ANEXO I:

MARCO DE LA POLÍTICA DE REGISTRO PARA LA EMISIÓN DE CERTIFICADOS DIGITALES

1. ENTIDAD DE REGISTRO

1.1. Declaración e implantación de las Prácticas de Registro

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

Los controles establecidos en el documento RPS 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 RPS.

A continuación, se describen los requerimientos que deben ser implementados en los procedimientos y operación de la Entidad de Registro y que además deben ser declarados en su documento RPS.

1.2. Provisiones

1.2.1. Introducción y alcance del servicio

Gestión del documento			
Explicación preliminar: Puesto que el documento Declaración de Prácticas de Registro es un documento normativo, que implica una obligación frente a los clientes de la ER, este documento debe ser adecuadamente gestionado a fin de mantener su autenticidad, vigencia, actualización y publicación.			
No	Requerimiento		Referencia
1	Introducción	En esta sección la ER puede identificar e introducir el conjunto de disposiciones que serán descritas en su RPS, e indicar los tipos de entidades y aplicaciones para las que el documento está dirigido.	
2	Visión general	En esta sección la ER puede ofrecer una introducción general al documento RPS. También se puede proporcionar una sinopsis de la PKI a los que se aplica el RPS.	
3	Nombre e identificación del documento	El documento de declaración deberá tener un código identificador, el cual deberá ser colocado de manera visible en la carátula del documento	
4	Control de	El documento deberá mostrar	

	versiones	en la carátula, el control de versiones respectivo.	
5	Participantes	La ER 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 espaciales, 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 ER puede ser más restringida que aquella establecida bajo el marco de la IOFE. La RPS de la ER debe detallar los requerimientos que se deben cumplir para ser	RFC 3647 sección 4.1.3: Participantes PKI

		considerados como terceros que confían dentro del ámbito de dicha ER	
6	Organización que administra los documentos de la ER	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 elaboración de los documentos normativos de la ER, en conformidad con la RFC 3647.	
7	Persona de contacto	Indicar los datos de contacto y canal de comunicación por el cual los terceros que confían y los titulares y los suscriptores de los certificados puedan referir sus consultas.	
8	Definiciones y Acrónimos	Esta sección debe contener una lista de definiciones de términos utilizados en el documento, así como una lista de siglas contenidas en el mismo y sus significados.	
9	Protección de integridad del documento	La RPS deberá ser firmada digitalmente con un certificado digital a nombre de la Entidad responsable o a nombre de la persona que determina la conformidad de la RPS. El formato del documento firmado	

		deberá permitir la verificación de la firma en formato PDF o XML. El certificado digital empleado deberá ser emitido por una EC reconocida por la IOFE.	
10	Publicación y difusión del documento	La ER debe publicar su RPS al entrar en operación con el logro de la acreditación, a través de un medio público que permita su constante consulta por parte de titulares, suscriptores y terceros que confían.	
11	Frecuencia de publicación	La ER deberá indicar la frecuencia con la cual es actualizado y publicado el documento. El documento RPS debe ser validado en las revisiones de supervisión que realiza la AAC siempre y cuando se hayan realizado actualizaciones. En caso de actualizaciones mayores estas deben ser presentadas a la AAC antes de realizar la modificación del documento. Una actualización mayor es aquella que afecta a los procesos de registro o verificación de identidad.	

12	Responsabilidades del suscriptor	Un suscriptor o titular debe estar obligado a cumplir las obligaciones de suscriptor establecidas en la CPS de la EC que emitirá su certificado digital. 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. Las obligaciones del suscriptor o titular pueden incluir una garantía de la exactitud de la	

		información provista en las aplicaciones del certificado, acordando la protección de claves y certificados frente a malos usos y el acuerdo de no empleo de las claves y certificados fuera del alcance de la IOFE. 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.	
13	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.	

14	Terceros contratistas	En caso de tercerizar las funciones de registro, las responsabilidades de los terceros deberán ser claramente definidas en la RPS. Sin embargo, la responsabilidad legal frente a la IOFE, los suscriptores, titulares y terceros que confían es de la entidad solicitante de la acreditación de la Entidad de Registro. La Entidad de Registro debe garantizar la seguridad y protección de los datos personales y confidenciales de la ER, así como la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, re-emisión, durante la ejecución de las actividades de tercerización.	

1.2.2. Certificados Digitales

Certificados digitales
Explicación preliminar: Existen diversos tipos de certificados digitales que una ER puede proporcionar, según su aplicación o propósito, según los procedimientos de registros establecidos por su respectiva EC, etc. Es necesario, que cada tipo de certificado relacionado a los servicios de registro de la ER sea descrito en el presente documento.

No	Requerimiento		Referencia
15	Certificados digitales (proporcionados por la EC, mediante los servicios de validación de la ER), uso apropiado	La ER deberá indicar los tipos de certificados digitales que ofrecerá como parte de sus servicios de registro, 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. Una EC puede brindar distintos 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	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 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 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.	

1.2.3. Solicitud de certificados de persona natural

Solicitud de certificados de persona natural			
Explicación preliminar: Antes de ser emitidos los certificados a personas naturales, que evidencien el no repudio de sus acciones, la ER debe garantizar que la persona natural es quien dice ser, y que no se trata de un intento de suplantación de identidad. Las personas naturales son tanto titulares como suscriptores de los certificados.			
No	Requerimiento		Referencia
16	Descripción de procedimientos	La ER debe describir cada procedimiento de validación de identidad que aplique para proporcionar certificados digitales a personas naturales, conforme al tipo de certificado a proporcionar De existir varios tipos de certificados para personas naturales, con procedimientos distintos de validación, todos estos procedimientos deberán ser declarados en la RPS.	

17	Verificación presencial	Los certificados de firma digital que garantizan el no repudio, deben ser emitidos luego de una verificación presencial de identidad realizada por parte de la ER. La ER podría realizar la verificación presencial por medio de un Notario Público autorizado por la AAC, u otra entidad autorizada o reconocida por la AAC. Los procedimientos de validación de identidad deberán estar descritos en el documento RPS de la ER y deberán ser conformes con la CPS o CP.	
18	Verificación mediante consulta a bases de datos nacionales	La identidad del solicitante debe ser verificada: • En el caso de ciudadanos peruanos, por las bases de datos del RENIEC o el sistema de verificación biométrica AFIS. (El PSC debe presentar los convenios respectivos con el RENIEC para cualquiera de estos mecanismos). • En el caso de extranjeros, por las bases de datos de Migraciones	
19	Verificación de los datos de la solicitud	La ER debe validar que los datos de la solicitud del certificado que es remitida a la EC para la emisión del certificado	

		correspondan a los datos de la identidad validada. A fin de impedir la suplantación de identidad, es preciso que se verifiquen que los datos incluidos en la solicitud PKCS 10 corresponden a la identidad validada	
20	No repudio de la solicitud	La solicitud de un certificado digital debe ser realizada por medios no repudiables, a fin de garantizar su autenticidad y no repudio.	
21	Aprobación o rechazo de la solicitud	La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE o si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento. Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales deben ser asumidas por la ER. En caso de cumplir con todos los requerimientos descritos en el presente documento y en la RPS, la ER debe comunicar a la EC la autorización de la solicitud y	

		solicitar al suscriptor o titular la firma del contrato correspondiente.	
22	No repudio de la invitación de generación de claves e instalación del certificado	La invitación para la generación de claves e instalación del certificado debe realizarse a través de un medio sobre el cual, sólo el suscriptor verificado tiene control, incluyendo el uso de módulos criptográficos que se encuentran bajo el control exclusivo de los suscriptores. En caso de realizarse la generación de claves fuera de las instalaciones de la ER, la petición PKCS#10 debe ser realizada a través de medios de comunicación no repudiables, de modo que no pueda ocurrir una suplantación de la petición PKCS#10.	
23	Contrato del suscriptor	El solicitante deberá firmar mediante un mecanismo no repudiable reconocido por la IOFE, el contrato del suscriptor. El contrato del suscriptor establece las responsabilidades de la ER en caso de compromiso de las claves del suscriptor o casos de suplantación de identidad ocasionado por las operaciones de registro.	

