# INSTALAR CERTIFICADO SSL EN APPLICATION SERVER APACHE

---

Este manual consta de tres secciones:

1. Crear CSR con OpenSSL
2. Instalar certificado
3. Verificación del sitio

## Crear CSR con OpenSSL

Para la creación del CSR (Certificate Signing Request) es necesario generar en su servidor la clave privada. Al realizar este proceso se genera la clave privada y el CSR que deberás facilitarnos.

1. Ejecutá el siguiente comando:

openssl req -out CSR.csr -new -newkey rsa:2048 -keyout claveprivada.key

Nota: Es importante que la clave privada utilice un mínimo de 2048 bit, si fuese en 1024 no será válido.

2. Ingresá la información correspondiente a tu organización:

**Country Code** — Corresponde al código de dos letras ISO del país en el que se encuentra la empresa. En el caso de Uruguay, ingresá ***"UY"***.
**State/Province** —Estado o Provincia. Ej: Montevideo.
**City/Locality** — Ciudad o localidad en la que se encuentra.
**Organization (O)**— Razón social de la empresa registrada en DGI.
**Organizational Unit (OU)** — Sector que solicita dicho certificado. Puede ser, por ejemplo: Departamento de Informática.
**Common Name** — Nombre del dominio en formato FQDN.

Si solicitaste un Wildcard (multi subdominio), tenés que agregar ***(.*)*** *en el campo common name*, Ej. ***" *.midominio.com"***.

3. Como resultado de esto obtendrás dos archivos, uno ***claveprivada.key*** (es importante que no pierdas o reemplaces este archivo) y otro ***CSR.csr, el archivo csr debes mandarlo a nosotros para continuar con el trámite.***

## Instalar certificado

1. **PASO A: DESCARGA DE CERTIFICADO:** Cuando el certificado SSL sea emitido, te enviaremos un mail.
   Este mail contendrá un enlace con la clave pública emitida necesaria para la instalación del SSL.
2. Verás que un certificado se puede descargar como tipo binario (.cer) o en formato plano . A efectos de aplicaciones, descargalo en formato binario (.cer).
3. Al certificado descargado renombrarlo como: ***"certificado.cer".***

4. Ahora descargá el **bundle (conjunto de certificados intermedios)**, de acuerdo al tipo de certificado que tramitaste:
   a. Para **Certificados DV** debes descargar el certificado del siguiente enlace:
      BUNDLE PARA CERTIFICADOS DV

   b. Para **Certificados OV** debes descargar el certificado del siguiente enlace:
      BUNDLE PARA CERTIFICADOS OV

   c. Para **Certificados EV** debes descargar el certificado del siguiente enlace:
      BUNDLE PARA CERTIFICADOS EV

5. Una vez tengas descargado ambos archivos, el certificado ***"certificado.cer"*** correspondiente a la clave pública emitida**,** tenes que cambiarle el formato de extensión a **.crt.**
   Se puede proceder a editar la extensión, directamente modificando el nombre, dado que mantendrá las propiedades Base-64.

6. Cuando tengas listo los archivos mencionados anteriormente, tenes que ubicarlos en una carpeta dentro de tu sistema. Ej., **/etc/ssl**

A efectos de este manual como ejemplo, se utilizará un certificado OV, dentro de la carpeta **/etc/ssl** deberían estar ubicados estos 3 archivos:

Clave privada: **claveprivada.key**
Clave pública: **certificado.crt**
Certificados Intermedios: **intermediosOV-Certum.pem**

7. **PASO B: CONFIGURACIÓN DEL CONECTOR:**

Para configurar el servidor y uso del certificado SSL tenes que acceder al archivo de configuración del servidor web.

El mismo se puede ubicar en uno de los siguientes sitios:

- Fedora/CentOS/RHEL: **/etc/httpd/conf/httpd.conf**
- Debian and Debian based: **/etc/apache2/apache2.conf**

Los nombres más comunes de este archivo pueden ser:

- httpd-ssl.conf
- ssl.conf
- O en el directorio: /etc/apache2/sites-enabled/

8. Dentro de este archivo sobre la configuración del VirtualHost del sitio, tendrás que tener los siguientes parámetros configurados:

- SSLEngine on
- SSLCertificateKeyFile /etc/ssl/ssl.key/claveprivada.key
- SSLCertificateFile /etc/ssl/ssl.crt/certificado.crt
- SSLCertificateChainFile /etc/ssl/ssl.crt/**intermediosOV-Certum.pem**

**Los paths presentados son solo de ejemplo, estos paths deben coincidir con la ubicación de los certificados.**

<u>Configuraciones adicionales:</u>

SSLProtocol all

En **Apache 2.4**, habilitá los protocolos SSLv3 y TLSv1 y opcionalmente TLSv1.1 y TLSv1.2 (en OpenSSL 1.0.1 y superiores versiones).

En **Apache 2.2.** SSLProtocol All -SSLv2.

SSLHonorCipherOrder On - server enforcement of the ciphers use order

SSLCipherSuite ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+3 DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS - setting priority for the strong ciphers while at the same time disabling the weak and obsolete ones.

## 9. PASO C: REINICIO DEL SERVIDOR:

Para que el servidor tome la nueva configuración es necesario que reinicies el servicio apache2.

- En Debian o Ubuntu : **/etc/init./apache2 restart**
- En RedHat/Fedora/CentOS: **apachectl restart**
- Otra forma: **/usr/sbin/httpsd restart o /etc/init.d/apache restart**