitudes que siguen a la revocación o expiración de certificados recibidos mediante la ER, son exactos, autorizados y completos.	RFC 3647 sección 4.4: Requerimientos operacionales del ciclo de vida del certificado
46	Emisión del certificado	d) La EC debe asegurar de una manera razonable que los certificados son generados y emitidos conforme a las prácticas declaradas en la CPS o Política de Certificación. e) Cuando un suscriptor genera su propio par de claves o par de claves del titular, las claves públicas correspondientes deben ser entregadas al emisor del certificado de manera tal que se asegure la autenticidad de dicho suscriptor. En los casos en que las ER acepten las claves públicas en representación de los emisores de los certificados, éstas deberán ser entregadas a dicho emisor de manera tal que se asegure el mantenimiento de la asociación que debe existir entre el titular y la clave f) El tamaño de las claves debe ser de al menos 2048 bits. g) El perfil de los certificados debe ser conforme a ISO 9594/X.509 h) Los campos correspondientes al periodo de validez y los campos de extensión deben ser definidos en formatos conformes a ISO 9594/X.509 i) Los certificados de los usuarios finales son firmados por la clave privada de la EC j) La EC debe emitir una notificación firmada a la ER cuando un certificado es	RFC 3647 sección 4.4: Requerimientos operacionales del ciclo de vida del certificado

		emitido a un suscriptor para el cual la ER presento una solicitud. k) Los certificados son emitidos en base a los registros aprobados de los suscriptores. l) Si los certificados expiran, son revocados o son suspendidos, las copias de los certificados son retenidas por el periodo apropiado de tiempo especificado en la Política de Certificación m) En el caso que una EC o ER genere las claves a nombre del suscriptor, deben implementarse controles que aseguren la confidencialidad de la clave privada asociada. En los casos en que las claves no son emitidas en presencia del suscriptor o titular, se debe permitir la emisión electrónica de claves, proveyendo canales seguros por separado para la emisión de la clave y para el código (o códigos) de activación de la misma. n) La activación de la clave privada de una EC raíz o intermedia acreditada (no certificados de atributos), debe estar sujeta a un método aprobado de control de acceso. o) La activación inicial de la clave privada generada por un titular requiere el uso de los datos de activación provistos al mismo por un canal diferente al empleado para la provisión de la clave. Se debe requerir a los suscriptores el uso de los datos de activación cuando empleen la clave privada para firmar. p) Los requisitos para los datos de activación deben estar en concordancia con el valor de los activos protegidos por la clave privada y cualquier otro control de acceso a dicha clave. La forma de generación de datos de activación puede ser elegida por los usuarios.	

47	Distribución del certificado	q) La EC debe mantener controles para proveer una razonable garantía que, en el momento de la emisión, los certificados completos y exactos son disponibles para los suscriptores y terceros que confían de acuerdo a las prácticas declaradas en la Política de Certificación o CPS (por ejemplo, mediante un repositorio). r) Sólo el personal autorizado administra el repositorio o mecanismo utilizado para la distribución del certificado. s) El funcionamiento del repositorio o mecanismo de distribución es monitoreado y gestionado. t) La integridad del repositorio o mecanismo de distribución es mantenida y administrada.	RFC 3647 sección 4.4: Requerimientos operacionales del ciclo de vida del certificado .
48	Revocación del certificado	u) La EC debe mantener controles para proveer una razonable garantía que, los certificados son revocados, basados en solicitudes validadas y autorizadas en un periodo de tiempo acorde con lo declarado en la CPS o en la Política de Certificación. v) La EC provee un medio de comunicación rápida para facilitar los procesos de revocación de manera segura y autenticada, considerando los siguientes casos: a. Uno o más certificados de uno o más suscriptores b. La serie de todos los certificados emitidos por una EC y firmados por un mismo par de claves c. Todos los certificados emitidos por una EC, independientemente del par de claves usado w) La EC verifica o requiere que la ER verifique la identidad y autoridad de la entidad o persona que presenta una solicitud de revocación x) Si la ER acepta solicitudes de revocación, la EC requiere que la ER presente solicitudes de certificados revocados firmados, en una manera autenticada. En este caso, la EC debe proveer un reconocimiento firmado de la	

		solicitud de revocación y una confirmación de las acciones frente a la ER solicitante y) La Lista de Certificados Revocados (CRL) y otros mecanismos de estado de certificado deben ser actualizados conforme a los periodos de tiempo especificado en la CPS o en la Política de Certificación en concordancia con el formato definido en el ISO 9594/X.509 z) La EC genera registros de auditoría de todas las solicitudes de revocación y sus resultados. aa) Los solicitantes de la revocación de un certificado pueden ser: i. Los titulares o suscriptores de certificados pueden solicitar la revocación de certificados. ii. También terceros pueden hacer la solicitud de revocación de un certificado, sin embargo, esta sólo puede realizarse de manera presencial en la ER. iii. Un representante asignado por la persona jurídica puede solicitar la revocación de los certificados de la entidad, para ello debe presentar a la ER, documentos que acrediten dicha representación y la voluntad de dicha persona jurídica. iv. La IOFE permite que un tercero (diferente de la EC, el suscriptor y el titular), pueda solicitar la revocación de un certificado. En este caso, el solicitante deberá presentar en la ER pruebas fehacientes del uso indebido del certificado de acuerdo a la ley vigente. v. La revocación puede ser también solicitada mediante una orden judicial, la cual debe ser recibida y procesada por la ER.	

49	Suspensión del certificado (si es brindado el servicio)	bb) La EC debe mantener controles para proveer una razonable garantía que los certificados son suspendidos en base a solicitudes validadas y autorizadas en un periodo de tiempo conforme a lo declarado en la CPS o en la Política de Certificación. cc) Si la ER brinda el servicio de suspensión, la EC debe requerir a la ER que presente las solicitudes de suspensión, garantizando el no repudio. En este caso, la EC debe proveer un reconocimiento firmado de la solicitud de suspensión y una confirmación de las acciones frente a la ER solicitante	RFC 3647 sección 4.4: Requerimientos operacionales del ciclo de vida del certificado
50	Validación del certificado	dd) La EC pone a disponibilidad de las entidades relevantes, información del estado del certificado usando mecanismos conformes a lo declarado en su CP o CPS: i. Método de petición respuesta – Una solicitud por un tercero que confía al proveedor del estado del certificado. En retorno, el Proveedor de Estado del Certificado emite una respuesta del estado de certificado (Por ejemplo, OCSP). Si está soportada la verificación en línea de la revocación o de su estado, ésta deberá estar disponible con la misma confiabilidad que la CRL o directorio que pudiera estar reemplazando o con el cual opera de manera conjunta. ii. Método de envío: Una CRL firmada por la EC es publicada en un periodo de tiempo establecido en la CP o CPS ee) La EC firma cada CRL que emite para proteger su autenticidad, integridad y fecha de emisión ff) La EC emite la CRL a intervalos periódicos, como es especificado en su CP o CPS, incluso si no ocurre ningún cambio desde la última emisión gg) Como mínimo, el registro de certificado revocado permanece en la CRL hasta que finalice el periodo de vigencia del certificado revocado.	RFC 3647 sección 4.4: Requerimientos operacionales del ciclo de vida del certificado

		hh) La CRL es archivada incluyendo los métodos de recuperación conforme a lo declarado en la CP o CPS ii) Si un certificado expira, es revocado o suspendido, una copia de este certificado debe ser mantenida por un periodo de tiempo conforme a lo declarado en la CP o CPS	

