CRMpolizas.com, mucho más que un CRM para pólizas
San Luis Potosí, SLP
44 41 42 63 69
CRM_polizas@cadena-software.com

San Luis Potosí, SLP. Noviembre 2022

Certificaciones de seguridad de datos en CRMpolizas.com

Contamos con múltiples certificados de seguridad de datos, divididos en 2 grupos:

1. Certificado SSL (TSL) (página 1 a 3)
2. Certificados del hosting (paginas subsecuentes)

1.- Certificado SSL (TSL)

Éste certificado es el estándar internacional de seguridad y encriptado de datos, sólo es posible poseerlo si se cumplen múltiples requisitos de software y bases de datos, además de los protocolos de seguridad para el encriptado de datos y comunicación entre el usuario y el sitio.

Para documentarse que es un certificado SSL (TSL) favor de visitar:
https://es.wikipedia.org/wiki/Seguridad_de_la_capa_de_transporte

Al final de este documento se anexa nuestro certificado SSL (TSL) vigente.

Por lo pronto resalto importantes conceptos (en imágenes) de lo que éste certificado implica:

Seguridad de la capa de transporte (en inglés: **Transport Layer Security** o **TLS**) y su antecesor **Secure Sockets Layer** (**SSL**; en español **capa de puertos seguros**) son protocolos criptográficos, que proporcionan comunicaciones seguras por una red, comúnmente Internet.[1]

Descripción [editar]

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, solo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (*Digital Signature Algorithm*) o Fortezza.
- Para cifrado simétrico: RC2, RC4, IDEA (*International Data Encryption Algorithm*), DES (*Data Encryption Standard*), Triple DES y AES (*Advanced Encryption Standard*).
- Con funciones hash: MD5 o de la familia SHA.

Funcionamiento [editar]

El protocolo SSL intercambia registros; opcionalmente, cada registro puede ser comprimido, cifrado y empaquetado con un código de autenticación del mensaje (MAC). Cada registro tiene un campo de *content_type* que especifica el protocolo de nivel superior que se está usando.

Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo *handshake* (o protocolo de acuerdo), que tiene el *content_type* 22.

El cliente envía y recibe varias estructuras *handshake*:

- Envía un mensaje *ClientHello* especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Este también envía bytes aleatorios que serán usados más tarde (llamados *Challenge de Cliente* o *Reto*). Además puede incluir el identificador de la sesión.
- Después, recibe un registro *ServerHello*, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.
- Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.[10]
- Cliente y servidor negocian una clave secreta (simétrica) común llamada *master secret*, posiblemente usando el resultado de un intercambio Diffie-Hellman, o simplemente cifrando una clave secreta con una clave pública que es descifrada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este *master secret* (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una *función pseudoaleatoria* cuidadosamente elegida.

TLS/SSL poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en el MAC.
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC). Esto se especifica en el RFC 2104).
- Protección contra varios ataques conocidos (incluyendo ataques *man-in-the-middle*), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.
- El mensaje que finaliza el protocolo *handshake* (*Finished*) envía un *hash* de todos los datos intercambiados y vistos por ambas partes.
- La función pseudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos *hash* diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.

Intercambio de claves [editar]

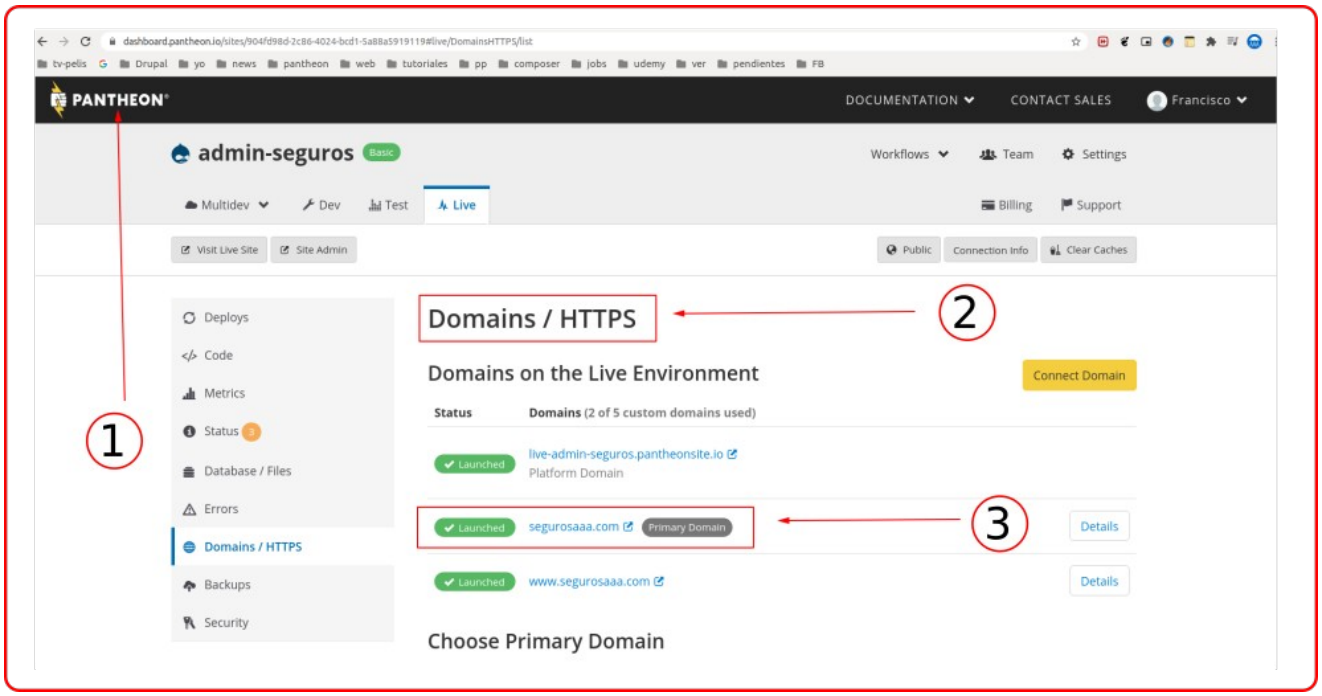
Antes de que un cliente y el servidor pueden empezar a intercambiar información protegida por TLS, deben intercambiar en forma segura o acordar una clave de cifrado y una clave para usar cuando se cifren los datos (ver Cifrado). Entre los métodos utilizados para el intercambio/acuerdo de claves son: las claves públicas y privadas generadas con RSA (denotado TLS_RSA en el protocolo de *handshake* TLS), Diffie-Hellman (llamado TLS_DH), Diffie-Hellman efímero (denotado TLS_DHE), Diffie-Hellman de Curva Elíptica (denotado TLS_ECDH), Diffie-Hellman de Curva Elíptica efímero (TLS_ECDHE), Diffie-Hellman anónimo (TLS_DH_anon),[2] y PSK (TLS_PSK).[11]

