ACTUALIZACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Referencia:	IZENPE-ACTUALIZACIÓN DPC
Nº Versión:	v 5.03
Fecha:	10 de Marzo de 2015

Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.com
info@izenpe.com
Tel.: 945 017 490

Información general

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	5.03
Fecha de aprobación:	10/03/2015
Documentación utilizada:	DPC 5.02
Autor (es)	Asesoría Jurídica de Izenpe Área técnica de Izenpe
Cambios/Comentarios	La versión 5.03 es la actualización de la versión 5.02

La Declaración de Prácticas de Certificación de Izenpe, S.A., de acuerdo a su epígrafe 9.11, permite realizar modificaciones a la Declaración de Prácticas de Certificación. A pesar de que estas modificaciones son recogidas en el presente documento, si Ud. solicita, usa o confía en los certificados emitidos por Izenpe, S.A., tiene la obligación de conocer la totalidad de la Declaración de Prácticas de Certificación actualizada.

ENTRADA 1_Adaptación

Enmienda:

Consecuencia de la auditoría realizada por Izenpe de acuerdo a las normas ETSI y la inclusión de nuevos servicios, se incluyen las siguientes modificaciones:

EPÍFRAGE	M□DIFICACIÓN
Todo el documento	**Reemplazados todos los "reconocidos" por "cualificados"**
1. Introducción	**□riginal:** IZENPE además sigue las indicaciones de los estándares de ETSI (Instituto Europeo de Estándares de Telecomunicaciones) y ha conseguido la certificación bajo las especificaciones técnicas (TS) de la norma 101 456 para la emisión de certificados cualificados y generados en un dispositivo seguro de creación de firma (QCP Public + SSCD) y de la norma 102 042 para la emisión de certificados de infraestructura de clave pública (PKI) siguiendo la política de certificados de validación extendida, EVCP, siguiendo las guías aprobadas por el CA/Browser Forum. **Cambiado:** IZENPE además sigue las indicaciones de los estándares de ETSI (Instituto Europeo de Estándares de Telecomunicaciones) y ha conseguido la certificación bajo las especificaciones técnicas (TS) de la norma 101 456 para la emisión de certificados cualificados y generados en un dispositivo seguro de creación de firma (QCP Public + SSCD) y de la norma 102 042 para la emisión de certificados cualificados y no cualificados. Para los certificados de servidor seguro que siguen la política de certificados de validación extendida (EVCP) y para los certificados de servidor seguro que siguen la política de validación de la organización (OVCP), se siguen además las guías aprobadas por el CA/Browser Forum. **□riginal:** Las especificaciones técnicas (TS) que se definen en estas normas, TS 101 456 y TS 102 042, marcan los requisitos básicos en los que se refieren a la gestión y prácticas de certificación de entidades certificadoras que emiten certificados cualificados y no cualificados dentro del marco legal de la directiva 1999/93/EC del Parlamento europeo incorporada al régimen jurídico español en la ley de firma electrónica 59/2003.

	Cambiado: Las especificaciones técnicas (TS) que se definen en estas normas, TS 101 456 y TS 102 042, marcan los requisitos básicos en los que se refieren a la gestión y prácticas de certificación de entidades certificadoras que emiten certificados cualificados y no cualificados dentro del marco legal de la directiva 1999/93/EC del Parlamento y Consejo Europeo incorporada al régimen jurídico español en la ley de firma electrónica 59/2003, y posteriormente del Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS).
1.1 Presentación	**Añadido:** • "El Servicio de Verificación permite a la Entidad Usuaria del servicio beneficiarse de la utilización de los certificados emitidos por IZENPE mediante la comprobación del estado de los certificados basándose en CRL (Certificate Revocation List). • La plataforma de servicios de firma ZAIN es una plataforma de servicios de confianza que incluye un conjunto de servicios de seguridad globales y estandarizados (autenticación, autorización, firma electrónica y protección de datos) como servicios Web. • IZENPE ofrece de forma gratuita id@zki. Una aplicación Java en forma de applet para poder ser integrada dentro de un navegador con funcionalidad de firma electrónica, cifrado • El servicio de portafirmas de Izenpe es una versión digital del portafirmas tradicional, que consiste en una bandeja donde una persona recibe los diferentes documentos que tiene que firmar. • El servicio de comunicación certificada ZIURRA actúa como Tercero de Confianza ("notario digital") de modo que da fe al envío de un email o SMS y recepción el mismo por el remitente. • El Servicio de Constancia y Acreditación de una Publicación permite acreditar fehacientemente el momento de inicio de la difusión pública de la información que se incluya en una contratación pública. • El Servicio de albergue de certificados en la nube EGOITZA permite albergar de forma segura los certificados de usuario final. " **Eliminado:** • "IZENPE dispone de un conjunto de aplicativos informáticos, así como de especificaciones técnicas para el desarrollo de aplicaciones que emplean la firma electrónica, que ofrece bajo licencia, a las Entidades Usuarias."

