MacroSeguridad

MAYORISTA EN SOLUCIONES DE SEGURIDAD INFORMATICA

# Certificados SSL


# Sobre Macroseguridad

**Mayorista exclusivo de Soluciones de Seguridad**

- ✓ **Seguridad Informática**
  Control de Acceso Lógico a la Red
  Acceso Remoto Seguro para VPN y SSLVPN
  Encripción de Datos Sensibles (HSM)
  Encripción de Datos Sensibles para empresas
  Web (SSL) Home-Banking
  e-Commerce; etc.
- ✓ **Identidad Digital**
  Soluciones Antiphishing
  Firma Digital
  Firma de E-mails
  Firma de Documentos Electrónicos
  Manejo Seguro de Certificados Digitales
  Portabilidad Segura de Certificados Digitales e Identidad Digital
  Code Signing, SSL
- ✓ **Administración de Derechos Digitales**
  Licenciamiento de Software
  Encripción de Datos
  Protección contra Piratería de Software, etc.

# ¿Qué es SSL?

**SSL** son las siglas de Secure Sockets Layer (Canal Seguro de Comunicación)

✓ Es la tecnología de seguridad estándar para crear un canal seguro y encriptado entre un servidor web y un navegador (browser).

✓ Este canal asegura que todos los datos que se intercambian entre ambos se mantengan íntegros y confidenciales.

✓ SSL es un estándar de la industria que se utiliza en millones de sitios web para la protección de las transacciones online con sus clientes.

## En otras palabras…

*SSL es la tecnología de seguridad que protege las transacciones sobre Internet de los clientes y provee a los visitantes una prueba de la identidad digital del sitio, brindando confianza en sus servicios.*

*Los visitantes verán que su transacción online es segura y confidencial y tendrán la confianza de que usted ha eliminado los riesgos asociados con el comercio en Internet.*

# Compatibilidad de los Certificados SSL

## Navegadores web:

- ✓ Microsoft Internet Explorer 5.01 +
- ✓ Mozilla Firefox 1.0+
- ✓ Mozilla 0.6+
- ✓ Google Chrome
- ✓ Konqueror (KDE)
- ✓ Netscape 4.77 +
- ✓ Opera 7.0+
- ✓ Apple Safari 1.2 +
- ✓ Camino 1.0+
- ✓ AOL 5+

## Micro Navegadores / PDAs:

- ✓ Apple iPhone, iPod Safari 1.0+
- ✓ Microsoft Windows Mobile 5/6*
- ✓ ACCESS NetFront Browser v3.4 +
- ✓ RIM Blackberry v4.2.1 +
- ✓ KDDI Openwave v6.2.0.12 +
- ✓ Opera Mini v3+
- ✓ Opera Mobile 6+
- ✓ Sony Playstation Portátil
- ✓ Sony Playstation 3
- ✓ Netscape Communicator 4.51+
- ✓ Nintendo Wii
- ✓ NTT / DoCoMo

# Categorías de Certificados SSL

1) ***Validación del Dominio (DV)*** – Confirmación de que la compañía controla el dominio. Se confirma usualmente a través de Who Is.
2) ***Validación de la Organización (OV)*** – Chequeo en la empresa para determinar que es legítima a través de la validación del dominio, presentación de documentos como registro comercial, facturas de servicios, etc.
3) ***Validación Extendida*** **(EV)** – Chequeo a través de una tercera parte confiable, acuerdo escrito firmado por un responsable de la organización y llamado a un número de teléfono publicado de la compañía.

   Un indicador del navegador confirma la identidad del sitio, por ejemplo en Internet Explorer 7 se muestra la barra de direcciones verde junto con el nombre de la entidad legal que controla el sitio web y el nombre de la autoridad de certificación.

**DV = Encripción**

**OV = Encripción + Validación**

**EV = Encripción + Validación + 100% Confianza**

# Validación del Dominio (DV)

## PROS

- ✓ Encripción

## CONTRAS

- ✓ Mensajes de error en algunos navegadores
- ✓ Cualquiera puede obtener un certificado de DV (domain validation), lo único que se necesita es una dirección de email @sudominio.com
- ✓ No valida la legitimidad de la empresa
- ✓ Sin logo de confianza
- ✓ Sin garantía
- ✓ Sin soporte

***Todos los Certificados SSL para dominio único encriptan información a 128 / 256 bits.***

***La diferencia es el nivel de validación y la Garantía del certificado.***

# Validación de la Organización (OV)

## PROS

- Encripción
- Validación de la Organización (garantizamos a sus clientes que usted es una organización real)
- Garantía (dependiendo de cuál OV adquiera)
- El candado dorado garantiza la encripción SSL, pero sólo la información impresa en el certificado informa la validación de la organización propietaria del sitio web.
- Soporte web o por email
- Esquina de confianza (Trust logo)