1.2.9. Gestión de certificados de EC Subordinadas y certificaciones cruzadas

EC Subordinadas y certificaciones cruzadas			
Explicación preliminar: La EC debe establecer y mantener controles efectivos para asegurar que las solicitudes de las EC Subordinadas fueron autenticadas de manera apropiada.			
No	Requerimiento		Referencia
51	Protección del ciclo de vida de EC subordinadas	La EC debe mantener controles que aseguren de manera razonable que: a) Las solicitudes de certificados de EC Subordinadas son exactas, autenticadas y aprobadas b) Las solicitudes de re-emisión de certificados de EC Subordinadas son exactas, autorizadas y completes c) Los certificados nuevos o re-emitidos son generados y emitidos en concordancia con lo declarado en la CP o CPS d) Al momento de la emisión, los certificados completos y exactos son disponibles para todos los suscriptores y terceros que confían en concordancia con las prácticas declaradas de la EC e) Los certificados son revocados en base a solicitudes validadas y autorizadas f) El estado del certificado completo y exacto se encuentra oportunamente disponible para	RFC 3647 sección 4.4: Requerimientos operacionales del ciclo de vida del certificado

		cualquier entidad (incluye CRL y cualquier otro mecanismo de verificación de estado.	
52	Certificación cruzada	Las Entidades de Certificación acreditadas pueden realizar certificaciones cruzadas con Entidades de Certificación extranjeras a fin de reconocer los certificados digitales que éstas emitan, incorporándolos como suyos dentro de la IOFE, siempre y cuando obtengan autorización previa de la AAC, mediante el respectivo proceso de auditoría y cumpliendo con todos los requerimientos de seguridad descritos en el presente documento. Las entidades que presten servicios de acuerdo a lo establecido en el párrafo precedente, asumirán responsabilidad de daños y perjuicios por la gestión de tales certificados.	Reglamento de la Ley de Firmas y Certificados Digitales/ D.S. 052-2008-PCM- Artículo 73°.- De la certificación cruzada

1.2.10. Controles de seguridad

Gestión de la seguridad		
Explicación preliminar: La EC debe implementar los controles necesarios para asegurar la información en sus operaciones		
No	Requerimiento	Referencia

53	Organización de la seguridad de la información	Debe existir un responsable de organizar y dirigir la seguridad de la información	
54	Política de seguridad de la información	Se debe implementar y establecer una Política de seguridad cuyo alcance cubra todas las operaciones de la EC La EC deberá asegurar la publicación de esta política y su comunicación a todos los empleados que participan de las operaciones de la EC.	
55	Planificación	La seguridad debe ser planificada, gestionada y soportada dentro del ámbito de la EC	
56	Gestión de riesgos	Se debe realizar un análisis de riesgos y establecer los controles de seguridad, los cuales deben ser proporcionales a las amenazas y riesgos detectados. Periódicamente se debe revisar la efectividad del análisis de riesgos y los controles implementados.	
57	Documentación	Los procedimientos operativos y de seguridad de las operaciones de la EC deben ser documentados.	RFC 3647 sección 4.5.2: Controles de procedimiento
58	Seguridad en el trato con terceros	• La seguridad debe ser mantenida cuando las funciones son tercerizadas a otra organización o entidad. La EC es	

		responsable de los servicios que brinda, incluyendo los que son realizados por terceros proveedores • Las responsabilidades de terceros deben ser definidas y deben establecerse acuerdos para asegurar que los terceros cumplen todos los controles requeridos • La EC deberá mantener la responsabilidad de declarar las prácticas relevantes de tercerización a todas las partes interesadas. • Se debe de requerir a los contratistas y a su personal el cumplimiento de controles de seguridad establecidos para la EC. Esto debe quedar plasmado en los contratos que se celebren. Los contratos deben especificar obligaciones, sanciones y reparaciones para las acciones llevadas a cabo por los contratistas y sus empleados.	
59	Clasificación y gestión de activos	La EC deberá mantener un inventario de todos los activos críticos, asignando una clasificación de sus requerimientos de protección, de manera consistente con el análisis de riesgos	.
60	Seguridad del personal	a) La EC deberá emplear personal que posea conocimiento especializado, experiencia y calificaciones necesarias para ofrecer los servicios, de acuerdo a las funciones que debe cumplir	RFC 3647 sección 4.5.2: Controles de procedimiento RFC 3647 sección 4.5.3: Controles de personal

		cada rol, los cuales deben ser documentados en la CPS o cualquier otro documento relevante. b) Los roles y responsabilidades referidas al cumplimiento de la Política de Seguridad, deben ser documentados en las descripciones de las funciones de cada rol. Los roles, de los cuales dependen las operaciones de la EC deberán ser identificados. La descripción de los roles debe ser realizada utilizando el criterio de separación de funciones e incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, se debe especificar también la separación de los roles que puedan presentar conflicto, estas condiciones deben ser puestas de manifiesto a las personas que ejercen dichas funciones; además se debe usar controles físicos y lógicos para verificar la identidad antes de permitir el acceso para cada rol. c) Las funciones del personal de la EC (temporal y permanente) deberán ser definidas considerando los criterios de separación de derechos y mínimo privilegio d) El personal deberá ejecutar sus funciones y procedimientos en función de los procedimientos y la Política de Seguridad.	

		e) El personal que administra las operaciones técnicas de la EC debe tener conocimiento de las tecnologías relacionadas a los servicios de la EC, como firma digital, gestión de certificados digitales, sello de tiempo, mecanismos de sincronización de relojes con la UTC, conocimientos de los procedimientos y responsabilidades de seguridad para la gestión de personal, conocimientos de seguridad de la información y evaluación de riesgos. f) Todo el personal que ocupe un rol debe ser libre de conflicto de interés que pueda perjudicar la imparcialidad de las operaciones de la EC g) Los roles deben incluir las siguientes responsabilidades, según corresponda a sus funciones: • Responsabilidad de administrar la implementación de las prácticas de seguridad • Aprobación de la generación, revocación y suspensión de certificados • Instalación, configuración y mantenimiento de los sistemas de la EC • Operaciones diarias de los sistemas de la EC, así como los sistemas de respaldo y recuperación • Inspección y mantenimiento de los	

		archivos y logs de auditoría de los sistemas de la EC • Funciones criptográficas del ciclo de vida de las claves, y • Desarrollo de sistemas de la EC h) El personal debe ser formalmente asignado a cumplir los roles, por parte del responsable gerencial de la seguridad i) La EC no deberá asignar en roles o administración a cualquier persona que es conocida por tener una participación en un crimen serio u otra ofensa la cual afecta su idoneidad para su puesto. j) El personal no deberá tener acceso a funciones de confianza hasta completar todas las verificaciones necesarias. k) Los accesos a los sistemas, oficinas y ambientes de la EC deben ser removidos al finalizar el periodo de contratación y desactivados mientras dure el periodo vacacional del personal. l) Todo el personal y los terceros contratados deben recibir capacitación y entrenamiento periódico apropiado respecto de las políticas y procedimientos de la organización, conforme sean relevantes para su función laboral. Las EC deben de establecer en su CP, CPS u otra documentación relevante los requisitos de capacitación para su personal y contratistas. Como mínimo las re-capacitaciones deben ser llevadas a cabo cuando	

		existan cambios significativos en los elementos tratados en la capacitación inicial y cada vez que se sustituya o rote al personal encargado m) Se debe identificar las labores que requieren de más de una persona para su realización. n) La EC debe establecer en su CPS u otra documentación relevante si implementará políticas de rotación en el trabajo, en ese caso se debe establecer documentalmente los procedimientos necesarios o) Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad p) Se debe entregar o poner a disposición del personal la documentación necesaria para el desempeño de sus funciones. Como mínimo, esto debe incluir: • Una declaración de funciones y autorizaciones. • Manuales para los equipos de software que deben de operar • Aspectos de la CP, CPS, Política de Seguridad, Plan de Privacidad y otra documentación relevante en relación a sus funciones. • Legislación aplicable a sus funciones. • Documentación respecto a sus roles frente a planes de continuidad del negocio y recuperación frente a desastres.	

