



ACTUALIZACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Referencia: IZENPE-ACTUALIZACIÓN DPC
Nº Versión: v 5.01
Fecha: 19 de julio de 2013

© IZENPE 2013

Este documento es propiedad de IZENPE. Únicamente puede ser reproducido en su totalidad

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

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



Información general

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 |



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

| EPÍFRASE | 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). |
| 9.6.2 | - 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. |