

Certificados de servidor seguro SSL/TLS

Guía de gestión de certificados SSL



SSL

¿Qué certificado escoger?

Existen diferentes tipos de certificados de servidor seguro según necesidad y nivel de seguridad requerido.

En el caso de las administraciones públicas un SSL cualificado es el indicado para sus sedes electrónicas.

Ventajas de un SSL

- Aseguran su sitio con **máximas garantías**.
- Están respaldados por un seguro de responsabilidad civil.
- Van firmados con algoritmos **SHA-2 y de 2048 bits**.
- Cumplen los más altos estándares criptográficos y las exigencias de CABForum.
- Están **reconocidos en los navegadores y sistemas operativos** más importantes
- **Mejoran el posicionamiento** en las búsquedas en Google, (ofrece un posicionamiento más alto a los sitios asegurados con SSL).
- Emitidos bajo la **comprobación de transparencia** exigida por Google.
- **Herramienta de gestión** de los certificados vivos, revocados y caducados.

Tipos de certificados SSL



CERTIFICADO DE DOMINIO SSL DV

- Validación rápida y sencilla
- Se comprueba exclusivamente el dominio
- Hasta dos nombres alternativos en precio base
- Permite incluir wildcard



CERTIFICADO DE ORGANIZACIÓN SSL OV

- Se comprueba el dominio y la organización
- Hasta dos nombres alternativos en precio base
- Permite incluir wildcard



CERTIFICADO CUALIFICADO SSL Q

- Cualificado según Reglamento Europeo 910/2014 (eIDAS)
- Hasta dos nombres alternativos en precio base

Perfiles necesarios



PERSONA REPRESENTANTE/CLIENTE

Firmará el alta de la entidad **TITULAR DEL DOMINIO** y autorizará la habilitación de las personas autorizados.

Los **cambios en personas autorizadas** suponen una nueva petición firmada por la persona representante.

Deberá **firmar todas las peticiones de certificados cualificados**.

Debe utilizar un **certificado cualificado Izenpe o eDNI** en vigor.



Gestión de
clientes/entidades



Gestión de
solicitudes y
certificados



PERSONAS AUTORIZADAS

Quienes están autorizados para gestionar SSL en nombre de una entidad. No es necesario que pertenezcan a la entidad titular.

Todos visualizarán las acciones de todos los certificados de todas las entidades donde estén autorizados.

Pueden utilizar cualquier certificado cualificado aceptado en las TSL.

Alta y autorización:

Requisitos para usar la aplicación



Acceso a la aplicación:

<https://servicios.izenpe.com/partners/>

Alta

- La solicitud de alta en la aplicación puede realizarla cualquier persona, no es necesario que pertenezca a la entidad titular.
- La solicitud generada (PDF) deberá firmarla la persona con poder/autoridad en la entidad, (ej. alcalde). Incluirá a las personas a las que se autoriza para la gestión de los certificados.
- Izenpe verificará el documento de solicitud y avisará de la habilitación para que las personas autorizadas puedan comenzar a tramitar.



Personas autorizadas

- Accederán a la aplicación con un medio de identificación electrónica de Izenpe profesional o personal (BakQ, ciudadano, corporativo...), o con un eDNI.
- Pueden pertenecer o no a la entidad, es decisión del representante.
- Una misma persona puede estar autorizada para diferentes entidades.

Esta dirección de correo electrónico recibirá todas las notificaciones relativas a las solicitudes de certificados DV u OV

Los datos nominales deben coincidir con la firma del representante con la que se va a hacer el alta. Debe tener en cuenta que el representante debe ser una figura dentro de la entidad con poderes necesarios para solicitar certificados SSL y delegar su gestión. **Si no lo tiene claro, es recomendable consultar con Izenpe.**

Teléfono: contacto del representante, se recoge únicamente para gestionar incidencias.
Email: a esta dirección de correo **llegarán las verificaciones de las solicitudes de certificados cualificados** - email con link para verificación (SSL Cualificados). Dichas verificaciones las deberá firmar el representante. Podéis indicar cualquier correo, pero **las verificaciones de solicitudes únicamente las podrá hacer el representante mediante firma digital y con el complemento Idazki desktop. Certificados admitidos para la firma de solicitudes cualificadas: eDNI, Izenpe.**

El certificado utilizado para firmar las solicitudes de SSL cualificado deben cumplir dos requisitos:

1. Es un certificado cualificados de Izenpe o un eDNI.
2. Para la emisión del mismo se ha realizado una identificación presencial.