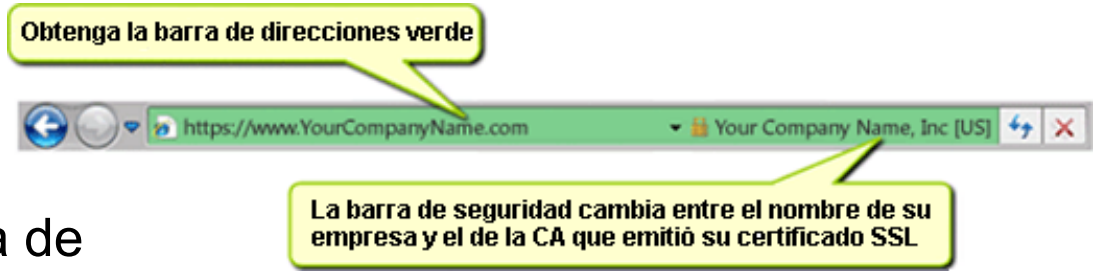
## CONTRAS

- Sin barra verde
- El usuario promedio no sabe la diferencia entre un DV y un OV.

# Validación Extendida (EV)

## PROS

- Encripción
- Barra de direcciones verde
- Manténgase al mismo nivel de sus competidores
- Cumpla con los estándares de la industria
- Indicación visual instantánea de confianza
- Usado por los mayores sitios de E-commerce y finanzas



# ¿Qué es la Garantía SSL?

La Garantía es una póliza de seguros que respalda la fuerza de las técnicas de validación de la CA, que valida todos los certificados según los más altos estándares. Si un certificado fuera emitido por error a una organización o individuo que no tuviera derecho a utilizarlo, y por ese motivo el público resultara defraudado – la garantía provee una compensación por los posibles daños.

MacroSeguridad
MAYORISTA EN SOLUCIONES DE SEGURIDAD INFORMATICA
www.macroseguridad.org

# Tipos de Certificados SSL

**Certificado para Dominio Único -** Un Certificado SSL que cubre un único dominio.

**Certificado EV (Validación Extendida) -** Un Certificado para dominio único que brinda el nivel más alto de seguridad y confianza, vuelve verde la barra de direcciones en algunos navegadores (IE7/IE8 y Firefox 3).

**Wildcard** – soporta sub-dominios. Se emite un certificado para todos los dominios en el mismo servidor. Si se utilizan servidores clustered (agrupados) se aplican cargos adicionales, y no es válido en certificados EV.

**Server Gated Cryptography (SGC) -** La Criptografía Activada por Servidor permite que los navegadores más antiguos, que encriptan a 40 bits, aumenten al estándar de la industria de 128 bits.

**Certificado Legacy –** para Exchange 2003.

**Certificados Unified Communications (UCC)** – MSX 2007, soporta múltiples dominios.

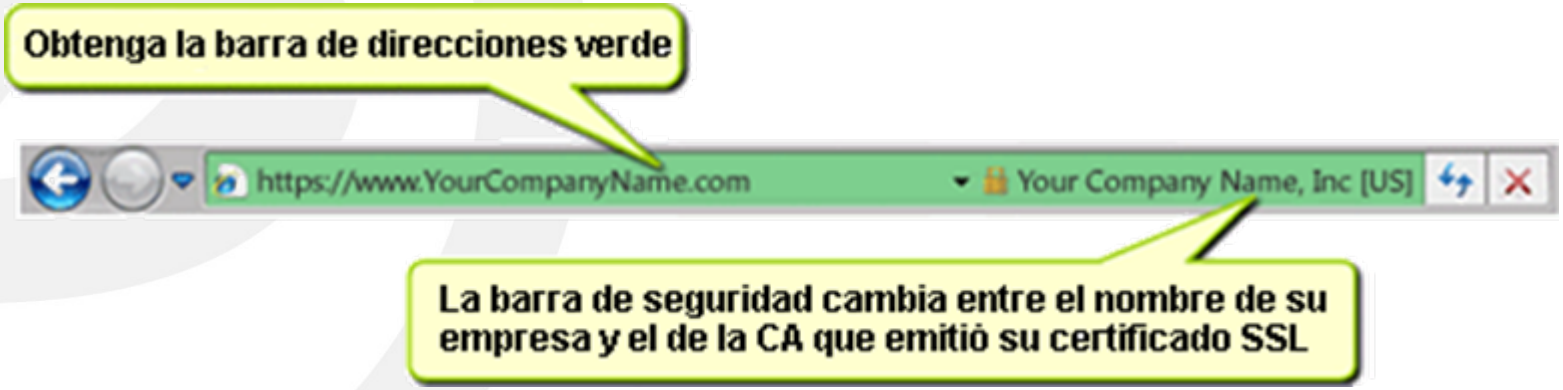
# *Certificado para Dominio Único*

- ✓ El certificado más habitual para trabajar
- ✓ Cubre un único nombre de dominio