	Añadida clasificación de persona física, jurídica y dispositivo en tabla
1.3.1 Autoridades de certificación	**Eliminado:** "Autoridades de certificación **subordinadas 2003.** Estas CAs se han migrado a la nueva CA raíz de Izenpe." **Eliminadas tablas de CAs subordinadas de CA 2003** **Eliminada tabla subCA SSL EV obsoleta**
1.3.3 Entidades finales usuarias de certificados	**Cambiado título de "Entidades finales usuarias" por "Entidades finales usuarias de certificados"**
1.3.4 Entidades finales usuarias de sellos de tiempo	**Creado el punto 1.3.4 "Entidades finales usuarias de sellos de tiempo"**
1.3.5 Terceras partes de confianza	**□ riginal:** "Dentro de esta Declaración de Prácticas de Certificación, las personas físicas o jurídicas que reciben certificados emitidos por IZENPE son terceros que confían en certificados emitidos por IZENPE y, como tales, les es de aplicación lo establecido por la presente Declaración de Prácticas de Certificación cuando deciden confiar efectivamente en tales certificados." **Cambiado:** "Dentro de esta Declaración de Prácticas de Certificación, las personas físicas o jurídicas que reciben certificados y sellos de tiempo emitidos por IZENPE son terceros que confían en certificados y sellos de tiempo emitidos por IZENPE y, como tales, les es de aplicación lo establecido por la presente Declaración de Prácticas de Certificación cuando deciden confiar efectivamente en tales certificados o sellos de tiempo." **□ riginal:** "Se considera que los terceros confían en los certificados en función del empleo objetivo que de los mismos realicen en sus relaciones con los suscriptores." **Cambiado:** "Se considera que los terceros confían en los certificados y sellos de tiempo

	en función del empleo objetivo que de los mismos realicen en sus relaciones con los suscriptores." **riginal:** "Los terceros deberán guardar la diligencia debida en el empleo de cada tipo de certificado y actuar con base en los principios de buena fe y lealtad, absteniéndose de realizar conductas fraudulentas o negligentes cuyo fin sea repudiar mensajes emitidos dentro del ámbito de confianza asociado a la categoría del certificado." **Cambiado:** "Los terceros deberán guardar la diligencia debida en el empleo de cada tipo de certificado y sello de tiempo y actuar con base en los principios de buena fe y lealtad, absteniéndose de realizar conductas fraudulentas o negligentes cuyo fin sea repudiar mensajes emitidos dentro del ámbito de confianza asociado a la categoría del certificado o sello de tiempo."
1.4.1 Usos apropiados del certificado	**Movido del apartado "Certificado cualificado" al apartado "Certificado no cualificado":** "Los certificados Sede y Sede EV se emiten para identificar de forma fiable sitios web. Los certificados de sede y sello electrónico se emiten a las administraciones públicas para la identificación de la sede electrónica y el sellado electrónico de documentos, según lo previsto en la *Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos*." **riginal en el apartado "Certificado de dispositivo informático":** "Se emiten certificados de servidor seguro (SSL y SSL EV) y de aplicación a entidades responsables de la operación de dispositivos informáticos." **Cambiado:** "Se emiten certificados de servidor seguro (SSL DV, SSL OV, SSL EV, Sede y Sede EV) y de aplicación a entidades responsables de la operación de dispositivos informáticos."
1.6.1 Definiciones	**Añadido:** "Autoridad de Sellado de Tiempo (TSA): autoridad que emite tokens de sello de tiempo"
2.2 Publicación de información de	**riginal:** "El acceso se encuentra disponible en la dirección http://www.izenpe.com,