61	Seguridad física y del entorno	a) Los medios de administración de los sistemas de la EC, incluyendo equipos y módulos criptográficos deberán ser operados en un ambiente protegido con controles de acceso físicos para proteger de accesos no autorizados a los sistemas y datos b) Se deben definir perímetros de seguridad que protejan las operaciones y sistemas críticos de la EC (tales como paredes y puertas de ingreso controlado o personal de seguridad). Las partes compartidas con otras organizaciones deberán ser afuera de este perímetro. No debe haber ambientes compartidos que permitan la visibilidad de las operaciones de la EC. c) Debe llevarse un registro de acceso a las áreas de la EC. d) Controles de seguridad física y ambiental deben ser implementados para proteger los medios que alojan los recursos informáticos y los medios usados para soportar su operación. Estos deben incluir: protección de acceso físico, la ubicación y diseño del local debe considerar la protección contra desastres naturales, detección y protección contra incendios, control de aniego, inundación, terremotos, contingencia en cortes de energías y comunicaciones, colapso de la estructura, protección contra robo, ruptura, explosiones, disturbios civiles, recuperación en caso de	RFC 3647 sección 4.5.1: Controles de seguridad física

		desastres, conforme a los resultados del análisis de riesgos. e) El equipo de energía y aire acondicionado, incluyendo el equipo de seguridad de los mismos, deben estar protegidos y en constante mantenimiento a efectos de asegurar su correcto funcionamiento f) Se deben implementar controles que impidan el retiro no autorizado de equipos, información, medios de almacenamiento, software y otros activos de la EC. g) Los controles establecidos deben prevenir la pérdida, robo o compromiso de activos y la interrupción de las actividades de negocio son prevenidas.	
62	Gestión de operaciones	a) La confidencialidad, integridad y disponibilidad de los componentes informáticos y la información deben ser protegidos contra virus y software malicioso o no autorizado. b) Se deben establecer controles para prevenir o detectar la modificación no autorizada del software o cambios en el sistema de configuración, la validación de la integridad del sistema debe ser realizada frecuentemente en base al análisis de riesgos. c) Se deben implementar y ejecutar procedimientos de reporte y respuestas a incidentes de seguridad de las operaciones de la EC d) Se debe proteger todos los medios de almacenamiento usados en los sistemas de la EC deben ser protegidos	RFC 3647 sección 4.6.5: Controles de seguridad computacional

		contra modificación o acceso no autorizados e) Se deben establecer procedimientos para todos los roles y administrativos que impactan en la provisión de servicios de la EC. f) Deben emplearse controles de acceso tanto físicos como lógicos para verificar la identidad y autorización antes de permitir el acceso para cada rol. Cómo mínimo debe existir un control de acceso biométrico para los roles que impliquen el ingreso al centro de cómputo, en especial a la sala donde se encuentran los equipos de certificación digital. El acceso a los ambientes donde se accede al software, hardware e información que permite el control, administración y operación sobre los equipos de certificación digital debe tener control biométrico o mediante certificado digital. g) Se deben implementar procedimientos para asegurar la adecuada planificación de la implementación, habilitación de activos y nuevos sistemas a fin de evitar errores e incompatibilidades con otros sistemas y vulnerabilidades de seguridad h) La limpieza de los ambientes debe ser adecuada para no dañar los equipos, y el personal debe ser supervisado para evitar robos de medios de almacenamiento e información	

63	Manejo de medios y seguridad	Todos los medios deben ser manejados de manera segura conforme a la clasificación de activos. Los medios de almacenamiento que contienen datos sensibles deben ser eliminados de manera segura cuando ya no sean requeridos. Se debe adoptar una política de gestión de residuos que permita la destrucción de cualquier tipo de material (físico o papel) que pudiera contener información, garantizando la imposibilidad de recuperación de esta información.	RFC 3647 sección 4.6.5: Controles de seguridad computacional
64	Planificación del sistema	Se debe administrar la capacidad de los sistemas, los cuales deben ser monitoreados, gestionados y planificados de acuerdo a la demanda futura a fin de asegurar la disponibilidad de los sistemas de procesamiento y almacenamiento.	RFC 3647 sección 4.6.6: Controles de seguridad del ciclo de vida
65	Reporte y respuesta a incidentes	La EC debe actuar de manera oportuna y coordinada para responder de manera rápida a los incidentes y limitar el impacto de los vacíos de seguridad. Todos los incidentes deben ser reportados tan pronto como sea posible.	RFC 3647 sección 4.5.7: Compromiso y recuperación de las claves

66	Seguridad en redes	• Debe definirse una política de acceso en redes • Las redes deben ser protegidas de acceso no autorizado y mal intencionado, • Se debe separar la zona de constante acceso con la red interna de procesamiento y almacenamiento de información crítica. De acuerdo a los diferentes niveles de seguridad, deben separarse las redes de datos de los sistemas de procesamiento central de la EC • Los accesos a dominios de redes internas de la EC deben ser protegidos de acceso no autorizado incluyendo a suscriptores y terceros que confían. Los firewalls deben ser configurados para prevenir el acceso no autorizado a los sistemas de la EC. • Deben implementarse sistemas de detección de intrusos para prevenir accesos de código malicioso o no autorizado • Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar. • Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos. • Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas. No se debe permitir la conexión de los usuarios de redes compartidas, especialmente aquellas que se extienden a	RFC 3647 sección 4.6.7: Controles de seguridad de redes

		través de los límites organizacionales. • Los módulos criptográficos que contienen las claves privadas usadas por las EC raíz para firmar a los certificados de las EC intermedias, no deben estar conectados a ninguna red. • En los casos en que los repositorios de certificados, claves públicas, certificados cruzados o de información de estado se encuentren conectados a redes abiertas, éstos deberán estar sujetos a controles de seguridad en redes, incluyendo firewalls. Además, deben estar configurados para permitir sólo las operaciones necesarias para el funcionamiento bajo el marco de la IOFE	
67	Monitoreo	• La continuidad y seguridad de las operaciones debe ser monitoreada. • Los usos no autorizados de los sistemas de la EC deben ser detectados y registrados • Los registros de auditoría y los reportes de eventos sobre errores y advertencias en el funcionamiento de los sistemas de la EC deben ser monitoreados • Medios de monitoreo y alarmas deben ser implementados para detectar, registrar y actuar oportunamente sobre accesos no autorizados o intentos irregulares de acceso a recursos.	RFC 3647 sección 4.6.5: Controles de seguridad computacional

68	Intercambio de datos y software	Se debe evaluar las vulnerabilidades y riesgos de seguridad relacionados al intercambio de datos y software, y estos deben ser manejados de manera apropiada de acuerdo a su impacto sobre las operaciones de la EC	RFC 3647 sección 4.6.5: Controles de seguridad computacional
69	Gestión de accesos a los sistemas	La EC debe asegurar que el acceso a los sistemas es limitado a individuos autorizados apropiadamente: • Se debe realizar una efectiva administración de accesos de usuarios (operadores, administradores y auditores), a sistemas que mantienen la seguridad de la EC. Esta gestión debe incluir una asignación de cuentas de usuario, auditoria, modificación o remoción oportuna de acceso. • El personal debe ser apropiadamente identificado y autenticado antes de tener acceso a aplicaciones críticas de la EC • El personal debe ser controlado respecto de las acciones que realiza en los sistemas de la EC, mediante registros de auditoria.	RFC 3647 sección 4.6.5: Controles de seguridad computacional