		Asimismo, deberá establecer las responsabilidades del titular y los términos y condiciones aplicables a los certificados de conformidad con la legislación de la materia, para garantizar el efecto legal de las transacciones realizadas empleando un certificado emitido por dicha EC, así como las consecuencias de no cumplir con el acuerdo. El contrato debe incluir la responsabilidad de los titulares y suscriptores de solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias: - Por exposición, puesta en peligro o uso indebido de la clave privada - Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada - Revocación de las facultades de representación y/o poderes de 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 los estipulado en el contrato del suscriptor y/o titular - Por decisión de la legislación respectiva. NOTA: En caso de cambios menores respecto a la información del titular que no tengan mayor impacto en los terceros que confían, puede no ser necesaria la revocación del certificado existente ni la emisión de uno nuevo. La ER debe establecer en el contrato de los suscriptores y titulares provisiones de garantía y responsabilidad, incluyendo limitaciones y exclusiones.	
24	Tiempo de procesamiento	La ER debe establecer en su RPS u otra documentación relevante el tiempo necesario para el procesamiento de solicitudes.	

1.2.4. Solicitud de certificados de persona jurídica – atributos

Solicitud de certificados de persona jurídica - atributos			
Explicación preliminar: Antes de ser emitidos los certificados a personas jurídicas, que evidencien el no repudio de sus acciones, la ER debe garantizar que la persona jurídica es quien dice ser, y que no se trata de un intento de suplantación de identidad. La persona jurídica adopta el papel de titular del certificado y las personas naturales (sus empleados) vienen a ser los suscriptores de los certificados. Los suscriptores de la persona jurídica deben estar de acuerdo con la responsabilidad que implica el obtener el certificado digital de atributos, por lo que la ER debe verificar que el suscriptor declarado por la persona jurídica está de acuerdo, y es quien recibe el certificado digital, y que no se trata de una suplantación de identidad de suscriptores.			
No	Requerimiento		Referencia
25	Descripción de procedimientos	La ER debe describir los procedimientos de validación de identidad de las personas jurídicas, conforme al tipo de certificado a proporcionar. De existir varios tipos de certificados de atributos, con procedimientos distintos de validación, todos estos procedimientos deberán ser declarados en la RPS	
26	Acreditar la existencia de la	El Representante Legal o una persona asignada por él deberá	

	persona jurídica	acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva.	
27	Reconocimiento de nombres y marcas registradas	La ER debe solicitar la documentación o información necesaria para garantizar que un nombre o marca pertenece al solicitante o representado de un certificado digital. En el caso de validación 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 resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.	
28	Acreditar las facultades del solicitante	El solicitante de los certificados deberá acreditar, mediante el documento legal respectivo o consulta a la base de datos respectiva, sus facultades como representante.	
29	Verificación mediante	La identidad de la persona jurídica debe ser verificada:	

	consulta a bases de datos nacionales	• En el caso de empresas con domicilio en Perú, la existencia y vigencia de la persona jurídica deberá acreditarse con el documento o consulta electrónica de vigencia emitidos por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente, se debe verificar también mediante la base de datos de SUNAT que el RUC se encuentre activo y habido. • En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente o consulta en línea expedida por la autoridad competente en su país de origen.	
30	Verificación de los datos de la solicitud	La ER debe validar que los datos de la solicitud del certificado emitida a la EC correspondan a los datos de la identidad validada.	
31	Aprobación o rechazo de la solicitud	La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE o si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este	

		documento. Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales deben ser asumidas por la ER. En caso de cumplir con todos los requerimientos descritos en el presente documento y en la RPS, la ER debe comunicar a la EC la autorización de la solicitud y solicitar al suscriptor o titular la firma del contrato correspondiente.	
32	Contrato del titular	El solicitante deberá firmar mediante un mecanismo no repudiable reconocido por la IOFE, el contrato del titular. El contrato del titular establece las responsabilidades de la ER en caso de compromiso de las claves del suscriptor o casos de suplantación de identidad, ocasionados por las operaciones de la ER. Asimismo, deberá establecer las responsabilidades del titular y los términos y condiciones aplicables a los certificados de conformidad con la legislación de la materia, para garantizar el efecto legal de las transacciones realizadas	

		empleando un certificado emitido por dicha EC, así como las consecuencias de no cumplir con el acuerdo. El contrato debe incluir la responsabilidad de los titulares y suscriptores de solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias: - Por exposición, puesta en peligro o uso indebido de la clave privada - Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada - Revocación de las facultades de representación y/o poderes de 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 los estipulado en el contrato del suscriptor y/o titular - Por decisión de la legislación	

		respectiva. NOTA: En caso de cambios menores respecto a la información del titular que no tengan mayor impacto en los terceros que confían, puede no ser necesaria la revocación del certificado existente ni la emisión de uno nuevo. La ER debe establecer en el contrato de los suscriptores y titulares provisiones de garantía y responsabilidad (seguros bancarios), incluyendo limitaciones y exclusiones.	
33	No repudio de la solicitud	La solicitud de certificados por parte de la persona jurídica debe ser realizada por medios no repudiables.	
34	Asignación de suscriptores	El representante autorizado, cuya identidad haya sido validada por la ER, designará a los suscriptores que recibirán certificados digitales en nombre de la persona jurídica, por medios no repudiables.	
35	Verificación de la identidad de los suscriptores	La identidad de los aspirantes a suscriptores debe ser verificada por la ER o un Notario Público	

		autorizado por la AAC, u otra entidad autorizada o reconocida por la AAC, en convenio con la ER, en cuya presencia se debe firmar el contrato del suscriptor, garantizando que el suscriptor acepta las responsabilidades que conlleva el uso del certificado digital de persona jurídica, a través de la firma del Contrato del suscriptor o un documento de aceptación de dichas responsabilidades. A fin de impedir la suplantación de identidad de suscriptores, o la asignación de responsabilidades sin contar con la autorización del empleado que adoptará el rol del suscriptor.	
36	Verificación de las facultades laborales de los suscriptores	En el caso que un certificado sea solicitado para acreditar el ejercicio de un cargo en concreto, la ER debe requerir a este solicitante las pruebas que evidencien su cargo, incluyendo las limitaciones y facultades de actuar como empleado de la persona jurídica correspondientes a dicho cargo.	
37	Verificación de los datos de la solicitud	La ER debe validar que los datos de la solicitud del certificado que es remitida a la EC para la	

		emisión del certificado correspondan a los datos de la identidad validada. A fin de impedir la suplantación de identidad, es preciso que se verifiquen que los datos incluidos en la solicitud PKCS 10 corresponden a la identidad validada	
38	Información no verificada del suscriptor o titular	De manera general, no debe incluirse en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se debe comprobar que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. Pero, la ER no tiene que comprobar ni la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, todo es responsabilidad del solicitante.	
39	No repudio de la invitación de generación de claves e instalación del	La invitación para la generación de claves e instalación del certificado debe realizarse a través de un medio sobre el cual, sólo el suscriptor verificado tiene	

	certificado	control, incluyendo el uso de módulos criptográficos que se encuentran bajo el control exclusivo de los suscriptores. La ER debe implementar políticas para asegurar que los medios no son compartidos, como por ejemplo: solicitar que se actualicen las contraseñas de usuario en los computadores o correos electrónicos, y que se brinden charlas de concientización. En caso de realizarse la generación de claves fuera de las instalaciones de la ER, la petición PKCS#10 debe ser realizada a través de medios de comunicación no repudiables, de modo que no pueda ocurrir una suplantación de la petición PKCS#10.	
40	Conformidad del titular	El titular deberá expresar su conformidad respecto de la re-emisión del certificado y las responsabilidades implicadas, de conformidad con la legislación de la materia, para garantizar el efecto legal de las transacciones realizadas empleando un certificado emitido por dicha EC, así como las consecuencias de	

		no cumplir con el acuerdo.	
41	Tiempo de procesamiento	La ER debe establecer en su RPS u otra documentación relevante el tiempo necesario para el procesamiento de solicitudes.	

