ACTUALIZACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Referencia: IZENPE-ACTUALIZACIÓN DPC.

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

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

La Declaración de Prácticas de Certificación de Izenpe, 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, tiene la obligación de conocer la totalidad de la Declaración de Prácticas de Certificación actualizada.

Información general_ versión 5.01 como actualización de la versión 5.0

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	5.01
Fecha de aprobación:	19/07/2013
Documentación utilizada:	DPC 5.0
Autor (es)	Asesoría Jurídica de Izenpe Área técnica de Izenpe
Cambios/Comentarios	La versión 5.01 es la actualización de la versión 5.0

Enmienda:

Consecuencia de la auditoria TUV IT de acuerdo a las normas ETSI, se incluyen las siguientes modificaciones:

EPÍFRAGE	MODIFICACIÓN
5.8.1	- Se dará por finalizada cualquier autorización de terceros con los que Izenpe mantenga un contrato de prestación de servicios (identificación, emisión, albergue, etc.)
9.6.1	- Cumplir la normativa y estándares de seguridad (LOPD, ISO, ETSI y Política de Seguridad de Izenpe). - Exigir a proveedores de albergue el cumplimiento de la normativa y estándares de seguridad (LOPD, ISO, ETSI y Política de Seguridad de Izenpe).
9.6.7	- Cumplimiento de la normativa y estándares de seguridad (LOPD, ISO, ETSI, Política de Seguridad de Izenpe).
9.11.2	- Se sustituye Izenpe por El Comité de Seguridad de IZENPE
6.1.1	- Para el caso de las claves generadas por el propio poseedor, éstas deberán ser generadas siguiendo las recomendaciones de algoritmo y longitud de clave mínimas definidas en ETSI TS 102 176.”
6.1.6	- El esquema de padding utilizado es emsa-pkcs1-v2.1 (según RFC 3447 sección 9.2).”
6.2.7	- En los casos en los que se almacenen claves privadas fuera de los módulos criptográficos, éstas estarán protegidas de forma que se asegure el mismo nivel de protección que si estuviesen físicamente en el interior de los módulos criptográficos. Todos los HSMs utilizados por Izenpe para almacenar claves privadas de Autoridades de Certificación poseen la certificación FIPS 140-2

	nivel 3.

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	5.02
Fecha de aprobación:	16/09/2014
Documentación utilizada:	DPC 5.01
Autor (es)	Asesoría Jurídica de Izenpe Área técnica de Izenpe
Cambios/Comentarios	La versión 5.02 es la actualización de la versión 5.01

Enmienda:

Consecuencia de la auditoria TUV IT de acuerdo a las normas ETSI, se incluyen las siguientes modificaciones:

EPÍFRAGE	MODIFICACIÓN
5.5.2	- Se aclara que la información y documentación relativa a los certificados se conserva, a partir de la fecha de emisión, 15 años para los certificados reconocidos y 7 para los no reconocidos.
6.1.5, 7.1.2 y 7.1.3	- Se sustituye el algoritmo SHA1 por SHA 2. - El tamaño de las claves pasan de 1024 a 2048.
6.2.3	- Se elimina la previsión por Izenpe de almacenamiento de claves privadas.
6.2.7	- Se informa que Izenpe sigue para la generación de las claves de las CAs las recomendaciones de ETSI TS 102 042, 7.2.1 g), y Baseline Requirement Guidelines 17.7

Información general _ versión 5.04 como actualización de la versión 5.03

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	5.04
Fecha de aprobación:	30/06/2016
Documentación utilizada:	DPC 5.04
Autor (es)	Asesoría Jurídica de Izenpe Área técnica de Izenpe
Cambios/Comentarios	La versión 5.04 es la actualización de la versión 5.03

CAMBIOS

Requerimientos adicionales	➢ Se han añadido los nuevos perfiles de representante, sello, SSL cualificado y ciudadano no cualificado ➢ Se ha identificado el nivel de aseguramiento de todos los perfiles (existentes y nuevos) ➢ Se han indicado las nuevas extensiones de certificado exigidas por las normas EN
Requerimientos actualizados	➢ Se han actualizado las referencias y requerimientos de las normas EN de ETSI, correspondientes al reglamento eIDAS
Aclaraciones	➢ Se han actualizado puntos para adaptarlos a las normas de ETSI y CABForum aplicables
Editorial	
Requerimientos eliminados	➢ Se han eliminado todos los requerimientos para el servicio de sellado de tiempo (TSA) ➢ Se ha eliminado toda referencia a SHA-1

