

Cómo hacer que tu web funcione con un certificado de seguridad SSL



← → ↻ **Es seguro** | **https://**www.acens.com

acens
the Cloud services company
Una compañía de *Telefónica*

empresa · Blog · actualidad · ayuda · contacto · 900 103 293 **PANEL**

Cloud · Hosting · Web y Tiendas · MKT y SEO · Correo

Home » Hosting » Hosting gestionado » Servicios adicionales » Certificado SSL

Hosting

CERTIFICADO SSL

 acens puede encargarse de la gestión de certificados digitales, si necesitas garantizar la confidencialidad de la información que circula entre tus servidores y los de tus clientes.

Gracias a los certificados digitales el visitante tiene la **seguridad de que el propietario del sitio ha seguido un proceso de identificación**, ante una autoridad reconocida de certificación.

La gestión de certificados por parte de acens comprende la generación de CSR y la recogida de documentación del cliente para el envío a la Autoridad de Certificación. Posteriormente se adquiere el certificado y se instala dentro de las especificaciones del proyecto.

GAMA DE CERTIFICADOS COMERCIALIZADOS POR ACENS

Desde hace algunas semanas, Google viene mostrando en su navegador un mensaje de “Sitio no seguro” en aquellas páginas web que no hacen uso de un **certificado de seguridad SSL**. Esto no significa que estén hackeadas o que tengan problemas de seguridad, sino que es un aviso al visitante de que la información que introduzca no irá encriptada. Con esta advertencia Google quiere dar importancia al uso de los certificados de seguridad, algo muy necesario sobre todo en **comercios online**.

Ante esta situación, a lo largo de nuestro White Paper explicaremos cómo crear el CSR en el panel de control Plesk, código necesario para solicitar un certificado de seguridad, así como los cambios necesarios en la configuración de nuestro portal para que empiece a funcionar con el SSL una vez lo tengamos contratado.

¿Qué es HTTPS y para qué sirve el certificado SSL?



Antes de meternos en materia es importante que hagamos una breve explicación de lo que hace un certificado de seguridad. De forma sencilla, se puede decir que su objetivo es proporcionar una conexión segura entre el cliente y el **servidor**, es decir, la información que sea enviada desde el cliente estará encriptada, por lo que en caso de que algún hacker capture esa información, no podrá conocerla a no ser que tenga la clave para descifrarla.

Una cosa debemos tener claro, la instalación del mismo no es suficiente, también debemos hacer uso del protocolo HTTPS. Se trata del protocolo que ofrece conexiones seguras y que se encarga de hacer que los datos enviados vayan por el cauce correcto.

Generar el CSR en Plesk

Para poder contratar un certificado de seguridad en nuestro sitio es necesario que previamente hayamos generado nuestro CSR, pero ¿qué es el CSR?

Un CSR (Certificate Signing Request) es un bloque de texto cifrado que es generado en el servidor donde será instalado el certificado SSL. Este código contiene información que será incluida en el certificado, como por ejemplo nuestro nombre o el nombre de la empresa. Además de esto incluirá una clave pública que será incluida en el certificado. Las Autoridades Certificadoras que generarán el SSL utilizará este CSR para generar el certificado.

La información que puede contener un CSR es la siguiente:

- **Common name:** El nombre del **dominio** o subdominio de nuestro sitio web. Debe coincidir exactamente con el nombre que escribirán los usuarios al acceder a la web.
- **Organización:** Nombre completo de la organización o de la empresa.
- **Sección/Departamento:** La sección de la empresa que gestionará el certificado.
- **Correo electrónico:** Cuenta de correo electrónico para contactar. Debe estar activa para recibir las notificaciones.
- **País:** El país donde está ubicada la organización.
- **Provincia:** La provincia donde está ubicada la organización.
- **Localidad:** La localidad donde está ubicada la organización.
- **Clave pública:** La clave pública que será insertada en el certificado. Se genera automáticamente.

Una vez que ya conocemos lo que es un CSR y la información que contiene, vamos a ver los pasos que debemos seguir para generar este código desde el **panel de control Plesk**. Para ello, una vez que estemos dentro, deberemos irnos a la sección donde pone **“Certificados SSL”**.



Una vez dentro deberemos pulsar en la opción **“Añadir certificado SSL”**.

Si creó una petición de firma de certificado en este servidor y recibió el archivo de certificado, cárguelo aquí. Si desea **certificado SSL**.