1.2.5. Solicitud de certificados de persona jurídica – agentes automatizados

Solicitud de certificados de persona jurídica – agentes automatizados			
Explicación preliminar: Antes de ser emitidos los certificados a personas jurídicas, para ser usados por agentes automatizados, la ER debe garantizar que la persona jurídica es quien dice ser, y que no se trata de un intento de suplantación de identidad.			
No	Requerimiento		Referencia
42	Descripción de procedimientos	La ER debe describir los procedimientos de validación de identidad de las personas jurídicas para certificados digitales a ser usados por agentes automatizados, conforme al tipo de certificado a proporcionar. De existir varios tipos de certificados para agentes automatizados, con procedimientos distintos de	

		validación, todos estos procedimientos deberán ser declarados en la RPS.	
43	Acreditar la existencia de la persona jurídica	El Representante Legal o una persona asignada por él deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva.	
44	Acreditar las facultades del solicitante	El solicitante de los certificados deberá acreditar, mediante el documento legal respectivo, sus facultades como representante.	
45	Verificación mediante consulta a bases de datos nacionales	La identidad de la persona jurídica debe ser verificada: • En el caso de empresas con domicilio en Perú, la existencia y vigencia de la persona jurídica deberá acreditarse con el documento o consulta electrónica de vigencia emitidos por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente, se debe verificar también mediante la base de datos de SUNAT que el RUC se encuentre activo y habido. • En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de	

		vigencia de la sociedad u otro instrumento equivalente o consulta en línea expedida por la autoridad competente en su país de origen.	
46	Reconocimiento de nombres y marcas registradas	La ER debe solicitar la documentación o información necesaria para garantizar que un nombre o marca pertenece al solicitante o representado de un certificado digital. En el caso de validación 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 resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.	
47	Verificación de los datos de la solicitud	La ER debe validar que los datos de la solicitud del certificado emitida a la EC correspondan a los datos de la identidad validada.	
48	Aprobación o rechazo de la solicitud	La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE o si el	

		resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento. Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales deben ser asumidas por la ER. En caso de cumplir con todos los requerimientos descritos en el presente documento y en la RPS, la ER debe comunicar a la EC la autorización de la solicitud y solicitar al suscriptor o titular la firma del contrato correspondiente.	
49	Contrato del titular	El solicitante deberá firmar mediante un mecanismo no repudiable reconocido por la IOFE, el contrato del titular. El contrato del titular establece las responsabilidades de la ER en caso de compromiso de las claves del suscriptor o casos de suplantación de identidad, ocasionados por las operaciones de la ER. Asimismo, deberá establecer las responsabilidades del titular y los términos y condiciones aplicables a los certificados de conformidad con	

		la legislación de la materia, para garantizar el efecto legal de las transacciones realizadas empleando un certificado emitido por dicha EC, así como las consecuencias de no cumplir con el acuerdo. El contrato debe incluir la responsabilidad de los titulares y suscriptores de solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias: - Por exposición, puesta en peligro o uso indebido de la clave privada - Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada - Revocación de las facultades de representación y/o poderes de 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 los	

		estipulado en el contrato del suscriptor y/o titular - Por decisión de la legislación respectiva. NOTA: En caso de cambios menores respecto a la información del titular que no tengan mayor impacto en los terceros que confían, puede no ser necesaria la revocación del certificado existente ni la emisión de uno nuevo. La ER debe establecer en el contrato de los suscriptores y titulares provisiones de garantía y responsabilidad, incluyendo limitaciones y exclusiones.	
50	No repudio de la solicitud	La solicitud de un certificado digital debe ser realizada por medios no repudiables.	
51	Procedimiento de petición del certificado	La ER debe establecer el procedimiento para realizar la generación de las claves y de la petición del certificado digital a ser instalado en el sistema automatizado.	
52	No repudio de la petición del certificado	La petición del certificado digital debe ser realizada por medios no repudiables y asegurar que proviene de la identidad validada	

		y por las personas autorizadas. En caso de realizarse la generación de claves fuera de las instalaciones de la ER, la petición PKCS#10 debe ser realizada a través de medios de comunicación no repudiables, de modo que no pueda ocurrir una suplantación de la petición PKCS#10.	
53	Tiempo de procesamiento	La ER debe establecer en su RPS u otra documentación relevante el tiempo necesario para el procesamiento de solicitudes.	

1.2.6. Entidades de Certificación afiliadas a la ER

Entidades de Certificación afiliadas a la ER			
Explicación preliminar: La vinculación y las limitaciones de responsabilidad entre la ER y las ECs debe ser accesible por los clientes y terceros que confían, a fin de que cuenten con la información completa para seleccionar los servicios de registro y certificación digital.			
No	Requerimiento		Referencia
54	Publicación de Entidades	La ER debe publicar la lista de Entidades de certificación a las cuales representan o tienen afiliación para realizar las	

		actividades de registro.	
55	Publicación de CP y CPS	La ER debe publicar los documentos CP y CPS vigentes de las Entidades de Certificación a las cuales representan o tienen afiliación para realizar las actividades de registro.	
56	Publicación de certificaciones	La ER debe publicar los certificados o reportes de auditoría que acreditan el logro de la certificación Webtrust for Certification Authorities, Resolución de Acreditación o cualquiera de sus equivalentes reconocidos por la AAC, correspondientes a las Entidades de Certificación a las que se encuentra vinculada.	
57	Publicación de un documento que acredite representación de la EC	La ER deberá publicar un documento que acredite su vinculación con cada Entidad de Certificación a la cual desee representar.	
58	Limitación de responsabilidades	La ER deberá publicar un documento que exprese las limitaciones de responsabilidad respecto de cada EC con la que tenga vinculación. Este documento deberá ser firmado por la respectiva EC. Se deben describir las responsabilidades	

		de la EC y de la ER respecto de cada acuerdo de vinculación. Las responsabilidades deberán cubrir los temas de compensación y garantías ofrecidas a los usuarios por casos de suplantación de identidad ocasionados por las operaciones de la Entidad de Registro o por las Entidades de Certificación.	

1.2.7. Re-emisión de certificados de personal natural

Re-emisión de certificados de persona natural			
Explicación preliminar: La re-emisión de certificado es un proceso que debe realizarse para obtener un nuevo par de claves y un nuevo certificado cuando su fecha de expiración es cercana, o el certificado haya expirado.			
No	Requerimiento		Referencia
59	Descripción de procedimientos	La ER debe describir los procedimientos de validación de identidad de las personas naturales para la re- emisión de sus certificados digitales, conforme al tipo de certificado a proporcionar. De existir varios tipos de certificados para personas naturales con procedimientos	RFC 3647 sección 4.3.3: Identificación y Autenticación para solicitudes de re-emisión de claves

		distintos de validación, todos estos procedimientos deberán ser declarados en la RPS.	
60	Frecuencia de re-emisión	La re-emisión sólo puede ser realizada una vez, para certificados cuya fecha de expiración es menor o igual a un año, antes de cumplirse el periodo de vigencia. El certificado re-emitido debe tener un periodo de vigencia máximo de un año. En el caso de certificados revocados o expirados, se deberá seguir el procesamiento inicial de verificación de identidad.	
61	Solicitantes	Sólo los titulares de certificados pueden solicitar la re-emisión de certificados.	
62	No repudio de la solicitud	La solicitud de re-emisión de un certificado digital debe ser realizada por medios confiables, a fin de garantizar su autenticidad y no repudio. O una tecnología acordada previamente en el contrato del suscriptor. No es indispensable la solicitud presencial. No puede utilizarse el certificado	

