

GUÍA PEDAGÓGICA N° 8

E.P.E.T. N° 1 de Jáchal.**Nivel: Secundario****Ciclo: Segundo****Año: Séptimo****División/es: 1ra y 2da****Turno: Mañana y Tarde****Área Curricular: PRÁCTICA PROFESIONALIZANTE****Docente/s:** Aballay Javier – Mihalich Romina**Contacto/s:** Javier +5492646700658 -Romina +5492644395209**Mail:** rmihalich@hotmail.com, javieraba@gmail.com**F. de presentación:** 13/11/2020.**Título de la propuesta:** Seguridad Informática y comercio Electrónico.**Contenidos:** Certificados digitales y seguridad en las transacciones via web.

¿Por qué el SSL hace un sitio más seguro?

Un certificado SSL contiene información verificada sobre el sitio web que asegura para ayudar a los usuarios a confirmar que se están comunicando con su sitio web. Extended Validation es el estándar de verificación más alto de la industria y proporciona la seguridad más visible para los usuarios: la barra de direcciones se vuelve verde en navegadores de alta seguridad.

Al mostrar el Sello del sitio, los usuarios pueden hacer clic en la marca de confianza para ver la información de identificación de sitio web, quién lo verificó, y la fecha de caducidad del certificado SSL. En los navegadores más recientes, la información de identificación de sitio web puede aparecer cuando los usuarios pasan por sobre la barra de direcciones. También pueden hacer clic en el icono de candado cerrado.

Fundamentos de SSL

Hay 3 elementos esenciales: un protocolo de comunicaciones (SSL), credenciales para establecer la identidad (el certificado SSL), y un tercero que da fe de las credenciales (la autoridad certificante).

- Los equipos utilizan protocolos para permitir diferentes sistemas trabajen juntos. Los servidores web y los navegadores se basan en el protocolo Secure Sockets Layer (SSL) para permitir las comunicaciones cifradas. La solicitud del navegador al servidor para que se identifique a sí mismo es una función del protocolo SSL.
- Las credenciales para establecer la identidad son comunes en nuestra vida diaria: la licencia de conducir, un pasaporte, la tarjeta de identificación de la empresa. Un certificado SSL es un tipo de certificado digital que sirve como una credencial en el mundo online. Cada certificado SSL identifica de forma exclusiva un dominio específico y un servidor web.
- Nuestra confianza en una credencial depende de nuestra confianza en la organización que lo emitió. Las autoridades certificadoras cuentan con una variedad de métodos para verificar la información proporcionada por los individuos u organizaciones. Las autoridades certificadoras establecidos son bien conocidas y de confianza para los proveedores de navegadores. Los navegadores extienden esa confianza a los certificados digitales que son verificados la autoridad certificante.

Por qué necesita SSL

Los certificados SSL mantienen las comunicaciones en línea privadas a pesar de que viajan a través de la red pública Internet, y ayudan a sus clientes a ganar confianza para realizar transacciones en sitio web.

Si Usted solicita a los usuarios de su sitio web que iniciar una sesión, si ingresan datos personales como números de tarjetas de crédito en línea, o si acceden a información confidencial, como registros médicos o cuentas financieras, Usted que necesita mantener la privacidad de los datos. También es necesario que los ayude a confirmar que su sitio web es auténtico.

SSL también se utiliza en los servidores de correo electrónico, en las aplicaciones basadas en la web, en las comunicaciones de servidor a servidor y mucho más.

Cifrado

El cifrado es un proceso matemático de codificación y decodificación de la información. El número de bits (40 bits, 56 bits, 128 bits, 256 bits) indica el tamaño de

la clave. Al igual que una contraseña larga, una clave más grande tiene más combinaciones posibles. De hecho, el cifrado de 128 bits es un billón de veces más fuerte que el cifrado de 40 bits.

Cuando se establece una sesión cifrada, la fortaleza del cifrado está determinada por el navegador web, el certificado SSL, el servidor web y el sistema operativo de la computadora cliente.

Qué certificado SSL me conviene

El certificado SSL adecuado para su organización depende de su sitio web y su público.

