



Certificados digitales SSL y TLS



OWASP

The Open Web Application Security Project

About Me



OWASP

The Open Web Application Security Project

- Ing. Didier Fallas Rojas, Mag.
- Director de Redes e Infraestructura en InterNexo
- difaro@internexo.com
- Twitter: didierfallas
- LinkedIn: didierfallas

Agenda



OWASP

The Open Web Application Security Project

- Introducción SSL/TLS
- Certificados digitales
- Validez certificados
- Detalles en los navegadores
- Tipos de certificados
- Empresas certificadoras
- Creando mi propio certificado

Introducción al SSL/TLS



OWASP

The Open Web Application Security Project

- SSL: Secure Sockets Layer
- TLS: Transport Layer Security
- Es una tecnología que establece una conexión segura entre un cliente (visitante de un sitio web) y un servidor (servidor web) y hacen que toda la comunicación sea cifrada

Introducción al SSL/TLS



OWASP

The Open Web Application Security Project

- Los referenciamos como un protocolo que provee un canal seguro entre dos dispositivos
- El diseño del SSL inicia en 1994 por la empresa Netscape Communications y su diseño estaba orientado exclusivamente a ambientes web

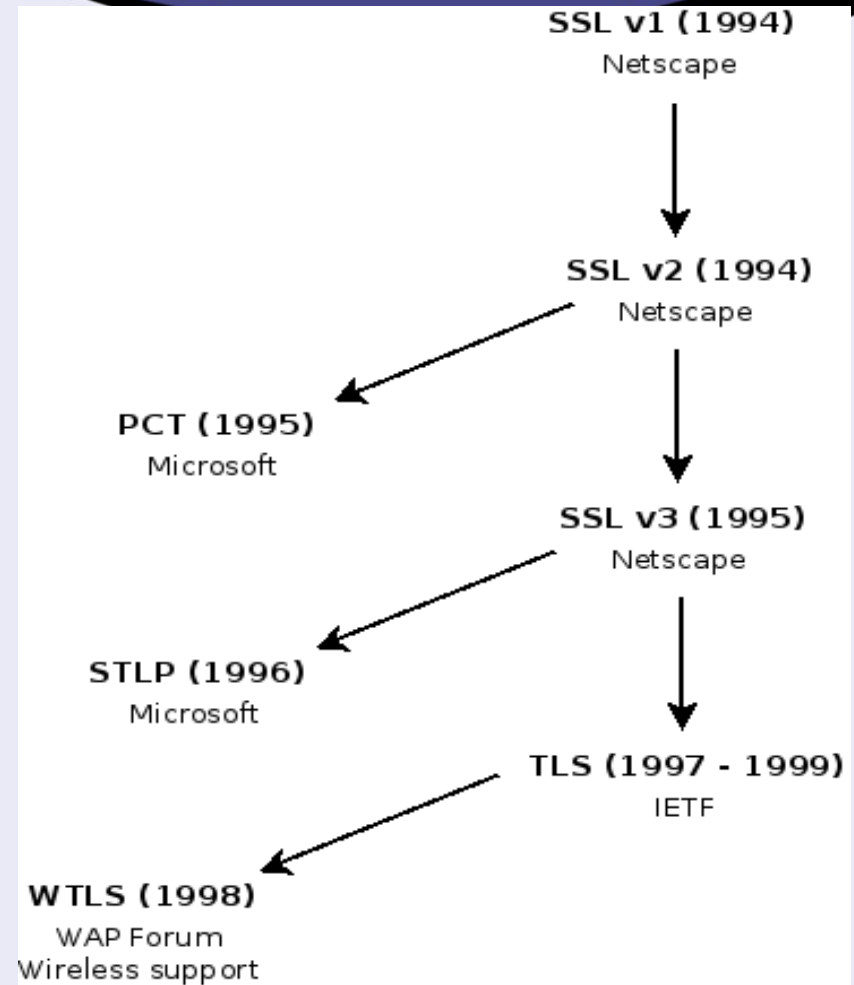
Introducción al SSL/TLS



OWASP

The Open Web Application Security Project

- Cronología
- IETF: Internet Engineering Task Force. Genera los documentos reconocidos como RFC. Muchos, estándares oficiales
- TLS: RFC 2246

