Análisis, desarrollo e implementación de sistema que permite detectar páginas fraudulentas

Santiago Hernan Duran Paredes[1], Jorge Eterovic[1], Luis Torres, Iris Sattolo[1].

[1]Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales,
Universidad de Morón.
Cabildo 134 - CP (1708) - Morón - Prov. de Bs. As. Tel: 5627-2000
sam.paredes@hotmail.com, jeterovic@hotmail.com, torreslu@ar.ibm.com,
iris.sattolo@gmail.com

Resumen. La seguridad informática requiere una actualización constante para enfrentar una amplia gama de amenazas y evitar que estos hechos se lleven a cabo. El phishing es una actividad ilícita, cuyo principal objetivo es robar datos. Uno de los métodos que se usa para evitar esta actividad ilícita es mediante campañas de prevención, pero las mismos se continúan presentando, generando malestar en la sociedad. Se propone elaborar una aplicación, que permita a los usuarios reconocer si están ante una página segura o no y así evitar proporcionar datos personales, a la página de dudosa procedencia. Deberá indicar que nivel de seguridad presenta la página, ya sea fuerte, moderada, baja o pobre, informando los métodos que usa el certificado digital, y dando puntaje a los mismos, indicando que tan seguro es.

Keywords: phishing, certificado digital, seguridad informática, sistema.

1 Introducción

Este trabajo pretende contribuir al problema de phishing mediante una aplicación que permita analizar certificados de seguridad de páginas web. Se ha realizado un análisis comparativo de ciertas páginas web que analizan certificados digitales informando y analizando dicho certificado.

Se llevó a cabo un análisis de la problemática actual de dicha actividad ilícita y se ha realizado una investigación exploratoria documental respecto a definiciones de phishing, certificado digital, los métodos de cifrado de datos y la actualidad de Argentina en los ataques de phishing y qué medidas se toman habitualmente para contrarrestar este mal.

A pocos días del inicio del año 2018, Bitglass (compañía que ofrece soluciones de seguridad en el servicio de nube) ha recopilado algunas de las predicciones que estiman se van a dar en 2018 en el campo de la seguridad. Las nuevas formas de phishing, el malware avanzado, los errores humanos, y las multas por la entrada en vigor del reglamento de protección de datos y la no adecuación de las compañías, son a juicio de esta empresa los elementos que mayor impacto tendrán en este ámbito [1].

En 2017, los ataques de todos los tipos de phishing financiero – ataques contra bancos, sistemas de pago y tiendas online – crecieron un 1.2, 4.3 y 0.8 puntos porcentuales respectivamente [2].

Hartmann refiere que por phishing se entiende que "son varias las metodologías para cometer fraude bancario, pero el phishing es sin dudas el más notable: se monta una escena o instancia de comunicación premeditadamente engañosa donde algún elemento persuasivo lleva al cliente, enceguecido, a entregar sus datos personales al hacker" [3].

Talens-Oliag define el certificado digital como, "Para los usuarios proporcionan un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo encriptado y/o firmado digitalmente, el control de acceso a recursos, etc." [4].

En si el certificado digital es una clase de archivo, informativo que su principal actividad es comunicar al usuario que está visitando dicha página web, es confiable, segura y que cumple con los protocolos básicos de seguridad, permitiendo al visitante, confiar plenamente en dicha página, sin preocuparse que la misma sea fraudulenta.

Talens-Oliag hace referencia a la criptografía de dos formas:

- Vista en términos sociales, es la ciencia de hacer que el costo de adquirir o alterar información de modo impropio sea mayor que el posible valor obtenido al hacerlo.
- Vista en términos más formales, es la práctica y el estudio de técnicas de *cifrado* y *descifrado* de información, es decir, de técnicas para codificar un mensaje haciéndolo ininteligible (*cifrado*) y recuperar el mensaje original a partir de esa versión ininteligible (*descifrado*) [5].

González Pérez, señalo en un estudio reciente que **la Argentina está entre los países del mundo que más mensajes de phishing recibe**. A la vez, expertos en seguridad informática señalan que las técnicas de engaño de esta modalidad delictiva se refinan cada vez más [6].

Un relevamiento (que realizó la empresa de seguridad Kaspersky Lab) que abarcó el tercer trimestre de 2017 ubicó a la Argentina como el **séptimo país del planeta con mayor cantidad de ataques de phishing recibidos**, en un ranking que encabeza Brasil y que tiene entre sus primeros diez puestos a Australia, Nueva Zelanda, China, Francia, Perú, Canadá, Qatar y Georgia [6].

