

*Instrucciones y guía de Solicitud de
Certificados SSL Globalsign Perú*

ÍNDICE DE CONTENIDO

1	INTRODUCCIÓN	3
2	SOLICITUD DEL CERTIFICADO	3
2.1	FORMULARIO DE SOLICITUD DEL CERTIFICADO	3
2.2	DATOS DE CONTACTO	3
3	PASOS UNA VEZ REALIZADA LA SOLICITUD DEL CERTIFICADO	4
3.1	VERIFICACIÓN DEL DOMINIO	4
3.2	VERIFICACIÓN DE LA SOLICITUD (SÓLO PARA SSL EV)	4
3.3	VERIFICACIÓN DE LA ORGANIZACIÓN	4
4	EMISIÓN DEL CERTIFICADO	5
5	CONVERSIÓN DEL CERTIFICADO A FORMATO .CER O .CRT	5

1 INTRODUCCIÓN

Este documento define el proceso de solicitud de un certificado SSL, así como los documentos y controles necesarios para que Globalsign, proveedor de Camerfirma, pueda emitir el certificado de SSL.

2 SOLICITUD DEL CERTIFICADO

2.1 FORMULARIO DE SOLICITUD DEL CERTIFICADO

El usuario introducirá los datos de solicitud del certificado SSL en el excel facilitado por el departamento de Operaciones. Para ello tendrá que disponer de un CSR e introducirlo en los datos del formulario y debe disponer de la clave privada para su instalación.

Datos a introducir:

- Dominio/dominios del certificado
- Nombre de la Organización
- CIF de la entidad
- Nombre y apellidos del solicitante
- Teléfono de contacto del solicitante
- Mail de contacto del solicitante
- Departamento del solicitante
- CSR del certificado que debe contener: url/urls, departamento solicitante, organización, provincia y municipio. (Si el CSR que nos facilitó en su día no tenía estos datos debe remitirnos uno nuevo con ellos)
- Método de control de dominio (ver punto 3.1)

2.2 DATOS DE CONTACTO

Debe facilitar los datos de contacto del certificado, que será la persona encargada de gestionar todos los pasos hasta la descarga del certificado.

3 PASOS UNA VEZ REALIZADA LA SOLICITUD DEL CERTIFICADO

3.1 VERIFICACIÓN DEL DOMINIO

El email de contacto de la solicitud recibirá un correo electrónico con las instrucciones a seguir para completar la validación del dominio.

Dicho control se puede realizar de una de las siguientes opciones:

- a) Tendríamos la opción de que confirmen la validación por cualquiera de estas direcciones de correo electrónico que propone el reglamento admin, administrator, webmaster, hostmaster, postmaster (@dominioasecurizar).
- b) Registro DNS: creación de un registro TXT especificado en el archivo de zona (DNS) de su nombre de dominio.

En el caso de la Opción a) se le enviará al correo electrónico a la dirección indicada (admin, administrator, webmaster, hostmaster, postmaster) con un mensaje para que acepte el control del dominio.

En el caso de la Opción b) se le enviará al correo electrónico del solicitante un código para que lo introduzca en su DNS para verificar el control del mismo.

3.2 VERIFICACIÓN DE LA SOLICITUD (SÓLO PARA SSL EV)

El email de contacto de la solicitud recibirá un correo electrónico con dos documentos adjuntos que deberán devolver firmados a la cuenta de email indicada.

3.3 VERIFICACIÓN DE LA ORGANIZACIÓN

Se le pedirá por parte de Globalsign que confirme la organización de referencia del certificado TLS-SSL de una de las siguientes formas de su elección:

- a) Llamada telefónica realizada a uno de los teléfonos oficiales de la entidad.
- b) Enviar una factura telefónica que acredite la titularidad de uno de los teléfonos oficiales de la entidad.
- c) Firmar con un certificado digital acreditado por parte del solicitante del certificado un formulario con los datos de solicitud del certificado junto con su número de pedido que será facilitado cuando se le remita el control del dominio.

NOTA: Tras este paso puede recibir una llamada al telefono introducido en la solicitud para confirmar la pertenencia a la organización.

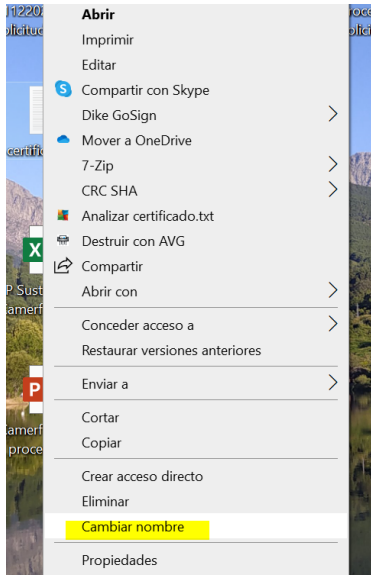
4 EMISIÓN DEL CERTIFICADO

Una vez se haya validado la documentación de respaldo y se haya verificado el control del dominio, se procede a la emisión del certificado. Con ello se envía al correo electrónico al solicitante del certificado con la clave pública del certificado.