70	Sistemas operativos	Las bases de datos y los sistemas operativos son actualizados y parchados en una manera oportuna considerando los resultados de los análisis de riesgo.	RFC 3647 sección 4.6.6: Controles de seguridad del ciclo de vida
71	Desarrollo y mantenimiento de sistemas confiables	a. Se debe realizar un análisis de los requerimientos de seguridad que deben ser cubiertos en las etapas de diseño y especificación de los proyectos de desarrollo de sistemas de la EC, para asegurar que dichos requerimientos son considerados en los sistemas críticos b. La EC debe mantener controles para proveer garantías razonables que las actividades de desarrollo de sistemas y mantenimiento son documentadas, testeadas, autorizadas, e implementadas apropiadamente para mantener la integridad de los sistemas de la EC	RFC 3647 sección 4.6.6: Controles de seguridad del ciclo de vida
72	Control de cambios	Se debe implementar procedimientos de control de cambios para poner en producción modificaciones o parches de emergencia de aplicaciones críticas de software de la EC, a fin de evitar posteriores fallas o incompatibilidad con otros sistemas.	RFC 3647 sección 4.6.6: Controles de seguridad del ciclo de vida
73	Gestión de Continuidad del	La EC debe mantener controles para proveer una garantía	RFC 3647 sección 4.5.7:

	Negocio	razonable de la continuidad de las operaciones en caso de desastre: a. El desarrollo y testeo de los planes de continuidad de negocio de la EC, que debe incluir procesos de recuperación de desastres para componentes críticos de los sistemas de la EC b. El almacenamiento de los equipos y dispositivos criptográficos en un local alterno c. El almacenamiento y respaldo de sistemas, datos e información de configuración en un local alterno d. La disponibilidad de un centro de datos alterno, que cuente con equipamiento y conectividad para habilitar la recuperación e. La EC deben disponer de copias de respaldo o de seguridad externa de toda la información sensible y de aquella considerada como necesaria para la persistencia de su actividad y la continuidad del negocio. Las copias de seguridad externa deben ser establecidas y mantenidas de conformidad con las políticas de archivo y continuidad del negocio y el plan de recuperación frente a desastres. Dichas copias deben ser	Compromiso y recuperación de las claves

		probadas con regularidad. f. La EC debe mantener controles para asegurar de manera razonable que las interrupciones potenciales de los servicios brindados a suscriptores y terceros que confían, por efectos de degradación o suspensión de los servicios de la EC, son minimizados. En particular los servicios de validación o revocación, deben ser reasumidos dentro de un plazo máximo de 24 horas. g. Se debe garantizar la continuidad de la recepción de solicitudes de revocación, revocación, emisión de la lista de certificados revocados y publicación de la lista de certificados revocados. h. Se debe establecer un procedimiento para probar el Plan de Continuidad de Negocio y Recuperación de Desastres con periodicidad mínima de 1 vez por año i. Los planes deben ser evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad.	

1.2.11. Compromiso de los servicios de la EC (Raíz e intermedias)

Compromiso de la EC			
Explicación preliminar: La EC debe adoptar los procedimientos de contingencia necesarios en caso de compromiso de sus servicios.			
No	Requerimiento		Referencia
74	Recuperación ante compromiso de las claves	La EC debe implementar un plan de recuperación de desastres que considere los casos: • Compromiso de la clave privada raíz • Compromiso de la clave privada intermedia • Compromiso de algún algoritmo o parámetro asociado usado por la EC o los suscriptores.	RFC 3647 sección 4.5.7: Compromiso y recuperación de las claves
75	Notificación	En el caso de compromiso de las operaciones de la EC, por sospecha de compromiso de su clave privada, la EC debe hacer disponible a todos los suscriptores y terceros que confían una descripción del compromiso ocurrido	RFC 3647 sección 4.5.7: Compromiso y recuperación de las claves
76	Interrupción de operaciones	En el caso de compromiso de las operaciones de la EC, de su clave privada, no deberán emitirse certificados hasta que se superar el incidente. El certificado comprometido de la EC deberá ser revocado. Los certificados firmados por ésta en el periodo comprendido entre el	RFC 3647 sección 4.5.7: Compromiso y recuperación de las claves

		compromiso de la clave y la revocación del certificado correspondiente dejarán de ser válidos. Se deberá comunicar inmediatamente a la AAC del INDECOPI el motivo del compromiso, así como las acciones realizadas. Sus titulares deberán solicitar a la EC la re-emisión de nuevos certificados, debiendo ésta emitirlos, conforme al procedimiento establecido.	
77	Mecanismos de verificación para terceros que confían	En el caso de compromiso de las operaciones de la EC, la EC deberá poner a disponibilidad de todos los suscriptores y terceros que confían información sobre el mecanismo que puede ser usado para identificar los documentos que han sido comprometidos, a menos que afecte una brecha de privacidad de los usuarios de los servicios de certificación, o genere una brecha en la seguridad de los servicios de la EC.	RFC 3647 sección 4.5.7: Compromiso y recuperación de las claves

1.2.12. Fin de operaciones de la organización que administra la EC

Fin de operaciones de la EC
Explicación preliminar: La EC debe adoptar las medidas necesarias para que su finalización no afecte de manera significativa a los suscriptores y terceros que confían.

No	Requerimiento		Referencia
78	Preparación antes del término	a) La EC debe poner a disponibilidad de los suscriptores y terceros que confían la información concerniente a la conclusión de sus operaciones. b) La EC deberá terminar con las autorizaciones de todos los subcontratistas que actúan en nombre de la EC, en el proceso de emisión de los certificados digitales c) La EC deberá transferir sus obligaciones a una parte confiable para mantener los archivos de los log de eventos y registros de auditorías necesarios para demostrar la correcta operación de la EC por un periodo razonable d) La EC deberá transferir sus obligaciones a una parte confiable para mantener disponible su clave pública o sus certificados a los terceros que confían por un periodo razonable de tiempo e) Las claves privadas de EC incluyendo las copias de respaldo deberán ser destruidos de tal manera que la clave privada no pueda ser recuperada f) Todos los datos necesarios para la continuación de las operaciones bajo el marco de la IOFE, en particular los certificados raíz, las listas de certificados revocados, son transferidas al propio INDECOPI o a otro PSC designado por éste. g) Cuando se trata de una operación de transferencia de titularidad, se debe asegurar que los nuevos dueños u operadores cumplan con los	RFC 3647 sección 4.5.8: Terminación de la EC o ER

		requisitos de acreditación del INDECOPI h) Las ECs deben establecer en su CPS u otra documentación relevante las provisiones de divisibilidad, supervivencia y fusión, si fueran aplicables, incluyendo las mismas en los contratos de suscriptor y tercero que confía.	
79	Capacidad financiera	La EC deberá tener un arreglo para cubrir los costos que implica implementar estos requerimientos mínimos en caso que la EC quiebre financieramente o por otras razones que inhabiliten su capacidad de cubrir los costos por sí misma.	RFC 3647 sección 4.5.8: Terminación de la EC o ER
80	Revocación del certificado de la EC	La EC deberá adoptar los pasos necesarios para revocar los certificados de la EC	RFC 3647 sección 4.5.8: Terminación de la EC o ER
81	Notificación	La EC debe informar al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.	