EJEMPLO: **http://www.macroseguridad.org**

# Certificado EV (Validación Extendida)

- ✓ Un certificado para dominio único que vuelve verde la barra de direcciones en algunos navegadores
- ✓ El nivel más alto de seguridad y confianza



# Certificado Wildcard

✓ Un wildcard cubre ilimitados sub-dominios de cualquier dominio simple. Por ejemplo, **http://www.macroseguridad.org** es un dominio simple. El wildcard cubre http://**loquesea**.macroseguridad.org. El asterisco se usa para dar a entender ilimitados sub-dominios:

Ejemplo: *.macroseguridad.org

✓ El certificado wildcard incluye un servidor. Cualquier servidor adicional requiere una licencia de servidor

MacroSeguridad
MAYORISTA EN SOLUCIONES DE SEGURIDAD INFORMATICA
www.macroseguridad.org

# Criptografía Activada por Servidor (SGC)

- ✓ Puede agregarse a cualquier certificado SSL (incluyendo el EV) o certificado wildcard para asegurar el más alto nivel de seguridad
- ✓ SGC aumenta la encripción de 40 bits de los navegadores más antiguos hasta 128 bits
- ✓ Garantiza que todos sus visitantes, aun los que utilicen versiones antiguas de Internet Explorer, participen de una sesión encriptada dentro de los parámetros de seguridad actuales.
- ✓ Proteja a la más amplia base de clientes imaginable: si sus clientes se conectan utilizando versiones antiguas de Internet Explorer, o no sabe cómo se conectan, con la tecnología SGC podrán participar de una sesión encriptada dentro de los parámetros de seguridad actuales.

C·O·M·O·D·O

# Mail Servers

- ✓ Los clientes que necesitan un certificado SSL para servidores de mail tienen Exchange 03 o Exchange 07

- ✓ Exchange 03 requiere un certificado Legacy, que tiene el certificado raíz de confianza para que los teléfonos móviles más antiguos tengan acceso a emails

- ✓ Exchange 07 y posteriores requieren un UCC (Certificado de Comunicaciones Unificadas) que está diseñado especialmente para Exchange 07 y trabaja con todos los dispositivos móviles

# Exchange 03 = Certificado Legacy

# Exchange 07 = Certificado UCC

# Resumen de Certificados SSL

- ✓ Certificado SSL para Dominio Único
- ✓ Certificado SGC para Dominio Único
- ✓ Certificado SSL EV
- ✓ Certificado SGC EV
- ✓ Certificado Wildcard
- ✓ Certificado Wildcard SGC
- ✓ Certificado Legacy
- ✓ Certificado UCC