Se ha detectado que hubo un incremento gradual de phishing no solo en este país (Argentina) sino en todas partes del mundo, a pesar de los esfuerzos de realizar campañas de concientización, esto continúa creciendo.

Se citan a continuación 6 formas de proteger a los usuarios de los ataques, intentan minimizar los efectos negativos de un ataque phishing y si es posible de impedirlo:

1. **No compartas tu nombre de usuario y contraseña con nadie**, incluso si la persona afirma ser un empleado del banco.
2. **Escoge un proveedor de correo electrónico que ofrezca autenticación en dos fases.** También es buena idea que tenga filtros de spam, malware y suplantación de identidad porque te mostrará un mensaje de alerta si algo parece sospechoso.
3. **Utiliza únicamente tus datos de acceso en la aplicación oficial del banco** (por ejemplo, el enlace de la app N26), nunca te descargues la aplicación de ningún otro sitio. Si eres cliente de N26, nunca utilices tus

datos de acceso en otro dominio que no sea https://app.n26.com o https://my.n26.com

4. **No hagas clic en los enlaces si recibes un correo electrónico que te pide que realices una acción que tú no has iniciado** (restablecer la contraseña, validar tu cuenta, etc.)
5. Comprueba siempre el enlace antes de hacer clic en él. **Coloca el ratón encima para obtener una vista previa de la URL** y fíjate cuidadosamente si hay faltas de ortografía u otras irregularidades.
6. Los sitios web de los bancos siempre usan HTTPS. **Si no ves el icono del candado verde en el navegador o no ves el prefijo «https» antes de la URL del sitio, \ es probable que el sitio no sea seguro [7]**.

Dado este contexto, este artículo presenta los servicios considerados para el análisis comparativo (Sección 2). Presenta una aplicación que permita analizar certificados de seguridad de páginas web (Sección 3) y un caso de estudio para la validación de la propuesta de la solución (Sección 4). Se formulan conclusiones y futuras líneas de trabajo (Sección 5).

2 Servicios considerados

En esta sección se presentan servicios que se han contemplado para el estudio comparativo: Qualys SSL Labs [8] (sección 2.1), Redalia [9] (sección 2.2), SSL Checker [10] (sección 2.3), ImmuniWeb® SSLScan [11] (sección 2.4). Por último, se presenta el resultado del análisis realizado (sección 2.5).

2.1 Qualys SSL Labs

Este servicio en línea gratuito realiza un análisis profundo de la configuración SSL de cualquier servidor de la web. Analiza el certificado como por ejemplo a quien provee el mismo, que métodos de encriptación usa, da un puntaje total en cuanto a que tan fuerte es el certificado, etc. Da bastante información que para un usuario común puede llegar a ser confusa y que no es necesaria para el objetivo de este trabajo. [8]

2.2 Redalia

La página Redalia que ofrece el servicio de análisis, ayuda a verificar que el certificado SSL del sitio web está correctamente instalado, y en caso contrario te muestra los problemas que presenta y la manera de solucionarlos. Pero no hace un análisis total de cada componente del certificado digital, sin indicar un resultado en su totalidad o de cada componente del certificado, informa las propiedades del certificado como una mera información. [9]

2.3 SSL Checker

El sitio SSL Checker realiza un análisis del certificado, indicando si cumple con cada parte del certificado, asignándole una puntuación por separado, pero no hace un análisis general en cuanto al certificado. Lo destacable del sitio se puede consultar las reseñas, que realizan los usuarios de dicha página, de la empresa que certifico la página que se está analizando [10].

2.4 ImmuniWeb® SSLScan

ImmuniWeb® SSLScan es un producto gratuito disponible en línea, proporcionado y operado por High-Tech Bridge.

Con el objetivo de permitir a cualquier persona evaluar cuán seguro y confiable es su conexión SSL / TLS con un servidor (en cualquier puerto), el servicio realiza cinco pruebas distintas:

- Prueba el cumplimiento de los requisitos de las PCI DSS;
- Prueba de conformidad con la guía de HIPAA;
- Prueba de conformidad con las Pautas de NIST;
- Prueba las vulnerabilidades y debilidades más recientes de SSL / TLS;
- Prueba contenido inseguro de terceros que pueda exponer la privacidad del usuario [11].

Este sitio es completo en cuanto al análisis del certificado de seguridad dando un análisis individual y total de la página analizada, también analiza contenido de terceros, que pueden ser imágenes, JavaScript o CSS.

