# ACTUALIZACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

| | |
|---|---|
| Referencia: | IZENPE-ACTUALIZACIÓN DPC |
| Nº Versión: | v 4.9 |
| Fecha: | 29 de marzo de 2011 |



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

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

# Control de Versiones

| Versión | Fecha | Autor(es) | Cambios/Comentarios |
|---|---|---|---|
| 4.9 Es la actualización de la versión 4.8 de la DPC | 29/03/2011 | Asesoría Jurídica de IZENPE | Modificaciones de la DPC versión 4.8 derivadas |

# Información general

## Control documental

| | |
|---|---|
| **Titulo :** | Actualización de Prácticas de Certificación. |
| **Código de referencia:** | |
| **Versión:** | 4.9 |
| **Fecha edición:** | 29/03/2011 |
| **Fecha de aprobación** | 29/03/2011 |
| **Documentación utilizada:** | DPC 4.8 |

La Declaración de Prácticas de Certificación de Izenpe, S.A., de acuerdo a su epígrafe 8, 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: PLAZOS CONSERVACIÓN DOCUMENTACIÓN

**Enmienda:**

Consecuencia de la emisión por IZENPE de certificados con *Validación Extendida* y tras la auditoría realizada en cumplimiento con la *Norma Webtrust for EV* se aclara que, tanto respecto a la documentación referente a los certificados del tipo *EV* como a los certificados no reconocidos, IZENPE conserva la información y documentación durante 7 años (ver epígrafe 2.1.2 Obligaciones de prestación del servicio).

## ENTRADA 2: ACLARACIONES VARIAS

**Enmienda:**

Con la finalidad de mejorar la comprensión de algunos epígrafes de la DPC, se realizan las siguientes aclaraciones,

I. *Certificado reconocido*.

- Los certificados reconocidos de firma electrónica pueden también emplearse, si así se define en el tipo de certificado correspondiente, para firmar mensajes de autenticación, en particular desafíos de cliente SSL o TLS, correo electrónico seguro S/MIME, cifrado sin recuperación de claves u otros.

  Se elimina la consideración estas opciones del certificado como equiparables con la manuscrita (ver epígrafe 1.3.4.1.1 *Certificado reconocido,* apartado b)).
- Se aclara que únicamente los certificados reconocidos del tipo *Sede* y *Sede EV,* se emiten para identificar de forma fiable sitios web (ver epígrafe 1.3.4.1.1 *Certificado reconocido,* apartado c)).

II. *Límites de uso de los certificados*.

Se aclara que ningún certificado objeto de regulación de esta Declaración de Prácticas de Certificación se puede emplear para realizar trámites Como Entidad de Registro (ver epígrafe 1.3.4.3. *Límites de uso de los certificados,* párrafo tercero*).*

III. Solicitud de certificado

Se adecúa la Declaración de Prácticas de Certificación a lo determinado en la *Documentación específica para cada certificado* estableciendo que *Acreditada la identidad del solicitante ante la Entidad de Registro, éste deberá firmar la Solicitud*

*de Emisión del certificado, aceptando de esta forma el Contrato de Suscriptor y las Condiciones de Uso* (ver epígrafe 1.4 *Solicitud de certificado*)

IV. Frecuencia de emisión de listas de certificados revocados

Se determina, en cuanto a las CRLs que, si no se producen revocaciones la Lista de Revocación de Certificados, ésta se regenera diariamente (ver epígrafe 4.4.10, *Frecuencia de emisión de listas de certificados revocados,* párrafo segundo).

V. Tamaños de claves y algoritmos utilizados

Además de en la CA raiz 2007, en las CAs subordinadas se ha emitido un segundo certificado con SHA-256 (ver epígrafe 6.1.5*, Tamaños de claves y algoritmos utilizados).*

VI. Generación de parámetros de clave pública

Tanto respecto a las claves generadas en soporte HSM como a las claves criptográficas generadas en dispositivo criptográfico: se siguen las recomendaciones FIPS 140-2 Nivel 3 (para las primeras y 2 para las segundas) (ver epígrafe 6.1.7).