Encryption with TLS Protocol version 1.2 and Web Sites Performance. A Case Study.

William-Rogelio Marchand-Niño[1]
william.marchand@unas.edu.pe

Edgar Etson Rueda Liberato[1]
edgar.rueda@unas.edu.pe

***Resumen*— El protocolo TLS ofrece una comunicación web segura porque la transmisión de información está encriptada entre el cliente y el servidor, gracias al intercambio de claves simétricas y asimétricas, garantizando la confidencialidad e integridad de los datos. El uso de algoritmos de encriptación robustos y el intercambio de claves son la base para la generación del canal encriptado utilizado en las conexiones web, conocido como HTTPS, sin embargo, esto agrega el consumo de recursos computacionales que afectan el tiempo de procesamiento, la velocidad y el número de conexiones simultáneas. Estas son una medida del rendimiento de los sitios web. Para medir el impacto del Protocolo TLS versión 1.2, se utilizaron cinco sitios web de producción de una empresa de desarrollo de aplicaciones y sitios web, donde se realizó la evaluación del rendimiento del sitio web**

Palabras clave*— *SSL/TLS, TLS, rendimiento web, autoridad de certificación, HTTPS, seguridad web.

I. INTRODUCCIÓN

El protocolo SSL/TLS fue creado por la empresa NetScape en el año 1994, inicialmente fue denominado SSL (Secure Socket Layer) [1] y posteriormente por medio de la IETF [2] y las mejoras realizadas a dicho protocolo paso a ser TLS (Transport Layer Security) [3]. Actualmente el término más usado es SSL cuando se refiere al protocolo SSL/TLS. El trabajo de investigación está enfocado al protocolo HTTPS, que es el protocolo HTTP sobre SSL/TLS [4].

Según el Informe de Telemetría del año 2017 [5] elaborado por David Holmes y publicado en el mes de abril del 2018, detalla que más del 80% de las páginas web a nivel mundial están haciendo uso del protocolo SSL/TLS.

Actualmente TLS en su versión 1.2 es la más utilizada en comparación con sus antecesoras y con la última versión 1.3 definida en agosto de 2018. Según el reporte por "Qualys SSL Labs" del mes de abril de 2019 [6], existe un 95% de sitios web seguros con soporte para TLS versión 1.2 sobre una base de 150,000 sitios web (ver Fig. 1), es así, como este protocolo desarrollado por la empresa Netscape Comunications e implementado en sus inicios por Netscape Navigator versión 1.1 llega a ser uno de los más importantes en cuanto al acceso seguro a la Wolrd Wide Web.

Cada vez son más los administradores que configuran los certificados digitales de pago o gratuitas emitidos por Autoridades Certificadoras como Let's Encryp, Godaddy, Start SSL que son algunas de las conocidas en el mercado.

Sin embargo, el aplicar un algoritmo de cifrado a cierta información hace que se requiera un mayor consumo de recursos computacionales en comparación que no se aplique. Esto debido a que la información pasa por un proceso computacional donde el texto legible será trasformado a texto sin sentido, además de establecer un proceso de negociación entre extremos para determinar los mecanismos y algoritmos a utilizar.

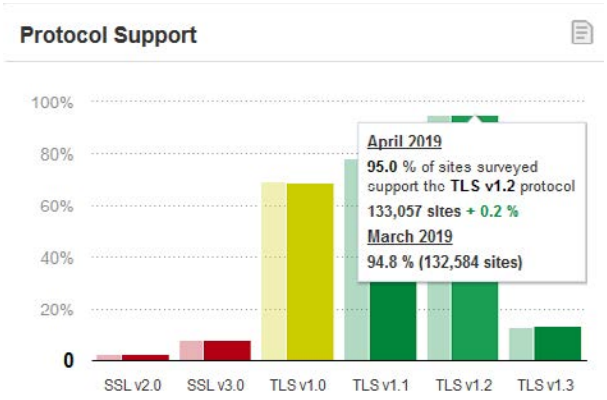

Fig. 1. Porcentaje de sitios web con soporte del protocolo TLS v.1.2 (SSLA Labs - Qualys)

Esta investigación se enfoca en el Protocolo Seguro de Transferencia de Hipertexto (HTTPS), que permite verificar la autenticidad de una página web por medio de un certificado digital. Este protocolo también hace uso de algoritmos de cifrado simétrico y asimétrico en el proceso de intercambio de claves entre navegador y servidor para establecer un canal seguro para la transferencia de la información.

Actualmente el uso de SSL/TLS con el protocolo HTTP es cada vez más importante, debido a las constantes vulnerabilidades asociadas a las comunicaciones e intercambio de datos por Internet; esas vulnerabilidades puedes ser aprovechadas por los actores de amenazas bajo diversas formas de amenazas, y una de ellas es la interceptación de los mensajes intercambiados entre los servicios web, y si estás viajan por los medios de transmisión sin la protección adecuada (cifrado), el riesgo es alto contra la confidencialidad por ejemplo.

El uso de nuevas versiones del protocolo SSL/TLS, específicamente TLS, permite disponer de suites de cifrado más complejas para proporcionar mayor seguridad. Muchas veces las organizaciones no cuentan con los recursos computacionales o buenas prácticas en optimización de los sitios web para que estas sean más ligeras (expresado en Megabytes del sitio web) y a la vez más rápidas ante

peticiones en grandes volúmenes.