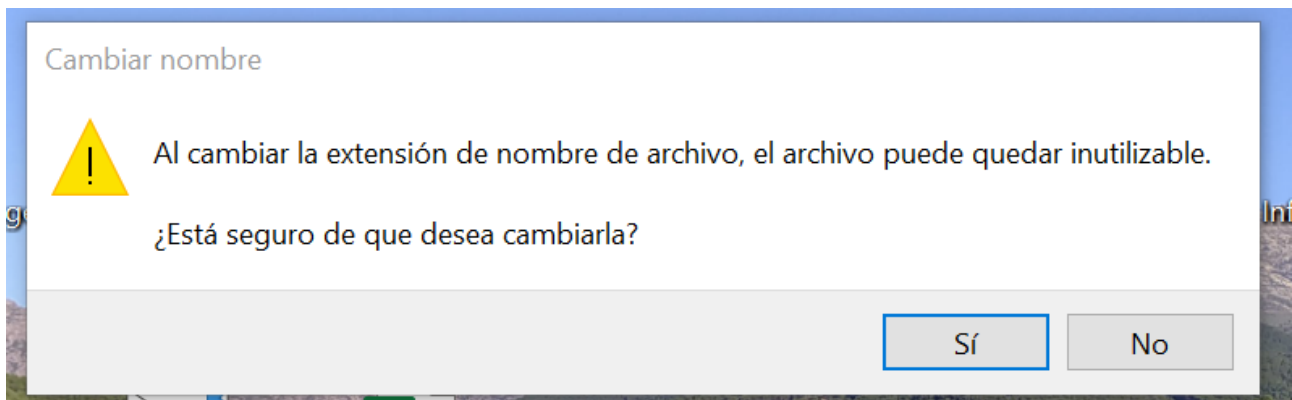
5 CONVERSIÓN DEL CERTIFICADO A FORMATO .CER O .CRT

El certificado lo recibirá en tipo texto, algo similar a esto

```
-----BEGIN CERTIFICATE-----
MIIGtDCCBZygAwIBAgIMHb59CJfqMRR/2xZtMA0GCSqGSIb3DQEBCwUAMGlxCzAJ
BgNVBAYTAKJFMRkwFwdfgyfyrhgfdf9iYWxTaWdulG52LXNhMTgwNgYDVQQDEy9H
bG9iYWxTaWdulEV4dGVuZGVkIFZhbGkYXRpb24gQ0EgLSBTSEEyNTYgLSBHMzAe
Fw0yMTAyMTgxMDM5sdfsdfsdfsdlxMDM5MzlaMIHoMR0wGwYDVQQPDBRQcmI2
NzwCAQMATAKVTMqswCQYDVQQGEWJFUzEPMA0GA1UECBMGTWVfcmIkMQ8wDQYDVQQH
EwZNYWRyaWQxIDAeBgNVBAKTF0MvIFJpYmVYYSBEZWwgTG9pcmEsIDEyMREwDwYD
VQLLEwhTaXN0ZW1hcEZMBcGA1UEChMQQUmgQ0FNRVJGSVJNQSBTQTEfMB0GA1UE
AxMwWbW9uaXRvci5jYW1lcmZpcmlhLmNvbTCCASlwdQYJKoZihvcNAQEBBQADggEP
ADCCAQoCggEBAOLzQzWp+zaDmYc9nqoAFPnLkId8wN8IrtC8iQnOvntkhNVUA18E
feH5fz3DVikgViaXT3rVbUk1qPWbP3MQ68ouOtdFmJfZZV9YfvkCl0Vs/A0755W
qSRITwx2OoDpUT34dxTgduh5LjNifWUS6TfasA1qS5kg+FSprz5WqiKDBUYB2R1
VR0OBBYEFJY5ixakbxHxIs6wmTRKmiHWy6PxMIIBBQYKKwYBBAHWeQIEAgSB9gSB
8wDxAHYAikVFB1IVJfaWP6Ev8fdthuAjlM0twEt/XcaDXG7iDwIAAAF3tLlmzQAA
BAMARzBFAiAFshDkSicuxJS06DRRHZbPVoSczUTfFrdYfzST0njfghAOx3K30k
qgxTYkUM9iKgmkwYM8mTyv2qc6FKLI2NjkP/AHcARqVV63X6kSAwtaKJafTzREs
QXS+/Um4havy/HD+bUcAAAF3tLlkxAAABAMASDBGAiEAwM9PjW49Qb4r2vRgbcir
SE0s+ZDK9FQgJf5ipjNo6TQCIQCMtwNiVOAgtn5N7KLFkFVGtcZ+q3D24rgo2Q9o
7Cr4hTANBqkqhkiG9w0BAQsFAAOCAQEAAexP2KW2HwoH+jXZIBP2znxOgx9dHEG7U
Yz/Rq3HyWDD7gQUkbPYjKJUUA4Lr8MbaIqK7URG2pQR8z47BEgffTznuIV55VBZ
3EVj7EMoa5vWubeGOWh95sRhme3LTbeq/9t3oi9d2n+aiBEUMBMRDgQhwiP5uLQA
uQm6e4xSNREXBzdyjOjYpXxusvxeF7lUskx86S4TxBiKcxhcxe09xTITWX3SjyZ
mflomMvViK3gyjLzEc9QeRSEiQyZYob6VZQd5Riceb/97IDvIrQHeQgUXSnWDWj
UlsprbyNlyrvmMvmQIXIT7YlgW5aB8GI68732Ogvcchw4Kr1doV8KA==
-----END CERTIFICATE-----
```

Cambiar .txt por .cer y pulsar en sí en el siguiente mensaje.



Y ya dispondrá de la parte pública del certificado para instalarlo en el servidor