1.2.13. Registros de información concerniente a la operación de los servicios de certificación digital

Registros de auditoría			
Explicación preliminar: La EC debe registrar los eventos que sean necesarios como evidencia legal de la confiabilidad de los servicios brindados.			
No	Requerimiento		Referencia
82	Eventos	a. La EC debe declarar en la CP o CPS los tipos de	

	registrados	eventos y datos que serán registrados. b. Los eventos significativos relacionados a los ambientes de la EC, la gestión de claves y certificados deben ser registrados de manera exacta y apropiada c. Los registros deben incluir los siguientes elementos: i. Fecha y hora de la entrada ii. Número de serie o secuencia iii. Tipo de entrada (según acción realizada) iv. Fuente de la entrada (terminal, puerto, locación, cliente, etc.) v. Identidad de la entidad que realiza la entrada d. La EC debe registrar los siguientes eventos relativos a la gestión del ciclo de vida de las claves de la EC y los certificados: i. Generación de claves de la EC ii. Instalación manual de claves criptográficas de EC y su resultado (con la identidad del operador) iii. Respaldo de claves de EC iv. Almacenamiento de claves de EC v. Recuperación de claves de EC vi. Actividades de repositorio de claves de EC vii. Uso de claves de la EC viii. Archivo de claves de EC	RFC 3647 sección 4.5.4: Procedimiento de registro de auditoría

		ix. Retiro de material usado para las claves del servicio x. Destrucción del certificado de la EC xi. Autorización de la operación con las claves de la EC xii. Identidad de las entidades que manejan cualquier material de las claves (como los componentes de las claves o las claves almacenadas en dispositivos portables o media) xiii. Datos de acceso a los dispositivos o los medios que alojan las claves xiv. Compromiso de una clave privada e. La EC debe registrar eventos relativos a la gestión del ciclo de vida de los dispositivos criptográficos: i. Dispositivo del equipo e instalación ii. Colocar dentro o remover un dispositivo del almacenamiento iii. Activación y uso del dispositivo iv. Desinstalación del dispositivo v. Designación de un dispositivo para el servicio y su reparación vi. Retiro del dispositivo f. Si la EC provee servicios de gestión de claves del suscriptor, la EC debe registrar eventos relacionados al ciclo de vida de las claves del suscriptor:	

		i. Generación de las claves ii. Distribución de las claves (si fuera aplicable) iii. Respaldo de las claves (certificados de cifrado) iv. Repositorio de las claves (certificados de cifrado) v. Almacenamiento de las claves (certificados de cifrado) vi. Recuperación de las claves (certificados de cifrado) vii. Archivo de las claves (si fuera aplicable) viii. Destrucción de las claves ix. Identidad de la entidad que autoriza las operaciones de gestión de las claves x. Compromiso de las claves g. La EC debe registrar o requerir a la ER el registro de la siguiente información para la solicitud de certificados: i. El método de identificación aplicados y la información usada para el cumplimiento de los requerimientos del suscriptor ii. Registro de la data, números o combinación, única de identificación o documentos de identificación iii. Locación de almacenamiento de las copias de los documentos de	

		identificación y las solicitudes iv. Identidad de la entidad que acepta las solicitudes v. Método usado para validar documentos de identificación vi. Nombre de la EC que recibe o de la ER que solicita vii. Aceptación del suscriptor del Acuerdo del Suscriptor viii. El consentimiento para permitir a la EC o ER guardar registros de datos personales, pasar esta información a terceras partes especificadas, y publicación de certificados. h. La EC debe registrar o requerir a la ER el registro de los eventos relativos a la gestión del ciclo de vida de los certificados: i. Recepción de solicitudes de certificados – incluyendo solicitudes iniciales de certificados y solicitudes de re-emisión ii. Cambio de una afiliación de una entidad iii. Generación de certificados iv. Distribución de la clave pública de la EC v. Solicitudes de revocación de certificados	

		vi. Revocación de certificados vii. Solicitudes de suspensión de certificados (si se brinda el servicio) viii. Suspensión y reactivación de certificados i. La EC debe registrar los siguientes eventos sensibles con respectos a la seguridad: i. Lectura o escritura de registros o archivos sensibles de seguridad, incluyendo los registros de auditoría por sí mismos ii. Acciones tomadas contra los datos sensibles de seguridad iii. Cambios de perfiles de seguridad iv. Uso de mecanismos de identificación y autenticación, considerando ambos casos exitosos y no exitosos (incluyendo múltiples intentos fallidos de autenticación) v. Fallos de los sistemas, del hardware y otras anomalías vi. Acciones tomadas por individuos en Roles de Confianza, operadores computacionales, administradores de sistemas, oficiales de seguridad de sistemas. vii. Cambios de la afiliación de una entidad	

		viii. Decisiones para saltar procesos y procedimientos de cifrado y autenticación, y ix. Acceso a los sistemas de la EC y cualquiera de sus componentes j. Los registros de auditoría no deberán registrar de ninguna manera las claves privadas (ya sea en texto claro o texto cifrado) Los relojes de los sistemas computacionales son sincronizados con una exactitud y la fuente de tiempo confiable. La periodicidad de la revisión de los registros de auditoría debe ser proporcional a la criticidad del activo que protegen.	
83	Protección de los registros	La confidencialidad e integridad de los registros vigentes y los archivados concernientes a la operación de los servicios de certificación digital debe ser mantenida. Los eventos deben ser registrados en un modo que ellos no puedan ser borrados o destruidos por un periodo mínimo de diez (10) años, en los cuales pueden ser requeridos como evidencia. Debe realizarse una copia de	RFC 3647 sección 4.5.5: Archivo de registros RFC 3647 sección 4.5.4: Procedimiento de registro de auditoría

		seguridad del registro de auditorías de manera periódica.	
84	Archivo de registros	Los registros concernientes a la operación de los servicios de certificación digital deberán ser archivados de manera completa y confidencial en concordancia con la CPS La EC deberá mantener la información relativa a los certificados, por un periodo mínimo de diez (10) años a partir de su cancelación (expiración o revocación). La destrucción de un archivo de auditoría correspondiente a un servicio brindado en el Estado Peruano sólo se podrá llevar a cabo con la autorización de INDECOPI. Los archivos tanto electrónicos como de papel y el material en general, debe estar protegido contra accesos no autorizados y destrucción tanto deliberada como accidental, incluyendo destrucción por fuego, temperatura, agua, humedad y magnetismo. Los soportes de información sensible se deben almacenar de forma segura en armarios, cajas fuertes o ambientes con controles contra incendios, según el tipo de soporte y la clasificación de la	RFC 3647 sección 4.5.5: Archivo de registros

		información en ellos contenida. El acceso a estos soportes debe estar restringido a personal autorizado. Los datos archivados deben consignar la fecha y hora, y la firma digital de la organización que genera dichos datos según la RFC 3161 (Time Stamping), o pueden ser protegidos de cualquier otra forma que pueda demostrar que los datos corresponden a la organización que los ha generado. Los procedimientos para la obtención y verificación de la información del archivo deben encontrarse de conformidad con los requisitos de confidencialidad y privacidad	
85	Eventos significativos	Debe ser registrado el tiempo preciso en el que ocurren eventos significativos en los ambientes de la EC, gestión de claves o sincronización del reloj.	RFC 3647 sección 4.5.4: Procedimiento de registro de auditoría
86	Notificación de eventos	Se debe establecer en la CP, CPS de la EC u otra documentación relevante si es que resulta factible realizar notificaciones a los titulares o suscriptores que causan los eventos. Debe tomarse en consideración la posibilidad de permitir la notificación a un titular	

		en los casos en que se establezca que el evento es de índole accidental y resulta probable que pueda volver a ocurrir.	
87	Evidencias legales	Los registros concernientes a la operación de los servicios de certificación digital deberán ser disponibles si son requeridos para propósitos de proveer evidencia de la correcta operación de los servicios de certificación digital para propósitos legales	RFC 3647 sección 4.5.4: Procedimiento de registro de auditoría
88	Archivo luego de expiración de la EC	Los registros concernientes a los servicios de certificación digital deberán ser mantenidos por un periodo mínimo de diez (10) años después de la expiración de la vigencia de las claves de firma de la EC	RFC 3647 sección 4.5.5: Archivo de registros
89	Privacidad	Cualquier información que es registrada acerca de los suscriptores deberá ser guardada de manera confidencial excepto si se obtiene el consentimiento del suscriptor para su publicación	RFC 3647 sección 4.9.4: Privacidad de información personal
90	Gestión de la clave de la EC	Se deben registrar eventos relacionados al ciclo de vida de la clave privada de la EC	RFC 3647 sección 4.5.4: Procedimiento de registro de auditoría