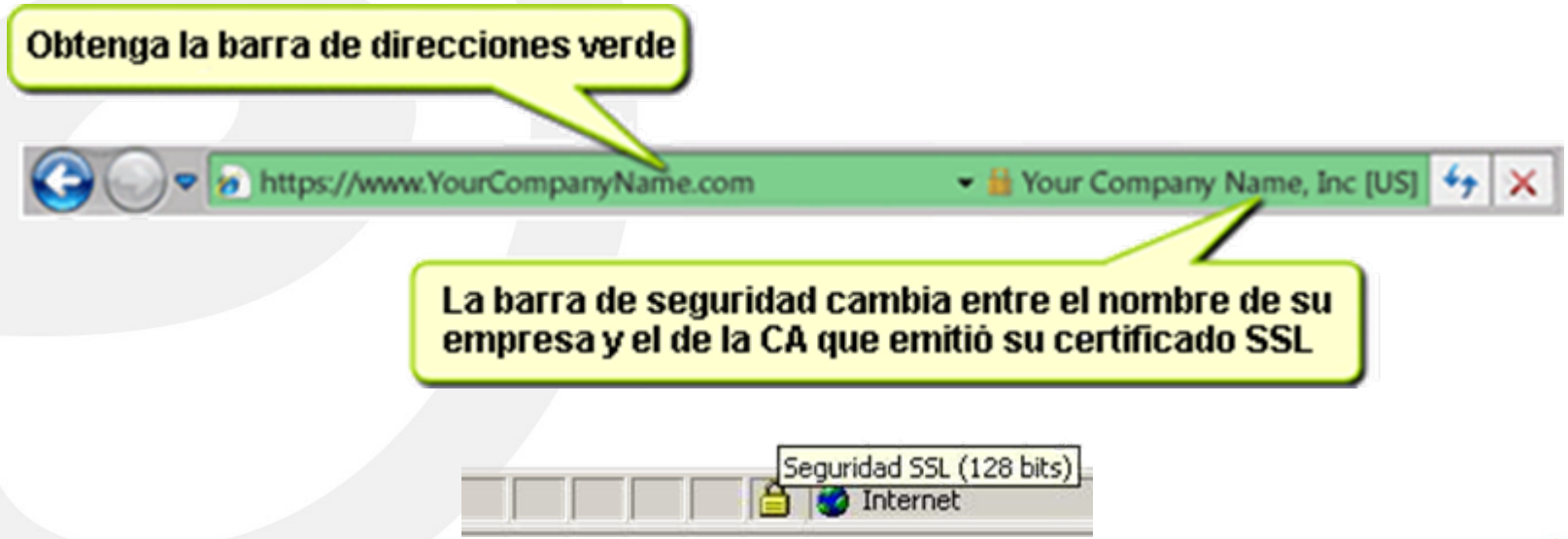
# Implementando un Certificado SSL

- ✓ Un servidor web necesita un Certificado SSL
- ✓ Para activar SSL en un servidor web el cliente debe completar una serie de preguntas sobre la identidad de su sitio web
  - ✓ URL del sitio web
  - ✓ Nombre y dirección de la organización
- ✓ Se crean un par de claves criptográficas – una Clave Privada y una Clave Pública
  - ✓ La Clave Privada se llama así por una razón – debe permanecer privada y segura
  - ✓ La Clave Pública no necesita ser secreta y figura en el Pedido de Certificado de Firma (CSR) – un archivo de datos que contiene los detalles del sitio web
- ✓ Entonces, Macroseguridad-Comodo:
  - ✓ Valida los detalles y emite el Certificado SSL
  - ✓ El servidor del cliente va a comparar el Certificado SSL emitido con su Clave Privada y va a establecer un canal encriptado entre el sitio web y el navegador del usuario final

# Mostrando el Candado de Seguridad SSL

El navegador mostrará un indicador (candado) para que los usuarios sepan que están protegidos por una sesión encriptada SSL.

*Así lo verán los usuarios de Internet Explorer:*



MacroSeguridad
MAYORISTA EN SOLUCIONES DE SEGURIDAD INFORMATICA
www.macroseguridad.org

# Background de los Certificados SSL

| Tipo | Validación | Término Máximo | Posibilidad de Fraude | Apariencia |
|---|---|---|---|---|
| SSL DV | Apenas validado | 10 años | Muy fácil | https + candado |
| SSL OV | Se revisan algunos documentos que suministra el cliente | 5 años | Difícil | https + candado |
| SSL EV | Revisión cuidadosa de las credenciales de la organización contra datos externos | 2 años | Muy difícil | **https + candado Autoridad Certificante + Propietario del Certificado + Barra Verde en el navegador** |

# Sobre MacroSeguridad-Comodo

- ✓ MacroSeguridad.org y Comodo son proveedores líderes brindando confianza y garantía de servicios para Internet, con más de 150.000 clientes en más de 100 países. Comodo ofrece servicios esenciales de confianza, a través de un portafolio de soluciones patentadas para identidad digital segura y comercio electrónico, todos ellos diferenciados respecto de sus competidores por un bajo TCO.

- ✓ Impulsado por el Laboratorio Digital de Confianza (DTL – Digital Trust Lab), Comodo está ayudando a las empresas de todo el mundo a proteger la integridad de su marca, fortalecer la confianza del cliente y la confianza en el comercio electrónico digital, y al mismo tiempo a crear operaciones digitales eficientes.

- ✓ MacroSeguridad.org, mayorista en soluciones de seguridad digital, y Comodo, líder de la industria, presentan soluciones escalables integradas que incluyen soluciones de gestión de web hosting, servicios de infraestructura de seguridad, servicios digitales de e-business, certificados digitales, seguridad de la identidad, privacidad del cliente y soluciones de administración de vulnerabilidades.

# ¿Dudas o Comentarios?

## tecnologia@macroseguridad.org