2.5 Dimensiones consideradas para el análisis

En esta sección se plantean las dimensiones que se han considerado para el análisis de las distintas aplicaciones que examinan el certificado digital. Ellas son:

- Puntaje final: una vez que se analizó todo el certificado digital, se debe informar un puntaje total indicando el nivel de seguridad que representa la página web.
- PFS: Perfect Forward Secrecy, cuando una conexión cifrada utiliza PFS, significa que las claves de sesión que se generan por el servidor son efímeras, incluso alguien que tenga el acceso a la clave secreta no puede utilizar la clave de sesión relevante que descifra cualquier sesión HTTPS. Por lo tanto, los datos cifrados interceptados están protegidos de miradas indiscretas en el futuro, incluso si la clave secreta del sitio web se ve comprometida posteriormente [12].
- TLS versión: Permite confiar información personal a sitios web, ya que los datos se ocultan a través de métodos criptográficos mientras se navega en sitios seguros[13].
- Key Exchange: El intercambio de clave encriptada es un protocolo, o conjunto de reglas, que permite a dos partes compartir una contraseña común

para comunicarse en una red insegura sin exponer esta contraseña. Este protocolo fue desarrollado originalmente por Steven Bellovin y Michal Merritt de Laboratorios AT&T Bell, quienes produjeron un trabajo seminal en el tema [14].

- Bulk Cipher: es un algoritmo de cifrado simétrico que se utiliza para cifrar y descifrar grandes cantidades de datos [15].
- MAC: los datos a enviar, junto con una clave secreta, se utiliza para generar un código de autenticación de mensaje. Los datos más el código se transmiten al receptor deseado. EL recepto realiza mediante el mismo algoritmo de clave secreta, un cálculo sobre los datos, utilizando la misma clave secreta para generar un nuevo código de autenticación de mensaje y compara el resultado con ese cálculo [16].

Tabla 1. Cuadro comparativo de métodos criptográficos que usan los analizadores de certificados digitales

	Qualys SSL Labs	**Redalia**	**SSL Checker**	**ImmuniWeb® SSLScan**
Puntaje final	X			X
PFS				X
TLS Versión	X			X
Key Exchange	X			
Bulk Cipher	X	X	X	X
MAC				

Los resultados de los análisis obtenidos a través de la tabla comparativa (Tabla 1) permiten formular las siguientes conclusiones: ninguna de las páginas pudo analizar todos los requisitos en su totalidad.

Por ejemplo, Redalia y SSL Checker en su totalidad de las dimensiones consideradas, no realiza análisis porque lo que hace es mostrar los datos que cuenta el certificado, pero no hace análisis total y de cada parte del mismo.

A diferencia de sus predecesores los sitios Qualys SSL Labs y ImmuniWeb® SSLScan, abarcaron casi todas las dimensiones excepto para el primer sitio PFS y el segundo Key Exchange y ambos coinciden que no pudieron analizar la MAC.

Como modalidad de todas estas páginas, se observó que no cuentan con un servicio automatizado a la hora de analizar los certificados web, sino que se debe ingresar el link del sitio a mano.

A partir del análisis realizado en el cual se detectaron las áreas de vacancia mencionadas, se propone el desarrollo de un sistema que considere las dimensiones analizadas.

(sección 3).

3 Diseño de aplicación de detección de páginas fraudulentas

La aplicación desarrollada (llamada SSLvalidations) es un addons (ayuda a modificar y personalizar la experiencia de la navegación agregando funcionalidades a Firefox) que va embebido en Firefox, y el mismo cuenta con un icono que, a medida que se va navegando, va indicando si la página cumple con los certificados de seguridad que se vieron en la sección anterior. A su vez, informa los métodos criptográficos que usa el certificado.

El sistema va analizando el certificando, pidiendo determinados valores para luego utilizarlos en el análisis.

En la figura 1 se presenta un diagrama de clase en el cual se visualizan las llamadas que el sistema va realizando al certificado, solicitando determinados parámetros, que serán utilizados para su posterior análisis.