1.2.14. Auditoría

Auditoría			
Explicación preliminar: La EC debe ser auditada anualmente por la AAC, respecto de la correcta operación de los servicios de certificación.			
No	Requerimiento		Referencia
91	Conformidad legal	La EC debe mantener controles para garantizar de manera razonable que sus prácticas son conformes con los requerimientos legales, regulatorios y contractuales relevantes.	RFC 3647 sección 4.8: Auditoría de cumplimiento y otras evaluaciones
92	Conformidad de la Política de seguridad	La EC debe mantener controles para garantizar de manera razonable el cumplimiento de la política de seguridad y sus procedimientos	RFC 3647 sección 4.8: Auditoría de cumplimiento y otras evaluaciones
93	Auditoría de registros	Los registros deben ser revisados como parte de la auditoría de la AAC, de manera anual.	RFC 3647 sección 4.8: Auditoría de cumplimiento y otras evaluaciones
94	Auditoría del archivo	El archivo debe ser revisado como parte de la auditoría de la AAC, de manera anual.	RFC 3647 sección 4.8: Auditoría de cumplimiento y otras evaluaciones
95	Auditoría de los procedimientos y controles	Los procedimientos y controles implementados deben ser auditados por la AAC de manera anual.	RFC 3647 sección 4.8: Auditoría de cumplimiento y otras evaluaciones

96	Auditor	El auditor debe: Ser autorizado por el INDECOPI. Ser independiente de la EC, y no haber realizado trabajos para ella dentro de los 2 años anteriores a la ejecución de la auditoría. Contar con experiencia significativa en tecnologías de la información, seguridad y tecnologías de PKI y criptográficas	RFC 3647 sección 4.8: Auditoría de cumplimiento y otras evaluaciones

1.2.15. Aspectos legales de la operación de la EC

Aspectos legales de la operación de la EC			
Explicación preliminar: La EC puede establecer provisiones legales aplicables a los servicios que brinda.			
No	Requerimiento		Referencia
97	Tarifas	La EC puede declarar en algún documento provisiones respecto de los cargos que son aplicables por los servicios brindados, por ejemplo: • Servicios de recepción solicitud de certificados digitales • Servicios de recepción de solicitudes de revocación • Servicios de soporte, etc. • Cargos de re- emisión de certificado; • Tarifas de acceso al certificado; • Revocación o tarifas de acceso a la información de	RFC 3647 sección 4.9.1: Tarifas

		estado; • Honorarios por otros servicios tales como el acceso a la correspondiente CP o CPS; y • Política de reembolso. Estos cargos deben incluirse o referenciarse en los contratos de suscriptores y terceros que confían.	
98	Políticas de reembolso	La EC puede establecer políticas de reembolso, incluyendo los siguientes casos: • Cuando un certificado no puede ser correctamente instalado • Cuando se proporciona un certificado de propósito o características tecnológicas diferentes En caso de existir, estas cláusulas deben incluirse o referenciarse en los contratos de suscriptores y terceros que confían.	
99	Responsabilidad financiera	La EC debe cumplir requisitos relacionados con los recursos que mantiene disponibles para apoyar el desempeño de sus responsabilidades operacionales de PKI, seguir siendo solvente y pagar daños y perjuicios en el caso que estén obligados a pagar una sentencia o resolución en relación con una demanda que surja de tales operaciones. Tales disposiciones	RFC 3647 sección 4.9.2: Responsabilidad financiera

		incluyen: • La EC debe mantener una cierta cantidad de cobertura de seguro para cubrir sus obligaciones frente a otros participantes; o • La EC debe tener acceso a otros recursos para soportar operaciones y pagos de daños para obligaciones potenciales, que puede ser expresado en términos de un nivel mínimo de activos necesarios para operar y cubrir las contingencias que pudieran ocurrir dentro de una PKI, donde los ejemplos incluyen los activos en el balance general de una organización, un bono de garantía, una carta de crédito, o un derecho bajo un acuerdo para una indemnización bajo ciertas circunstancias; o • La EC deber ofrecer un seguro de responsabilidad civil o la protección de garantía a otros participantes en conexión con el uso de la PKI. La EC debe establecer en su CPS o en los contratos del suscriptor o tercero que confía, cláusulas de garantía y responsabilidad, incluyendo limitaciones y excepciones. Cuando una EC terceriza las funciones de repositorio, se debe establecer la responsabilidad de la EC y de aquellas organizaciones que realizan las actividades tercerizadas.	

		La EC debe asegurar que las organizaciones realizando las actividades tercerizadas, realizan dichas funciones de conformidad con la CP, CPS y otra documentación de la EC, estableciendo provisiones de responsabilidad respecto a los eventuales errores y omisiones que pudieran generarse. En particular, la EC debe establecer responsabilidad en relación a errores u omisiones en la producción y distribución de certificados, directorios y listas de revocación de certificados, incluyendo la disponibilidad de dichos directorios y CRL. En el caso que exista cobertura de seguro o garantía disponible para los suscriptores, la EC debe establecer en su CPS los tipos correspondientes, lo cual deberá también ser referenciado en el contrato de suscriptor, incluyendo los términos y condiciones de dicha cobertura. En el caso que exista cobertura de seguro o garantía disponible para los terceros que confían, esto deberá encontrarse referenciado en la CPS, en donde deben incluirse los términos y condiciones de la cobertura para el tercero que confía.	

100	Información confidencial	La EC debe describir disposiciones relativas al tratamiento de información comercial confidencial que los participantes pueden comunicar entre sí, tales como planes de negocios, información de ventas, secretos comerciales, y la información recibida de un tercero en virtud de un acuerdo de confidencialidad. Tales disposiciones deben incluir: • El alcance de lo que se considera información confidencial, • El tipo de información que se consideran fuera del alcance de la información confidencial, y • Las responsabilidades de los participantes que reciben información confidencial para asegurarla en casos de compromiso, y se abstenga de utilizar o revelarla a terceros. • Se debe permitir la revelación de información personal a oficiales encargados del cumplimiento de leyes o como parte de un descubrimiento civil, donde se hace una solicitud de conformidad con la ley aplicable en la jurisdicción en donde el PSC se encuentra localizado. Cuando la solicitud de divulgación de información proviene de otra jurisdicción, debe permitirse la aplicación de leyes de asistencia mutua.	RFC 3647 sección 4.9.3: Confidencialidad de información del Negocio