Datos cliente

Debe rellenar todos los datos obligatorios (marcados con *)

Datos entidad

CIF entidad*

Nombre oficial entidad*

Nombre comercial entidad

Calle: Número: Piso: Mano:

Localidad: Provincia: País: Código Postal:

Email notificaciones (DV, OV)*

Datos de Contacto Representante

Extranjero

Nombre:* Primer Apellido:* Segundo Apellido:*

DNI:* Email:* Teléfono:*

CIF entidad* Cargo representante:*

Nombre entidad*

Datos Facturación

Copiar datos cliente

Calle: Número: Piso: Mano:

Localidad: Provincia: País: Código Postal:

Términos y Condiciones

[Referencia a contrato suscriptor](#)

Listado de solicitantes autorizados

[Añadir solicitante](#)

[Imprimir solicitud](#)

[Alta/Modificación Cliente](#) [Cancelar](#)

CIF entidad: letras mayúsculas, sin espacios.
Nombre oficial entidad: se recupera de la BBDD asociada al CIF
Dirección Postal: esta debe ser la dirección postal de la entidad / sede.

Términos y Condiciones

[Referencia a contrato suscriptor](#)

Listado de solicitantes autorizados

Añadir solicitante

Imprimir solicitud

Alta/Modificación Cliente Cancelar

Permite ir añadiendo personas autorizadas para esa entidad cliente. Añadimos los solicitantes a los que el representante va a dar permiso para gestionar las solicitudes SSL. Se pueden cargar los solicitantes mediante un fichero de texto con el formato JSON que se indica en el aviso informativo.

Imprimir solicitud: Una vez cumplimentado el formulario, se imprimimos la solicitud.

Se guarda un documento PDF donde figurará la información de la solicitud. Comprobamos que todo es correcto y ya se lo podemos facilitar al representante para que lo firme. Una vez descargado el PDF salimos de la aplicación pulsando “Alta/Modificación Cliente”

Alta/Modificación cliente: Guarda los cambios introducidos en el formulario.

Cancelar: Elimina los cambios introducidos y no guardados anteriormente.

Carga Solicitud Firmada

Cuando dispongamos del impreso de alta cliente firmado por el representante, volvemos a acceder a la aplicación mediante “Alta/Modificación Cliente” y al final de la página tendremos activo el menú “Subir Solicitud Firmada”:

Subimos la solicitud firmada pulsando “Alta/Modificación Cliente”:

Y esperamos a recibir la notificación correspondiente al VºBº del alta. Normalmente entre 1-3 días.

En caso de ser rechazada, os podéis poner en contacto en la dirección operaciones@izenpe.eus para conocer el motivo.

Subir Solicitud Firmada

Solicitud Firmada

Seleccionar archivo | Ningún archivo seleccionado

The screenshot displays a web interface for client management. At the top, there are two tabs: 'Activos' (selected) and 'Pendientes'. Below the tabs, there are two buttons: 'Nuevo cliente' and 'Volver'. The main content area is titled 'Gestión de clientes' and contains a table with the following data:

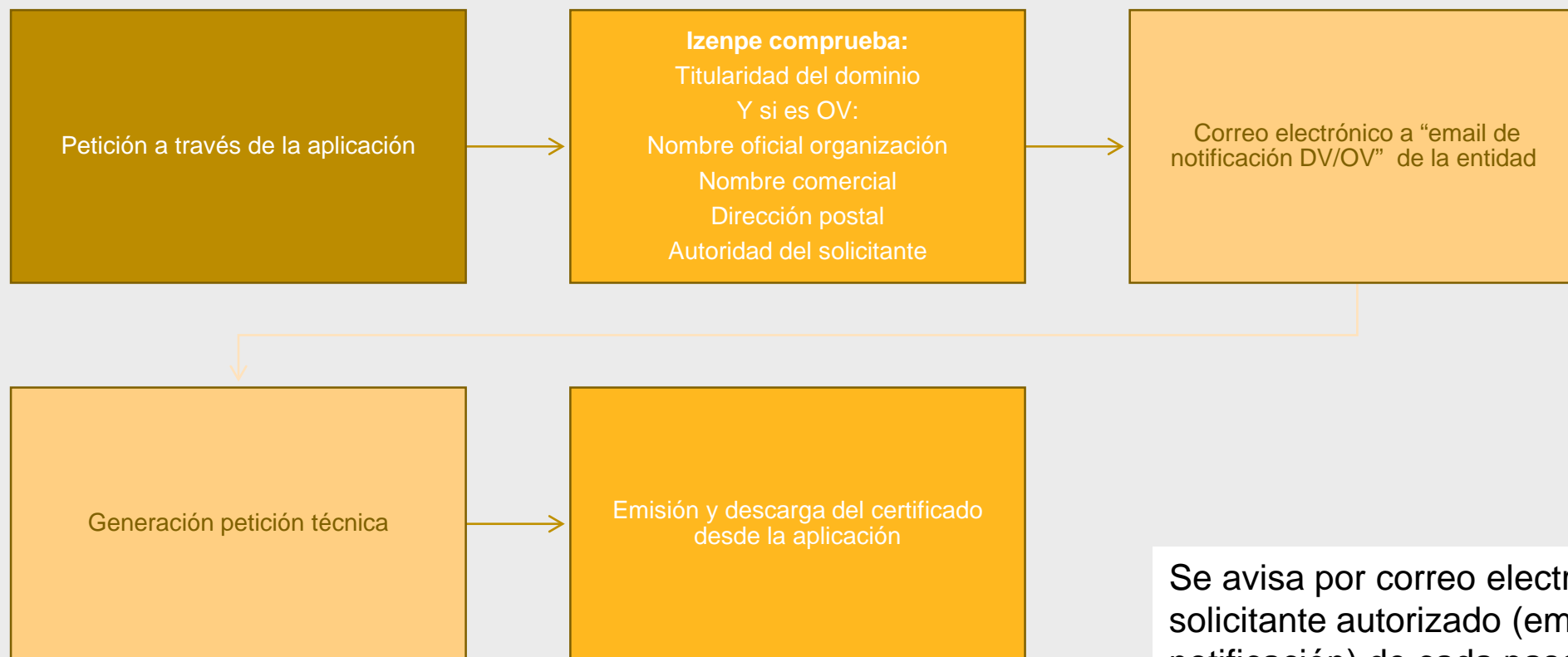
Nombre	NIF	Acciones
AYTO DE MASSACHUSSETS	C99395279	Editar
EL CORTE INGLES	A28017895	Editar

