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 06 77 23

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.	

Información general _ versión 6.2 como actualización de la versión 6.1

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	6.2
Fecha de aprobación:	04/12/2018
Documentación utilizada:	DPC 6.1.
Autor (es)	Asesoría Jurídica de Izenpe. Área Técnica de Izenpe.
Cambios/Comentarios	La versión 6.2 es la actualización de la versión 6.1

CAMBIOS

	EPÍGRAFE / ACLARACION
Actualizaciones respecto a la versión anterior	– 9.6.8. Obligaciones del solicitante del certificado: se añade la exigencia de abono del importe del certificado. – 5.3.2 Requisitos de Formación: se añaden los requisitos de formación de operadores de RA. – 9.4. Protección de datos de carácter personal: se adecúa a la normativa vigente.
Aclaraciones	
Actualizaciones de formato.	
Eliminaciones.	

Información general _ versión 6.3 como actualización de la versión 6.2

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	6.3
Fecha de aprobación:	04/04/2019
Documentación utilizada:	DPC 6.2.
Autor (es)	Asesoría Jurídica de Izenpe. Área Técnica de Izenpe.
Cambios/Comentarios	La versión 6.3 es la actualización de la versión 6.2

CAMBIOS

	EPÍGRAFE / ACLARACION
Actualizaciones respecto a la versión anterior	– Apartado 1.1: actualizado el nivel de aseguramiento de los perfiles en HSM. Corregido error en nivel de aseguramiento del profesional en software – Apartado 1.1: añadido el perfil de dispositivo – Apartado 1.3.1: actualizado el árbol de CAs
Aclaraciones	
Actualizaciones de formato.	
Eliminaciones.	

Información general _ versión 6.4 como actualización de la versión 6.3

Control documental

Título :	Actualización de Prácticas de Certificación.
Versión:	6.4
Fecha de aprobación:	03/06/2020
Documentación utilizada:	DPC 6.3
Autor (es)	Responsable Seguridad
Cambios/Comentarios	La versión 6.4 es la actualización de la versión 6.3

CAMBIOS

EPÍGRAFE	ACLARACION
1. Introducción	• Actualizadas versiones de normas ETSI
1.1 Presentación	• Añadida la lista de servicios de confianza cualificados y no cualificados • Añadida la columna de tipo de firma eIDAS en cada perfil de certificado • Añadidos los perfiles de Mobile, seudónimo NQC y dispositivo IoT
1.3.1 Autoridades de Certificación	• Añadidos los perfiles de la CA raíz y de todas las CAs
1.4.2 Usos prohibidos del certificado	• Eliminada la prohibición de usar certificados para realizar trámites como RA
1.5.2 Datos de contacto	• Actualizado el teléfono de contacto
1.5.4 Procedimiento de aprobación de la DPC	• Actualizado el “Consejo de Administración” por “Comité de Seguridad” como el órgano responsable de la aprobación de la DPC
1.6.1 Definiciones	• Añadido el Reglamento de Protección de Datos • Reemplazada la definición de PSC por la de TSP
2.2 Publicación de información de certificación	• Eliminadas las referencias al servicio de publicación en www.izenpe.eus • Se ha añadido la referencia a las URLs test de SSLs de Izenpe
2.2.1 Política de publicación y notificación	• Eliminada obligación de mantener durante 30 días los cambios realizados en la DPC, y la de retirar las versiones antiguas
3.1.3 Unicidad de los nombres	• Se elimina el texto “Izenpe no emite certificados anónimos”

4.4.1 Proceso de aceptación del certificado	• Se sustituye la referencia a “contrato suscriptor” por “Términos y Condiciones de Uso”
4.4.3 Notificación de la emisión del certificado por la CA a otras entidades	• Se actualiza la política de publicación en los CT de Google
4.9.2 Quién puede solicitar la revocación	• Se detallan los perfiles que pueden solicitar la revocación, y se quita la referencia a cada política. En cada política se deberá referenciar a este apartado de la DPC
4.9.3 Tratamiento de las peticiones de revocación	• Se actualiza la relación de canales disponibles para solicitar una revocación. En cada política se deberá referenciar a este apartado de la DPC
4.9.10 Otras formas de avisos de revocación disponibles	• Se elimina la excepción de los corporativos para las notificaciones de revocaciones
5.1.2 Acceso físico a RAs	• Se actualiza la obligación de cumplir la Política de Seguridad de Izenpe por la Política de Seguridad de Proveedores
5.3.4 Requisitos y frecuencia de actualización formativa	• Se añade el requisito de formación anual en “Trusted Roles”
5.3.7 Requisitos de contratación de personal	• Se añade la obligación de cumplir con la Política de Seguridad de Proveedores por parte del personal subcontratado
6.1.1 Generación del par de claves	• Se añade la APP como contenedor de claves
6.1.5 Tamaños de claves y algoritmos utilizados	• Se actualiza SHA-256 con SHA-2
6.2.8 Método de activación de la clave privada	• Se redirige a la política específica para conocer los mecanismos de activación en cada caso
6.2.9 Método de desactivación de la clave privada	• Se corrige para redirigir a la política específica para conocer los mecanismos de desactivación en cada caso
6.3.2 Periodos de operación del certificado y periodos de uso del par de claves	• Se añade la duración de las subCAs diferentes a la de los EV
6.7 Controles de seguridad de red	• Se añade la existencia de sistemas IPS
7.3.3 Otros aspectos del OCSP	• Se añade información sobre la respuesta OCSP a consultas de certificados que no son de Izenpe
9.6.4 Obligaciones de información a usuarios	• Se sustituyen las referencias a “Condiciones de uso” por “Términos y Condiciones de uso y Acuerdo de Divulgación de Infraestructura de Clave Pública (PKI-PDS)” • Se eliminan las referencias al servicio de publicación de Izenpe

9.6.7 Obligaciones de la Entidad de Registro	• Añadida la obligación de firmar un acuerdo antes de comenzar a funcionar como Entidad de Registro, en caso de delegarse • Añadida la obligación de cumplir la Política de Seguridad de Proveedores
9.7.1 Responsabilidades de la autoridad de certificación	• Eliminado el importe del Seguro de Responsabilidad Civil
9.11.1 Procedimiento para los cambios	• Sustituido el Consejo de Administración por el Comité de Seguridad

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
Fecha: 2020.07.16 12:50:08 +02'00'