101	Información privada	La EC debe mantener de manera confidencial la siguiente información: • Material comercialmente reservado de los PSC, de los suscriptores de la empresa y de los terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual; • Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores, titulares y los terceros que confían; • Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían. • Se debe asegurar la reserva de toda información que mantiene, la cual pudiera perjudicar la normal realización de sus operaciones. Se permite la publicación de información respecto a la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión. La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.	RFC 3647 sección 4.9.4: Privacidad de información personal
102	Información no privada	Se debe permitir la publicación de certificados (siempre que el suscriptor lo autorice en el contrato	RFC 3647 sección 4.9.4: Privacidad de información personal

		del suscriptor) e información de estado de certificados, así como de información en relación a la revocación de un certificado sin revelar la razón de dicha revocación. La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.	
103	Derechos de Propiedad intelectual	De ser aplicable, la EC puede establecer cláusulas contractuales de respecto de obligaciones y derechos relacionados a la propiedad intelectual, de sus tecnologías y procesos tales como los derechos de autor, secretos de patentes, marcas comerciales, que ciertos participantes puedan usar, o especificar si es necesario obtener una licencia de uso.	RFC 3647 sección 4.9.5: Privacidad de información personal
104	Representaciones y garantías	La EC debe establecer regulaciones y garantías que aseguren que las prácticas de las diversas entidades involucradas están en conformidad con la CP o CPS. Por ejemplo, una CPS que sirve como un contrato puede contener algún tipo de garantía de la EC de que la información contenida en el certificado es exacta. Alternativamente, una CPS podría contener una menos extensa garantía al sentido de que la	RFC 3647 sección 4.9.6: Representaciones y garantías

		información contenida en el certificado es verdadera, ya que se realizaron procedimientos de autenticación de la identidad. También se pueden incluir requisitos de que las representaciones y garantías aparezcan en ciertos acuerdos, como el acuerdo del suscriptor o tercero que confía. Por ejemplo, una CP puede contener el requisito de que todas las entidades de registro utilicen un acuerdo de suscriptor, y que dicho acuerdo debe contener una garantía exigida por la EC.	
105	Excepciones de responsabilidad de garantías	La EC debe incluir en su CPS la negación de garantías expresas que de otra manera se entenderá que existen en un acuerdo, y excepciones de responsabilidad de garantías implícitas que de otra manera pueden ser impuestas por la legislación aplicable, tales como las garantías mercantiles o de aptitud para un propósito determinado. El CP o CPS debe indicar expresamente dichas renuncias, o en su defecto indicar que las renuncias aparecen en acuerdos asociados, como los acuerdos del suscriptor o terceros que confían. No cabe excepción de responsabilidad para aquellas	RFC 3647 sección 4.9.7: Excepciones de responsabilidad de garantías

		garantías establecidas por la legislación vigente. La EC debe establecer en su CPS o en los contratos del suscriptor o tercero que confía, cláusulas de garantía y responsabilidad, incluyendo limitaciones y excepciones, si fueran aplicables.	
106	Notificaciones y comunicaciones entre participantes	La EC debe declarar los mecanismos de comunicación con sus clientes y otros participantes. Por ejemplo, una ER podría informar a la EC que desea terminar su acuerdo con ésta. Este requisito es diferente a las publicaciones y repositorios, ya que aquellas esta dirigidas a una amplia audiencia de destinatarios, en este requisito se plantean comunicaciones individuales entre participantes. Se deberá establecer mecanismos de comunicación e indicará el procedimiento para dirigir este tipo de comunicaciones, tales como un mensaje firmado digitalmente, comunicaciones de correo electrónico a una dirección especificada, seguido por un acuse de recibo, o por correo electrónico de recibo firmado. Los cambios en las políticas y	

		prácticas de los PSC acreditados deben ser notificados a los suscriptores, terceros que confían y otras partes tales como otras infraestructuras cuando dichos cambios puedan afectarles. Cualquier cambio en los términos y condiciones básicas deberá ser notificado a los suscriptores y terceros que confían.	
107	Correcciones o enmiendas	Ocasionalmente será necesario modificar una CP o CPS. Algunos de estos cambios no reducirán significativamente la seguridad de que una CP o su implementación ofrecen. El administrador de la política juzgará si tiene un efecto sobre la aceptabilidad de certificados. Tales cambios en una CP o CPS no imponen un cambio en el OID de la CP o el puntero de la CPS (URL). Por otro lado, algunas modificaciones cambiarán sustancialmente la aceptabilidad de certificados para fines específicos, y puede requerirse un OID de la CP o un puntero (URL) de la CPS distintos, en tales casos la EC debe comunicar estos cambios al INDECOPI. La EC también debe establecer la siguiente información: • Los procedimientos mediante los cuales la CP o CPS y / u otros documentos deben o	RFC 3647 sección 4.9.12: Correcciones o enmiendas

		pueden ser modificados. En el caso de las enmiendas de la CP o CPS, los procedimientos de cambio pueden incluir un mecanismo de notificación para proporcionar la notificación de las enmiendas propuestas a las partes afectadas, tales como suscriptores y partes de confianza, un período de comentarios, un mecanismo por el que los comentarios son recibidos, crítica e incorporación al documento, y un mecanismo por el cual se hacen modificaciones finales y efectivas. • Las circunstancias en que las enmiendas a la CP o CPS llevarían a cambiar el OID de la CP o el puntero de la CPS (URL). • Los cambios efectuados a las políticas y prácticas documentadas deben ser revisados por INDECOPI.	
108	Procedimiento de resolución de disputas	La EC debe establecer los procedimientos a utilizarse para resolver disputas que surjan de discrepancias frente a los establecido en la CP, CPS, y/o acuerdos vinculantes. Ejemplos de tales procedimientos incluyen requisitos para que las disputas sean resueltas en cierto foro o por mecanismos alternativos de solución de controversias. De ser posible y permitido por las leyes correspondientes, debe considerarse el empleo de resolución de disputas en línea.	

109	Conformidad con la Ley aplicable	La EC debe declarar que la legislación de una determinada jurisdicción rige la interpretación y la ejecución de la CP, CPS o acuerdos.	RFC 3647 sección 4.9.14: Ley aplicable
110	Cumplimiento de la Ley aplicable	Esta sección se refiere a los requisitos establecidos para que los participantes cumplan con la legislación aplicable respecto de sus operaciones, por ejemplo, las leyes relativas a hardware y software criptográfico que puede estar sujeto a leyes de control de exportación de una jurisdicción determinada. El CP o CPS podría imponer dichos requisitos o puede requerir que tales disposiciones aparezcan en otros acuerdos. "La EC debe identificar, en su CPS, u otra documentación relevante o en su sitio web, la ley aplicable a sus operaciones de acuerdo a la Ley N° 27269, Ley de Firmas y Certificados Digitales, su reglamento aprobado por el D.S. 052-2008-PCM y sus modificatorias. Los requerimientos legalmente significativos deben de estar establecidos o referenciados en los contratos de suscriptores y terceros que confían.	RFC 3647 sección 4.9.15: Cumplimiento de la Ley aplicable

111	Limitaciones de responsabilidad	La EC debe incluir limitaciones de responsabilidad en una CP, CPS o en acuerdos asociados, como un acuerdo del suscriptor o terceros que confían. Estas limitaciones pueden caer en una de dos categorías: limitaciones en los elementos de daños y perjuicios exigibles y limitaciones en la cantidad de los daños recuperables, también conocido como límites de la responsabilidad. A menudo, los contratos contienen cláusulas que impiden la recuperación de elementos de daños tales como daños incidentales y consecuentes, y a veces daños punitivos. Con frecuencia, los contratos contienen cláusulas que limitan la posible recuperación de una parte o la otra para una cantidad determinada o en un importe correspondiente a un punto de referencia, tales como la cantidad que un proveedor se pagó en virtud del contrato. Los derechos y los deberes asociados a la condición de EC, no podrán ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad podrá subrogarse en la posición jurídica de dichas entidades. La EC acreditada debe establecer en su documentación	RFC 3647 sección 4.9.8: Limitaciones de responsabilidad