A nivel técnico, el análisis del uso del protocolo SSL/TLS y de la suite de cifrado en su versión TLS 1.2 en los sitios web, permite entender si este genera un impacto en el rendimiento

[1] Grupo de Investigación en Redes, Seguridad y Gestión de TI
Universidad Nacional Agraria de la Selva - Tingo María, Perú

https://doi.org/10.12804/si9789587844337.17

de los sitios web, considerando la confidencialidad, integridad y autenticación de la información.

El estudio de este protocolo permite a los administradores web y a los usuarios finales, quienes hacen uso de un navegador web, comprender la importancia y la influencia que genera el uso del protocolo SSL/TLS, específicamente TLS v1.2 cuando se navega en Internet, con esto se pretende generar confianza tanto para los administradores web respecto al nivel de rendimiento y seguridad informática, como también para los usuarios consumidores de los sitios web respecto a la navegación confiable y segura en Internet.

La evaluación del impacto generado en el rendimiento de los sitios web del caso de estudio permite demostrar su impacto en el rendimiento, consolidando la aplicación de buenas prácticas en cuanto al uso y adecuada configuración del protocolo TLS v.1.2 para la organización y los clientes que administran sus sitios web. Otro factor adicional es, validar las recomendaciones realizadas por los fabricantes y marcas de la industria respecto a SSL/TLS.

Ante este escenario, la interrogante planteada es ¿Cuál es el impacto del cifrado con el protocolo TLS v1.2 en el rendimiento de sitios web? Para responder a la interrogante se tiene en un escenario de pruebas para la medición del rendimiento de cinco sitios web en producción alojados en un Servidor Web de la empresa Web-Out S.A. como parte del caso de estudio. Por el lado del cliente en estas pruebas se usó Windows 10 como anfitrión y máquinas virtuales con Centos 7 minimalista y Ubuntu 19; para la virtualización se ha empleado la herramienta Virtual Box en su versión 6.0.6.

II. Escenario de Pruebas

A. *Objetivo*

Evaluar el impacto del cifrado con el protocolo SSL/TLS en TLS versión 1.2 en el rendimiento de los sitios web. Caso empresa Web-Out S.A.

B. *Escenario para las pruebas*

El ambiente que se ha utilizado se expresa en la Fig. 2, con las características de los VPS (Servidor Virtual Privado) mostradas en la Tabla I y II.

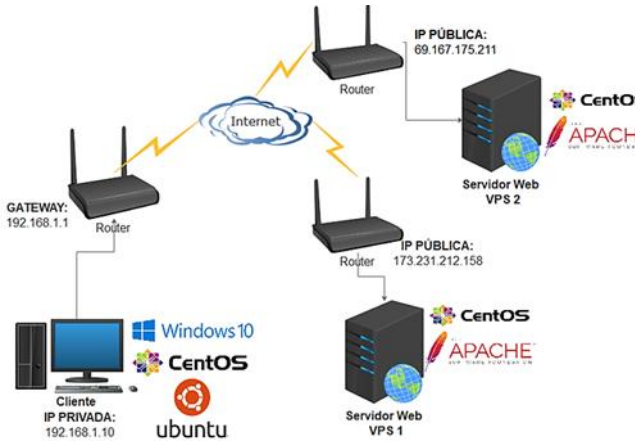

Fig. 2. Topología del caso de estudio, indicando distribución y direcciones IP.

TABLA I. Características Técnicas De Hardware Y Software Del Servidor Web (VPS 1)

CENTOS 7.6 MINIMALISTA (VPS 1)	**HARDWARE**	
	Disco Duro	150 Gb - SSD
	Memoria RAM	6 Gb
	Procesador	48 Procesadores
	Dirección IP Pública	173.231.212.158
	Ancho de banda	5 TB
	Número de núcleos	12
	Alta Disponibilidad	SI
	SOFTWARE	
	Servidor Web	Apache 2.4.39
	Modulo SSL/TLS	mod_ssl
	Criptografía	OpenSSL versión 1.0.2k-
	PHP	versión 7.1.28
	Mysql	10.2.24-MariaDB

TABLA II. Características Técnicas De Hardware Y Software Del Servidor Web (VPS 2)

CENTOS 7.6 MINIMALISTA (VPS 2)	**HARDWARE**	
	Disco Duro	2 Gb - HDD
	Memoria RAM	4 Gb
	Procesador	48 Procesadores
	Dirección IP Pública	69.167.175.211
	Ancho de banda	40 GB
	SOFTWARE	
	Servidor Web	Apache 2.4.39
	Modulo SSL/TLS	mod_ssl
	Criptografía	OpenSSL versión 1.0.2k-
	PHP	versión 5.6
	Mysql	5.6

Se recopilo la información de los cinco sitios web, como dirección IP pública, puerto empleado en la conexión por HTTPS, protocolos habilitados y deshabilitados en el servidor para cada sitio web que se muestran en la Tabla IV empleando la herramienta SSLRobot.