El método de acuerdo de claves TLS_DH_anon no verifica el servidor o el usuario y por lo tanto rara vez se utiliza puesto que es vulnerable a un ataque de suplantación de identidad. Solo TLS_DHE y TLS_ECDHE proporcionan secreto-perfecto-hacia-adelante.

Los certificados de clave pública que se utilizan durante el intercambio/acuerdo también varían en el tamaño de las claves de cifrado públicas/privadas utilizadas durante el intercambio y, por tanto, en la solidez de la seguridad que proveen. En julio de 2013, Google anunció que dejaría de utilizar claves públicas 1024 bits y cambiaría a claves de 2048 bits para aumentar la seguridad del cifrado TLS que proporciona a sus usuarios.[12]

2.- Certificados del hosting

https://CRMpolizas.com esta alojado en https://pantheon.io dentro de un **servidor dedicado** en USA (es exclusivo y no compartido) y al contener estas y otras características posemos múltiples certificaciones de seguridad de datos demostradas en las siguientes imágenes:



En la imagen anterior (punto 1 y 3) vemos que CRMpolizas esta alojado en https://pantheon.io la cual es la plataforma mundialmente mas grande y segura para alojamientos de Drupal.
En el punto 2 muestra que contamos con un protocolo HTTPS (la última 'S' implica seguridad, SSL).

En las siguientes páginas mostraré en imágenes algunos de los certificados con los que contamos en cuanto a la seguridad de datos, para leer todo lo aquí descrito favor de acceder a: https://pantheon.io/security

Certificados de seguridad de datos del servidor:

Cumplimiento y seguridad de la información

Pantheon es revisado periódicamente por terceros para verificar la seguridad, la privacidad y el cumplimiento de la plataforma, y trabajamos constantemente para ampliar esta cobertura. Obtenga más información sobre la conformidad de Pantheon con las siguientes políticas y certificaciones de seguridad de la información:

[SOC 2]

SOC 2

SOC 2 compliance provides third party assurance to our customers about the adequacy of Pantheon's information security system. Our SOC 2 compliance covers the Security and Availability Trust Services Criteria.

SOC 2

El cumplimiento de SOC 2 proporciona garantía de terceros a nuestros clientes sobre la idoneidad del sistema de seguridad de la información de Pantheon. Nuestro cumplimiento de SOC 2 cubre los criterios de servicios de confianza de seguridad y disponibilidad.

The General Data Protection Regulation (GDPR)

GDPR

The General Data Protection Regulation (GDPR) is a data privacy law that defines a framework for how companies use and protect personal information about European Union citizens. Pantheon complies with all applicable data privacy laws including GDPR.

GDPR

El Reglamento General de Protección de Datos (GDPR) es una ley de privacidad de datos que define un marco para cómo las empresas usan y protegen la información personal de los ciudadanos de la Unión Europea. Pantheon cumple con todas las leyes de privacidad de datos aplicables, incluido el RGPD.

The Family Educational Rihts agnd Privacy Act (FERPA)

FERPA

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. Pantheon's security policies and infrastructure allow customers to be FERPA compliant.

FERPA

La Ley de Privacidad y Derechos Educativos de la Familia (FERPA) es una ley federal que protege la privacidad de los registros educativos de los estudiantes.
Las políticas e infraestructura de seguridad de Pantheon permiten a los clientes cumplir con FERPA.

[Escudo de la Privacidad Unión Europea-Estados Unidos]

EU-US & US-Swiss Privacy Shield

Pantheon complies with the requirements of the EU-US & US-Swiss Privacy Shield frameworks on data privacy. We recently expanded our Privacy Shield coverage to accommodate the United Kingdom's withdrawl from the European Union. To learn more about these programs and to view Pantheon's Privacy Shield registration, please visit privacyshield.gov.

Escudo de la Privacidad Unión Europea-Estados Unidos

Pantheon cumple con los requisitos de los marcos de protección de privacidad UE-EE. UU. Y EE. UU.-Suiza sobre privacidad de datos. Recientemente ampliamos nuestra cobertura del Escudo de privacidad para dar cabida a la retirada del Reino Unido de la Unión Europea. Para obtener más información sobre estos programas y ver el registro del Escudo de privacidad de Pantheon, visite privacyshield.gov.