certificación	durante 24 horas, los 7 días de la semana." **Cambiado:** "El acceso se encuentra disponible en la dirección www.izenpe.com, durante 24 horas, los 7 días de la semana." **□ riginal:** "En cuanto a la publicación de las Listas de Certificados Revocados, se garantiza un acceso a los usuarios y suscriptores de los certificados de forma segura y rápida" **Cambiado:** "En cuanto a la publicación de las Listas de Certificados Revocados, se garantiza un acceso a los usuarios y suscriptores de los certificados de forma segura, rápida y gratuita"
2.2.1 Política de publicación y notificación	**□ riginal:** "Los cambios en las especificaciones o en las condiciones del servicio serán comunicados por IZENPE a los usuarios a través de la página principal de IZENPE http://www.Izenpe.com." **Cambiado:** Los cambios en las especificaciones o en las condiciones del servicio serán comunicados por IZENPE a los usuarios a través de la página principal de IZENPE www.izenpe.com"
3.2.1 Métodos para probar la posesión de la clave privada	**□ riginal:** Cuando el par de claves es generado, • Por una Entidad de Registro, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del dispositivo criptográfico y del correspondiente certificado y par de claves almacenados en su interior. • Por el poseedor de claves del certificado, la demostración de posesión de la clave privada consiste en la correcta utilización del certificado. **Cambiado:** Cuando el par de claves es generado, • Por una Entidad de Registro y las claves están alojadas en una tarjeta criptográfica, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación de la tarjeta criptográfica y del correspondiente

	certificado y par de claves almacenados en su interior. • Por una Entidad de Registro y las claves están alojadas en un HSM, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de custodia en el HSM y del procedimiento fiable para el acceso exclusivo a las claves por parte del suscriptor. • Por el poseedor de claves del certificado, la demostración de posesión de la clave privada consiste en la correcta utilización del certificado.
3.3 Identificación y autenticación para peticiones de reemisión de claves	**□riginal:** "En los certificados, tras la revocación del certificado y emisión de uno nuevo, siempre se lleva a cabo la renovación de las claves." **Cambiado:** "En los certificados en los que Izenpe genera las claves, tras la revocación del certificado y emisión de uno nuevo, siempre se lleva a cabo la renovación de las claves."
4.1 Solicitud de certificado	**□riginal:** "A tal fin se recogen con exactitud, dentro de los límites de longitud derivados de los condicionantes técnicos establecidos en el contenido del certificado, el nombre y apellidos recogidos en los documentos de identificación" **Cambiado:** "A tal fin se recogen con exactitud, dentro de los límites de longitud derivados de los condicionantes técnicos establecidos en el contenido del certificado, los datos identificativos recogidos en los documentos de identificación"
4.2.2 Aprobar o rechazar solicitudes	**Añadido:** "Cuando esta solicitud sea para un certificado que incluya un nombre de dominio para la autenticación de un servidor, Izenpe examinará el registro de la CAs autorizadas, CAA, según la RFC 6844, y si esos registros CAA están presentes y no permiten a Izenpe emitir esos certificados porque no se encuentra registrado, Izenpe no emitirá ese certificado pero permitirá a los solicitantes volver a realizar la solicitud una vez Izenpe haya podido subsanar esa posible incidencia."
4.2.3 Custodia de la clave privada	**Añadido:** "En el caso del servicio "certificado en la nube" las claves privadas de

	certificados de usuario final se encuentran custodiadas en dispositivos criptográficos seguros certificados con la norma FIPS 140-2 nivel 3. “
4.3 Emisión del certificado	**Añadido:** **“**No se entregarán códigos de desbloqueo (PIN o PUK) en el caso de certificados en los que Izenpe no genere las claves.”
4.3.1 Acciones de la CA durante la emisión	**riginal:** “Según el tipo de certificado, la emisión puede efectuarse en dispositivo criptográfico o en soporte software.” **Cambiado:** Según el tipo de certificado, la emisión puede efectuarse en smartcard, en HSM o en soporte software.” **riginal:** “Procedimiento de emisión en caso de certificado emitido en dispositivo criptográfico:” **Cambiado:** “Procedimiento de emisión en caso de certificado emitido en smartcard:” **Añadido:** I. “Procedimiento de emisión en caso de certificado emitido en HSM: • La Entidad de Registro comprueba la validez de la documentación presentada por los solicitantes. • Concluida la autenticación la Entidad de Registro solicita a IZENPE un certificado. • Comprobado que la petición proviene de una Entidad de Registro autorizada, IZENPE emite el certificado conforme al procedimiento establecido y lo envía a la Entidad de Registro. • Una vez la Entidad de Registro ha comprobado que la petición proviene de IZENPE, procede a cargar el certificado en el dispositivo de creación de firma de acuerdo a un proceso seguro de gestión de dispositivos criptográficos. • Si por alguna razón IZENPE decide no emitir el certificado (aunque los procedimientos de autenticación hubieran sido correctos), se notifican los motivos al solicitante.” **riginal:** “Junto con el formulario de solicitud, el solicitante habrá generado el par de