Los cinco sitios web para las pruebas del estudio han sido desarrollados utilizando el CMS (Sistema de Gestión de Contenidos) Drupal versión 7 y 8, conteniendo código HTML (Lenguaje de Marcado de Hipertexto), CSS (Hojas de Estilo en Cascada) y JavaScript como lenguaje de programación. Los cinco sitios web están alojados en dos VPS así como se detalla en la Tabla III

TABLA III. Sitios Web, Url De Acceso Y Ubicación En El VPS

Sitio Web	URL	VPS
Web-Out S.A.	www.web-out.com	VPS 1
Facultad de Ciencias Económicas y Administrativas de la UNAS	www.fceaunas.edu.pe	VPS 1
Hotel Oro Verde	www.hotel-oroverde.com	VPS 2
Hotel Natural Green	www.hotelnaturalgreen.com	VPS 1
Cámara de Comercio Canadá - Perú	www.canadaperu.org	VPS 1

TABLA IV. INFORMACIÓN DEL PROTOCOLO SSL/TLS DE LOS CINCO SITIOS WEB

	Web-Out	Facultad de Ciencias Económicas y Administrativas de la UNAS	Hotel Oro Verde	Hotel Natural Green	Cámara de Comercio Canadá – Perú
Servidor Virtual Privado	VPS 1	VPS 1	VPS 2	VPS 1	VPS 1
IP pública	173.231.212.158	173.231.212.158	69.167.175.211	173.231.212.158	173.231.212.158
Puerto	443	443	443	443	443
Protocolos Habilitados	TLS 1.2 TLS 1.1 TLS 1.0	TLS 1.2 TLS 1.1 TLS 1.0	TLS 1.2 TLS 1.1 TLS 1.0	TLS 1.2 TLS 1.1 TLS 1.0	TLS 1.2 TLS 1.1 TLS 1.0
Protocolos Deshabilitados	SSL 3.0 SSL 2.0	SSL 3.0 SSL 2.0	SSL 3.0 SSL 2.0	SSL 3.0 SSL 2.0	SSL 3.0 SSL 2.0

Al instalar el mod_ssl el servidor Web posee un nuevo fichero de nombre ssl.conf en las que se configura el nombre de dominio, dirección local del certificado digital que ha sido auto-firmado por medio de la herramienta OpenSSL [7]

III. ANTECEDENTES Y REVISIÓN BIBLIOGRÁFICA

Existen diversas investigaciones que se enfocan en la implementación del protocolo SSL/TLS en las comunicaciones entre cliente y servidor, en las que se realizaron un análisis en servidores web con una configuración del modSSL en Apache para la entrega segura por medio de TLS, obteniendo como resultado que los cálculos RSA son la operación más costosa en TLS hablando en términos de rendimiento, ya que consume entre un 13% a 58% del tiempo pasado en el servidor web. También mencionan que a medida que el rendimiento de las CPU continúa creciendo, la sobrecarga de TLS disminuirá. Es por eso por lo que invertir en CPU más rápidas o adicionales parece ser una estrategia preferible para maximizar el rendimiento del servidor web TLS. [8]

En otros casos se evalúa el impacto en el rendimiento del uso de TLS como protocolo de transporte para servidores SIP. También evalúa el costo de TLS experimentalmente utilizando un banco de pruebas con OpenSIPS, OpenSSL y Linux ejecutándose en un servidor que está basado en Intel. Se evalúan los costos de TLS como el cifrado masivo de datos, el cifrado de clave pública, el descifrado de clave privada y la verificación basada en MAC. Como resultado se obtuvo que el uso de TLS puede reducir el rendimiento hasta en un factor de 20 en comparación con el caso típico de SIP sobre UDP [9].

Otros trabajos intentan explicar y proponer la forma de evitar o reducir las operaciones criptográficas utilizadas en los mecanismos basados en claves públicas estándar en TLS, bajo un análisis sistemático y una comparación del rendimiento entre los mecanismos de intercambio de claves pre-compartidas y los mecanismos de intercambio de claves públicas. Las métricas de rendimiento fueron el tiempo de procesamiento y la cantidad de datos transmitida para una sesión. Además, se evaluó la interacción entre la duración global del handshake de TLS y el entorno de red; llegando a la conclusión que al comparar RSA con DHE PSK, este último funciona mejor que RSA solo cuando se usan tamaños de clave pequeños y tienen un rendimiento de red bajo. Aunque DHE PSK puede tener un rendimiento peor que RSA al usar tamaños de clave grandes o alto rendimiento de red, DHE PSK proporciona Perfect Forward Secrecy (PFS) para garantizar una comunicación más segura entre los cifradores de clave pre-compartida [10].

Para el tratamiento de la sobrecarga de solicitudes simultaneas se propuso el balanceo de handshake con el algoritmo EAMRSA que mejora el rendimiento mediante la técnica de transferencia de carga en el protocolo de enlace SSL/TLS. Esta técnica facilita en la distribución de carga favorable al requerir que los clientes realicen más trabajo (como parte de la encriptación) y servidores para realizar un trabajo proporcionalmente menor, lo que resulta en un mejor rendimiento de SSL. Como resultado se obtuvo que el método puede acelerar el procesamiento de las operaciones de claves privada RSA por un factor de entre 4.5 a 18 dependiendo del tamaño de clave RSA [11].