Una vez añadido un certificado SSL a un dominio, deberá activar el soporte para SSL y seleccionar dicho certificado e

Cargue el certificado aquí

Certificado (*.crt) *

Seleccionar archivo

Ningún archivo seleccionado

Cargar certificado

Añadir certificado SSL

Eliminar

No se ha encontrado ningún elemento.

Lo siguiente que deberemos hacer será rellenar los datos que hemos comentado anteriormente y que formarán parte del CSR.

Añadir certificado SSL

Nombre del certificado *

Configuración

Use este formulario para generar una petición de certificado, para comprar un certificado a su proveedor o

Una petición es un archivo CSR que contiene información acerca del dominio especificado en el formulario, que aparecen a continuación.

Un certificado autofirmado es un certificado de identidad firmado por su creador. Si usa este tipo de certificado porque creen que son menos seguros.

Bits	<input type="text" value="2048"/>
País *	<input type="text" value="Spain"/>
Estado o provincia *	<input type="text" value="madrid"/>
Lugar (ciudad) *	<input type="text" value="madrid"/>
Nombre de la empresa *	<input type="text" value="Mi Empresa"/>
Nombre del departamento/división de la empresa	<input type="text" value="Internet"/>
Nombre de dominio *	<input type="text" value="www.midominio.com"/>
Email *	<input type="text" value="info@midominio.com"/>

Cuando hayamos cumplimentado todos los datos pulsaremos en el botón **“Solicitar”**. De esta forma ya tendremos el CSR creado, que tendrá un aspecto similar a lo que os dejamos a continuación.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3DCCAcQCAQAwgZYxCzAJBgNVBAYTAkVMTQ8wDQYDVQQIEwZtYWRYaWQxZDZAN
BgNVBACwBm1hZHZjZDEtMjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
ZXJ1ZXQxGjAYBgNVBAMTEXd3dy5taWRvbWluaW8uY29tMSEwHwYJKoZIhvcNAQkB
FhJpbmZvQG1pZG9taW5pby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCcYAhTdfC1K01Zvz5WC5sww01dkgCUhrjfjCbhrcZ0/LsXYRJeWSFLQy8B
6yiyuezAREEmuULrdJ+QNT0yE7Ju+3EBm1LkF8Jq5wHvDTtTIEdh/kV83/oEZBXy
sggEfW0Sx1sz0DuP0cyZvtKsWpTF+9RjnZkFCa+PB9K/hTg5r0QW40CBS1GoGUCf
g1RVZywID37HIe/JfvTnYhGju5akNI0cPN+xF7DxkmXgJpMdfZTLtzk3T3xQjrOn
TgVxDM/voBIwMcNEBwACF82ePLuWIRxaJ8LSiHPPJOAYuNx6mi0Tbd3VZHiJ4G/M
qYc9SIDEcpi/GWBUNMPiG17QVoAvAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCQAQEA
IdA1U2e0zG/RGsvXCYvDePA40MbnCq8WxuapmbdshfGf+g2zr/qAp5djJk0zxqas
gDSjadusSsw4vdMd1Wg5Y5WNGA0yUEtwbNVI7dPG7ITK/4L6z4xyPoNL0JCzsJrP
```

