Certificados SSL

	Validez 1 año	Validez 2 años
SSL WEB SERVER con validación extendida	950 €	1500 €

Condiciones Particulares del servicio.

Le recordamos que deberá solicitarnos la renovación de su certificado con la antelación suficiente. Para ello deberá remitir un correo a la cuenta altas@ibercom.com, con 1 mes de antelación a caducidad de su certificado, en el que nos comunique su deseo de renovación.

Es importante que dicha renovación se haga con bastante antelación (idealmente un mes, al menos dos semanas), el proceso de renovación puede llevar varios días e incluso semanas si la autoridad de certificación no consigue realizar las validaciones oportunas. Si eso ocurre el certificado existente mostrará un mensaje de advertencia a los visitantes de su web. En dichas renovaciones también es importante confirmar la persona de contacto por si hubiera habido cambios en su organización.

Ibercom no renovará su certificado salvo que usted nos lo solicite por la vía detallada anteriormente.

Preguntas frecuentes

¿Qué es un certificado digital de servidor?

Un certificado digital de servidor es un componente que habilita las siguientes características de seguridad en un servidor WEB:

- Cifrado de datos: Los datos intercambiados entre el navegador del usuario y el servidor se cifrarán, con lo que no serían directamente inteligibles en caso de intercepción en su tránsito por la red. Esta característica es muy útil si se utilizan formularios para que el usuario envíe datos críticos o personales, o si el contenido del web o parte del mismo es un área privada cuyos datos son confidenciales y deben ser únicamente accesibles por un grupo cerrado de personas.
- Autenticación del servidor: El visitante podrá saber que el propietario de la web indicada en el certificado ha seguido un proceso de identificación ante un tercero (autoridad de certificación) que es quien emite el certificado. Este proceso de identificación varía según el emisor del certificado y el tipo de certificado, y puede ir desde la validación por correo electrónico del propietario del dominio hasta la validación documental de la existencia de la organización propietaria del dominio.

¿Quién puede solicitar el servicio de certificado digital de servidor?

Cualquier cliente que posea una web alojada con nosotros mediante uno de los siguientes servicios:

- Un plan de alojamiento
- Un servidor privado
- Un servidor dedicado
- Servidores propios en régimen de housing (co-location) alojados en uno de nuestros CPDs.

¿Qué es una autoridad de certificación y qué proceso de identificación realiza?

Es la entidad que emite los certificados y se encarga de realizar las validaciones oportunas sobre la propiedad del dominio y existencia de la empresa solicitante de certificados digitales.

¿Qué significa exactamente sin validación documental y con validación documental?

Los Certificados sin validación documental solo requieren que el solicitante del certificado tenga el control sobre la cuenta de correo que figura como contacto del dominio bajo el que se está solicitando el certificado. Por ejemplo, si se pretende solicitar un certificado para el servidor http://seguro.dominio.com se solicitará autorización por correo electrónico a la cuenta de correo que figura como titular del dominio dominio.com.

La autoridad de certificación emitirá el certificado si la persona que lee la cuenta de correo que figura en la información del dominio DNS hace click en un enlace web y acepta la emisión del certificado. Para ambos casos es importante que los datos del registro del dominio sean exactos y veraces, y que la persona que gestiona la cuenta de correo que aparece como contacto asociada al dominio para el que se pide el certificado siga las instrucciones que reciba por correo electrónico.

Los Certificados con validación documental además requieren la comprobación de la existencia de la organización que figura como propietaria del dominio. Por ejemplo, si se pretende solicitar un certificado para el servidor http://seguro.dominio.com y dominio.com está a nombre de la compañía "ACME S.A." se pueden pedir los datos y documentos necesarios para demostrar que "ACME S.A." existe y que el solicitante es una persona autorizada en dicha organización. **La autoridad de certificación realiza una llamada de comprobación a una persona que se proporcione como contacto y que tenga poder de representación de la organización propietaria del dominio.** Es importante que dicha persona de contacto esté al tanto de que va a recibir esa llamada de verificación y autorice la emisión de certificado. En el caso de que dicha llamada falle o la autoridad de certificación lo estime necesario es posible que se soliciten de forma adicional los siguientes datos y posibles documentos:

- Fotocopia de la tarjeta del CIF.
- Fotocopia de alta de la sociedad en el IAE (Impuesto de Actividades Económicas) y Fotocopia del último pago del IAE. Esto se puede sustituir por por una nota registral emitida por el registro mercantil donde se certifica la inscripción de dicha sociedad en el registro mercantil y que está activa.
- Factura reciente de un número de teléfono (conviene que sea del número de teléfono que se dé como contacto para autorizar la petición de certificado en la organización)
- Número DUNS si la empresa tiene uno (http://dbspain.dnb.com/). Si se proporciona agiliza el trámite e incluso para certificados Verisign puede que baste con este dato. Se puede solicitar/consultar dicho número en el teléfono 902446688.

¿Qué ocurre si se solicita un certificado con validación documental y el dominio está a nombre de un particular o de otra empresa?

Si el dominio bajo el que se encuentra el nombre del servidor para el que se solicita el certificado está a nombre de un particular la autoridad de certificación solicitará una serie de documentos para validad su identidad (varían para cada caso).

Si el dominio está a nombre de otra empresa normalmente la autoridad de certificación proporcionará una carta de autorización que debe ser firmada por la persona titular del dominio.

¿Qué es un CSR?

Un CSR (Certificate Signing Request) es la petición de certificado que se envía a la autoridad de certificación. Mediante la información contenida en el CSR la autoridad de certificación puede emitir el certificado una vez realizadas las comprobaciones que correspondan.