	claves en el propio servidor entregando a IZENPE la clave pública." **Cambiado:** "Junto con el formulario de solicitud, el solicitante habrá generado el par de claves en el propio servidor entregando a IZENPE la petición técnica."
4.4.3 Notificación de la emisión del certificado por la CA a otras entidades	**riginal:** "IZENPE no notifica a otras entidades la emisión de sus certificados" **Cambiado:** "IZENPE no notifica a otras entidades la emisión de sus certificados, excepto los certificados EV publicados en el servicio de Izenpe Certificate Transparency Log Server"
4.5.1 Clave privada del suscriptor y uso del certificado	**riginal:** **"**El suscriptor," **Cambiado:** "El suscriptor que custodia sus claves," **Añadido:** El suscriptor que tiene sus claves albergadas en Izenpe, • Empleará adecuadamente el certificado y, en concreto, cumplirá con las limitaciones de uso de los certificados. • Será diligente en la custodia de su clave de activación, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4 de la Declaración de Prácticas de Certificación. • Notificará a IZENPE y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables: ○ La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa. ○ Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor, instando la revocación del certificado cuando dicha modificación constituya causa de revocación del mismo. • Dejará de emplear la clave privada transcurrido el periodo de validez del certificado. • Transferirá a los poseedores de claves las obligaciones específicas de los mismos.

	• No monitorizará, manipulará o realizará actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de la Entidad de Certificación. • No comprometerá intencionadamente la seguridad de los servicios de certificación. • No empleará las claves privadas correspondientes a las claves públicas contenidas en los certificados, con el propósito de firmar ningún certificado, como si se tratase de una Entidad de Certificación. • El suscriptor de certificados cualificados que genere firmas digitales empleando la clave privada correspondiente a su clave pública listada en el certificado, debe reconocer, en el debido instrumento jurídico, que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se emplee dispositivo criptográfico, conforme a lo preceptuado en el artículo 3.4 de la LFE.
4.9.3 Tratamiento de las peticiones de revocación	**Eliminado:** "Se requerirá para la identificación: ○ Contraseña de Identificación Telefónica (remitido en la hoja de claves) ○ DNI / NIE ○ NIF de la entidad en caso de certificado de persona jurídica" **Añadido:** "Consultar la Documentación Específica correspondiente al tipo de certificado para conocer qué se requerirá para la identificación".
4.9.4 Tiempo de plazo de la CA para procesar la revocación	**□ riginal:** "Una vez realizado lo indicado en el apartado 4.9.3, y la revocación debidamente tramitada por la RA, la revocación se hará efectiva inmediatamente de acuerdo con la legislación actual." **Cambiado:** "Una vez realizado lo indicado en el apartado 4.9.3, y la revocación debidamente tramitada por la RA, la revocación se hará efectiva de acuerdo con la legislación actual."
4.9.10 □ tras formas de avisos de revocación disponibles	**□ riginal:** "IZENPE no dispone de otras formas de aviso para comprobar el estado de