```
t5M00ENTsQ8HcdWstw4YS01WUqia42G4QcAe/ENy7FAH/Jx13gVBIYkbucvqHKEZ
1xNyBR7hN/HcgCQm5kBRn1L9LWBudD8IrSs6DbuLxMY9fLu0+0mbJzONZitOr2NH
G9sL3emacG5F6hrA1/Zqu19emoKg0BvU9Vc0dKEY4Kb9H+K0z0WLDQ0FrZsHxaAS
EsKwW09Em2goGydL4Lr5Ag==
-----END CERTIFICATE REQUEST-----
```

Una vez que tenemos esta información tendremos que proporcionárselo a la empresa donde contrataremos el SSL.

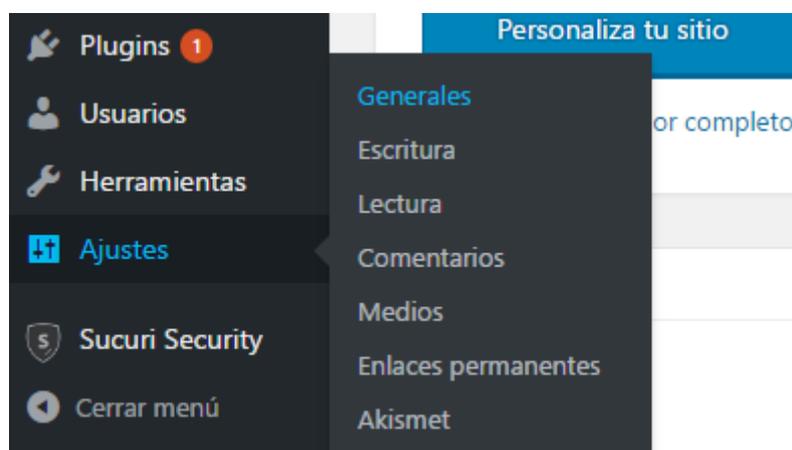
¿Qué configurar una vez contratado el SSL?



Una vez que se ha contratado el certificado es necesario realizar algunos cambios en nuestro [portal web](#) para que empiece a utilizarlo. Dependiendo de la plataforma utilizada o si se trata de un desarrollo a medida, estos cambios podrían variar. En resumen, lo que debemos hacer es indicar que todas las urls de nuestro sitio utilizarán "https" en vez de "http". Veamos cómo hacer estos cambios en las principales plataformas.

WordPress

En el caso del CMS más utilizado en la red a la hora de crear páginas web, activar el protocolo SSL es un proceso muy sencillo. Para hacerlo, deberemos entrar en la administración e irnos a la zona de **"Ajustes -> Generales"**.



En la siguiente pantalla nos deberemos fijar en los campos "Dirección de WordPress (URL)" y "Dirección del sitio (URL)".



Ajustes generales

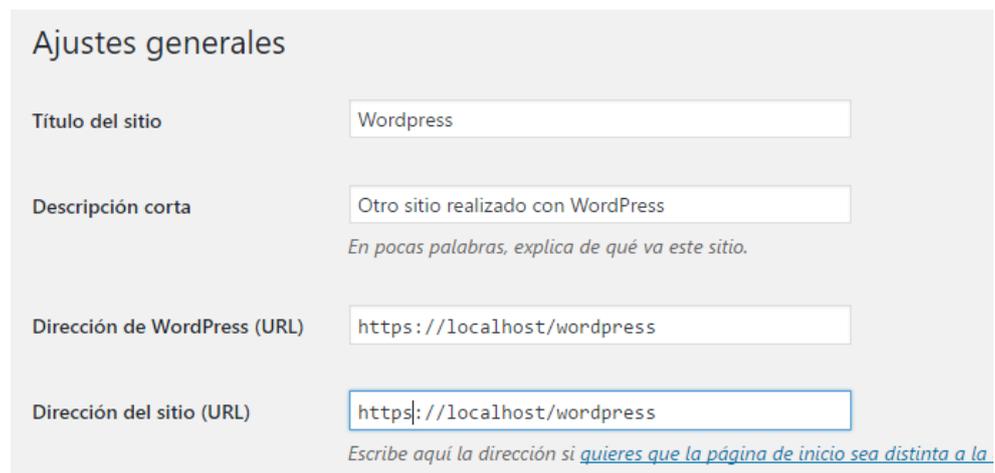
Título del sitio

Descripción corta
En pocas palabras, explica de qué va este sitio.