At the bottom of the interface, there are two buttons: 'Nuevo cliente' and 'Volver'.

Gestión de clientes/entidades:

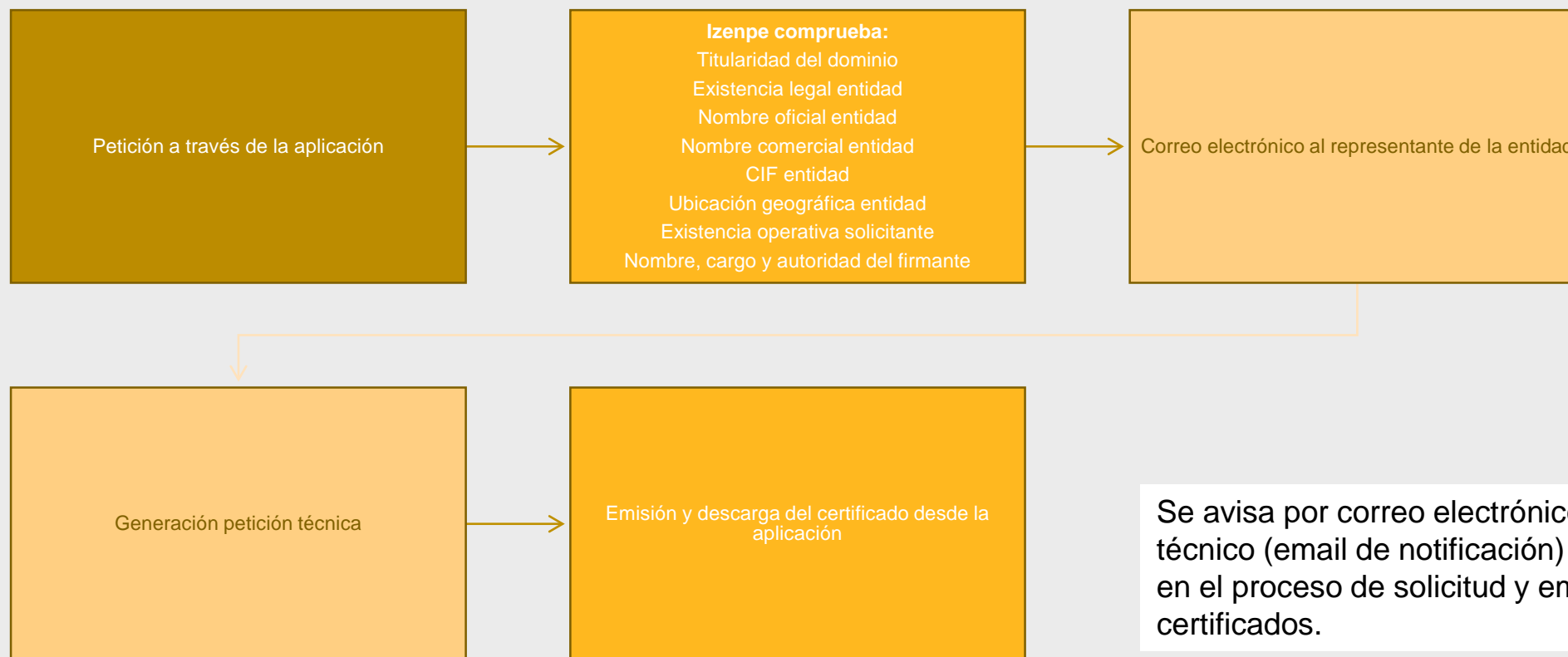
Cada persona autorizada encontrará en el panel de gestión las diferentes entidades para las que puede gestionar certificados y la posibilidad de modificar los datos de dicha entidad, sus representantes y autorizados.