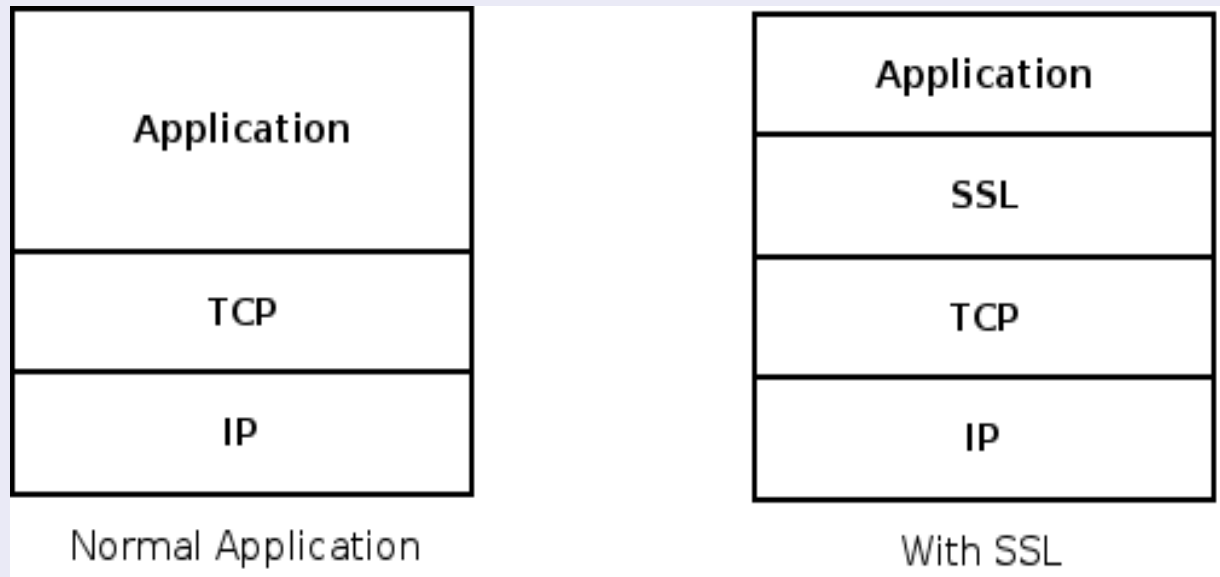


Ref. SSL and TLS.
Designing and
Building Secure
Systems

Introducción al SSL/TLS



- SSL en la capa de protocolos:



Ref. SSL and TLS. Designing and Building Secure Systems

Introducción al SSL/TLS



OWASP

The Open Web Application Security Project

- Aplicaciones conocidas que usan protocolo de seguridad:
 - Web
 - Correo
 - FTP (FTPS)
 - VPN

HTTP sobre SSL



OWASP

The Open Web Application Security Project

- HTTP fue el primer protocolo en usar una capa de seguridad SSL
- HTTP sobre SSL comúnmente le conocemos como HTTPS
- Puerto 443



- Para los certificados digitales se requiere que el dominio tenga una IP dedicada
- Si se usan servidores virtuales (virtual hosts), la forma de conocer el dominio a acceder es mediante el encabezado *Host* del protocolo HTTP, sin embargo, cuando se hace la negociación SSL, esta información no se ha enviado



- La solución es usar IP reales dedicadas para cada dominio, pues esta información si puede ser considerada en el flujo de datos SSL



OWASP

The Open Web Application Security Project

- ¿Qué es un certificado digital?
- Un certificado digital es un documento electrónico el cual valida la identidad de una entidad (persona, empresa, programa) y asocia esa identidad a una llave pública



OWASP

The Open Web Application Security Project

- Es un contenido de código almacenado en el servidor con el fin de:

La tecnología Secure Sockets Layer (SSL) protege sus transacciones en línea y le ayuda a mejorar la confianza de su sitio web de tres maneras esenciales:



1. Un certificado SSL permite el **cifrado** de información confidencial durante las transacciones en línea.



2. Cada certificado SSL es una **credencial** única que identifica al propietario del certificado.

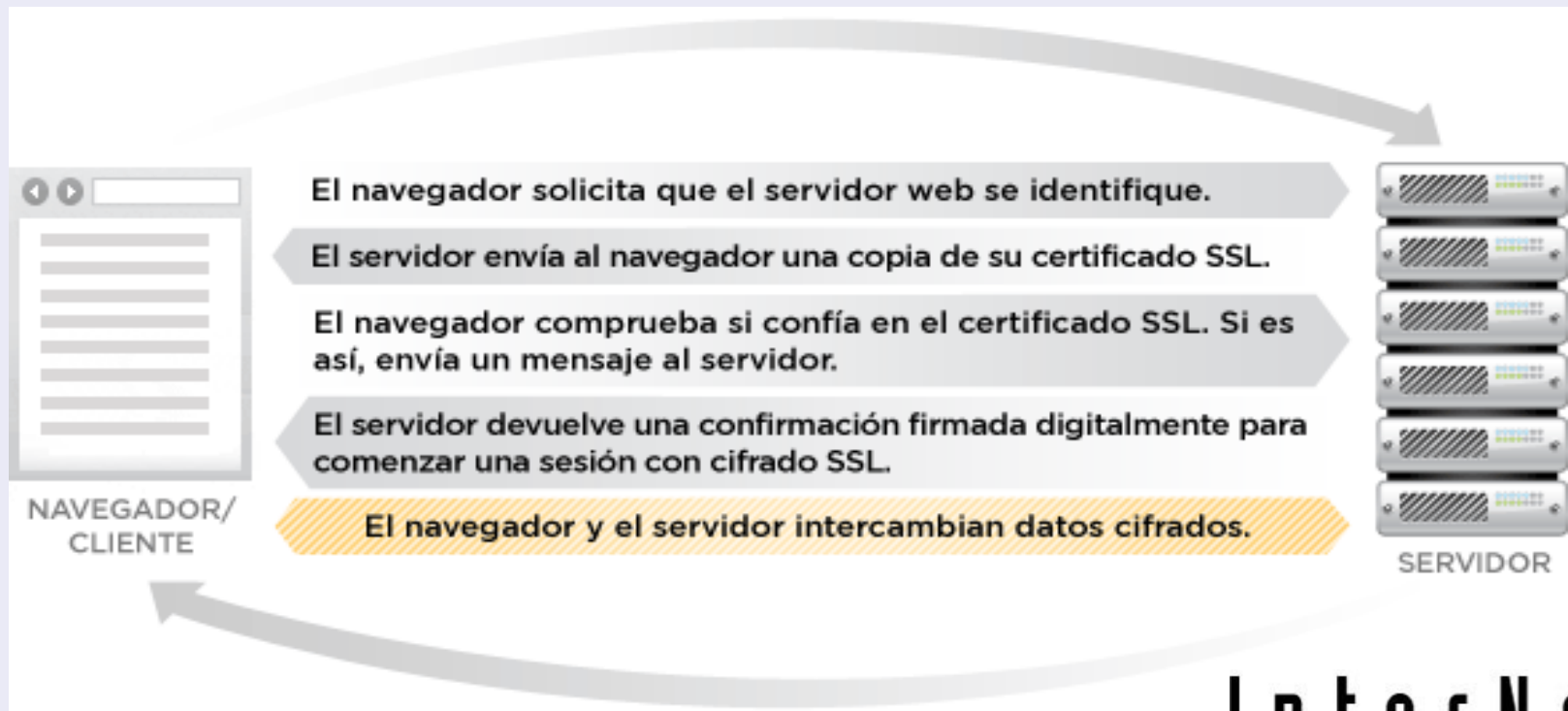


3. Una autoridad de certificación **auténtica** la identidad del propietario del certificado antes de emitirlo.

Ref. Verisign



- Comunicación entre el servidor y el navegador



Ref. Verisign



OWASP

The Open Web Application Security Project

- Comprobación de la validez de un certificado
- Existen tres condiciones para que el certificado sea válido y aceptado por los navegadores
- Si no se cumple alguna condición el navegador alerta y recomienda no continuar con la sesión