A. Cifrado Web mediante el Protocolo SSL/TLS

El protocolo SSL/TLS ha ido evolucionando desde su implementación en el año 1994 y la publicación de TLSv1.0 en 1999; estos protocolos operan entre la capa de transporte y la de aplicación según el modelo TCP/IP. Las diversas versiones de SSL y TLS ofrecen servicios de seguridad, como la confidencialidad, autenticación de servidor y la integridad del mensaje. Asimismo, estos protocolos se han diseñado considerando características como la eficiencia y extensibilidad, lo que implica un mejor uso de recursos en las comunicaciones reutilizando parámetros de conexión en sesiones simultaneas y la posibilidad de agregar nuevas combinaciones de algoritmos de cifrado además de las predefinidas [12] [13] [14].

B. Rendimiento de un sitio web

Uno de los puntos clave del éxito de un sitio web será el nivel de comodidad de nuestros usuarios, que la experiencia al visitar nuestro sitio sea agradable, que la respuesta que obtengan a sus acciones sea fluida, sin retrasos en las respuestas, etc., esto nos hace afirmar que la percepción del usuario está en función del rendimiento del sitio web en términos de tiempo de procesamiento o respuesta, concurrencia de usuarios, y la seguridad de la comunicación [15] [16] [17] [18].

Los sitios web siguen una arquitectura cliente servidor, donde el cliente es una máquina que solicita un determinado servicio al servidor que es la máquina que lo proporciona. El rendimiento de un sitio web va a depender de ambas partes, ya que el servidor será quien realice el procesamiento de las diversas peticiones haciendo que el consumo de recursos computacionales aumente y por ello el rendimiento del sitio web se vea afectado, así como también depende del cliente que es quien por medio de un navegador consume el servicio web. Este intercambio de mensajes se realiza antes de iniciar con el proceso de transmisión de información en cuestión de segundos, lo que provoca que el tiempo sea superior que cuando la información no fuera cifrada. En ese sentido una comunicación no cifrada además de ser vulnerable va a ser mucho más rápido en tiempo de respuesta. Con la investigación se conoce la diferencia de tiempo y en cuanto puede influir en el rendimiento del sitio web.

La cantidad total de clientes que pueden ser atendidos en simultaneo [17] por un Servidor Web está dada por la formula (1)

$$Max\_Clientes = Total\_RAM / Max\_Proceso\_Hijo \quad (1)$$

Asimismo, existen diversas herramientas en línea de fabricantes como como Google y Mozilla que permiten medir el rendimiento de un sitio web alojado en internet cada quien, con sus respectivos estándares y valoraciones, en la gran mayoría de los casos nos muestran el tiempo de carga, almacenamiento en cache, peso de la página, tiempo de respuesta, entre otros. Esta información debe de ser considerada ya que evidencia el rendimiento que pueda tener el sitio web.

Existen herramientas como OpenSSL, CypherScan, Wireshark por mencionar los más comunes que permiten obtener información más específica respecto a un sitio web como son: los algoritmos criptográficos utilizados, versiones de TLS aceptados, tiempo de respuesta, peso del sitio web, versión de http utilizado, puertos por defecto, entre otra información.

Asimismo, una forma de medir el consumo de recursos computacionales en función del tiempo de carga. Para calcular el porcentaje de incremento del tiempo de carga de cada sitio web cuando es accedido por HTTPS y HTTP, se empleó la siguiente formula [19].

$$Tasa\ de\ crecimiento\ (\%) = \frac{|Valor\ 1 - Valor\ 2|}{|Valor\ 2|} \times 100\%$$

Valor 1: Población al final del periodo.

Valor 2: Población al principio del periodo.

En esta investigación se reemplazó el Valor 1 por el "Tiempo de carga total de HTTPS" y para valor 2 el "Tiempo de carga total por HTTP" para el mismo sitio web, el cual nos permitió calcular el incremento porcentual existente entre estos dos tiempos.

$$\frac{|Tiempo\ carga\ HTTPS - Tiempo\ carga\ HTTP|}{|Tiempo\ carga\ por\ HTTP|} \times 100\%$$

Como antecedente, dicha fórmula también fue empleada con el objetivo de ver la diferencia de tamaños de datos cifrados y no cifrados que existe cuando el sitio web es accedido por HTTP y HTTPS [20].

Para configurar la versión más adecuada del protocolo SSL/TLS es posible realizarlo dentro del archivo de configuración ssl.conf con la directiva SSLProtocol [21], según la Fig. 5 podemos ver que se han deshabilitado las versiones de SSLv2 y SSLv3, para poder trabajar con todas las versiones de TLS.

Por otro lado, tanto cliente como servidor deben establecer los métodos y algoritmos de cifrado. Esto se realiza durante el proceso de establecimiento de sesión, que es el intercambio de información entre el cliente y servidor que permite lograr un acuerdo de algoritmos y claves a utilizar de manera segura, con la finalidad de garantizar la confidencialidad e integridad. El proceso de negociación básico publicado en el RFC 5246 se muestra en la Fig. 2 [22] [23] [24]

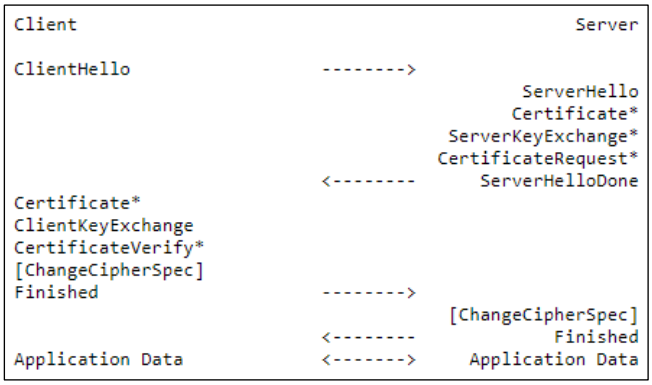

Fig. 3. Proceso de negociación de una sesión SSL/TLS.