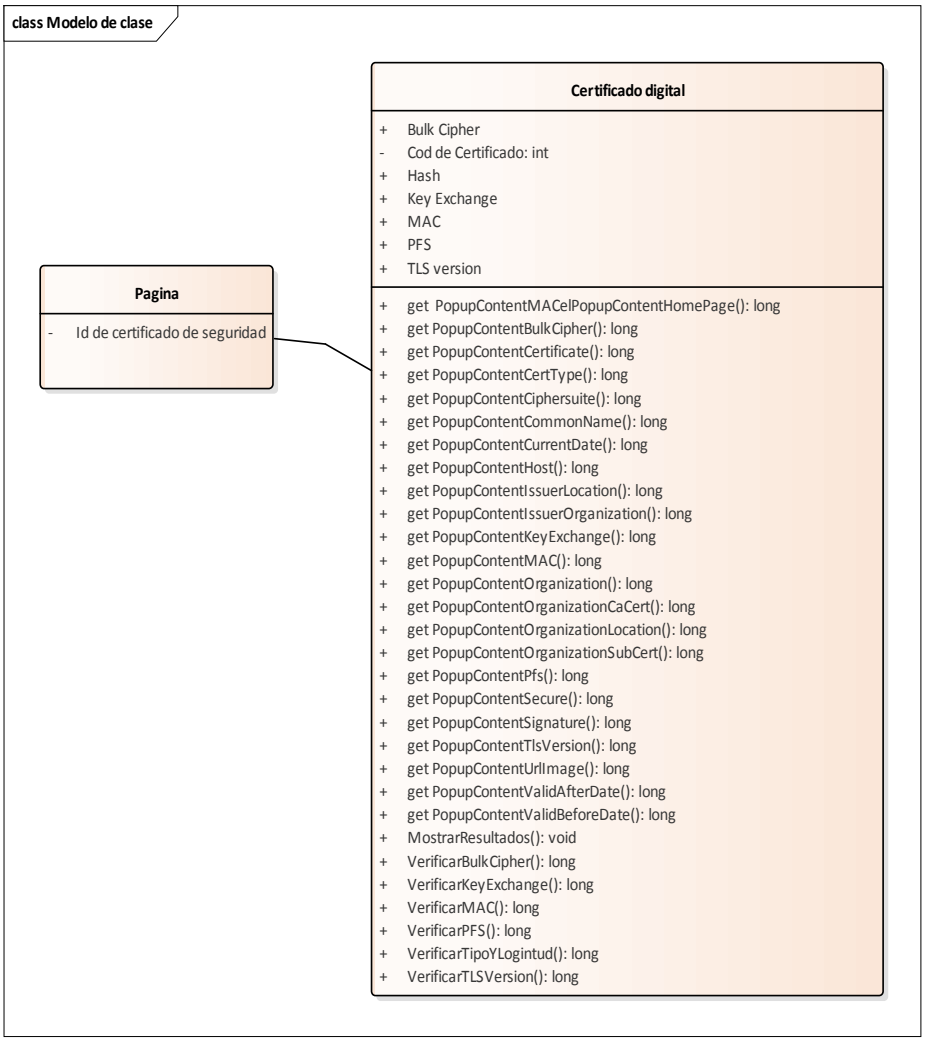
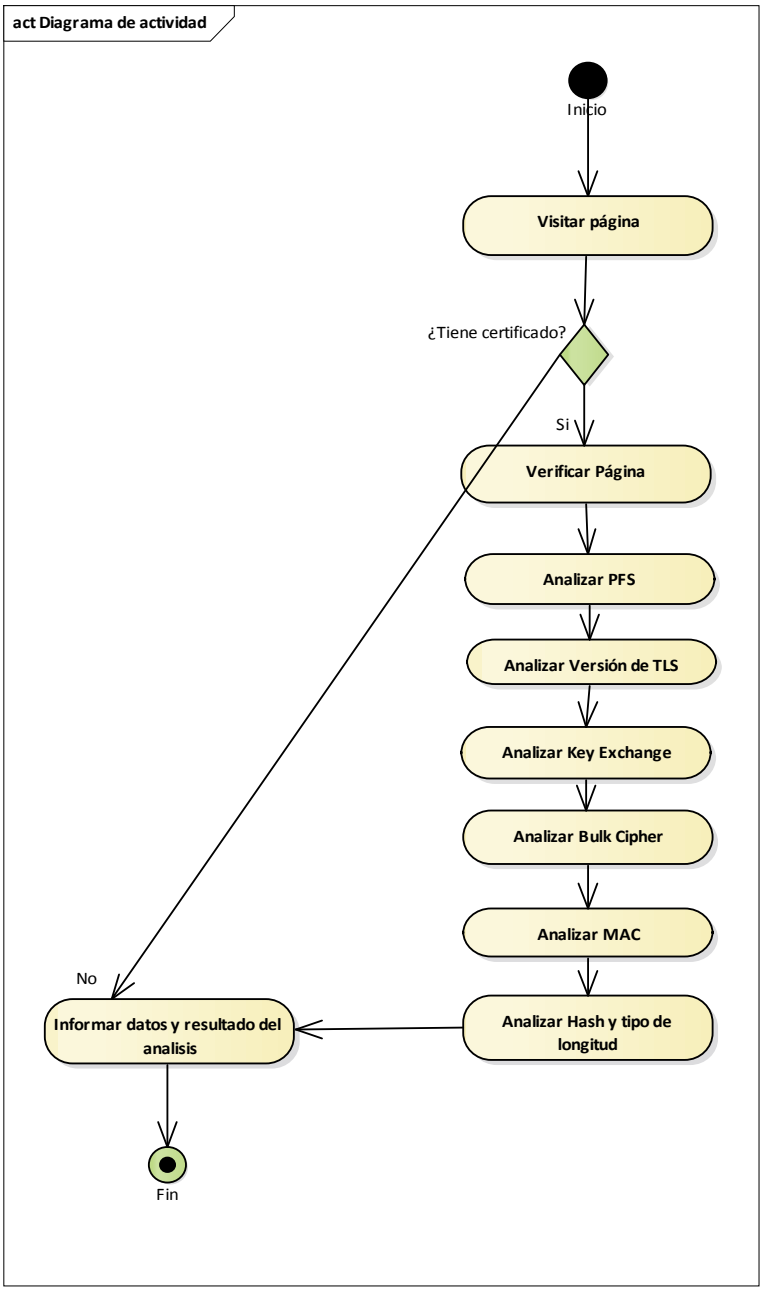