Dirección de WordPress (URL)

Dirección del sitio (URL)
Escribe aquí la dirección si [quieres que la página de inicio sea distinta a la](#)

En esos dos campos, deberemos cambiar donde pone "http" por "https". Quedaría de la siguiente forma.



Ajustes generales

Título del sitio

Descripción corta
En pocas palabras, explica de qué va este sitio.

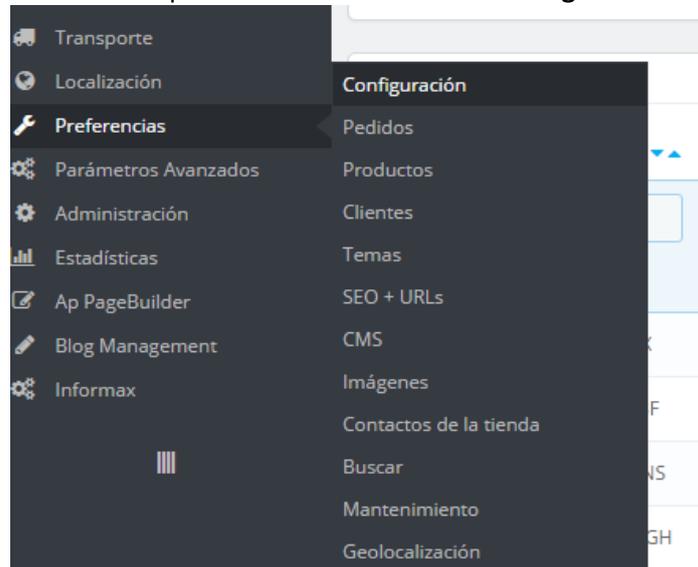
Dirección de WordPress (URL)

Dirección del sitio (URL)
Escribe aquí la dirección si [quieres que la página de inicio sea distinta a la](#)

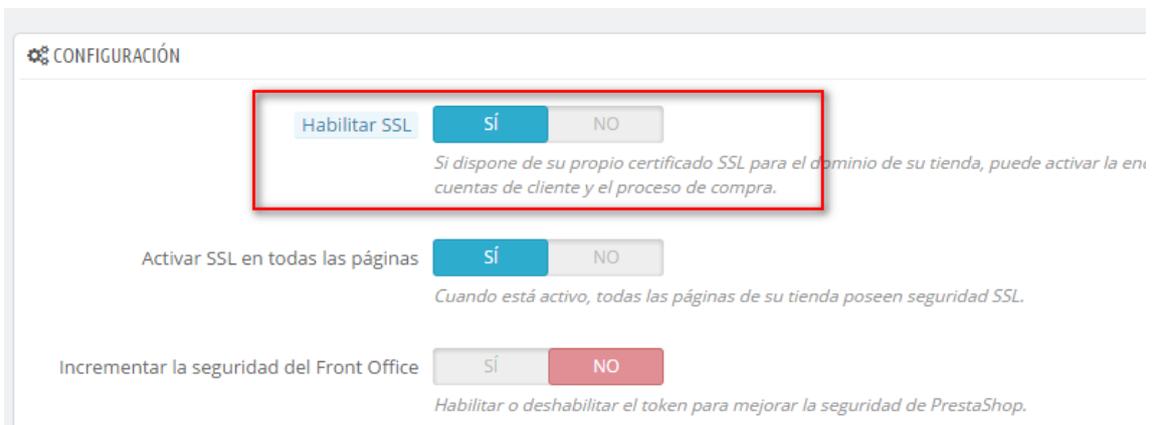
Una vez hecho este cambio, lo guardaremos y ya lo tendremos listo.

PrestaShop

Al igual que ocurre en WordPress la activación en PrestaShop también es realmente sencilla. En este caso, deberemos pulsar en el menú de la izquierda en "**Preferencias -> Configuración**".



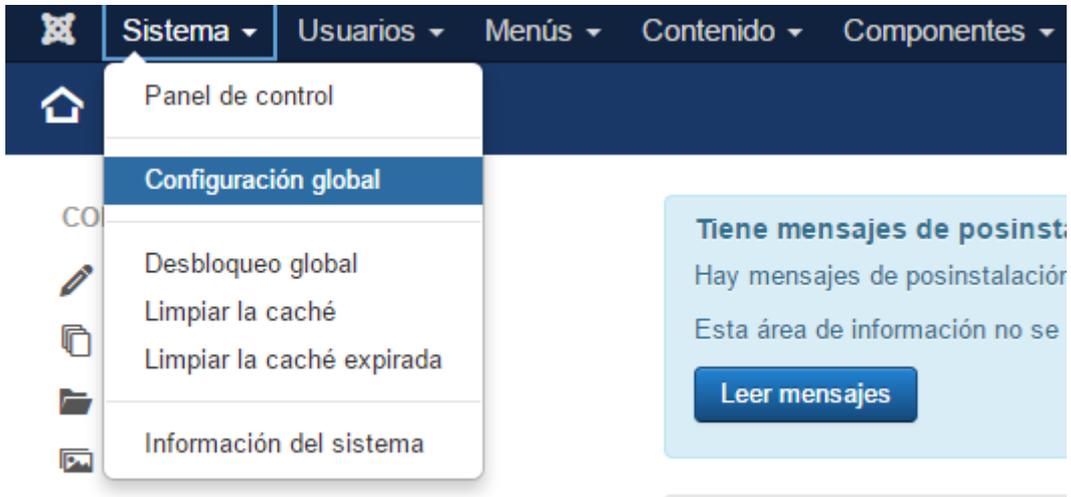
En la siguiente página únicamente deberemos pulsar sobre la opción que pone "**Habilitar SSL**".



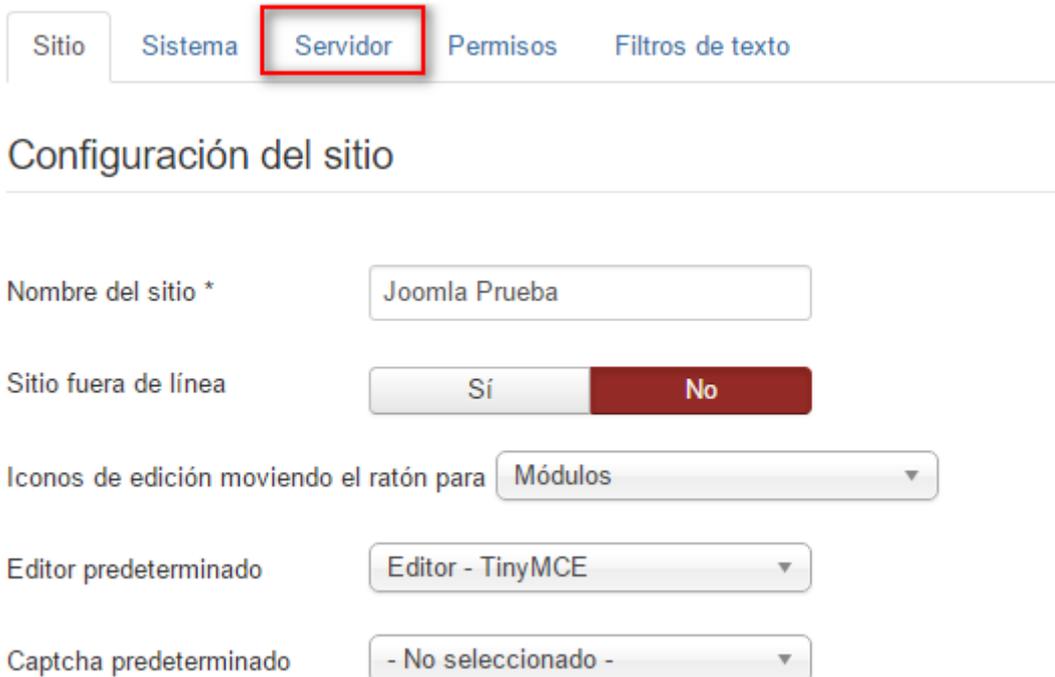
Si lo deseamos también podemos activar la opción que pone "**Activar SSL en todas las páginas**". De esta forma, todas las páginas de la tienda online utilizarán el protocolo seguro. Si no se activa, sólo se utilizará en aquellas páginas donde se hace un intercambio de información sensible.

Joomla

