

Una solicitud de firma de certificado (CSR) es uno de los primeros pasos para obtener su propio certificado SSL. Debe ser generado en el mismo servidor en que va a instalar el certificado, si tiene dudas sobre el proceso puede consultar nuestra página web o hacer click en el siguiente [link](#).

El CSR contiene información (por ejemplo, nombre común, organización, país) que utilizará la autoridad de certificación (CA) para crear su certificado. También contiene la clave pública que se incluirá en su certificado y se firmará con la clave privada correspondiente.

¿Qué información se incluye en un CSR?

La CA utilizará los datos del CSR para crear su certificado SSL. Las piezas clave de información incluyen lo siguiente:

1. Información sobre su empresa y el sitio web que está intentando equipar con SSL, ejemplo: www.tusitio.com (se dedica a la venta de artículos informáticos) deberá incluir:

Nombre Común (CN) (según ejemplo: tusitio.com)	El nombre de dominio completo (FQDN) de su servidor.
Organización (O)	El nombre legal de su organización. No abreviar e incluir cualquier sufijo, como Inc., Corp., o LLC. Para los certificados SSL EV y OV, esta información es verificada por la entidad emisora de certificados y se incluye en el certificado.
Unidad Organizacional (OU)	Rubro de la empresa (según el ejemplo sería «Ventas»)
Ciudad / Localidad (L)	La ciudad donde se encuentra su organización. Esto no debe ser abreviado.
Estado / Condado / Región (S) Campo no excluyente	El estado / región donde se encuentra su organización. Esto no debe ser abreviado.
País (C)	El código de dos letras para el país donde se encuentra su organización.
Dirección de correo electrónico Campo no excluyente	Una dirección de correo electrónico utilizada para ponerse en contacto con su organización.

2. La clave pública que se incluirá en el certificado. SSL utiliza claves públicas o criptografía asimétrica para cifrar datos transmitidos durante una sesión SSL. La clave pública se utiliza para cifrar y la clave privada correspondiente se utiliza para descifrar.
3. Información sobre el tipo de clave y la longitud. El tamaño de clave más común es RSA 2048.

¿Cómo se ve un CSR?

El propio CSR suele crearse en un formato PEM basado en la Base 64. Puede abrir el archivo CSR utilizando un editor de texto simple y se verá como el ejemplo a continuación.

Debe incluir el encabezado — *BEGIN NEW CERTIFICATE REQUEST* — y el pie de página — *END NEW CERTIFICATE REQUEST* — y pegar el CSR en medio.

—BEGIN NEW CERTIFICATE REQUEST—

```
MIIDVDCCAr0CAQAweTEeMBwGA1UEAxMVd3d3Lmpvc2VwaGNoYXBtYW4uY29tMQ8w
DQYDVQQLEwZEZXNpZ24xZjAUBgNVBAoTUDUpvc2VwaENoYXBtYW4xZjAUBgNVBAcT
CU1haWRzdG9uZTENMA5GA1UECBMES2VudDELMAkGA1UEBhMCR0lwgZ8wDQYJKo
ZI
hvcNAQEBBQADgY0AMIGJAoGBAOEFDpnOKRabQhDa5asDxYPnG0c/neW18e8apjOk
1yuGRk+3GD7YQvuhBVS1x6wkw1D2RnmnZgN1nNUK0cRK7slvOyCh1+jgD7u46mLk
81j+b4YSEmYZGPLluclucyocPDm0hXayjCUqWt7z6LMIKpLym8gayEZzz9Gn97PsbP
kVFBAGMBAAGgggGZMBoGCisGAQQBgjcNAgMxDBYKNS4xLjI2MDAuMjB7BgorBgEE
AYI3AgEOMW0wazAOBgNVHQ8BAf8EBAMCBPAwRAYJKoZIhvcNAQkPBDCwNTAOBgg
q
hkiG9w0DAglCAIAwDgYIKoZIhvcNAwQCAgCAMAcGBSsOAwIHMAoGCCqGS1b3DQMH
MBMGA1UdJQQMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHlo
A
TQBpAGMAcgbvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAg
AEMA
cgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABIAHIDgYkAk0kf
HSkr4jsEVya3mgUoyaYMO456ECNZr4Cb+WHPgexfjOO5qwOG1oDOTaKycrkc5pG+
IPBQnq+4cotT8hWJQwpc+qGb8xUETpxCokhrhN5079vFXq/5dsHkmtOTwkSqSnz9
yruVoxYeDQ8jl3KG3HTgxwFto8oZnm+E+Y4oshUAAAAAAAAAADANBkgqhkiG9w0B
AQUFAAOBgQAuAxetLzgfjBdWpjixevYZXuPZ+6jvZNL/9hOw7Fk5pVVXWdr8csJ
6JUW8QdH9KB6ZIM4yg8Df+vat1/DG6GuD2hiIR7fQ0NtPFBQmbrSm+TTBo95lwP+
ZSZTusPFTLKaQValdnS9Uw+6Vq7/I4ouDA8QBluaTFtPOp+8wEGBHQ==
—END NEW CERTIFICATE REQUEST—
```

Importante: La generación del CSR dependerá de la plataforma que esté utilizando.