InterNexo

tecnologías internet



1. Nombre común CN (Common Name)
Debe coincidir con la dirección URL
que el usuario digita en el navegador

Visualizador de certificados: www.personas.bancobcr.com

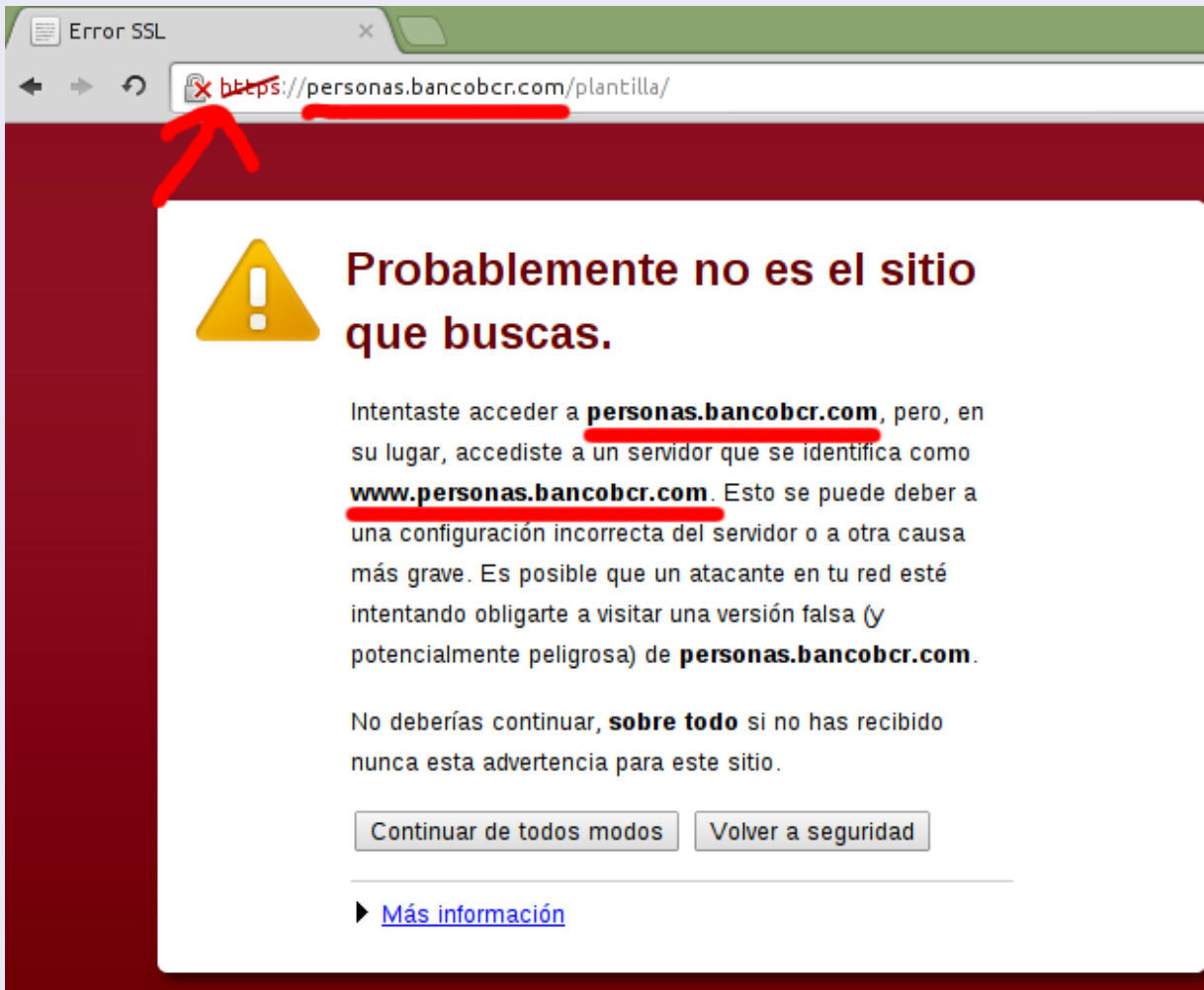
General Detalles

Este certificado se verificó para los siguientes usos:
Certificado del servidor SSL

Emitido a

Nombre común (NC)	<u>www.personas.bancobcr.com</u>
Organización (O)	Banco de Costa Rica
Unidad organizativa (UO)	Gerencia de Procesamiento de Datos
Número de serie	17:45:8D:C7:14:0D:AE:73:4E:01:10:C8:ED:68:34:

Si el Common Name no coincide



Error SSL

<https://personas.bancobcr.com/plantilla/>

Probablemente no es el sitio que buscas.

Intentaste acceder a **personas.bancobcr.com**, pero, en su lugar, accediste a un servidor que se identifica como **www.personas.bancobcr.com**. Esto se puede deber a una configuración incorrecta del servidor o a otra causa más grave. Es posible que un atacante en tu red esté intentando obligarte a visitar una versión falsa (y potencialmente peligrosa) de **personas.bancobcr.com**.

No deberías continuar, **sobre todo** si no has recibido nunca esta advertencia para este sitio.

[▶ Más información](#)

Certificados digitales



Si a pesar de la advertencia, acepto ingresar al sitio

A screenshot of a web browser window. The address bar shows a URL starting with "https://", which has a red 'X' over it, indicating a security warning. A red arrow points to this warning. The page content includes the BCR logo with the tagline "SOMOS EL BANCO DE COSTA RICA". Below the logo is a navigation bar with "Oficina Virtual" and "Pe". On the left, there is a login form titled "Ingreso Seguro" with fields for "Código de Identificación" and "Contraseña (Password)". On the right, a black box contains a security alert: "¡ALERTA DE SEGURIDAD! Nunca entregue o digite todos los valores, no re fotografías de su Tarjeta de Clave Dinámica. Es de uso personal y confidencial. Las coordenadas para confirmar las transacciones que usted origina en ¡Prevenamos juntos la delincuencia virtual!". At the bottom right, there is a logo for "interNexo" with the text "tecnologías internet" below it.