Otro CMS muy utilizado para el desarrollo de portales web es Joomla. Al igual que los casos anteriores, empezar a utilizar el certificado de seguridad es muy sencillo. En este caso, deberemos pulsar sobre la opción "**Sistema -> Configuración Global**" del menú superior.



En la siguiente pantalla nos iremos a la pestaña "**Servidor**".



Entre las opciones que nos aparecerán deberemos localizar "**Forzar HTTPS**". Del menú desplegable seleccionaremos "**Todo el sitio**".

Configuración del servidor

Ruta hacia la carpeta temporal

Compresión 'Gzip' de páginas

Informe de errores

Forzar HTTPS

Configuración de localización

Zona horaria del servidor

Por último, guardaremos los cambios realizados.

Página con programación a medida

Se puede dar el caso de que no hagamos uso de ningún CMS sino que nuestro portal web esté hecho con programación a medida. Si no tenemos ninguna opción para activar el SSL lo podemos hacer mediante el archivo .htaccess. Para ello deberemos añadir las siguientes líneas al principio.

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
```

Como habéis podido ver a lo largo de este White Paper, el proceso de contratación y activación de un certificado de seguridad es relativamente sencillo, y los beneficios de utilizarlos muchos. Así que si queréis proporcionar a vuestros usuarios un entorno más seguro, pasaos por la sección de [certificado de seguridad SSL de acens](#) para contratar el que mejor se adapta a vuestras necesidades.