		expirado o revocado para realizar la solicitud. Por ejemplo, la solicitud de re-emisión puede ser realizada por un certificado vigente, por la intervención de una solicitud firmada por un Notario Público autorizado o por una entidad autorizada por la AAC.	
63	Verificación de los datos de la solicitud	La ER debe validar que los datos de la solicitud del certificado que es remitida a la EC para la emisión del certificado correspondan a los datos de la identidad validada. A fin de impedir la suplantación de identidad, es preciso que se verifiquen que los datos incluidos en la solicitud PKCS#10 corresponden a la identidad validada	
64	Aprobación o rechazo de la solicitud	La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE o si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento. Una EC puede decidir establecer en su CPS u otra documentación	

		relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales deben ser asumidas por la ER. En caso de cumplir con todos los requerimientos descritos en el presente documento y en la RPS, la ER debe comunicar a la EC la autorización de la solicitud y solicitar al suscriptor o titular la firma del contrato correspondiente.	
65	No repudio de la invitación de generación de claves e instalación del certificado	La invitación para la generación de claves e instalación del certificado debe realizarse a través de un medio sobre el cual, sólo el suscriptor verificado tiene control, incluyendo el uso de módulos criptográficos que se encuentran en posesión de los suscriptores o los casos de generación en sistemas centralizados de gestión de claves. La ER debe implementar políticas para asegurar que los medios no son compartidos, como por ejemplo: solicitar que se actualicen las contraseñas de usuario en los computadores o correos electrónicos, y que se brinden charlas de concientización.	

		En caso de realizarse la generación de claves fuera de las instalaciones de la ER, la petición PKCS#10 debe ser realizada a través de medios de comunicación no repudiables, de modo que no pueda ocurrir una suplantación de la petición PKCS#10.	
66	Contrato del suscriptor	El solicitante deberá firmar mediante un mecanismo no repudiable reconocido por la IOFE, el contrato del titular. El contrato del suscriptor establece las responsabilidades de la ER en caso de compromiso de las claves del suscriptor o casos de suplantación de identidad ocasionado por las operaciones de registro. Asimismo, deberá establecer las responsabilidades del titular y los términos y condiciones aplicables a los certificados de conformidad con la legislación de la materia, para garantizar el efecto legal de las transacciones realizadas empleando un certificado emitido por dicha EC, así como las consecuencias de no cumplir con el acuerdo. El contrato debe incluir la	

		responsabilidad de los titulares y suscriptores de solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias: - Por exposición, puesta en peligro o uso indebido de la clave privada - Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada - Revocación de las facultades de representación y/o poderes de 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 los estipulado en el contrato del suscriptor y/o titular - Por decisión de la legislación respectiva. NOTA: En caso de cambios menores respecto a la información del titular que no tengan mayor impacto en los	

		terceros que confían, puede no ser necesaria la revocación del certificado existente ni la emisión de uno nuevo. La ER debe establecer en el contrato de los suscriptores y titulares provisiones de garantía y responsabilidad, incluyendo limitaciones y exclusiones.	
67	Tiempo de procesamiento	La ER debe establecer en su RPS u otra documentación relevante el tiempo necesario para el procesamiento de solicitudes.	

1.2.8. Re-emisión de certificados de persona jurídica – atributos

Re-emisión de certificados de persona jurídica -atributos			
Explicación preliminar: La re-emisión de certificado es un proceso que debe realizarse para obtener un nuevo par de claves y un nuevo certificado cuando su fecha de expiración es cercana, el certificado haya expirado o haya sido revocado			
No	Requerimiento		Referencia
68	Descripción de procedimientos	La ER debe describir los procedimientos de validación de identidad de las personas jurídicas para la re-emisión de sus certificados digitales de	RFC 3647 sección 4.3.3: Identificación y Autenticación para solicitudes de re-emisión de claves

		atributos, conforme al tipo de certificado a proporcionar. De existir varios tipos de certificados para personas naturales con procedimientos distintos de validación, todos estos procedimientos deberán ser declarados en la RPS.	
69	Autorizado para realizar la solicitud	Sólo la persona autorizada y acreditada ante la ER puede realizar las solicitudes del certificado a nombre de la persona jurídica	
70	Frecuencia de re-emisión	En el caso de certificados expirados, la re-emisión sólo puede ser realizada una vez, para certificados cuya fecha de expiración es menor o igual a dos años. El certificado re-emitido debe tener un periodo de vigencia máximo de un año. En el caso de certificados revocados, la re-emisión requiere de una validación inicial de identidad.	
71	Solicitantes	Sólo los titulares de certificados pueden solicitar la re-emisión de certificados. Los suscriptores empleados de los certificados no podrán solicitar la re-emisión de	

		certificados.	
72	No repudio de la solicitud	La solicitud de re-emisión de un certificado digital debe ser realizada por medios no repudiables, a fin de garantizar su autenticidad y no repudio. O una tecnología acordada previamente en el contrato del suscriptor. No es indispensable la solicitud presencial. No puede utilizarse un certificado expirado para realizar la solicitud. Por ejemplo, la solicitud de re-emisión puede ser realizada por un certificado vigente, por la intervención de una solicitud firmada por un Notario Público autorizado o por una entidad autorizada por la AAC.	
73	Verificación de los datos de la solicitud	La ER debe validar que los datos de la solicitud del certificado que es remitida a la EC para la emisión del certificado correspondan a los datos de la identidad validada. A fin de impedir la suplantación de identidad, es preciso que se verifiquen que los datos incluidos en la solicitud PKCS#10	

		corresponden a la identidad validada	
74	Aprobación o rechazo de la solicitud	La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE o si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento. Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales deben ser asumidas por la ER. En caso de cumplir con todos los requerimientos descritos en el presente documento y en la RPS, la ER debe comunicar a la EC la autorización de la solicitud y solicitar al suscriptor o titular la firma del contrato correspondiente.	
75	No repudio de la invitación de generación de claves e instalación del certificado	La invitación para la generación de claves e instalación del certificado debe realizarse a través de un medio sobre el cual, sólo el suscriptor verificado tiene control, incluyendo el uso de módulos criptográficos que se encuentran en posesión de los	

		suscriptores o los casos de generación en sistemas centralizados de gestión de claves. La ER debe implementar políticas para asegurar que los medios no son compartidos, como por ejemplo: solicitar que se actualicen las contraseñas de usuario en los computadores o correos electrónicos, y que se brinden charlas de concientización. En caso de realizarse la generación de claves fuera de las instalaciones de la ER, la petición PKCS#10 debe ser realizada a través de medios de comunicación no repudiables, de modo que no pueda ocurrir una suplantación de la petición PKCS#10.	
76	Conformidad de los suscriptores	Los suscriptores deberán expresar su conformidad respecto de la re-emisión del certificado y las responsabilidades implicadas, a través de medios no repudiables.	
77	Tiempo de procesamiento	La ER debe establecer en su RPS u otra documentación relevante el tiempo necesario para el procesamiento de	

		solicitudes.	