		cualquier limitación en la subrogación de derechos o delegación de obligaciones. La EC debe establecer en su CPS o en los contratos del suscriptor o tercero que confía, cualquier limitación de responsabilidad que fuera aplicables.	
112	Indemnizaciones	La EC debe incluir en su CPS disposiciones por las cuales una de las partes hace un conjunto de pagos por pérdidas o daños que afectan a la segunda parte, normalmente resultantes de actuaciones de la primera parte. Pueden aparecer en una CP, CPS, o en un acuerdo. Por ejemplo, una CP puede requerir que los acuerdos de suscriptor contengan un término en el que el abonado es responsable de indemnizar a una entidad emisora de las pérdidas de la EC emisora que surjan de declaraciones fraudulentas de un suscriptor en la solicitud de certificado en virtud del cual la EC emitió el certificado incorrecto. Del mismo modo, una CPS puede decir que una EC utiliza un acuerdo de las partes, en virtud del cual las partes de confianza son responsables para indemnizar a una entidad emisora de las pérdidas de la EC sostiene que surja del uso de un certificado sin	RFC 3647 sección 4.9.9: Indemnizaciones

		comprobar debidamente la información de revocación o el uso de un certificado para propósitos más allá de lo permitido por la EC La EC debe establecer en su CPS o en los contratos del suscriptor o tercero que confía, cualquier obligación de indemnización que fuera aplicable.	
113	Vigencia y conclusión	La EC debe incluir el período de tiempo en el que una CP o CPS sigue vigente y las circunstancias en que el documento, partes del documento, o su aplicabilidad a una determinada participante puede terminarse. Además, la CP o CPS puede indicar los requisitos, duración y cláusulas de terminación aparezcan en los acuerdos, como los acuerdos de suscriptor o terceros de confianza acuerdos. En particular, tales condiciones pueden incluir: • El término de un documento o acuerdo, es decir, cuando el documento se hace efectivo y cuando expira si no es capitulado primero. • Disposiciones de terminación que indica las circunstancias bajo las cuales los documentos, ciertas partes del mismo, o su aplicación a un participante en particular deja de permanecer en vigor. • Las consecuencias de la terminación del documento. Por ejemplo, ciertas disposiciones de un acuerdo	RFC 3647 sección 4.9.10: Termino y terminación

		pueden sobrevivir a su terminación y permanecerá en vigor. Los ejemplos incluyen los reconocimientos de derechos de propiedad intelectual y disposiciones sobre confidencialidad. Además, la terminación puede desencadenar la responsabilidad de las partes en devolver información confidencial a la parte que la divulgó.	
114	Provisiones misceláneas	La EC debe incluir en su CP, CPS o en los contratos varias disposiciones que pueden incluir: • Una cláusula de acuerdo íntegro, que normalmente identifica el documento o documentos que comprenden la totalidad del acuerdo entre las partes y establece que tales acuerdos reemplazan todos los previos y contemporáneos escritos o comprensiones orales relativos a la misma materia; • Una cláusula de asignación, que puede actuar para limitar la capacidad de una parte en un acuerdo, en la asignación de sus derechos en virtud del acuerdo respecto de la otra parte (tales como el derecho a recibir una serie de pagos en el futuro) o limitar la capacidad de una parte para delegar sus obligaciones en virtud del acuerdo; • Una cláusula de divisibilidad, que establece las intenciones de las partes en el caso de que una corte u otro tribunal determine que una cláusula dentro de un acuerdo es, por alguna razón, no válida o de propósito inaplicable, y cuyo	RFC 3647 sección 4.9.16: Provisiones misceláneas

		es con frecuencia para evitar la inaplicabilidad de una cláusula de causar la inaplicabilidad de todo el acuerdo; y • Una cláusula de ejecución, lo que puede indicar que una parte predominante en cualquier disputa que surja de un acuerdo tiene derecho a honorarios de abogados como parte de su recuperación, o pueden indicar que la renuncia de una parte de un incumplimiento de contrato no constituye una renuncia continua o una renuncia futura de otros incumplimientos de contrato. • Una cláusula de fuerza mayor, comúnmente usado para excusar el comportamiento de una o más partes en un acuerdo debido a un evento fuera del control razonable de la parte afectada o partes. típicamente, la duración de la actuación justificada sea acorde con la duración de la demora causada por el evento. La cláusula también puede prever la conclusión del acuerdo en virtud de circunstancias y condiciones especificadas. Los eventos que se consideran constitutivas de "fuerza mayor" puede incluir los llamados "actos de Dios", las guerras, terrorismo, huelgas, desastres naturales, fallas de ejecución de los proveedores o vendedores, o fallas de Internet u otra infraestructura. Las cláusulas de fuerza mayor deben ser redactadas de forma que sean coherentes con otras partes de la estructura y sean	

		aplicables a acuerdos de nivel de servicio. Por ejemplo, las responsabilidades y capacidades para la continuidad del negocio y recuperación de desastres pueden colocar algunos eventos dentro del control razonable de las partes, tales como la obligación de mantener la energía eléctrica de respaldo frente a cortes de energía. En caso de existir, estas cláusulas deben ser establecidas explícitamente en los contratos de suscriptor y tercero que confía.	
115	Otras provisiones	La EC debe incluir en su CPS o en los contratos otras disposiciones donde las responsabilidades y los términos que no encajan perfectamente dentro de una de las secciones anteriores pueden ser impuestas a los participantes de la PKI.	RFC 3647 sección 4.9.17: Otras provisiones

1.2.16. Registro de tiempo

Registro de tiempo		
Explicación preliminar: Los registros de tiempo contenidos en los certificados y en las CRL deben ser confiables		
No	Requerimiento	Referencia

116	Fuente de tiempo confiable	a) La EC debe utilizar una fuente de tiempo confiable reconocida por el BIPM para registrar los periodos de vigencia de los certificados digitales y de la CRL. b) La sincronización con la fuente de tiempo confiable debe ser menor a 1s.	RFC 3628 – Política de Requerimientos para Autoridades de Sellado de Tiempo

1.2.17. Identificador único de certificados

Objeto Identificador			
Explicación preliminar: El registro debe ser provisto por una organización internacional autorizada para evitar la confusión entre las aplicaciones.			
No	Requerimiento		Referencia
117	Generación del OID	a) La EC debe utilizar un identificador único para los certificados digitales y las respectivas políticas de certificación, cuyo arco debe ser provisto por una organización internacional autorizada por la ITU. b) Los algoritmos OID deben estar de conformidad con el RF5280 y RFC 5758.	

1.2.18. Perfiles de los certificados, CRL y OCSP

Perfiles de los certificados, CRL y OCSP			
Explicación preliminar: Los perfiles de los certificados y la CRL deben ser conformes con la RFC 5280			
No	Requerimiento		Referencia
118	Perfil del certificado	La EC debe definir en su CP, CPS u otro documento normativo temas como los siguientes • Número (s) de versión compatible: X.509 v3 (El perfil de los certificados debe ser conforme a ISO 9594/X.509) • Identificadores de algoritmos objetos de cifrado: Mínimo RSA 2048 y familia SHA-2 • Formato conforme a la RFC 5280 • El contenido del campo “uso de clave” del certificado debe diferenciarse entre las claves de firmado, autenticación y cifrado. Los bits CertSign y CRLSign, sólo deben ser utilizados por ECs acreditadas. • Se debe soportar y usar las extensiones de certificado X.509 v3. • Restricciones de nombres utilizados y las formas de nombres utilizados en el nombre; • OID de la Política de Certificación aplicable (s); • Extensiones de restricciones de uso de la Política; • Calificadores de sintaxis y semántica de las políticas; y • Procesamiento de semántica para las extensiones críticas de la política.	RFC 3647 sección 4.7.1: Perfil del certificado
119	Perfil CRL	La EC debe definir en su CP, CPS u otro documento normativo temas como los	RFC 3647 sección 4.7.2: Perfil de CRL

		siguientes: • Número (s) de versión compatible: X.509 v2 • Formato conforme a la RFC 5280 • CRL y su criticidad.	
120	Perfil OCSP	La EC debe definir en su CP, CPS u otro documento normativo temas como los siguientes • Formato conforme a la RFC 6960	RFC 3647 sección 4.7.3: Perfil de OCSP