Verificando el Common Name del certificado como usuario

The screenshot shows a web browser window with the address bar containing <https://personas.bancobcr.com/plantilla/>. A red underline is drawn under the domain part of the URL. An overlay window titled "Visualizador de certificados: www.personas.bancobcr.com" is open, showing the "General" tab. The text in the overlay reads: "Este certificado se verificó para los siguientes usos: Certificado del servidor SSL". Below this, under the heading "Emitido a", there is a table of certificate details:

Nombre común (NC)	www.personas.bancobcr.com
Organización (O)	Banco de Costa Rica
Unidad organizativa (UO)	Gerencia de Procesamiento de Datos
Número de serie	17:45:8D:C7:14:0D:AE:73:4E:01:10:C8:

In the bottom right corner of the screenshot, the logo for "InterNexo tecnologías internet" is visible.



2. El certificado debe estar firmado por una EC (Entidad Certificadora) válida

The screenshot shows a browser's certificate viewer interface. At the top, the address bar displays "Banco de Costa Rica [CR] https://www.personas.bancobcr.com/plantilla/". Below this, the title of the viewer is "Visualizador de certificados: www.personas.bancobcr.com". There are two tabs: "General" (selected) and "Detalles". Under the "General" tab, the text reads: "Este certificado se verificó para los siguientes usos: Certificado del servidor SSL". Below this, there is a section titled "Emitido a" with the following details:

Nombre común (NC)	www.personas.bancobcr.com
Organización (O)	Banco de Costa Rica
Unidad organizativa (UO)	Gerencia de Procesamiento de Datos
Número de serie	17:45:8D:C7:14:0D:AE:73:4E:01:10:C8:ED:68:34:8B

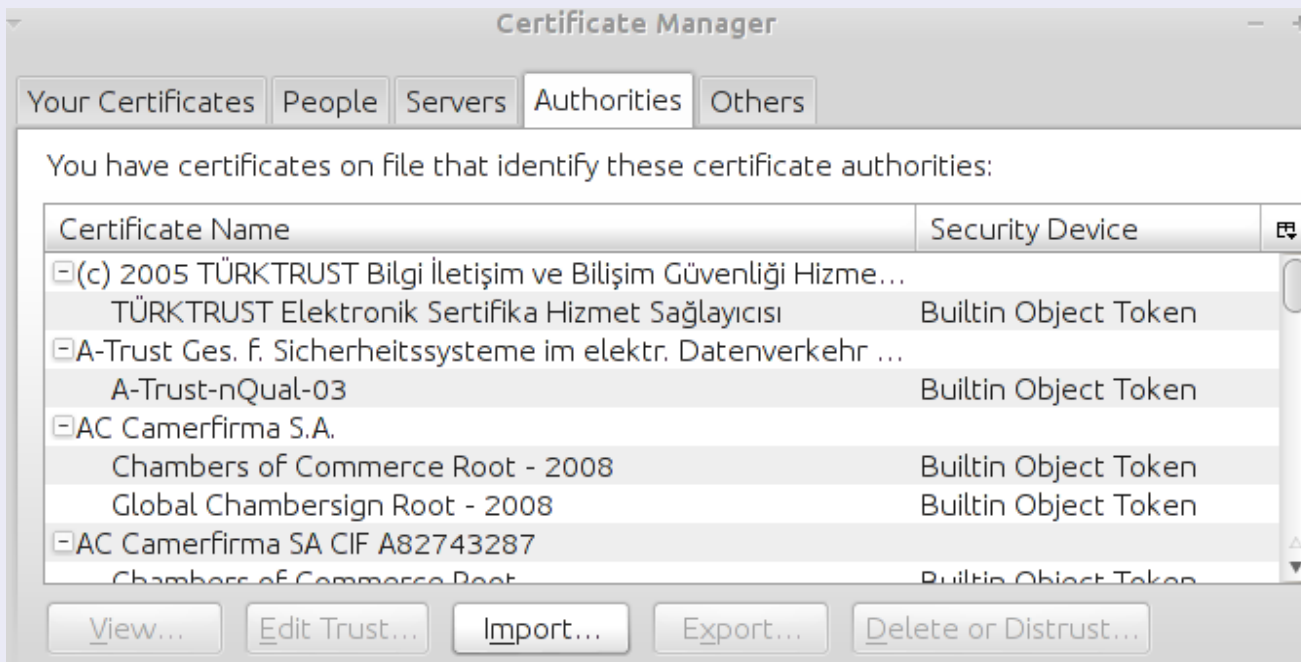
Below the "Emitido a" section is a section titled "Proporcionada por" (underlined in red in the image) with the following details:

Nombre común (NC)	VeriSign Class 3 Extended Validation SSL SGC CA
Organización (O)	VeriSign, Inc.
Unidad organizativa (UO)	VeriSign Trust Network



Entidades certificadoras registradas en los navegadores:

Firefox Edición → Preferencias → Avanzado → Cifrado → Ver Certificados





Chrome Configuración → Mostrar configuración avanzada → HTTPS/SSL → Administrar certificados → Autoridades

Administrador de certificados

Tus certificados Servidores **Autoridades** Otros

Tienes certificados archivados que identifican a estas entidades de certificación:

- ▼ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı
- ▼ A-Trust Ges. F. Sicherheitssysteme im elektr. Datenverkehr GmbH
A-Trust-nQual-03
- ▼ AC Camerfirma S.A.
Chambers of Commerce Root - 2008
Global Chambersign Root - 2008
- ▼ AC Camerfirma SA CIF A82743287
Chambers of Commerce Root
Global Chambersign Root
- ▼ AddTrust AB
AddTrust Class 1 CA Root
AddTrust External CA Root
AddTrust Public CA Root

Ver...

Edición...

Importar...

Exportación...

Eliminar...

InterNexo

tecnologías internet



3. El periodo de validez del certificado

A screenshot of a web browser displaying a certificate viewer for "Banco de Costa Rica [CR]". The address bar shows the URL "https://www.personas.bancobcr.com/plantilla/". The page title is "Visualizador de certificados: www.personas.bancobcr.com". There are two tabs: "General" (selected) and "Detalles". The main content area shows the following information:

Este certificado se verificó para los siguientes usos:
Certificado del servidor SSL

Emitido a

Nombre común (NC)	www.personas.bancobcr.com
Organización (O)	Banco de Costa Rica
Unidad organizativa (UO)	Gerencia de Procesamiento de Datos
Número de serie	17:45:8D:C7:14:0D:AE:73:4E:01:10:C8:ED:68:34:8B

Proporcionada por

Nombre común (NC)	VeriSign Class 3 Extended Validation SSL SGC CA
Organización (O)	VeriSign, Inc.
Unidad organizativa (UO)	VeriSign Trust Network

Período de validez

Emitido el	20/05/12
Vence el	<u>20/08/14</u> ←

A red arrow points to the expiration date "20/08/14", which is underlined in red.

Certificados digitales



OWASP

The Open Web Application Security Project

Signos visibles en el navegador

Costa Rica Flores - Envío de F...
https://www.costaricaflores.com

Costa Rica Flores.com

English Inicio Ingres

Banco de Costa Rica
https://www.personas.bancobcr.com/plantilla/

Banco de Costa Rica [CR]

Banco de Costa Rica
SOMOS EL BANCO DE COSTA RICA

InterNexO
tecnologías internet



OWASP

The Open Web Application Security Project

Detalle en Opera



Security & Trust

- ✓ **Securely connected**
www.costaricaflores.com
- ✓ **Clean security record**
This site has a clean security record.

Details...

- ✳ **Para él**
- ♥ **Amor y Aniversarios**
- ★ **Toda ocasión**
- ✳ **Difuntos**



Security & Trust

- ✓ **Securely connected**
www.personas.bancobcr.com
- ✓ **Verified identity**
This site is operated by Banco de Costa Rica (CR).
- ✓ **Clean security record**
This site has a clean security record.

Details...

 **Ingreso Seguro**

Código de Identificación

Contraseña (Password)

Ingresar>>

InterNexo
tecnologías internet



Usos:

- Transacciones, se requiere validar la autenticidad del dueño de un sistema
- Comercio electrónico
- Páginas de autenticación
- Cifrado de las comunicaciones



Shared Certificates

- Brindados por empresas hospedaje
- No hay relación con el nombre del dominio
- Mensajes de alerta en el navegador
- Cumplen función básica
- Se pueden usar para asegurar conexión con una sección admin.



OWASP

The Open Web Application Security Project

Validación nombre de dominio

- Solo se valida el nombre del dominio
- No hay alerta por parte del navegador
- Ideal para asegurar comunicación entre sitio web y visitantes



OWASP

The Open Web Application Security Project

Validación de organización

- El ente certificador valida la existencia de una organización
- Más validación → Más seguridad
- Son muy usados



OWASP

The Open Web Application Security Project

De validación extendida (EV)

- Top de los certificados
- Mejor proceso de validación
- Barra verde exclusiva
- Navegadores muestran nombre organización





Wildcard

- Permiten usar un único certificado en múltiples subdominios
- Por ejemplo, se pueda usar para:
 - midominio.com
 - www.midominio.com
 - dev.midominio.com
 - compras.midominio.com



OWASP

The Open Web Application Security Project

Multi-dominio

- Se puede usar en múltiples dominios, con nombre igual de segundo nivel y diferente de primer nivel
- Ejemplos:
 - midominio.com
 - midominio.net
 - midominio.org



OWASP

The Open Web Application Security Project

Empresas certificadoras

- Comodo: <http://ssl.comodo.com/>
- DigiCert: <http://www.digicert.com/>
- EnTrust: <http://www.entrust.com/>
- GeoTrust: <http://www.geotrust.com/ssl/>
- GoDaddy: <http://www.godaddy.com/ssl/ssl-certificates.aspx?ci=8979>
- Network Solutions: <http://www.networksolutions.com/SSL-certificates/index.jsp>
- Thawte: <http://www.thawte.com/>
- VeriSign: <http://www.verisign.com/>



OWASP

The Open Web Application Security Project

Creando mi propio certificado (self-signed certificates)

- Yo soy mi propia autoridad certificadora. Son los certificados privados
- Los navegadores no los reconocen y envían una alerta
- Agregando mi ente certificador para que no esté alertando



OpenSSL

- Es una biblioteca de cifrado
- Se derivó de SSLeany
- La primera versión liberada de OpenSSL fue en 1998
- Hay un programa con una amplia variedad de comandos
- <http://www.openssl.org/>




OWASP

The Open Web Application Security Project

Ingresando a mi sitio certificado

Error SSL

<https://www.midominio.com>

 **El certificado de seguridad del sitio no es de confianza.**

Has intentado acceder a **www.midominio.com**, pero el servidor contiene un certificado emitido por una entidad que no es de confianza para el sistema operativo de tu computadora. Esto puede suponer que el servidor haya generado sus propias credenciales de seguridad, en las que Google Chrome no puede confiar en relación con la información de identidad o que un atacante haya intentado interceptar tus comunicaciones.

No deberías continuar, **sobre todo** si no has recibido nunca esta advertencia para este sitio.

► [Más información](#)

InterNexo
tecnologías internet



Si avanzo a pesar del mensaje de advertencia de navegador

The image shows a browser window with a warning message about a certificate. The address bar shows a red 'X' over the 'https://' part of the URL. The page content is partially obscured by a certificate viewer window. The certificate viewer shows details for a certificate issued to 'www.midominio.com' by 'www.internexo.com'.

Visualizador de certificados: www.midominio.com

General Detalles

Este certificado se verificó para los siguientes usos:

Emitido a

Nombre común (NC)	www.midominio.com
Organización (O)	Mi Dominio Inc.
Unidad organizativa (UO)	Internet
Número de serie	01

Proporcionada por

Nombre común (NC)	www.internexo.com
Organización (O)	Organizacion de Prueba
Unidad organizativa (UO)	Internet Authority

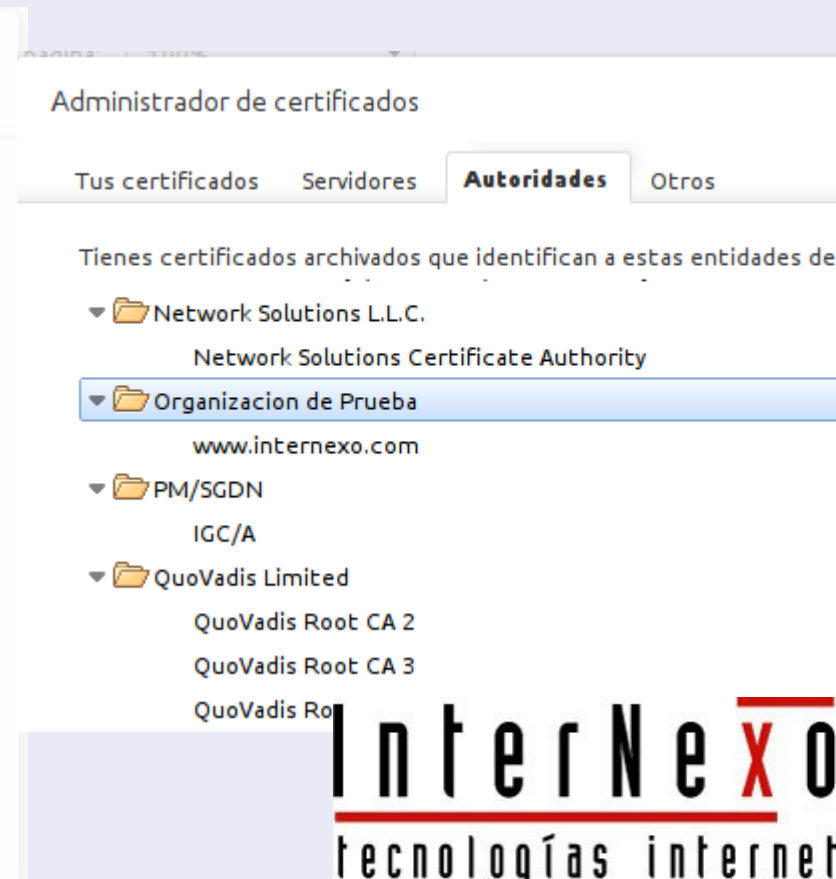
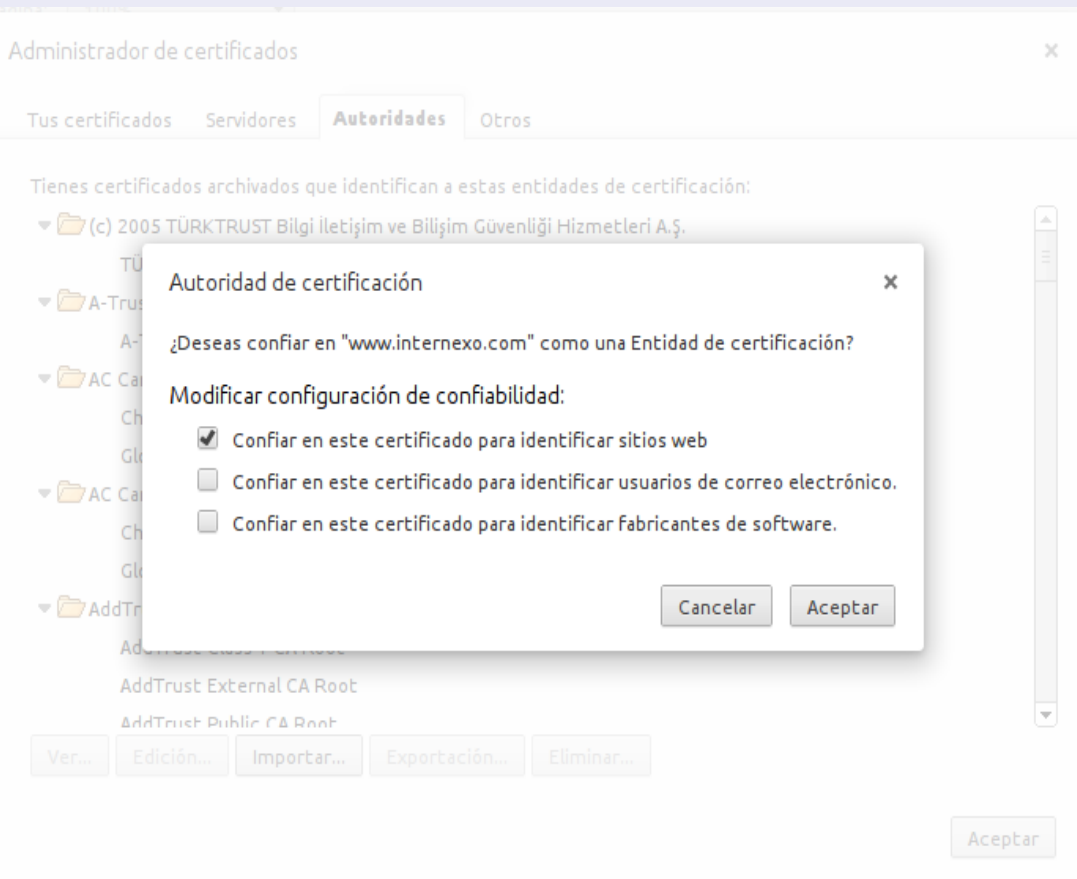
Período de validez

Emitido el	25/10/12
Vence el	23/10/22

Internexo
tecnologías internet



Agregando la autoridad de certificación al navegador





OWASP

The Open Web Application Security Project

¡Gracias!

difaro@internexo.com

Twitter: didierfallas

LinkedIn: didierfallas