1.2.9. Re-emisión de certificados de persona jurídica – agentes automatizados

Re-emisión de certificados de persona jurídica – agentes automatizados			
Explicación preliminar: La re-emisión de certificado es un proceso que debe realizarse para obtener un nuevo par de claves y un nuevo certificado cuando el certificado haya sido revocado.			
No	Requerimiento		Referencia
78	Descripción de procedimientos	La ER debe describir los procedimientos de validación de identidad de las personas jurídicas para la re-emisión de sus certificados digitales de atributos, conforme al tipo de certificado a proporcionar. De existir varios tipos de certificados para personas naturales con procedimientos distintos de validación, todos estos procedimientos deberán ser declarados en la RPS	
79	Autorizado para realizar la solicitud	Sólo la persona autorizada y acreditada ante la ER puede realizar las solicitudes del	

		certificado a nombre de la persona jurídica	
80	Frecuencia de re-emisión	La re-emisión de certificados para agentes automatizados sólo puede ser realizada una vez, cuando haya sido revocado un certificado digital antes de ser cumplido su periodo de vigencia.	
81	No repudio de la solicitud	La solicitud de re-emisión de un certificado digital debe ser realizada por medios no repudiables, a fin de garantizar su autenticidad y no repudio. O una tecnología acordada previamente en el contrato del suscriptor. No es indispensable la solicitud presencial. No puede utilizarse un certificado expirado para realizar la solicitud. Por ejemplo, la solicitud de re-emisión puede ser realizada por un certificado vigente, por la intervención de una solicitud firmada por un Notario Público autorizado o por una entidad autorizada por la AAC.	
82	Verificación de los datos de la solicitud	La ER debe validar que los datos de la solicitud del certificado que es remitida a la EC para la	

		emisión del certificado correspondan a los datos de la identidad validada. A fin de impedir la suplantación de identidad, es preciso que se verifiquen que los datos incluidos en la solicitud PKCS#10 corresponden a la identidad validada	
83	Aprobación o rechazo de la solicitud	La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE o si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento. Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales deben ser asumidas por la ER. En caso de cumplir con todos los requerimientos descritos en el presente documento y en la RPS, la ER debe comunicar a la EC la autorización de la solicitud y solicitar al suscriptor o titular la firma del contrato correspondiente.	

84	No repudio de la invitación de generación de claves e instalación del certificado	La invitación para la generación de claves e instalación del certificado debe realizarse a través de un medio sobre el cual, sólo la persona autorizada por el titular, cuya identidad haya sido verificada por la ER verificado tiene control. La ER debe implementar políticas para asegurar que los medios no son compartidos, como por ejemplo: solicitar que se actualicen las contraseñas de usuario en los computadores o correos electrónicos, y que se brinden charlas de concientización. En caso de realizarse la generación de claves fuera de las instalaciones de la ER, la petición PKCS#10 debe ser realizada a través de medios de comunicación no repudiables, de modo que no pueda ocurrir una suplantación de la petición PKCS#10.	
85	Tiempo de procesamiento	La ER debe establecer en su RPS u otra documentación relevante el tiempo necesario para el procesamiento de solicitudes.	

1.2.10. Revocación de certificados de persona natural o jurídica

Revocación de certificados de persona natural o jurídica			
Explicación preliminar: Una persona natural o jurídica que sospeche que su clave privada ha sido comprometida o puede ser utilizada sin su autorización, debe solicitar la revocación de su certificado. Las personas jurídicas cuyos empleados terminen su vinculación contractual deben también solicitar la revocación de sus respectivos certificados de atributos. Esta solicitud puede ser realizada directamente a la EC o a la ER.			
No	Requerimiento		Referencia
86	Descripción de procedimientos	La ER debe describir los procedimientos de validación de identidad de las personas naturales para la revocación de sus certificados digitales, conforme al tipo de certificado a proporcionar. De existir varios tipos de certificados para personas naturales con procedimientos distintos de validación, todos estos procedimientos deberán ser declarados en la RPS	RFC 3647 sección 4.4.9: Revocación y suspensión del certificado

87	Solicitantes	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 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.	
88	No repudio de la solicitud	La solicitud de revocación de un certificado digital debe ser realizada por medios no repudiables, a fin de garantizar su autenticidad y no repudio. O una tecnología acordada previamente en el contrato del suscriptor. No es indispensable la solicitud presencial. No puede utilizarse el certificado expirado o revocado para realizar la solicitud. Por ejemplo, la solicitud de	

		revocación puede ser realizada por un certificado vigente, por la intervención de una solicitud firmada por un Notario Público autorizado o por una entidad autorizada por la AAC.	
89	Aprobación o rechazo de la solicitud	La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE o si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento. Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales deben ser asumidas por la ER.	
90	Ejecución de la revocación	La ER debe publicar los tiempos máximos que puede tardar la ejecución de la revocación de los certificados, desde la solicitud de los titulares o suscriptores. Una vez aceptada la solicitud este tiempo no debe ser mayor a 2 horas para la actualización de la base de datos de las consultas OCSP y de 24 horas para la actualización de la lista CRL.	

91	Tiempo de procesamiento	La ER debe establecer en su RPS u otra documentación relevante el tiempo necesario para el procesamiento de solicitudes.	

1.2.11. Suspensión de certificados de persona jurídica

Suspensión de certificados de persona jurídica			
Explicación preliminar: Una persona jurídica puede solicitar la suspensión de los certificados digitales de sus suscriptores, por un periodo hasta cumplirse la fecha de expiración de sendos certificados.			
No	Requerimiento		Referencia
92	Descripción de procedimientos	La ER debe describir los procedimientos de validación de identidad de las personas jurídicas para la suspensión de sus certificados digitales, conforme al tipo de certificado a proporcionar. De existir varios tipos de certificados para personas naturales con procedimientos distintos de validación, todos estos procedimientos deberán ser declarados en la RPS	RFC 3647 sección 4.4.9: Revocación y suspensión del certificado
93	Solicitantes	Sólo los titulares de certificados o sus representantes autorizados y	

		acreditados ante la ER, pueden solicitar la suspensión de sus certificados digitales de atributos. Por ejemplo, para el caso de empleados que salen de vacaciones, se les suspende el certificado digital de atributos de modo que no pueda ser utilizado de manera inadecuada.	
94	Periodo de suspensión	El tiempo máximo en el que un certificado puede ser suspendido está limitado por su periodo de expiración.	
95	No repudio de la solicitud	La solicitud de suspensión de un certificado digital debe ser realizada por medios no repudiables, a fin de garantizar su autenticidad y no repudio. O una tecnología acordada previamente en el contrato del suscriptor. No es indispensable la solicitud presencial. No puede utilizarse el certificado expirado o revocado para realizar la solicitud. Por ejemplo, la solicitud de revocación puede ser realizada por un certificado vigente, por la intervención de una solicitud	

		firmada por un Notario Público autorizado o por una entidad autorizada por la AAC.	
96	Aprobación o rechazo de la solicitud	La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE o si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento. Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales deben ser asumidas por la ER.	
97	Tiempo de procesamiento	La ER debe establecer en su RPS u otra documentación relevante el tiempo necesario para el procesamiento de solicitudes.	

1.2.12. Protección de registros

Protección de los registros
Explicación preliminar: Los registros de las solicitudes de emisión, re-emisión, revocación, modificación o suspensión de certificados deben ser protegidas y almacenadas para servir como evidencia en caso de procesos judiciales.

No	Requerimiento		Referencia
98	Tipos de eventos registrados	• Información de contacto de los solicitantes de los servicios de la ER, incluyendo a suscriptores y titulares • Solicitudes de emisión, re-emisión, revocación, suspensión o modificación de certificados digitales, realizadas mediante un medio no repudiable por parte del titular y/o suscriptor de los certificados. • Resultados y evidencias de cada proceso de validación de identidad de persona jurídica o natural, incluyendo procesos con resultados positivos como procesos fallidos en los que se denegó el servicio a un cliente. • Contratos del suscriptor y titular. • Registros o evidencias de las solicitudes de emisión, re-emisión, revocación, suspensión o modificación de certificados digitales realizadas por parte de los operadores de registro a la Entidad de Certificación, indicando el operador de registro que realizó la transacción. • Registro de contratación de operadores de registro	

99	Protección de los registros	La ER debe restringir el acceso físico y lógico a la modificación y traslado, borrado de registros a personal responsable de la seguridad de la información de la ER, el cual debe ser distinto a los operadores de registro.	
100	Archivo de los registros	Los registros deben ser archivados para ser conservados íntegros en un lugar seguro, que posea los controles ambientales y físicos necesarios para garantizar su duración en el tiempo, incluyendo controles anti-incendios, acceso físico y aniego. Ningún personal no autorizado debe tener acceso al archivo de los registros.	
101	Tiempo de almacenamiento del archivo	La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años.	