El CSR se genera en el servidor que aloja el WEB. De forma simultánea se genera una clave privada que nunca debe ser transmitida fuera del servidor.

¿Cómo sabrán los visitantes de mi web que están conectando a un servidor web con certificado digital?

Normalmente observarán lo siguiente en su navegador:

- La ventana de dirección del navegador comienza por https:// en lugar del habitual http://
- En la esquina inferior derecha se observa el símbolo de un candado cerrado, y pulsando sobre él se muestran los datos del certificado digital de servidor.

De forma coloquial lo anterior puede recibir distintos nombres:

- Conexión segura
- Navegación segura
- Conexión HTTPS
- Conexión SSL

¿Qué condiciones se tienen que cumplir para que el certificado sea admitido como válido por un navegador?

Para que la conexión segura se realice sin problemas entre el servidor web y el navegador del usuario se deben cumplir las siguientes condiciones en el certificado:

- Que haya sido emitido por una autoridad de certificación reconocida por el navegador. Cada autoridad de certificación está incluida en una serie de navegadores por defecto, conviene revisar la lista de compatibilidad de cada autoridad de certificación para saber cual es la que se adapta a las necesidades concretas de cada caso.
- Que el nombre del certificado coincida con el nombre del web al que el navegador se está conectando, es decir, que el certificado haya sido emitido para el nombre de servidor al que el browser se está conectando. Si el certificado ha sido emitido para el nombre de web "compras.dominio.com" no puede ser utilizado para que los usuarios accedan de forma segura a "ventas.dominio.com".
- Que no haya sido emitido para una fecha posterior o que no esté caducado. Los certificados tienen un periodo de vida útil asignado por la autoridad de certificación (normalmente 1 ó 2 años). Al emitir el certificado la autoridad de certificación marca: La fecha a partir de la cual comienza a ser válido el certificado y la fecha a partir de la cual deja de ser válido el certificado. En el momento de la conexión la hora actual tiene que estar entre ambas fechas, es decir, en el periodo de vida útil del certificado.

Si alguna de las tres condiciones anteriores no se cumple aparecerá una ventana de aviso en el navegador del usuario indicando el error.

¿Qué se puede hacer cuando se acerca la fecha de caducidad de un certificado?

Con la antelación suficiente se debe solicitar su renovación ante la autoridad de certificación correspondiente. La autoridad de certificación emitirá un nuevo certificado válido para otro periodo de tiempo. Es importante que dicha renovación se haga con bastante antelación (idealmente un mes, al menos dos semanas), el proceso de renovación puede llevar varios días e incluso semanas si la autoridad de certificación no consigue realizar las validaciones oportunas. Si eso ocurre el certificado existente mostrará un mensaje de advertencia a los visitantes de su web. En dichas renovaciones también es importante confirmar la persona de contacto por si hubiera habido cambios en su organización.

¿Cuántos certificados debo solicitar?

Usando certificados normales se debe solicitar un certificado por cada nombre de servidor web seguro que se quiere que aparezca en la barra de direcciones del navegador, es decir, estos certificados se piden por cada nombre de servidor, no por cada dominio. No obstante existen los certificados wildcard que se emiten para todos los nombres de un dominio concreto. Por ejemplo, si queremos que el usuario se conecte de forma segura a https://compras.dominio.com y a https://ventas.dominio.com será necesario solicitar dos certificados diferentes o solicitar un certificado wildcard por *.dominio.com. Los certificados wildcard pueden no funcionar correctamente con navegadores y servidores antiguos. Si el usuario visualiza las propiedades del certificado aparecerá que ha sido emitido para *.dominio.com en lugar de nombreservidor.dominio.com

¿Cuántos certificados puedo instalar en función del servicio de alojamiento contratado?

- En alojamiento compartido solo se permite un certificado por plan.
- En servidores privados solo se permite un certificado para instalarlo en el puerto estándar. Si se necesitan más certificados digitales en un servidor será necesario configurarlo en un puerto no estándard y las direcciones serían del tipo: https://nombre.dominio.com:XXXX/
- En servidores dedicados y housing (co-location) depende del rango de direcciones IP que tenga asignado. La regla general es un certificado por dirección IP, a no ser que empleen puertos no estándard como se comenta en el punto anterior.

¿Cómo puedo mostrar en mi web un sello para que los usuarios vean la información del certificado?

- Algunas autoridades de certificación proporcionan logos o sellos para mostrar en la página web que tiene instalado un certificado.
- Al hacer click en el sello se muestra una página de verificación con los datos del certificado.
- Para mostrar este sello en su web hay que insertar un código web, dicho código se puede obtener en las siguientes páginas en función del tipo de certificado:

Certificados Thawte (Site Seal)
https://www.thawte.com/ssl/secured-seal/installation-agreement/index.html

Certificados Verisign (Secured Seal)
http://www.verisign.com/ssl/secured-seal/installation-agreement/index.html

En dichas páginas se le solicitará que escoja el tipo de logo e introduzca el nombre de su web.

¿Qué son los certificados EV o con “Extended Validation”?

- Son certificados en los que se realiza una validación documental más profunda sobre la existencia de la organización para la que se emiten. El proceso de validación por parte de la autoridad de certificación lleva por lo tanto más tiempo.
- Tienen la característica de que al conectarse al sitio que tiene este certificado la barra de direcciones del navegador se pone de color verde y muestra el nombre de la organización al que pertenece el certificado.
- El efecto de mostrar la barra en verde solo funciona con los navegadores de versiones más modernas.

Parque empresarial Zuatzu Edificio Easo, 2º
20018 San Sebastián
María Tubau, 8 4ª planta
28050 Madrid

www.ibercom.es
comercial@ibercom.com
tel. 902 200 265
fax. 902 197 186