	sus certificados." **Cambiado:** "Izenpe envía un email informativo al suscriptor del certificado cuando se produce la revocación de un certificado cualificado"
6.1.1 Generación del par de claves	**riginal:** • "Certificados de usuario emitidos en dispositivo hardware criptográfico: las claves son generadas por el dispositivo criptográfico" **Cambiado:** • Certificados de usuario emitidos en tarjeta criptográfica o HSM: las claves son generadas por el dispositivo criptográfico
6.1.2 Distribución de la clave privada al suscriptor	**riginal:** • "Certificados emitidos en dispositivo hardware criptográfico: las claves privadas de autenticación y de firma electrónica avanzada se entregan con el dispositivo criptográfico" **Cambiado:** • "Certificados emitidos en tarjeta criptográfica: las claves privadas de autenticación y de firma se entregan con el dispositivo criptográfico" **Añadido:** • Certificados emitidos en HSM: las claves privadas de autenticación y de firma se albergan en el dispositivo criptográfico.
6.1.5 Tamaños de claves y algoritmos utilizados	**riginal:** • Al menos 2048 bits para claves de personas físicas, servidor OCSP, servidor TSA y certificados técnicos. **Cambiado:** • Al menos 2048 bits para claves de personas físicas, jurídicas y de dispositivo, Servidor OCSP y Servidor TSA y certificados técnicos.
6.1.6 Algoritmos de firma de certificados	**riginal:** "El identificador de algoritmo (AlgorithmIdentifier) que emplea IZENPE para firmar los certificados es SHA-1 (algoritmo de hash) con RSA (algoritmo de firma) que corresponde al identificador para "Identifier for SHA-1 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc.". A partir de 2007 se comienza la implantación del algoritmo SHA-256 y se realizará de forma paulatina según el entorno tecnológico. El esquema de padding utilizado es emsa-pkcs1-v2.1 (según

	RFC 3447 sección 9.2)". Los certificados de usuario final están firmados con RSA con SHA-1. IZENPE recomienda a los usuarios finales que utilicen RSA con SHA-1 o superior (SHA-224 o SHA-256) a la hora de firmar con el certificado." **Cambiado por:** "El identificador de algoritmo (AlgorithmIdentifier) que emplea IZENPE para firmar los certificados es SHA-2 (algoritmo de hash) con RSA (algoritmo de firma) que corresponde al identificador para "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc.". El esquema de padding utilizado es emsa-pkcs1-v2.1 (según RFC 3447 sección 9.2)". Los certificados de usuario final están firmados con RSA con SHA-2. IZENPE recomienda a los usuarios finales que utilicen RSA con SHA-2 o superior a la hora de firmar con el certificado."
6.2.1 Estándares de módulos criptográficos	**riginal:** **"**En cuanto a los dispositivos criptográficos con certificados para firma electrónica avanzada, aptas como dispositivos seguros de creación de firma (DSCF)…" **Cambiado:** "En cuanto a los dispositivos criptográficos con certificados para firma electrónica cualificada, aptas como dispositivos seguros de creación de firma (DSCF)"
6.2.3 Custodia de la clave privada	**riginal:** "Será responsabilidad del suscriptor mantener bajo su exclusivo control la clave privada" **Cambiado:** "En los casos en los que el suscriptor custodie la clave privada éste será el responsable de mantenerla bajo su exclusivo control."
6.2.5 Archivado de la clave privada	**Eliminado:** "La CA no archivará nunca las claves privadas de los certificados reconocidos de los suscriptores."
6.2.6 Trasferencia de la clave privada a o desde el módulo criptográfico	**riginal:** "Sólo en el caso de contingencia se utiliza el procedimiento descrito en el apartado 6.2.4 para introducir las claves privadas en los módulos criptográficos." **Cambiado por:**

	"Sólo en el caso de contingencia se utiliza el procedimiento descrito en el apartado 6.2.4 para recuperar las claves privadas en los módulos criptográficos."
6.2.7 Almacenamiento de la clave privada en el módulo criptografico	**Añadido:** "Izenpe sigue para la generación de las claves de los certificados de usuario final almacenados "en la nube" las recomendaciones de la Comisión Europea (eIDAS) y de CEN/TS 419241."
6.2.8 Método de activación de la clave privada	**Añadido:** "El acceso de la clave privada del suscriptor en el caso del certificado alojado "en la nube" se habilitará un segundo factor de autenticación, que podrá variar en función del tipo de certificado."
6.2.9 Método de desactivación de la clave privada	**riginal:** "La extracción del dispositivo criptográfico del lector supone la finalización de cualquier acción de operación en curso." **Cambiado:** "La extracción de la tarjeta criptográfica del lector supone la finalización de cualquier acción de operación en curso."
6.2.10 Método de destrucción de la clave privada	**Añadido:** "En el caso de las claves privadas de los certificados alojados "en la nube", éstas serán eliminadas una vez finalice la relación con Izenpe, o caduquen. " **riginal:** "Este procedimiento no se aplica a las claves de firma o autenticación de usuario al no ser creadas por la CA salvo, en el caso de renovación de claves reutilizando el mismo dispositivo criptográfico, en el cual se destruirá la clave anterior y se generarán nuevas claves sobre el mismo soporte." **Cambiado:** "Este procedimiento no se aplica a las claves de firma o autenticación de usuario emitidas en tarjeta criptográfica salvo, en el caso de renovación de claves reutilizando el mismo dispositivo criptográfico, en el cual se destruirá la clave anterior y se generarán nuevas claves sobre el mismo soporte."
6.4.1 Generación e instalación de datos de activación	**Añadido:** • Certificados emitidos en "la nube": la utilización de la clave privada asociada a cada certificado requiere de un segundo factor de autenticación.