1.2.13. Seguridad en las comunicaciones con la EC

Seguridad en las comunicaciones con la EC
Explicación preliminar: Las comunicaciones con la EC, respecto de las autorizaciones para la emisión, re-emisión, revocación, modificación o suspensión de

certificados deben ser seguras a fin de impedir ataques que puedan vulnerar los sistemas y permitir la suplantación de identidad de los clientes de la ER.			
No	Requerimiento		Referencia
102	Uso de canales seguros	La comunicación entre los sistemas de registro y los sistemas de certificación de la EC deben ser realizadas por un canal cifrado SSL, mediante un certificado digital emitido por un EC con el sello de Webtrust o una certificación equivalente. Las comunicaciones entre la ER y la EC deben ser llevadas a cabo a través de mecanismos que permitan una comunicación ininterrumpida para garantizar la atención oportuna de las solicitudes de emisión del certificado, así como la actualización de la relación de certificados emitidos y revocados. Las comunicaciones referidas a la aprobación o revocación de certificados deben ser llevadas a cabo mediante un mecanismo que garantice el no repudio.	
103	Autenticación de operadores de registro	Los operadores de registro pueden autenticarse en los sistemas de registro mediante un certificado digital, mecanismos	

		de biometría o mediante mecanismos de autenticación en doble factor, antes de tener acceso a solicitar la emisión, re-emisión, revocación, modificación o suspensión de certificados.	
104	Registros de auditoría	Los sistemas de registro deben generar registros de auditoría sobre las solicitudes de misión, re-emisión, revocación, modificación o suspensión de certificados, indicando el personal que hizo la solicitud, y el resultado positivo o fallido de la misma.	
105	Seguridad Computacional	Los computadores utilizados por los operadores de registro deberán tener una aplicación antivirus y los parches del sistema antivirus actualizados.	
106	Gestión de residuos	Los medios de almacenamiento, media y documentos en papel que contengan información confidencial o privada debe ser eliminada de manera segura, es decir, la información debe ser borrada de manera irrecuperable.	

1.2.14. Seguridad del personal

Seguridad del personal

Explicación preliminar: Los registros de las solicitudes de emisión, re-emisión, revocación, modificación o suspensión de certificados deben ser protegidas y almacenadas para servir como evidencia en caso de procesos judiciales.

No	Requerimiento		Referencia
107	Definición de roles	La ER debe definir los roles y sus privilegios de acceso y facultades asignadas dentro de las operaciones de registro. Las responsabilidades de administrar los sistemas para solicitar la emisión, re-emisión, revocación, suspensión o modificación de los certificados digitales deben ser claramente asignadas. La descripción de los roles debe incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que deben ser puestas de manifiesto a las personas que ejercen dichas funciones. Se debe obtener constancia por escrito del conocimiento de las mismas.	
108	Verificación de antecedentes	El personal de la ER deberá ser verificado respecto de sus antecedentes penales, policiales y crediticios.	

		A fin de reducir las posibilidades de que un personal autorizado pueda prestarse a remitir certificados de suplantación de identidad.	
109	Cualidades, requisitos, experiencia y certificados	Los responsables de administrar los sistemas para solicitar la emisión, re-emisión, revocación, suspensión o modificación de los certificados digitales deben contar con experiencia y conocimiento en el uso de certificados digitales o seguridad de la información. La ER debe declarar los requisitos de experiencia y calificaciones que exige a sus empleados.	
110	Compromiso contractual de confidencialidad	El personal de la ER deberá firmar términos contractuales respecto de la protección de la privacidad y confidencialidad de toda la información presentada por los clientes de la ER. Las ER deben establecer en su RPS u otra documentación relevante, los términos de confidencialidad y provisiones de no revelación que gobierna al mismo, así como la legislación que rige a las transacciones que	

		se realizan bajo el marco de la IOFE, la legislación relativa al régimen de los trabajadores y cualquier otra legislación relevante, de conformidad con la Norma Marco sobre Privacidad presentada en el anexo 6 de la Guía de Acreditación de ER. Esta información debe ser entregada por escrito a los empleados y contratistas, debiéndose obtener declaración por escrito por parte de estas personas respecto al conocimiento de toda esta información. Esta información debe ser incorporada en todos los contratos de trabajo o servicio.	
111	Responsabilidades contractuales	Definir cláusulas contractuales respecto de las responsabilidades y las consecuencias laborales y penales en caso de ocurrir eventos de compromiso de las operaciones de la ER, incluyendo casos de suplantación de identidad por intervención del personal.	
112	Compromiso de cumplir la política de seguridad	Definir cláusulas contractuales respecto del cumplimiento de la política de seguridad de la ER por parte de su personal	

113	Capacitación	El personal de la ER, que administra los sistemas para la solicitud, re-emisión, revocación, modificación o suspensión, debe recibir una capacitación continua respecto: • Certificados digitales • Firma digital • Regulación de la IOFE • Política de registro. • Políticas de seguridad y privacidad de la ER • RPS • Plan de contingencia • Funciones respecto de su rol. • Seguridad de la Información. La frecuencia de la capacitación deberá ser de al menos una vez antes de operar en la ER y luego de manera anual.	
114	Sanciones por acciones no autorizadas	La ER debe establecer cláusulas contractuales respecto de las sanciones que pueden ejecutarse en caso de ocurrir acciones no autorizadas o que pongan en riesgo la autenticidad de las operaciones de registro. Así como acciones penales en caso de participación en hechos de suplantación de identidad. Como mínimo, en el caso de una acción real o potencial no	

		autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona debe ser inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.	
115	Rotación en el trabajo	La ER debe establecer políticas y controles para asegurar que las responsabilidades de seguridad y protección de privacidad de datos personales se mantienen incluso en casos de rotación del personal, retirando los permisos de acceso físico y lógico a los Operadores de Registro cuando terminan su relación con la ER o cuando cambian de rol.	

1.2.15. Auditoría

Auditoría			
Explicación preliminar: La ER debe ser auditada anualmente por la AAC, respecto de la correcta operación de los servicios de registro.			
No	Requerimiento		Referencia
116	Auditoría de registros	Los registros deben ser revisados como parte de la auditoría de la AAC, de manera anual.	

117	Auditoría del archivo	El archivo debe ser revisado como parte de la auditoría de la AAC, de manera anual.	
118	Auditoría de los procedimientos y controles	Los procedimientos y controles implementados deben ser auditados por la AAC de manera anual. Las auditorías internas deben llevarse a cabo, como mínimo, una vez al año en la ER.	
119	Auditor	El auditor debe: • Ser autorizado por el INDECOPI. • El auditor no deberá haber laborado para la ER, ni deberá haber tenido ninguna relación comercial con la misma, ni de efectos de auditoría en el mismo alcance de evaluación, en los últimos 2 años calendario.	