Las Autoridades Certificadoras (AC o CA por sus siglas en ingles Certification Autority) son las encargadas de emitir certificados digitales (documento electrónico identificado por un único número de serie con periodo de validez incluido en el propio certificado) el cual permite identificar a determinados equipos y sitios web ante terceros [25].

C. *Fortaleza de los algoritmos criptográficos*

La fortaleza del algoritmo de cifrado tanto simétrico como asimétrico forman parte de una comunicación por medio de HTTPS. La seguridad y la fuerza del algoritmo de cifrado está relacionada con el tiempo, cada vez más las computadoras son mucho más rápidas y accesibles a un menor costo, permitiendo que los algoritmos de cifrado de mayor complejidad puedan ser procesados con mucha facilidad en comunicaciones por HTTPS. La fortaleza está vinculada con el tamaño de la clave utilizada y por los recursos computacionales con el cual puede ser vulnerado [26].

IV. Evaluación del Rendimiento De Un Sitio Web

En esta sección se describirá las pruebas realizadas para evaluar el impacto del uso del protocolo TLS v1.2 en los cinco sitios web que actualmente se encuentran en producción, con el uso de herramientas como Apache Bench, SSLRobot, Qualys SSL Labs.

A. *Evaluación con Apache Bench*

En la Tabla V se muestra el análisis de rendimiento de los cinco sitios web de producción con Apache Bench (ab), donde se puede observar un mayor tiempo de carga y un menor número de solicitudes atendidas cuando se hace uso del protocolo TLS v1.2 a diferencia del sitio web sin el uso del protocolo de este. El comando utilizado con Apache Bench fue:

#ab -n 1000 -c 25 https://www.web-out.com...(Con SSL/TLS)

ab -n 1000 -c 25 http://www.web-out.com…(Sin SSL/TLS)

Donde:

ab: Comando a usar para el análisis del rendimiento.

-n: Indica el número de solicitudes al servidor.

-c: Indica la cantidad de peticiones concurrentes.

Se realizaron cinco pruebas por cada sitio web con el objetivo de tener un valor promedio con mayor precisión, aumentando la cantidad de peticiones concurrentes para poder evaluar el impacto entre una comunicación cifrada y no cifrada por el protocolo TLS v1.2 tal como se muestra en la Tabla V.

Se consideran algunas características para la prueba, las cuales son:

- Time taken: Tiempo promedio que se mide desde el momento que se crea la primera conexión de socket hasta recibir la última respuesta.
- Requests per Second: Número promedio de solicitudes por segundo, resultado de número de solicitudes entre en tiempo total.

En la Tabla VI Se puede observar el resumen de las pruebas realizadas a los cinco sitios web obteniendo un Time Taken superior y Requests per Second inferior cuando es accedido por HTTPS.

TABLA V. ANÁLISIS DE RENDIMIENTO DEL SITIO WEB-OUT CON APACHE BENCH

WEB1 (WWW.WEB-OUT.COM) - 1,100 Y 500 SOLICITUDES							
SOLICITUDES	**# Peticiones Concurrentes**	**HTTPS**		**HTTP**		**Diferencia del Tiempo de Prueba entre HTTP y HTTPS (segundos)**	**Diferencia de Peticiones por segundo entre HTTP y HTTPS (#/s.)**
		Tiempo de la Prueba (segundos)	**Media de Peticiones atendidas por segundo (#/s.)**	**Tiempo de la Prueba (segundos)**	**Media de Peticiones atendidas por segundo (#/s.)**		
1	**1**	0.278	4.028	0.250	4.024	**0.03**	**0.00**
100	**20**	4.153	24.214	3.801	26.362	**0.35**	**2.15**
	40	5.047	20.948	4.067	24.848	**0.98**	**3.90**
	60	4.154	24.428	3.907	26.204	**0.25**	**1.78**
	80	5.858	18.672	4.352	24.470	**1.51**	**5.80**
	100	3.829	26.150	3.659	27.384	**0.17**	**1.23**
500	**20**	24.339	21.070	22.734	22.146	**1.61**	**1.08**
PROMEDIO:						**0.7**	**2.277**

TABLA VI. TIME TAKEN Y REQUEST PER SECOND ATENDIDAS POR EL SERVIDOR ENTRE HTTP Y HTTPS

Sitio Web	**Diferencia de *Time Taken* de HTTP y HTTPS**	**% de diferencia de *Time Taken* de HTTP y HTTPS**	**Diferencia de Requests per Second HTTP y HTTPS**	**% de diferencia de Requests per Second HTTP y HTTPS**
Web-Out	0.7 s	11%	2.227 #/s	11%
Facultad de Ciencias Económicas y Administrativas de la UNAS	0.25 s	18%	17.82 #/s	23%
Hotel Oro Verde	1.41 s	4%	3.97 #/s	4%
Hotel Natural Green	0.52 s	17%	0.24 #/s	20%
Cámara de Comercio Canadá - Perú	1.08 s	4%	0.12 #/s	4%

Existen diversas combinaciones de valores y técnicas con el cual se pueden obtener diversos resultados para "ab". Para ver más detalles del protocolo SSL/TLS de un sitio web como Cipher Suite y versión de TLS tal como se muestra en Fig. 4, se utilizó el comando:

ab -n 1 -v 2 https://www.web-out.com

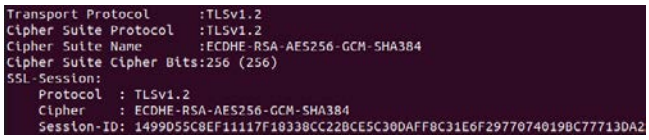

Fig. 4. Información de Protocolo, Suite de Cifrado, ID-Session y valides de certificado del sitio web https://www.web-out.com.