Ciclo de emisión: SSL DV y OV



Se avisa por correo electrónico a cada solicitante autorizado (email de notificación) de cada paso dado en el proceso de solicitud y emisión de los certificados.

Ciclo de emisión: SSL cualificados



Se avisa por correo electrónico al responsable técnico (email de notificación) de cada paso dado en el proceso de solicitud y emisión de los certificados.

Gestión de solicitudes y certificados:

Cómo utilizar la aplicación



Acceso a la aplicación:

<https://servicios.izenpe.com/partners/>



Cada pestaña permite gestionar los certificados según su estado:

- Gestión certificados **pendientes**: nuevas solicitudes o completar solicitudes en trámite.
 - Gestión certificados **emitidos**
 - Gestión certificados **caducados**
 - Gestión certificados **revocados**
- } Ciclo de vida del certificado

Pendientes

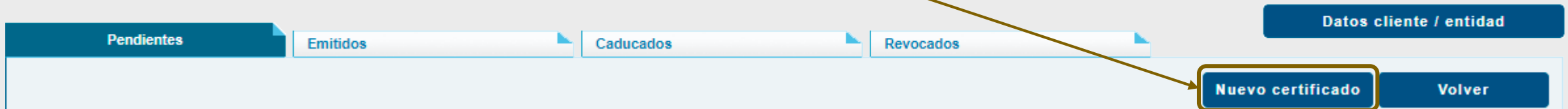
Emitidos

Caducados

Revocados

Petición de un certificado

Al seleccionar “Nuevo certificado”, se desplegará el formulario parcialmente completado con los datos de entidad y persona solicitante.



Primero debemos escoger el tipo de certificado:

The 'Nuevo certificado' form is displayed. It starts with a header 'Nuevo certificado' and a note: 'Debe rellenar todos los datos obligatorios (marcados con *)'. Under the heading 'Solicitud de certificado', there is a sub-section 'Tipo de certificado' containing three fields: 'Tipo Certificado:*' with a dropdown menu, 'Duración Certificado: 395 días', and 'Precio Certificado:' with a dropdown menu.

Petición de un certificado

Al final del formulario completaremos los datos de dominio y debemos escoger el modo de comprobación de la titularidad, así como adjuntar la petición técnica – csr – del certificado.

Se enviará un correo electrónico para validar la petición: en DV y OV al autorizado, en los CUALIFICADOS al representante de la entidad.

Datos certificado


Dominio:*

Nombre alternativo 1:

Nombre alternativo 2:

Nombre alternativo 3:

Modo comprobación de titularidad preferido:*

Solicitud Técnica (Máx: 10KB): 

SAN adicionales

SAN Adicional

Modos de comprobación titularidad dominio

Puede escogerse el modo deseado

CAMBIO DNS

Izenpe envía un email con un valor aleatorio que el solicitante debe utilizar para añadir un registro TXT en el DNS del dominio. El solicitante debe seguir las instrucciones del email.

WEB

Izenpe envía un email con un fichero que el solicitante debe publicar en la ruta dominio/.well-known/pki-validation/. El solicitante debe seguir las instrucciones del email.

WHOIS

Izenpe envía un email con un valor aleatorio a la dirección que aparece en el contacto de whois (Registrant, administrativo o técnico). El contacto debe seguir las instrucciones del email. Este método sólo es posible en el caso de dominios *.eus*

Estados y acciones en una petición

Se mantendrá el estado “sin emitir” hasta que los 4 *flags* sean ok.

Además, según el estado de los *flags* se podrán llevar a cabo diferentes acciones de gestión de la petición.

Estados / <i>Flags</i>	Acciones
Confirmación de Representante	Consulta: despliega el formulario de petición
Comprobación Titularidad Dominio	Descarga PDF: descarga el formulario de solicitud.
Subido CSR	Editar: permite realizar cambios en una petición aún NO tramitada
Emisión Izenpe	Descargar certificado

Estados de un certificado

Una vez emitido un certificado los estados de su ciclo de vida y las posibles acciones en cada una de ellas son:

Estados	Acciones
Emitido	Descargar
Vivo	Renovar
Caducado	Revocar
Revocado	

Autorizados multientidad

Gestión de entidades diferentes desde un mismo perfil

Cuando una misma persona autorizada gestione certificados de diferentes entidades al autenticarse deberá escoger el cliente del cual quiere gestionar los certificados.



Mila esker

Gracias

www.izenpe.eus

<https://serviciosdes.izenpe.com/partners/>