1.2.16. Medidas de contingencia

Medidas de Contingencia		
Explicación preliminar: Es necesario que la ER cuente con medidas de contingencia frente a casos de compromiso de las claves del suscriptor e indisponibilidad de servicios.		
No	Requerimiento	Referencia

120	Protección contra compromisos de las claves del suscriptor	La ER debe establecer procedimientos que debe seguir una persona natural o jurídica en caso de compromiso de la clave privada de un suscriptor dentro de las operaciones de registro. Se debe establecer y declarar las responsabilidades y garantías financieras que ofrece la ER en caso de compromiso de las claves del suscriptor dentro de las operaciones de la ER. Los compromisos de las claves privadas de los suscriptores dentro de las operaciones de registro deben ser reportados a la AAC para su análisis y corrección. En caso que no se adopte la corrección acordada, la ER perderá su acreditación.	
121	Compromiso de las claves del operador de registro	La ER debe establecer procedimientos en caso de compromiso de las claves del operador de registro.	
122	Contingencia en caso de indisponibilidad de servicios de recepción de solicitudes de	La ER debe establecer canales alternos de recepción de solicitudes de revocación de certificados, en caso que estos no puedan ser recibidos por la ER. Entendiéndose que la	

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

1.2.17. Finalización de la ER

Finalización de la ER			
Explicación preliminar: La ER debe tomar medidas para proteger la continuidad en el mantenimiento de los registros generados, a fin de que sirvan de evidencia en casos judiciales.			
No	Requerimiento		Referencia
124	Procedimiento de finalización	La ER debe establecer un procedimiento para realizar la finalización de sus operaciones, indicando lo siguiente: • Protección de los registros de auditoría • Comunicación a sus	

		clientes con 30 días de anticipación • Comunicación a la AAC con 60 días de anticipación	
125	Transferencia de los registros de auditoría	La ER debe tomar medidas para transferir los registros de auditoría a la AAC u otra entidad de registro, por el periodo establecido por la AAC de 10 años luego de generado el registro.	
126	Garantías y responsabilidades	La ER debe establecer procedimientos para el cumplimiento de las cláusulas de garantías y responsabilidades de la ER luego de su finalización.	
127	Transferencia de las operaciones de registro para las solicitudes de revocación y re-emisión	La ER debe tomar medidas para transferir a otra Entidad de Registro, los servicios de recepción de solicitudes de revocación o re-emisión para sus clientes titulares y suscriptores de certificados.	

1.2.18. Aspectos legales de la operación de la ER

Aspectos legales de la operación de la ER
Explicación preliminar: La ER puede establecer provisiones legales aplicables a los servicios que brinda.

No	Requerimiento		Referencia
128	Tarifas	La ER 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 estado; • Honorarios por otros servicios tales como el acceso a la correspondiente CP o CPS; y • Política de reembolso. Estos cargos deben estar establecidos o referencias en los contratos de suscriptores y terceros que confían. Las tarifas a ser pagadas por participar de la IOFE deben estar de acuerdo a la legislación vigente. La ER en convenio con las EC vinculadas, deben establecer el	RFC 3647 sección 4.9.1: Tarifas

		monto de sus tarifas.	
129	Políticas de reembolso	La ER puede establecer políticas de reembolso, incluyendo los siguientes casos: • Cuando un certificado no puede ser correctamente instalado debido a inconvenientes con la ER. • Cuando se proporciona un certificado de propósito o características tecnológicas diferentes En caso de existir, estas cláusulas deben estar establecidas o referencias en los contratos de suscriptores y terceros que confían.	
130	Responsabilidad financiera	La ER 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 incluyen: • La ER debe mantener	RFC 3647 sección 4.9.2: Responsabilidad financiera

		una cierta cantidad de cobertura de seguro para cubrir sus obligaciones frente a otros participantes; o • La ER 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 ER deber ofrecer un seguro de responsabilidad civil o la protección de garantía a otros participantes en conexión con el uso de la PKI. La ER debe establecer en su RPS 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 registro o custodia	

		de información, se debe establecer la responsabilidad de la ER y de aquellas organizaciones que realizan las actividades tercerizadas. La ER debe asegurar que las organizaciones que están realizando las actividades tercerizadas, realizan dichas funciones de conformidad con la RPS y otra documentación de la ER, estableciendo provisiones de responsabilidad respecto a los eventuales errores y omisiones que pudieran generarse. En el caso que exista cobertura de seguro o garantías disponibles para los suscriptores, la ER debe establecer en su RPS 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 garantías disponibles para los terceros que confían, esto deberá encontrarse referenciado en la RPS, en donde deben incluirse los términos y condiciones de la cobertura para el tercero que	

		confía.	
131	Información confidencial	La ER 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	RFC 3647 sección 4.9.3: Confidencialidad de información del Negocio

		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.	
132	Información privada	La ER 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.	RFC 3647 sección 4.9.4: Privacidad de información personal

		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.	
133	Información no privada	Se debe permitir la publicación de certificados (siempre que el suscriptor lo autorice en el contrato 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.	RFC 3647 sección 4.9.4: Privacidad de información personal
134	Derechos de Propiedad intelectual	De ser aplicable, la ER 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, o	RFC 3647 sección 4.9.5: Privacidad de información personal

		comerciales, que ciertos participantes pueden tener o reclamar en una RPS, certificados, nombres, y claves, o son objeto de una licencia para o desde los participantes.	
135	Representaciones y garantías	La ER debe establecer disposiciones que regulen las garantías que las declaraciones de diversas entidades han sido hechas de conformidad con la RPS. Por ejemplo, una RPS 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 RPS podría contener una menos extensa garantía al sentido de que la información contenida en el certificado es verdadera para mejor conocimiento de la ER después de realizar ciertos procedimientos de autenticación de la identidad. También se pueden incluir requisitos que las representaciones y garantías aparecen en ciertos acuerdos, como el acuerdo del suscriptor o tercero que confía. Por ejemplo, una RPS puede contener el requisito de que todas las entidades emisoras utilizan un	RFC 3647 sección 4.9.6: Representaciones y garantías

		acuerdo del suscriptor, y que dicho acuerdo debe contener una garantía por la ER que la información contenida en el certificado es exacta.	
136	Excepciones de responsabilidad de garantías	La ER puede incluir en su RPS la negación de garantías expresas que de otra manera se entenderá que existen en un acuerdo, y exenciones 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 pueden imponer directamente dichas renuncias, o la CP o CPS pueden contener el requisito de que las renuncias aparecen en acuerdos asociados, como los acuerdos del suscriptor o terceros que confían. No cabe exención de responsabilidad para aquellas garantías establecidas por la legislación vigente. La ER debe establecer en su RPS o en los contratos del suscriptor o tercero que confía,	RFC 3647 sección 4.9.7: Excepciones de responsabilidad de garantías

		cláusulas de garantía y responsabilidad, incluyendo limitaciones y excepciones, si fueran aplicables.	
137	Notificaciones y comunicaciones entre participantes	La ER debe declarar los mecanismos de comunicación con sus clientes y otros participantes. Este requisito es diferente de funciones de publicación y repositorio, porque a diferencia de comunicaciones de individuo que se describen en este subcomponente, la publicación y anuncio a un repositorio son para el propósito de comunicar a una amplia audiencia de destinatarios, como todas las partes de confianza. Este subcomponente podrá establecer mecanismos de comunicación e indicará la información de contacto que se utilizará para enrutar este tipo de comunicaciones, tales como un mensaje firmado digitalmente, las comunicaciones de correo electrónico a una dirección especificada, seguido por un acuse de recibo 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.	
138	Correcciones o enmiendas	Ocasionalmente será necesario modificar una RPS. Algunos de estos cambios no reducirán significativamente la seguridad de que una RPS o su implementación ofrece, el administrador de la política juzgará si tiene un efecto insignificante sobre la aceptabilidad de certificados. Por otro lado, algunos cambios en una especificación cambiarán sustancialmente la aceptabilidad de certificados para fines específicos, y estos cambios pueden requerir una comunicación formal al INDECOPI. La RPS también puede contener la siguiente información: • Los procedimientos	RFC 3647 sección 4.9.12: Correcciones o enmiendas Guidelines for the Certificate Policy and Certificate Practices Framework for issuing certificates capable of being used in Cross Jurisdiction eCommerce – APEC – Mayo 2005/ Sección 9.12 Amendments