Información general _ versión 5.05 como actualización de la versión 5.04

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	5.05
Fecha de aprobación:	26/10/2016
Documentación utilizada:	DPC 5.04
Autor (es)	Asesoría Jurídica de Izenpe Área técnica de Izenpe
Cambios/Comentarios	La versión 5.05 es la actualización de la versión 5.04

CAMBIOS

Requerimientos adicionales	➢ Epígrafe 1.1. *Presentación*: se incluye el tipo de certificado de representante en soporte contenedor.
Requerimientos actualizados	➢ Epígrafe 4.4.3. *Notificación de la emisión del certificado por la CA a otras entidades*: se eliminado el CT de Izenpe. ➢ Epígrafe 5.8.1. *Terminación de la CA o RA*: se incluye la previsión "o persona/as designadas por el Consejo de Administración, quien decidirá el mecanismo más adecuado" entre los responsables de notificar ante un cese de servicio de emisión de certificados (5.8.1). ➢ Epígrafe 4.9.9. Requisitos de comprobación de revocación online: se añade a "*Los certificados revocados que expiren serán retirados de la CRL*" el texto *"Los certificados revocados que expiren serán retirados de la CRL, sin embargo se seguirá ofreciendo información del estado del certificado a través de la comprobación online, independientemente de que esté caducado."*
Aclaraciones	
Editorial	
Requerimientos eliminados	

Información general _ versión 5.06 como actualización de la versión 5.05.

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	5.06
Fecha de aprobación:	10/11/2016
Documentación utilizada:	DPC 5.05
Autor (es)	Asesoría Jurídica de Izenpe Área técnica de Izenpe
Cambios/Comentarios	La versión 5.06 es la actualización de la versión 5.05

CAMBIOS

Requerimientos adicionales	➢
Requerimientos actualizados	➢
Aclaraciones	
Editorial	
Requerimientos eliminados	➢ Eliminadas todas las referencias de HSM y certificado en la nube

Información general _ versión 5.07 como actualización de la versión 5.06

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	6.0
Fecha de aprobación:	1/06/2017
Documentación utilizada:	DPC 5.06
Autor (es)	Asesoría Jurídica de Izenpe Área técnica de Izenpe
Cambios/Comentarios	La versión 6.0 es la actualización de la versión 5.06

CAMBIOS

	EPÍGRAFE / ACLARACION
Actualizaciones respecto a la versión anterior	– Introducción. Izenpe tendrá en cuenta las recomendaciones de ETSI EN 301 549. – 1.1. Presentación. Se actualizan las referencias a los medios de identificación expedidos por Izenpe según lo requerido por el reglamento eIDAS. – 4.9.3. Se actualiza la dirección web de Izenpe, ahora www.izenpe.eus. – 5.8.1. En caso de cese de la actividad, se especifica que Izenpe informara sobre este cese al órgano competente con una antelación mínima de 2 meses.
Aclaraciones	
Actualizaciones de formato.	
Eliminaciones.	

Información general _ versión 6.1 como actualización de la versión 6.0

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	6.1
Fecha de aprobación:	16/03/2018
Documentación utilizada:	DPC 6.0
Autor (es)	Asesoría Jurídica de Izenpe Área técnica de Izenpe
Cambios/Comentarios	La versión 6.1 es la actualización de la versión 6.00

CAMBIOS

	EPÍGRAFE / ACLARACION
Actualizaciones respecto a la versión anterior	– 1.1. Presentación. Se actualizan las referencias a los medios de identificación expedidos por Izenpe según lo requerido por el reglamento eIDAS. – 4.9.3., 6.1.7., 9.10 Se actualiza la dirección web de Izenpe, ahora www.izenpe.eus. – 5.8.1. En caso de cese de la actividad, se especifica que Izenpe informara sobre este cese al órgano competente con una antelación mínima de 2 meses. – 6.1.1. Generación del par de claves. Se indica que – Todas las claves criptográficas deben ser generadas siguiendo lo definido en ETSI TS 119 312. – El valor del exponente público es un número primo igual o superior a 3. – 6.5.1. Requisitos técnicos específicos de seguridad informática Se indica que todas las cuentas de operador con capacidad de emitir certificados tienen control de acceso basado en doble factor. – 7.2. Perfil de la lista de revocación de certificados Según se describe en RFC 6962, un precertificado no será considerado un certificado con las características definidas en la RFC 5280.

	– 7.3. Perfil OCSP.
	  – Conformidad de las respuestas OCSP conforme a la norma RFC 6960.
	  – 7.3.3. Se incorporan otros aspectos referentes al OCSP.
	– 9.13. Normativa aplicable. Actualización.
	– 9.14. Cumplimiento de la normativa aplicable. Actualización.

Aclaraciones	
Actualizaciones de formato.	
Eliminaciones.	