Fig. 2. Diagrama de modelo de clase de SSL validation

En la figura 2 se grafica lo que el sistema va a analizar de cada componente del certificado de seguridad.



Fig, 2. Diagrama de actividad del sistema .

4 Caso de estudio para validación de desarrollo

El caso de estudio seleccionado para validar la aplicación que se diseñó consiste en consultar una página web que tenga un certificado de seguridad no muy confiable. El link se tomó del sitio "anti-phishing", que cuenta con una base de datos de las páginas denunciadas como fraudulentas.

La selección de este caso de estudio es para demostrar que la aplicación funciona correctamente para todo sitio.

Agregar que es la figura 3

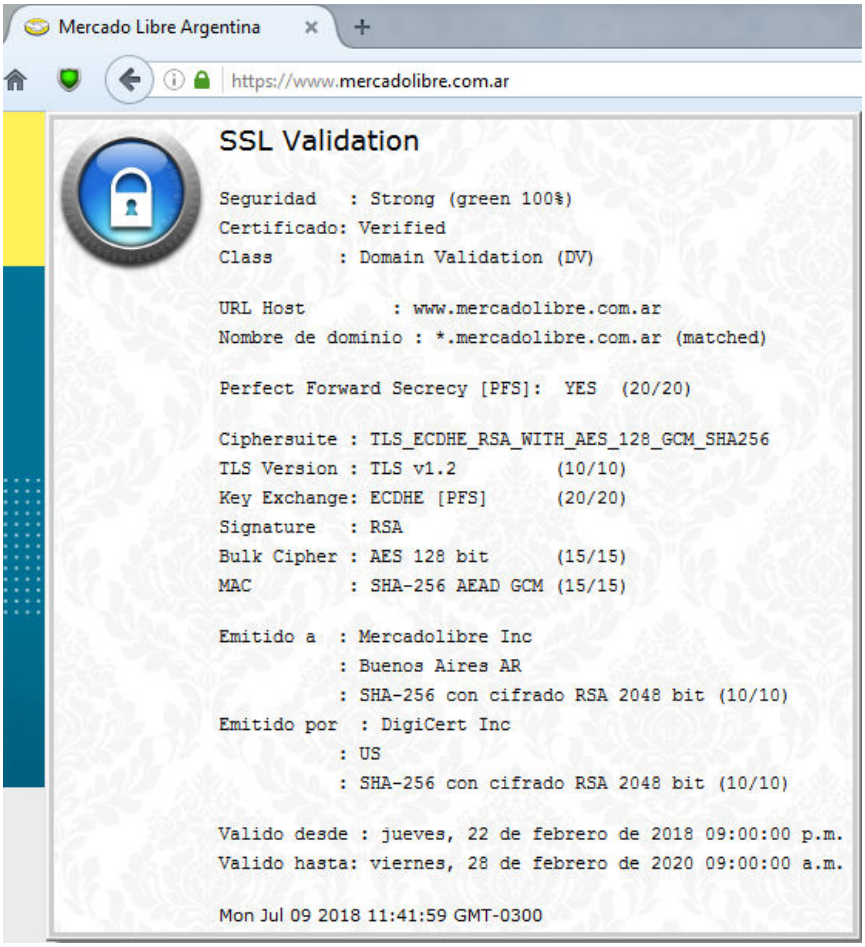


Fig. 3. Análisis y datos que contiene el certificado digital del sitio www.mercadolibre.com.ar

5 Conclusiones y futuras líneas de trabajo

Se arribó a la conclusión que el addons, funcionó de forma correcta indicando con un ícono de color rojo que la página tiene un bajo nivel de seguridad, e informando con que métodos criptográficos contaba el mismo. La conclusión es que no es confiable, dejando a decisión del usuario si confía los datos a dicha página o no.
Se ha presentado una revisión sistemática de páginas que realizan análisis, dando una puntuación final del análisis del certificado digital.

Se ha logrado de forma exitosa la construcción de una aplicación compuesta por un analizador de métodos criptográficos.

Como futuras líneas de trabajo se identifican:

- Ampliar la capacidad de analizar los certificados, de acuerdo con las nuevas medidas de seguridad informática que se apliquen, acorde a los nuevos estándares de seguridad para los certificados.
- Poder migrar el programa a otros browsers, ya sea Chrome, Internet Explorer y Safari.
- Actualizar el programa de acuerdo con las futuras versiones de Firefox que vayan apareciendo.

Referencias

1. Redacción de It Digital Security, en 2018 los esquemas de phishing serán mucho más sofisticados, It digiral security, miercoles 20 de diciembre de 2018 http://www.itdigitalsecurity.es/actualidad/2017/12/en-2018-los-esquemas-de-phishing-seran-mucho-mas-sofisticados