		mediante los cuales la RPS y / u otros documentos deben o pueden ser modificados. En el caso de las enmiendas de la RPS, 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 RPS harían requerir un cambio que sea declarado al INDECOPI • Los cambios efectuados a las políticas y prácticas documentadas deben ser revisados por INDECOPI.	
139	Procedimiento de resolución de disputas	La ER puede establecer los procedimientos utilizados para resolver disputas que surja de las RPS, y/o acuerdos. Ejemplos de tales procedimientos incluyen requisitos 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.	
140	Conformidad con la Ley aplicable	La ER debe declarar que la legislación de una determinada jurisdicción rige la interpretación y la ejecución de la RPS o acuerdos.	RFC 3647 sección 4.9.14: Ley aplicable
141	Cumplimiento de la Ley aplicable	Esta sección se refiere a los requisitos establecidos que los participantes cumplen 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. La RPS podría pretender imponer dichos requisitos o puede requerir que tales disposiciones aparecen en otros acuerdos. "La ER debe identificar, en su RPS, otra documentación relevante o su sitio web, la ley aplicable a sus operaciones de acuerdo a la Ley N° 27269 y el Reglamento de Ley de Firmas y Certificados Digitales, aprobado por el D.S. 004-2007-PCM. Los requerimientos legalmente	RFC 3647 sección 4.9.15: Cumplimiento de la Ley aplicable

		significativos deben de estar establecidos o referenciados en los contratos de suscriptores y terceros que confían, y también deben estar acorde a la Ley N° 29733 de protección de datos personales.	
142	Limitaciones de responsabilidad	La ER puede incluir limitaciones de responsabilidad en una RPS o limitaciones que aparecen o deben aparecer en un acuerdo asociado con el RPS, 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	RFC 3647 sección 4.9.8: Limitaciones de responsabilidad

		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 ER, 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 ER acreditada debe establecer en su documentación cualquier limitación en la subrogación de derechos o delegación de obligaciones. La ER debe establecer en su RPS o en los contratos del suscriptor o tercero que confía, cualquier limitación de responsabilidad que fuera aplicables.	
143	Indemnizaciones	La ER puede incluir en su RPS 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 RPS, o en un acuerdo. Por ejemplo, una RPS puede requerir que los	RFC 3647 sección 4.9.9: Indemnizaciones

		acuerdos de suscriptor contengan un término en el que el abonado es responsable de indemnizar a una entidad emisora de las pérdidas de la ER 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 RPS puede decir que una ER 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 ER sostiene que surja del uso de un certificado sin comprobar debidamente la información de revocación o el uso de un certificado para propósitos más allá de lo permitido por la ER La ER debe establecer en su RPS o en los contratos del suscriptor o tercero que confía, cualquier obligación de indemnización que fuera aplicable.	
144	Vigencia y conclusión	La ER puede incluir el período de tiempo en el que una RPS sigue vigente y las	RFC 3647 sección 4.9.10: Termino y terminación

		circunstancias en que el documento, partes del documento, o su aplicabilidad a una determinada participante puede terminarse. Además o alternativamente, la RPS puede indicar que los requisitos que cierta duración y cláusulas de terminación aparecen 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 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.	
145	Provisiones misceláneas	La ER puede incluir en su RPS y en los contratos disposiciones varias 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	RFC 3647 sección 4.9.16: Provisiones misceláneas

		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 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.	

146	Otras provisiones	La ER puede incluir en su RPS o en los contratos otras disposiciones donde las responsabilidades y los términos que no encajan perfectamente dentro de uno de las secciones anteriores pueden ser impuestas a los participantes de la PKI.	RFC 3647 sección 4.9.17: Otras provisiones

1.2.19. Seguridad de la Gestión del ciclo de vida de las claves del suscriptor

Controles de gestión del ciclo de vida del módulo criptográfico del suscriptor		
Explicación preliminar: Si la ER administra módulos criptográficos que serán entregados a los suscriptores, tarjetas inteligentes, tokens, etc. estos deben ser protegidas a fin de impedir su suplantación y las copias no autorizadas de las claves privadas.		
No	Requerimiento	
147	Obtención de los módulos criptográficos	La ER debe mantener controles para garantizar de manera razonable que: a) Las obtenciones del módulo son controladas por la EC o ER b) El uso del módulo es habilitado por la ER antes de emitir el módulo c) La desactivación y reactivación del módulo son controlados de manera segura por la ER d) Los módulos son almacenados y distribuidos de manera segura por la ER e) Los módulos que retornan a la EC son destruidos o borrados de manera segura, sin la capacidad de recuperación de la clave privada f) Si la ER contrata a un tercero encargado de gestionar y proteger los módulos, debe existir un contrato formal entre ambas partes. La ER mantiene la responsabilidad y obligaciones de garantizar la protección de los módulos.

		g) Los módulos deben ser lógicamente protegidos durante su transporte desde su fabricación hasta su emisión mediante una clave de transporte o una frase de paso h) Los módulos cumplen los estándares FIPS 140-2 nivel 2 o Common Criteria EAL 4+ como mínimo.
148	Preparación y personalización	a) En caso que la personalización y generación de las claves sea gestionada por la ER debe garantizar la seguridad y autenticidad de los procesos de personalización del módulo, los cuales incluyen lo siguiente: i. La carga de la información de identificación dentro del módulo ii. La generación de las claves del suscriptor iii. La carga del certificado del suscriptor en el módulo garantizando que no existen generación de copias ni uso no autorizado de la clave, y que solamente el suscriptor tiene acceso y control sobre la misma iv. Protección lógica del módulo de acceso no autorizado b) La ER debe generar registros de auditoría de los procesos de preparación y personalización c) El módulo no puede ser emitido sino ha sido personalizado por la ER o el tercero asignado. d) Un módulo no puede ser utilizado sino se encuentra en estado de activación o reactivación
149	Almacenamiento y distribución del módulo criptográfico	a) Deben implementarse procedimientos para la distribución y registro seguro de la recepción segura del módulo por parte del suscriptor. b) Los datos de activación del módulo son comunicados de manera segura al suscriptor garantizando que sólo él suscriptor tiene acceso a los mismos, y en el caso de usar contraseña, el suscriptor debe ser requerido de realizar su modificación. La contraseña de acceso debe ser entregada por un canal seguro diferente a la entrega de las claves o el módulo criptográfico. c) La distribución y activación del módulo es registrado para efectos de auditoría por la ER o un tercero asignado.

150	Uso del módulo criptográfico	a) El suscriptor debe ser provisto de un mecanismo que protege el acceso a los datos del módulo incluyendo el almacenamiento de las claves privadas. b) Las claves del suscriptor no deben poder ser exportadas por una aplicación para realizar funciones criptográficas c) El suscriptor debe ser requerido para usar mecanismos de autenticación para aplicaciones criptográficas y funciones del módulo d) La aplicación del módulo del suscriptor debe generar registros de auditoría, incluyendo casos de intentos de acceso en el proceso de verificación del titular del módulo.
151	Desactivación y reactivación	a) La activación y desactivación del módulo criptográfico, que contiene la clave privada del suscriptor debe ser controlada solamente por el suscriptor, y no debe poder ser manipulada por los empleados o contratistas de la ER. No se admite el depósito, almacenamiento o copia de claves privadas de firma y autenticación de los usuarios finales, ni de los módulos hardware que los contienen, estando estos en modo activado.
152	Reemplazo del módulo criptográfico	a) Se deben establecer procedimientos para reemplazar módulos perdidos o dañados. b) En caso de pérdida o daño del módulo, las claves y certificados del suscriptor deben ser revocados y re-emitidos c) El reemplazo del módulo debe ser registrado para efectos de auditoría de la ER o el tercero asignado.
153	Terminación del módulo criptográfico	a) Todos los módulos retornados a la ER deben ser desactivados o destruidos de manera segura con el contenido no recuperable o reutilizable para prevenir el uso no autorizado, Esta desactivación o destrucción debe ser realizada al momento en el que módulo es retornado a la ER, de modo que se garantiza que sólo el suscriptor ha tenido control sobre su clave privada. b) La terminación del módulo debe ser controlado por el emisor del módulo. c) Se deben generar registros de auditoría de la terminación de un módulo. No deberán ser archivadas las claves privadas empleadas para la firma y autenticación de los usuarios finales, ni de los archivos electrónicos que los contengan (por ejemplo, los archivos con extensión PFX).