Es importante conocer cuál es la suite de cifrado, validez del certificado digital, la versión de protocolo que está habilitado, entre otros datos. Esto permite al administrador tomar medidas correctivas si es necesario.

Para identificar las suites de cifrado y su prioridad al momento de ingresar al sitio web de web-out, se usó la herramienta Cipherscan desarrollada por Mozilla tal como muestra la Fig. 5.

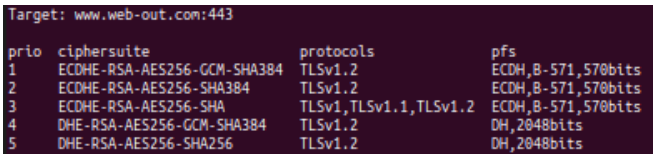

Fig. 5. Prioridad de Suite de Cifrado SSL/TLS del sitio web https://www.web-out.com

Para automatizar el trabajo de obtención de la información con la herramienta Apache Bench (ab) de ambos sitios web, se creó un script con bash, cuyo código es el siguiente:

```
#!/bin/bash
echo "Analisis de la Información de Test de Rendimiento"
echo "----------------------------------------"
echo "Quiere realizar un analisis del sitio:"
echo "1 -> Análisis con TLS v1.2"
echo "2 -> Análisis sin TLS v1.2"
echo "----------------------------------------"
read var1
if [ $var1 -eq "1" ]; then
   echo "Análisis con TLSv1.2
   echo "----------------------------------------"
   echo "Ingrese el Sitio Web a evaluar:"
   echo "1 - https://www.web-out.com/"
   echo "2 - https://www.fceaunas.edu.pe/"
   echo "3 - https://www.canadaperu.org/"
   echo "4 - https://www.hotel-oroverde.com/"
   echo "5 - https://www.hotelnaturalgreen.com/ "
   echo "----------------------------------------"
   read site
   echo "----------------------------------------"
   case $site in
      1) siteeval='https://www.web-out.com/'
      ;;
      2) siteeval='https://www.fceaunas.edu.pe/'
      ;;
      3) siteeval='https://www.canadaperu.org/'
      ;;
      4) siteeval='https://www.hotel-oroverde.com/'
      ;;
      5) siteeval='https://www.hotelnaturalgreen.com/'
      ;;
    esac
   echo 'El sitio a evaluar es:' $siteeval
   rm -f resumen_con_ssl.txt
array=(20 40 60 80 100)
   echo 'Iniciando Test...'
   for i in ${array[@]};
   do
   ab  -n 100 -c $i $siteeval > web_con_ssl_$i.txt;
   echo $i
```

```
done
for i in ${array[@]};
do
ls | grep "Concurrency Level" web_con_ssl_$i.txt >> resumen_con_ssl.txt
ls |  grep  "Time taken for tests" web_con_ssl_$i.txt  >> resumen_con_ssl.txt
ls |  grep "Requests per second" web_con_ssl_$i.txt >> resumen_con_ssl.txt
echo "-------------" >> resumen_con_ssl.txt
done
fi

if [ $var1 -eq "2" ]; then
echo "Análisis sin TLS v1.2"
   echo "----------------------------------------"
   echo " Ingrese el Sitio Web a evaluar:"
   echo "1 - http://www.web-out.com/"
   echo "2 - http://www.fceaunas.edu.pe/"
   echo "3 - http://www.canadaperu.org/"
   echo "4 - http://www.hotel-oroverde.com/"
   echo "5 - http://www.hotelnaturalgreen.com/ "
   echo "----------------------------------------"
   read site
   echo "----------------------------------------"
   case $site in
      1) siteeval='http://www.web-out.com/'
      ;;
      2) siteeval='http://www.fceaunas.edu.pe/'
      ;;
      3) siteeval='http://www.canadaperu.org/'
      ;;
      4) siteeval='http://www.hotel-oroverde.com/'
      ;;
      5) siteeval='http://www.hotelnaturalgreen.com/'
      ;;
    esac
   echo 'El sitio a evaluar es:' $siteeval
   rm -f resumen_sin_ssl.txt
   array=(20 40 60 80 100)
   echo 'Iniciando Test...'
   for i in ${array[@]};
    do
      ab  -n 100 -c $i $siteeval > web_sin_ssl_$i.txt;
      echo $i
    done
for i in ${array[@]};
do
ls |  grep "Concurrency Level" web_sin_ssl_$i.txt >> resumen_sin_ssl.txt
ls |  grep "Time taken for tests" web_sin_ssl_$i.txt >> resumen_sin_ssl.txt
ls |  grep "Requests per second" web_sin_ssl_$i.txt >> resumen_sin_ssl.txt
echo "-------------" >> resumen_sin_ssl.txt
done
fi
```

B. Tiempo de procesamiento

El uso del Protocolo SSL/TLS genera un tiempo de latencia el cual genera un tiempo superior cuando un sitio web está siendo accedido por HTTPS, esto debido al proceso de negociación que existe entre el cliente y servidor, en la Fig. 6 se describe tiempos aproximados en ms para cada intercambio de información entre cliente y servidor.

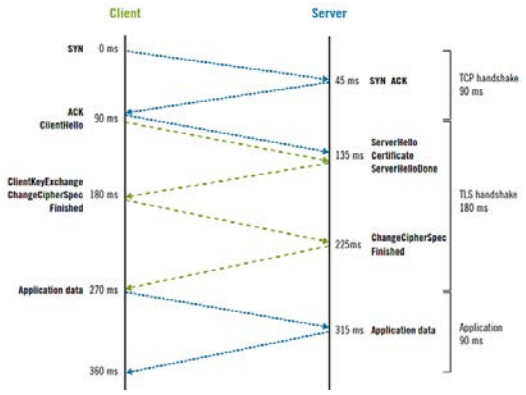

Fig. 6. Latencias de TCP Handshake y TLS Handshake

El tiempo de carga de los cinco sitios web cuando es accedido por HTTP y HTTPS se detallan en la Tabla VII. En la que se puede apreciar un leve incremento cuando el sitio web es accedido por HTTPS, esta información ha sido obtenida mediante la herramienta de desarrollo del navegador Mozilla Firefox.

TABLA VII. DIFERENCIA DE NÚMERO DE SOLICITUDES Y TIEMPO DE CARGA TOTAL DEL SITIO WEB.

Sitio Web	Núm. de Solicitudes HTTP	Núm. de Solicitudes HTTPS	Tiempo en cargar todas las solicitudes HTTP	Tiempo en cargar todas las solicitudes HTTPS	% de Incremento del Tiempo de cada de los sitios web
web-out.com	86	86	8.928 s	10.300 s	15%
fceaunas.edu.pe	106	106	6.386 s	6.500 s	2%
hotel-oroverde.com	94	94	18.692 s	19.842 s	6%
hotelnaturalgreen.com	107	107	9.572 s	9.906 s	3%
canadaperu.org	146	146	20.234 s	21.324 s	5%

C. Algoritmos de cifrado

Una de las consideraciones importantes para el uso adecuado del protocolo TLS v1.2 es la selección de los algoritmos de cifrado robustos y descartar aquellos que no presentan tal característica. Algunas herramientas como "Analize" (desarrollada en leguaje Python y disponible como parte de la suite de Cipherscan) ayudan a identificar los algoritmos que se deberían descartar. El resultado de ejecutar el comando "./analize.py -t https://www.web-out.com" con esta herramienta en el servidor web se muestra en la Fig. 7.

```
Changes needed to match the old level:
* enable SSLv3
* use a certificate with sha1WithRSAEncryption signature
* use DHE of 1024bits and ECC of 160bits
* enforce server side ordering

Changes needed to match the intermediate level:
* consider using DHE of at least 2048bits and ECC 256bit and greater
* enforce server side ordering
* increase priority of DHE-RSA-AES256-GCM-SHA384 over ECDHE-RSA-AES256-SHA
* increase priority of ECDHE-RSA-AES128-GCM-SHA256 over AES256-SHA
* increase priority of DHE-RSA-AES128-GCM-SHA256 over ECDHE-RSA-AES128-SHA
* increase priority of ECDHE-RSA-DES-CBC3-SHA over AES128-SHA
* fix ciphersuite ordering, use recommended intermediate ciphersuite

Changes needed to match the modern level:
* remove cipher ECDHE-RSA-AES256-SHA
* remove cipher DHE-RSA-AES256-GCM-SHA384
* remove cipher DHE-RSA-AES256-SHA256
* remove cipher DHE-RSA-AES256-SHA
* remove cipher AES256-GCM-SHA384
* remove cipher AES256-SHA256
* remove cipher AES256-SHA
* remove cipher ECDHE-RSA-AES128-SHA
* remove cipher DHE-RSA-AES128-GCM-SHA256
* remove cipher DHE-RSA-AES128-SHA256
* remove cipher DHE-RSA-AES128-SHA
* remove cipher AES128-GCM-SHA256
* remove cipher AES128-SHA256
* remove cipher AES128-SHA
* remove cipher ECDHE-RSA-DES-CBC3-SHA
* remove cipher EDH-RSA-DES-CBC3-SHA
* remove cipher DES-CBC3-SHA
* disable TLSv1.1
* disable TLSv1
```

Fig. 7. Recomendaciones de suites de cifrado a modificar en el Servidor Web.

Asimismo, es posible considerar las recomendaciones de Mozilla, en la que se puede obtener la configuración moderna, intermedia y antigua relacionadas con las versiones de software de servidor y de OpenSSL.

En la Tabla VIII se detalla información del certificado digital obtenido con la herramienta SSL Robot de los cinco sitios web, indicando el tipo y tamaño de clave pública, la Autoridad Certificadora y el algoritmo de firma del Certificado Digital generado para cada sitio web.