- Para los sitios web públicos, donde los clientes ingresan sus tarjetas de crédito u otra información de alto valor, Usted tiene que mostrar rápidamente a los usuarios una prueba de identidad de su sitio web y que utiliza cifrado. Un certificado con Validación Extendida (EV) que muestra la barra de direcciones verde en los navegadores de alta seguridad y el nombre de la organización verificada, facilita que los usuarios confíen en su sitio.
- Si su sitio requiere inicio de sesión (log-in), los certificados con Validación de Organización (OV) ofrecen garantías de la identidad y la seguridad de su sitio. El cifrado es tan fuerte como con un certificado EV, sin embargo, sin la visibilidad y la seguridad de la barra de direcciones verde.
- Si sus usuarios se conectan utilizando navegadores antiguos o no están seguros de cómo se conectan, considere los certificados SSL con SGC. La mayoría de los certificados SSL son capaces de cifrado fuerte (128 bits o superior). Sin embargo, sin la tecnología SGC, algunos navegadores y sistemas operativos antiguos pueden permitir el cifrado de 128 bits. Los certificados SSL con SGC habilitan el cifrado de 128 ó 256 bits a más del 99,9% de los usuarios de Internet

Para mantener la privacidad de las comunicaciones en Intranets, elija un certificado con Validación de Dominio (DV) que proporciona cifrado para sus empleados y usuarios. Sólo se verifica el nombre de dominio.

Ejemplo de empresa Certificante:



CertiSur es una empresa especializada en brindar soluciones de seguridad para promover la confianza en los canales electrónicos que cuenta con clientes en toda América Latina. Comercializa una amplia cartera de Certificados SSL, Autenticación Segura, Firma Digital, Firma Biométrica, Sistemas de Detección de Amenazas Web, Documentos Electrónicos y TimeStamping.

Datos de contacto:
Valeria Marinelli
Marketing Digital
vmarinelli@yahoo.com
11 4311-2457
Av. Santa Fe 788, C.A.B.A, Argentina

Actividades:

1. Investigue que empresas argentinas utilizan Certificados de Seguridad, nómbrelas. Sugerencias Bancos, Fravega, Garbarino, Movistar, etc. Cadenas hoteleras.
2. De acuerdo a los sitios que permiten realizar compras electrónicas, mencione detalladamente su organización. Ejemplo: el detalle de la mercadería es claro las imágenes son claras y visibles tienen navegador de características por ejemplo tiene imágenes que muestren todos los ángulos de la mercadería suela, frente, perfil, talles disponibles, formas de entrega, etc, si se tratara de venta de calzado por ejemplo. O por ejemplo venta de celulares. si compara sitios muestre imágenes de las páginas que no cuentan con estos detalles y las que si.
3. De las empresas locales verifique y emita un informe de las características visibles en los sitios, es decir si permiten la compra on-line o si solo publican la información. Ejemplo CASTILLO SRL, Las olivas, Roca Basal <https://roca-basal3.webnode.com>, TRIPLE SPORT, o cualquier otra página que se dedique a la venta. Verifique si tiene certificados digitales.
4. Si la página estudiada cuenta con venta indique si tiene su propio capturador de datos de venta número de tarjeta, datos personales o si utiliza un tercero para completar la venta, ejemplo Mercado Pago o cadenas de Tarjetas independientes, por ejemplo estudie como se cobran las tarjetas de crédito VISA, MASTERCARD, FALABELLA, y si estas utilizan algún medio que asegure su información de pago.
5. Investigue que es un carrito de compras, y mencione páginas que cuenten con esta herramienta. De la que encuentre verifique si tienen certificados de

seguridad. Ejemplos: Páginas de Shoppings, MercadoLibre, cadenas de ventas internacionales. Canales de Televisión prepaga, Wish

Forma de Presentación:

Deberá enviar un archivo pdf con este archivo, a la/s casillas de mail consignadas al principio de la guía o foto adjunta con las respuestas pueden ser manuscritas. Siempre consignar el URL de la página estudiada y la captura para poder entender el informe que realice.

Equipo de conducción:

- Directora: Prof. Nancy M. Heredia.
- Vicedirector: Prof. Rodolfo A. Reiloba.
- Regente: Prof. Iris B. Gómez.