6.8 Fuente de tiempo	**□riginal:** "La descripción del protocolo NTP se puede encontrar en el estándar de IETF PKIX, RFC 1305." **Cambiado:** "La descripción del protocolo NTP se puede encontrar en el estándar de IETF RFC 5905".
7.3 Perfil □CSP	**□riginal:** Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP (RFC 2560) June 1999 **Cambiado:** Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP (RFC 6960) June 2013
8 Declaración de Prácticas del Servicio de Sellado de Tiempo (TSA)	**Creado el punto 8 "Declaración de Prácticas del Servicio de Sellado de Tiempo (TSA)"**
10.4.6 Estructura de los ficheros con datos de carácter personal	**□riginal:** • Recursos Humanos: nivel medio de seguridad • Currículo Vitae: nivel medio de seguridad **Cambiado:** • Recursos Humanos: nivel básico de seguridad • Currículo Vitae: nivel básico de seguridad
10.6.1 □bligaciones de prestación del servicio	**□riginal:** "No almacenar ni copiar los datos de creación de firma de la persona a la que haya prestado sus servicios" **Cambiado:** "No copiar los datos de creación de firma de la persona a la que haya prestado sus servicios"
10.6.2 □bligaciones de operación fiable	**□riginal:** "se asegura que se informa de la extinción o suspensión de la eficacia de los certificados de forma segura e inmediata" **Cambiado:** "se asegura que se informa de la extinción de la eficacia de los certificados de forma segura e inmediata

	riginal: “Garantizar que pueda determinarse con precisión la fecha y hora en las que se expidió un certificado o se extinguió o suspendió su vigencia” **Cambiado:** “Garantizar que pueda determinarse con precisión la fecha y hora en las que se expidió un certificado o se extinguió su vigencia”
10.6.7 bligaciones de la Entidad de Registro	**Eliminado:** • “Solicitar la suspensión del certificado a IZENPE durante el tiempo necesario para comprobar la documentación que acredite la causa que origina la revocación del certificado.” **riginal:** • Cumplir en el desempeño de sus funciones de gestión de emisión, renovación, revocación y reactivación de los certificados los procedimientos establecidos por IZENPE y la legislación vigente en esta materia. **Cambiado:** • Cumplir en el desempeño de sus funciones de gestión de emisión, renovación, y revocación de los certificados los procedimientos establecidos por IZENPE y la legislación vigente en esta materia.
10.6.10 bligaciones del usuario verificador de certificados	**riginal:** • Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados. **Cambiado:** • Verificar la validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
10.6.11 bligaciones de la Entidad Emisora de Sellos de Tiempo	**Creado el punto 10.6.11 “bligaciones de la entidad emisora de sellos de tiempo”**
10.6.12 bligaciones del suscriptor de sellos de tiempo	**Creado el punto 10.6.12 “bligaciones del suscriptor de sellos de tiempo**
10.6.13 bligaciones de terceras partes verificadoras de sellos de tiempo	**Creado el punto 10.6.13 “bligaciones de terceras partes verificadoras de sellos de tiempo”**

10.7.2 Responsabilidad de la Autoridad de Sellado de Tiempo	**Creado el punto 10.7.2 "Responsabilidad de la Autoridad de Sellado de Tiempo"**
10.13 Normativa aplicable	**Añadido:** • Reglamento Europeo 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS)