



## DOCUMENTACIÓN ESPECÍFICA PARA EL CERTIFICADO DE SERVIDOR SEGURO SSL

Referencia: IZENPE-Doc. Servidor Seguro SSL  
Nº Versión: v 1.0  
Fecha: 16 de noviembre de 2009

---

© IZENPE 2009

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](http://www.izenpe.com)  
[info@izenpe.com](mailto:info@izenpe.com)  
Tel.: 945 017 490



## Contenido

<i>Capítulo/sección</i>	<i>Página</i>	
1	Introducción	4
1.1	Presentación	¡Error! Marcador no definido.
1.2	Descripción del certificado	4
1.3	Identificación	4
1.4	Comunidad y aplicabilidad	4
1.4.1	Tendrán la consideración de partes intervinientes,	4
1.4.1.1	Suscriptores de certificados	5
1.4.1.2	Solicitantes de certificados	5
1.4.1.3	Firmante del certificado	5
1.4.2	Aplicabilidad	5
1.5	Validez del certificado	6
2	Disposiciones generales	7
2.1	Obligaciones de identificación	7
2.2	Obligaciones del suscriptor/a del certificado	7
2.3	Responsabilidad civil del suscriptor/a de certificado	7
3	Requisitos operativos	8
3.1	Solicitud de certificado	8
3.2	Acreditación	8
3.2.1	De la identidad del/la solicitante	8



3.2.2	De la organización	9
3.3	Validación	10
3.4	Emisión de certificado	14
3.5	Entrega de certificado	14
3.6	Devolución de los certificados	14
3.7	Suspensión y reactivación de certificados	14
3.8	Revocación de certificados	17
3.9	Renovación de certificados	18
3.10	Auditorias e incidentes	18
4	Gestión del cambio	20
5	Perfiles de certificados y listas de certificados revocados	21



## 1 Introducción

---

El presente documento recoge la *Documentación específica del certificado de Servidor Seguro SSL* emitido por “Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.” (en adelante, IZENPE).

Su finalidad es detallar y completar para este tipo de certificado lo definido de forma genérica en la Declaración de Prácticas de Certificación de IZENPE.

El presente documento estará publicado en [www.izenpe.com](http://www.izenpe.com) y accesible con una disponibilidad de 24x7.

### 1.1 Descripción del certificado

El certificado de Servidor Seguro (SSL) se utiliza para establecer comunicaciones de datos en servidores web vía TLS/SSL.

### 1.2 Identificación

Con el objeto de identificar el certificado del tipo *Servidor Seguro SSL*, IZENPE le ha asignado el siguiente identificador de objeto (OID).

CERTIFICADO	OID
Certificado de Servidor Seguro SSL	1.3.6.1.4.1.14777.1.2.1

### 1.3 Comunidad y aplicabilidad

#### 1.3.1 Tendrán la consideración de partes intervinientes,

1. Suscriptor del certificado
2. Solicitante



3. Firmante
4. Poseedor de claves

#### **1.3.1.1 Suscriptor del certificado**

El/La suscriptor/a es la entidad identificada en el certificado.

#### **1.3.1.2 Solicitante del certificado**

El certificado de *Servidor Seguro SSL* debe ser solicitado por una persona, en su propio nombre o en nombre de una organización.

#### **1.3.1.3 Firmante del certificado**

El firmante es la entidad identificada en el certificado.

#### **1.3.1.4 Poseedor de claves**

El poseedor de claves será el propio servidor que realiza la operación de forma automática bajo la responsabilidad del suscriptor/a del certificado.

### **1.3.2 Aplicabilidad**

Los certificados del tipo *Servidor Seguro SSL*, serán utilizados por los/as suscriptores/as para:

- La identificación de la Entidad titular del sitio web, proporcionando una garantía razonable para el/la usuario/a de un navegador de Internet de que el sitio web al que accede es titularidad de la entidad identificada en el certificado.
- La encriptación de las comunicaciones entre los/as usuarios/as y el sitio web, facilitando el intercambio de las claves de cifrado necesarias para el cifrado de la información a través de Internet.
- Además, IZENPE se compromete a cumplir, por medio de la implantación de lo indicado en las guías del CAB Forum que se publican en [www.cabforum.org](http://www.cabforum.org) incluyendo la aceptación de los programas de auditoría especificados en las mismas.



## 1.4 Validez del certificado

IZENPE emite los certificados de *Servidor Seguro SSL* con una validez de 3 años. Transcurrido este plazo, el certificado quedará caducado y no será operativo al estar la fecha de caducidad incluida en el propio certificado. El certificado no aparece en los mecanismos de verificación de revocaciones.

La renovación implicará la obligación del solicitante de presentar de nuevo la documentación establecida en el apartado 3 de la presente *Documentación específica para el Certificado de Servidor Seguro SSL, Requisitos Operativos*.

.



## 2 Disposiciones generales

---

### 2.1 Obligaciones de identificación

IZENPE comprueba en los registros correspondientes, por si misma o por medio de las Entidades Usuarias con las que suscriba el correspondiente convenio, la identidad y cualesquiera otras circunstancias personales de los solicitantes, suscriptores/as de los certificados.

### 2.2 Obligaciones del suscriptor/a del certificado

En el supuesto del Certificado de SSL, son obligaciones del/la solicitante las recogidas en el apartado 2.1.5 de la Declaración de Prácticas de Certificación, *Obligaciones del suscriptor*, excepto las establecidas en la letra j).

### 2.3 Responsabilidad civil del suscriptor/a de certificado

En cuanto a la responsabilidad civil del suscriptor/a del certificado, ver Declaración de Prácticas de Certificación apartados 2.2.3 *Responsabilidad civil del suscriptor de certificado* y 2.2.4 *Responsabilidad civil de los terceros que confían en los certificados*



## 3 Requisitos operativos

---

### 3.1 Solicitud de certificado

Las Entidades realizarán las solicitudes de certificados para los servidores que estimen oportuno.

El/La solicitante, deberá completar el formulario de solicitud del certificado y aportar la documentación indicada.

La tramitación del formulario de solicitud se realizará ante IZENPE a través de 2 vías:

- Vía telemática: en la dirección web <http://www.izenpe.com> los/as interesados/as disponen del formulario de solicitud, que podrá ser completado y enviado telemáticamente a IZENPE almacenándolo como un prerregistro.
- O presencialmente: El/La solicitante podrá personarse en cualquiera de las Entidades de Registro señaladas en el listado publicado en <http://www.izenpe.com> y realizar la solicitud de certificado.

Estas solicitudes serán gestionadas por IZENPE o, en su caso, por la Entidad de Registro que determine IZENPE (en adelante las referencias a IZENPE se entenderán realizadas a IZENPE o a la Entidad de Registro).

Previamente, el/la suscriptor/a habrá generado un par de claves en el propio servidor entregando a IZENPE la clave pública junto con el formulario de solicitud.

### 3.2 Acreditación

#### 3.2.1 De la identidad del/la solicitante

El/La solicitante del certificado deberá personarse ante la Entidad de Registro y presentar original o copia auténtica de la siguiente documentación:

- a. DNI o pasaporte, en el caso de ciudadano nacional.
- b. En caso de ciudadano extranjero:



- I. Miembro de la Unión Europea o de Estados parte del Espacio Económico Europeo, será exigible un NIE acompañado de un documento de identidad en vigor a efectos de comprobación de su identidad.
  - II. En relación a ciudadanos extracomunitarios, será exigible la tarjeta de residencia.
- c. Podrá prescindirse de la personación ante la Entidad de Registro:
- Si la firma de/la solicitante en la solicitud de emisión del certificado ha sido legitimada en presencia notarial.
  - O en los supuestos contemplados en el artículo 13.4 de la LFE, salvo que en el procedimiento de emisión fuera exigible la personación del/la solicitante a efectos distintos a la identificación, por ejemplo garantizar una entrega segura del certificado.

La Entidad de Registro levantará acta de comprobación de la identidad del/la solicitante.

### 3.2.2 De la organización

Se entregará la siguiente documentación **sobre la entidad solicitante**,

- Número de Identificación Fiscal (N.I.F.) de la Entidad.
- Los organismos y sociedades públicas aportarán la resolución legal (ley, decreto,...) dictada por el organismo constituyente y al cual estén adscritos. Debe constar fecha y referencia a dicha norma legal.
- Las sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Mercantil, acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado del Registro Mercantil relativo a los datos de constitución y personalidad jurídica de las mismas.
- Las Asociaciones, Fundaciones y Cooperativas acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado del registro público donde consten inscritas, relativo a su constitución.
- Las sociedades civiles y demás personas jurídicas, aportarán original o copia auténtica del documento público que acredite su constitución de manera fehaciente.



El/La **solicitante** del certificado deberá aportar la **siguiente documentación**,

- Original o copia auténtica de la escritura pública o documento oficial donde derive la representación acompañada de una manifestación responsable del solicitante confirmando sus facultades y la vigencia de las mismas.
- El solicitante deberá aportar la documentación exigida en este apartado únicamente en la primera solicitud de emisión del certificado, bastando en las sucesivas solicitudes una declaración de que no se han modificado las circunstancias del solicitante ni de la persona jurídica a la que representa.
- No será necesario obtener la justificación documental de la existencia de la entidad ni de las facultades de representación de quien actúa en su nombre, siempre que estos hechos estuvieran regulados por norma.

La Entidad de Registro levantará acta de comprobación de la documentación

### **3.3 Validación**

IZENPE validará la documentación aportada por el/la solicitante y no iniciará el proceso de emisión de certificados hasta que la documentación requerida haya sido entregada y validada.

La Asesoría Jurídica de IZENPE, verificará la documentación referente a la entidad usuaria,

- De forma general, se admitirá como válido y no será necesario comprobar la validez de documentos que hayan sido certificados por un notario.
- Boletines oficiales de ámbito nacional o regional de los organismos públicos a los que pertenecen organismos y empresas públicas.
- Registros públicos en los que legalmente deben estar registradas entidades.
- Con respecto a dominios y direcciones de Internet, IZENPE consultará únicamente en registradores asignados por ICANN/IANA para nombres de dominio y direcciones asociadas al certificado.
- Se verifica que el dominio no consta en los listados como de riesgo (*ver capítulo 3.8*).



- Constitución, fecha, razón social, NIF: se comprobará la constitución del organismo solicitante, verificando mediante consulta al registro o boletín oficial donde deba constar su existencia y coincidencia con la documentación aportada por el solicitante.
- Dirección: se comprobará si los datos del registro coinciden con la documentación aportada.

En el caso de que ambas direcciones no sean coincidentes IZENPE verificará que la dirección que consta en la solicitud corresponde a una ubicación en la que la entidad solicitante opera de manera estable. Esta verificación se podrá llevar a cabo mediante declaración firmada o justificantes del pago de impuestos.

- Teléfono. IZENPE deberá comprobar que el teléfono (deberá ser un teléfono fijo, no móvil) pertenece a la entidad solicitante (consulta en el registro en paginas amarillas y posterior comprobación mediante llamada).
- Evidencias de la actividad de la organización: Certificado emitido por una entidad bancaria acreditativo de la existencia de una cuenta a nombre de la entidad solicitante, justificantes de pago de impuestos locales.
- Sobre el dominio de Internet (*no es aplicable para dominios internos*):
  - Consulta a la base de datos *whois*, verificar que el dominio está registrado, consultando registradores válidos. Se adjuntará copia impresa de la consulta *whois* al acta de validación.
  - Existe un listado de registradores admitidos por tipo de dominio (<http://www.iana.org/domains/root/db/>) ya sean genéricos (gTLD's) o de país (*country-code*, ccTLDs) que indica cual es el registrador oficial delegado para cada tipo de dominio. En concreto, *se puede consultar el whois para los más habituales en*

Dominios .com .net .org .info	Network Solutions	<a href="http://www.networksolutions.com/whois/index.jsp">http://www.networksolutions.com/whois/index.jsp</a>
Dominos .es	EsNIC	<a href="http://www.nic.es">http://www.nic.es</a>

- Se comprobará que el titular (*registrant*) coincide con la organización solicitante. En caso de no coincidir, el solicitante deberá aportar documentación que justifique el derecho de uso por parte del titular. IZENPE contactará con el titular que figure en el

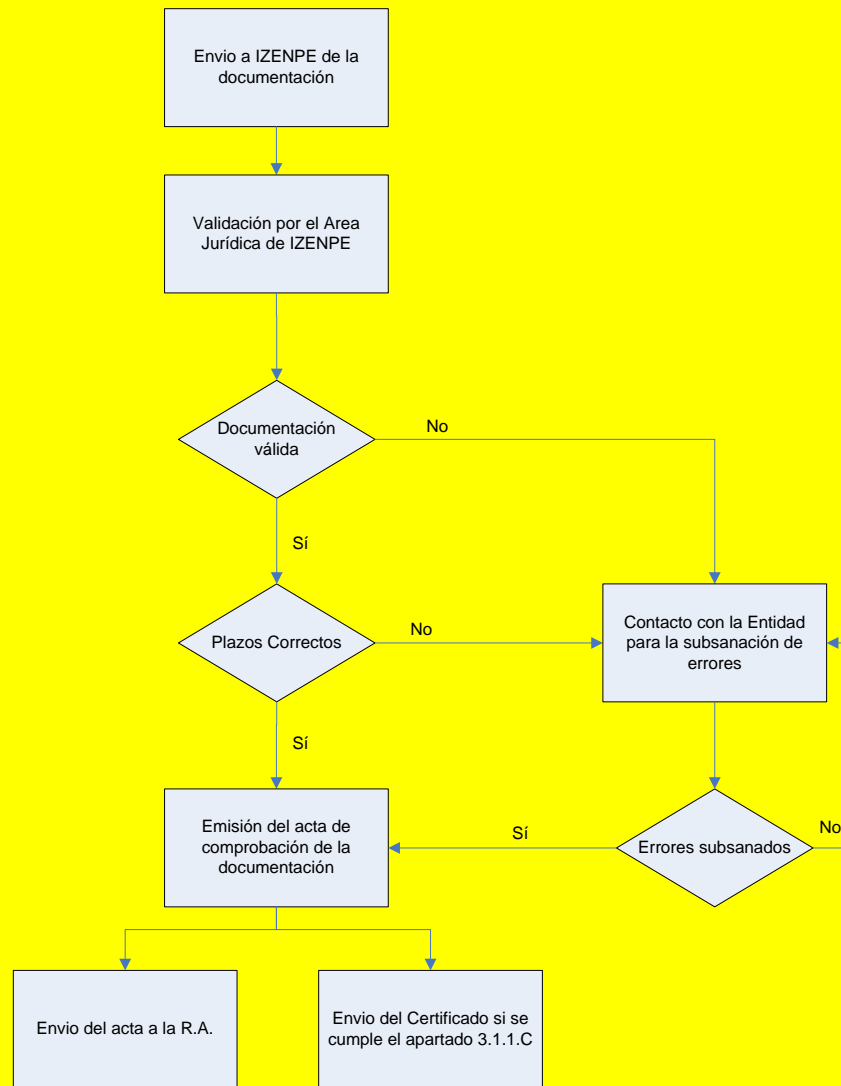


*whois* para verificar que el solicitante tiene el derecho de uso del dominio o subdominio.

La petición técnica es revisada y validada por el Área Técnica de IZENPE.

La Asesoría Jurídica de IZENPE levantará Acta de Comprobación presentada por el solicitante. Hará constar en el acta además, el registro público utilizado para validar la información.

Procedimiento de verificación de documentación a efectos de emisión del certificado SSL EV



\* Según Documentación específica para el certificado de Servidor Seguro SSL EV



### **3.4 Emisión de certificado**

Acreditada la identidad del/la solicitante ante la Entidad de Registro y comprobada la documentación exigida, éste deberá entregar la clave pública, firmar la solicitud de emisión del certificado, aceptando de esta forma el contrato de suscriptor, e IZENPE procederá a la emisión del certificado.

Cualquier modificación relativa a las circunstancias que constaran en el certificado con posterioridad a la emisión del mismo, deberá ser comunicada a IZENPE, ya que podría conllevar su revocación.

### **3.5 Entrega de certificado**

IZENPE entregará el certificado, por un medio seguro (por ejemplo, correo electrónico firmado, entrega presencial. etc.), al/lareponsable técnico.

El/la responsable técnico informará al titular del certificado y a IZENPE de la recepción e instalación del certificado.

El solicitante deberá devolver firmada a IZENPE la Hoja de Entrega y Aceptación en el plazo máximo de 1 mes, en caso contrario se revocará el certificado.

### **3.6 Devolución de los certificados**

La organización dispone de un plazo de 15 días, desde la entrega del certificado, para comprobar el correcto funcionamiento del mismo y en caso de que fuera necesario devolverlo a IZENPE.

Si la devolución se debiese a defectos de funcionamiento por causas técnicas (entre otras, mal funcionamiento del soporte del certificado, problemas de compatibilidad de programas, error técnico en el certificado, etc.) o a errores en los datos contenidos en el certificado, IZENPE revocará el certificado emitido y procederá a emitir un nuevo certificado.



### 3.7 Suspensión y reactivación de certificados

El poseedor de claves podrá solicitar la suspensión vía telefónica (902 542 542) identificándose y dando su contraseña de identificación telefónica o en su defecto los datos requeridos por IZENPE que permiten la correcta identificación del solicitante.

IZENPE tiene capacidad permanente (24x7) para tramitar la suspensión de certificados. Una vez suspendido un certificado éste queda incluido en la nueva lista de revocación (CRL) que se genera automáticamente y en el servicio de verificación avanzada. En cualquier caso la CRL se actualiza cada día.

Para un certificado suspendido el/la suscriptor o el poseedor/a de claves que haya solicitado previamente la suspensión del certificado pueden solicitar su reactivación.

Para ello debe personarse ante una Entidad de Registro e identificarse, presentando los documentos requeridos a efectos de autenticación de la identidad de una persona físico.

Si no se solicita la reactivación de un certificado suspendido, éste pasa automáticamente a ser revocado en un plazo de 15 días naturales.

En el caso de que la suspensión del certificado con la finalidad de cumplir con un plazo inmediato en la suspensión de certificados una vez que se produce la solicitud del usuario se define el siguiente proceso

Tarea	Comentarios	Documen tos
<b>1.- Llamada de usuario</b>	<b>Llamada del usuario al número del CAU</b>  En el caso de la suspensión de un certificado tiene una entrada específica, y en el caso de los certificados SSL el procedimiento varía ya que en este caso, y al pulsar la opción adecuada, la llamada se redirige inmediatamente al operador	
<b>2.- Conexión a la aplicación de apoyo</b>	Si la llamada contiene una solicitud de suspensión el operador se conectará a través de Internet a la aplicación de suspensión de certificados de Izenpe para ejecutar la suspensión, para ello usará su certificado digital y a través de un túnel abierto VPN accederá a la aplicación de gestión de certificados	



<p><b>3.- Identificación de usuario</b></p>	<p><b>Identificación de usuario</b></p> <p>Una vez conectado a la aplicación, el operador, que se identifica como operador de IZENPE, solicita al usuario solicitante de la suspensión, la siguiente información</p> <ul style="list-style-type: none"> <li>▪ Nombre, empresa, cargo</li> <li>▪ O clave de identificación telefónica para la suspensión del certificado.</li> </ul> <p>Si el usuario se identifica correctamente se procede a la suspensión del certificado.</p> <p>Si no dispone de la clave o la información aportada no coincide, se indica al usuario que no se puede hacer la suspensión.</p>	
<p><b>4- Suspensión de certificados</b></p>	<p><b>Suspensión de certificados</b></p> <p>Una vez identificado correctamente el solicitante de la suspensión, el operador mediante la aplicación de suspensión de certificados de IZENPE ejecutará la suspensión.</p> <p>Una vez realizada la comprobación, el operador informa al usuario que el certificado ya no es operativo y que dispone de 15 días naturales para solicitar la reactivación del certificado personándose en una Oficina de Registro y que de no hacerlo será revocado definitivamente.</p>	<p>Manual de usuario de la aplicación de suspensión</p>
<p><b>5.- Notificación a IZENPE</b></p>	<p><b>Notificación al Responsable de Seguridad IZENPE</b></p> <p>El operador generará un aviso (J99) al Responsable de seguridad de IZENPE, indicando</p> <ul style="list-style-type: none"> <li>▪ Fecha/hora de llamada de usuario</li> <li>▪ Fecha/hora de llamada de operador.</li> <li>▪ Datos del usuario solicitante (SIN la clave).</li> <li>▪ Algo que identifique el certificado implicado.</li> <li>▪ Si disponía de la clave correcta             <ul style="list-style-type: none"> <li>○ Resultado de la operación de suspensión</li> </ul> </li> <li>▪ O si no disponía de la clave correcta</li> </ul>	<p>Acceso a J99</p>



	<ul style="list-style-type: none"><li>o No se ha suspendido ningún certificado</li><li>▪ Cualquier otra incidencia producida durante la suspensión del certificado.</li></ul>	
<b>6.- Análisis y apertura de incidente</b>	<b>Análisis y apertura de incidente</b>  El Responsable de Seguridad analizará el incidente reportado y en caso de considerarlo necesario. <ul style="list-style-type: none"><li>▪ Reportará el problema al APWG</li><li>▪ Registrará la incidencia en la base de datos de incidentes de seguridad de IZENPE para futuros solicitantes.</li></ul>	

### 3.8 Revocación de certificados

El/La solicitante de la revocación de un certificado debe personarse ante IZENPE e identificarse, presentando los documentos de identificación requeridos a efectos de autenticación de la identidad de una persona física (ver apartado 3.2.1). En caso de no ser horario de apertura de las Entidades de Registro deberá solicitarse la suspensión del certificado vía telefónica.

Deberá cumplimentar la solicitud de revocación justificando la causa y si fuera necesario, aportar la documentación que acredite la existencia del hecho que origina la pérdida de vigencia del certificado.

Las personas autorizadas para solicitar la revocación son las mismas que las autorizadas para solicitar la emisión en las mismas condiciones que se describen en 3.1 "Solicitud de certificado".

Los administradores de IZENPE y las Entidades de Registro están autorizados para solicitar la revocación de certificados de suscriptor de entidad final. Se autentica la identidad de los administradores a través de control de acceso utilizando SSL y autenticación de cliente, antes de permitir que se realicen funciones de revocación / suspensión.

Además de lo previsto en la Declaración de Prácticas de Certificación *Causas de revocación de certificados*, de acuerdo con la presente *Documentación específica para el certificado de Servidor seguro*, IZENPE deberá,

1. Presentar a los/as suscriptores/as, a terceras partes y a los navegadores de Internet instrucciones claras para la presentación de denuncias o sospechas de compromiso de la



clave privada, de mal uso de certificados SSL o de otros tipos de fraude, compromiso, mal uso, o conducta impropia en relación con los Certificados SSL.

2. IZENPE investigará los informes de problemas dentro de las veinticuatro horas siguientes a su recepción y decidirá sobre la revocación como mínimo atendiendo a los siguientes criterios:
  - La naturaleza del supuesto problema;
  - El número de informes recibidos de problemas de un Certificado SSL o página web.
  - La identidad de los denunciantes.
  - La legislación vigente.
3. IZENPE mantiene una capacidad 24x7 para responder a cualquier incidente de prioridad alta con respecto a estos certificados, y en su caso, comunicar la revocación del certificado SSL objeto de denuncia.

### **3.9 Renovación de certificados**

Para renovar un certificado, bien porque haya sido revocado o porque haya caducado, el suscriptor deberá solicitar un nuevo certificado, siguiendo el proceso de emisión de certificados establecido.

IZENPE notifica la caducidad vía correo electrónico con 30 días de antelación a la caducidad del certificado al/la titular y al/la representante técnico/a para proceder a su renovación, remitiendo el formulario de solicitud. Si no hay respuesta contactará telefónicamente.

La documentación que debe aportar el/la solicitante y los pasos de validación, emisión y entrega de certificados son los mismos que para la emisión de un certificado nuevo.

### **3.10 Auditorías e incidentes**

IZENPE mantiene los siguientes criterios con relación a la información disponible para auditorías y análisis de incidentes que pueda haber con los certificados SSL emitidos y el tratamiento de los mismos:

- Los usuarios de certificados pueden comunicar a IZENPE quejas o sugerencias a través de los siguientes medios:
  - Vía telefónica: 902 542 542



- Vía mail: [info@izenpe.com](mailto:info@izenpe.com)
- Mediante la cumplimentación del formulario disponible en la dirección [www.izenpe.com/](http://www.izenpe.com/)
  - Existe un registro interno de incidentes que se hayan producido con los certificados emitidos (incidentes de seguridad gestionados por el Comité de Seguridad de IZENPE). Estos incidentes se registran, analizan y solucionan según los procedimientos del SGSI de IZENPE.
  - En la planificación anual de auditorías se audita específicamente la operativa de emisión de los certificados SSL con una muestra mínima del 3% de los certificados emitidos.
  - En la DPC (capítulo 4.6.2) se define el periodo de conservación de la documentación (actas de identificación, solicitudes,...).
  - Se mantienen registros de las operaciones realizadas con certificados SSL (*logs*) por un periodo igual o mayor a 7 años (en relación al capítulo 4.5.3 de la DPC).
  - IZENPE reporta aquellos casos que considere como incidentes (casos de fraude, phishing, etc.) en el sitio web del Anti-Phising Work Group ([www.apwg.org](http://www.apwg.org)) y verifica antes de la emisión que el solicitante o representantes no estén listados en la base de datos interna de incidentes de seguridad de IZENPE; en todo caso se reserva el derecho de emitir certificados ante situaciones sospechosas.



## 4 Gestión del cambio

---

Las modificaciones de este documento serán aprobadas por la Dirección General de IZENPE con el visto bueno del Comité de Seguridad de IZENPE. Estas modificaciones estarán recogidas en un documento de Actualización de Documentación Específica por certificado cuyo mantenimiento está garantizado por IZENPE.

Las versiones actualizadas de la documentación específica podrán ser consultadas en la dirección [www.izenpe.com](http://www.izenpe.com).



## 5 Perfiles de certificados y listas de certificados revocados

Campo / extensión	Opcional / Crítica	Contenido
<b>version</b>		Versión 3
<b>serialNumber</b>		Número secuencial único
<b>signature</b>		sha-1WithRSAEncryption
<b>issuer</b>		Igual al campo subject del certificado de la CA emisora
<b>validity</b>		3 años
<b>subject</b>		
CN		Dominio DNS o dirección IP
OU		Departamento
O		Nombre de la organización
L		Localidad
ST		Provincia
C		ES
<b>subjectPublicKeyInfo</b>		RSA 1024 bits mínimo
<b>extensions</b>		
<b>issuerAltName</b>		Igual a la extensión subjectAltName del certificado de la CA emisora
<b>subjectAltName</b>	Opcional	Igual a la extensión subjectAltName de la petición, si está presente
<b>extendedKeyUsage</b>		serverAuth
<b>netscapeCertType</b>		SSL_server
<b>subjectKeyIdentifier</b>		Identificador de la clave pública
<b>authorityKeyIdentifier</b>		Incluir campos keyIdentifier y IssuerAndSerialNumber
<b>certificatePolicies</b>		



<b>policyIdentifier</b>		1.3.6.1.4.1.14777.1.2.1 (1.3.6.1.4.1.14777.101.2.1 en Desarrollo)
<b>cpsURI</b>		<a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>
<b>userNotice</b>		Bermeen mugak ezagutzeko <a href="http://www.izenpe.com">www.izenpe.com</a> Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en <a href="http://www.izenpe.com">www.izenpe.com</a> Consulte el contrato antes de confiar en el certificado
<b>cRLDistributionPoints</b>		<a href="http://crl.izenpe.com/cgi-bin/crlinterna2">http://crl.izenpe.com/cgi-bin/crlinterna2</a>
<b>authorityInfoAccess</b>		ocsp <a href="http://ocsp.izenpe.com:8094">http://ocsp.izenpe.com:8094</a>
<b>keyUsage</b>	Crítica	digitalSignature, nonRepudiation, keyEncipherment