2. Redacción Byte TI, la mitad de los ataques de phishing son financiero, revista bye - España, lunes 26 de marzo de 2018. https://www.revistabyte.es/actualidad-byte/ataques-phishing-financiero/
3. Hartmann, Phishing bancario, la manipulación sigilosa y entradora para obtener datos, Diario Clarin - Argentina, domingo 19 de enero de 2018. https://www.clarin.com/suplementos/zona/phishing-bancario-manipulacion-sigilosa-entradora-obtener-datos_0_BkxH7iAEM.html
4. Talens-Oliag, Sergio, Introducción a los certificados digitales https://www.uv.es/~sto/articulos/BEI-2003-11/certificados_digitales.pdf
5. Talens-Oliag, Sergio, Introducción a la criptografia. https://www.uv.es/sto/articulos/BEI-2003-04/criptologia.html#id2448661
6. Pérez González Leo, Argentina, entre los países que más phishing reciben en el mundo, Diario Clarin - Argentina, martes 7 de noviembre de 2017 https://www.clarin.com/sociedad/argentina-paises-phishing-reciben-mundo_0_SkrEtz1kM.html
7. Redacción equipo de seguridad de n26. Revista n26 - España https://mag-es.n26.com/c%C3%B3mo-prevenir-un-ataque-de-phishing-en-tu-cuenta-bancaria-de17a79db18a
8. qualys ssl labs, SSl Server Test, https://www.ssllabs.com/ssltest/
9. Redalia, https://www.redalia.es/herramientas/comprobar-ssl/
10. SSL Checker, https://www.sslshopper.com/
11. ImmuniWeb® SSLScan, https://www.htbridge.com/ssl/

12. Parket Higgins, Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection, Electronic Frontier Foundation, miercoles 28 de agosto de 2013 https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection
13. Dante Odín Ramírez López, Carmina Cecilia Espinosa Madrigal, El cifrado web (SSL/TLS), Universidad Nacional Autónoma de México https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls
14. David Dunning,¿Como funciona el "intercambio de clave encriptada"?, Diarion, La voz de Houston, Estados Unidos. https://pyme.lavoztx.com/cmo-funciona-el-intercambio-de-clave-encriptada-5765.html
15. IBM, Bulk ciphers https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/bulkcip.html
16. Departamento de Ingeneria de Sistemas Telematicos - ETSIT - UPM - España https://www.dit.upm.es/~pepe/401/2911.htm#!-alone