Se puede apreciar una similitud en los cinco sitios web que emplean el algoritmo RSA con un tamaño de clave de 2048 bits. Para el campo de algoritmo de firma todos los sitios web emplean como algoritmo de hash a SHA-256 excepto para el sitio web del Hotel Oro Verde que emplea SHA-384, y como algoritmo de firma es RSA-2048.

TABLA VIII. CERTIFICADO DIGITAL EMPLEADO EN LA CONEXIÓN CON LOS CINCO SITIOS WEB POR HTTPS

	Clave	CA	Algoritmo de Firma
Web-Out	RSA 2048	COMODO RSA Domain Validation Secure Server CA	SHA 256 WITH RSA
Facultad de Ciencias Económicas y Administrativas	RSA 2048	COMODO RSA Domain Validation Secure Server CA	SHA 256 WITH RSA
Hotel Oro Verde	RSA 2048	CPANEL INC. Certification Authority	SHA 384 WITH RSA
Hotel Natural Green	RSA 2048	COMODO RSA Domain Validation Secure Server CA	SHA 256 WITH RSA
Cámara de comercio Canadá - Perú	RSA 2048	COMODO RSA Domain Validation Secure Server CA	SHA 256 WITH RSA

D. Evaluación con Qualys SSL Labs

Es una herramienta completa que muestra información respecto al nivel de seguridad que cuenta un sitio web respecto a su configuración del protocolo SSL/TLS, funciona online y asigna una valoración del sitio web respecto a tres criterios: "Soporte de Protocolo", "Intercambio de llaves" y "Fuerza de cifrado".

Categoría	Puntuación
Soporte de protocolo	30%
Intercambio de llaves	30%
Fuerza de cifrado	40%

Numerical Score	Grade
score >= 80	A
score >= 65	B
score >= 50	C
score >= 35	D
score >= 20	E
score < 20	F

Fig. 8. Puntuación a las categorías para SSL Labs.

En la Tabla IX se puede visualizar la calificación final obtenida por la herramienta Qualys SSL Labs para los cinco sitios web, existiendo un intervalo de calificación de A-F, siendo A la nota más alta y F la nota más baja respecto a los criterios descritos en la Fig. 9.

TABLA IX. CALIFICACIÓN OBTENIDA POR QUALYS SSL LABS PARA LOS CINCO SITIOS WEB

Sitio Web	Calificación General
Web-Out	B
Facultad de Ciencias Económicas y Administrativas - UNAS	B
Hotel Oro Verde	A
Hotel Natural Green	B
Cámara de Comercio Canadá - Perú	B

E. Evaluación con OpenSSL

En la Tabla X se puede visualizar que el algoritmo RSA conforme aumenta la longitud de clave, el proceso de firmado es mucho más lento que el proceso de verificación de la firma. Así mismo nos indica que el servidor mediante el algoritmo RSA 2048 bits es posible realizar 331.8 firmas/segundo. Con el algoritmo ECDSA 256 bits es posible 3572 conexiones TLS por segundo con un proceso de verificación mucho más lento que usando RSA.

TABLA X. RENDIMIENTO DEL ALGORITMO DE FIRMA RSA, DSA Y ECDSA EN UNA COMUNICACIÓN HTTPS

Algoritmo/Longitud de clave	Firma	Verificación	Firmas /s.	Verificación/s.
RSA 512 bits	0.000625 s.	0.000030 s.	1599.8	33411.8
RSA 1024 bits	0.000812 s.	0.000069 s.	1231.4	14534.3
RSA 2048 bits	**0.003014 s.**	**0.000203 s.**	**331.8**	**4922.8**
RSA 3072 bits	0.021355 s.	0.000439 s.	46.8	2277.7
RSA 4096 bits	0.042895 s.	0.000699 s.	23.3	1430.7
RSA 7680 bits	0.364444 s.	0.002103 s.	2.7	475.6
DSA 512 bits	0.000997 s.	0.000572 s.	1003.1	1749
DSA 1024 bits	0.001378 s.	0.001071 s.	725.5	934.1
DSA 2048 bits	0.0081 s.	0.0056 s.	202	433.7
ECDSA 256 bits (nistp256)	**0.0003 s.**	**0.0007 s.**	**3572.1**	**1512**
ECDSA 384 bits (nistp384)	0.0189 s.	0.0138 s.	52.8	72.5

V. RESULTADOS

De acuerdo con los resultados presentados en la Tabla VI sobre las pruebas con Apache Bench, los valores de tiempo de carga (time taken) el protocolo SSL/TLS no influye significativamente en el nivel de solicitudes que pueda atender un servidor web, habiendo realizado 5 pruebas de saturación del servidor para cada sitio web, existiendo un total de 25 pruebas mediante la herramienta ApacheBench (ab) donde se realizaron 1, 100 y 500 solicitudes con una concurrencia de peticiones de 1, 20, 40, 60, 80 y 100 hacia el VPS 1 y VPS 2. La variación de los tiempos de carga y la velocidad de respuesta por solicitud no varían significativamente existiendo un margen de diferencia de 1.5 segundos adicionales para las conexiones por HTTPS (TLS versión 1.2) y existiendo una mayor velocidad de atención de solicitudes por medio de HTTP, siendo mucho más rápido en un 11% para el sitio web de Web-Out S.A.; un 23% para el sitio web de la Facultad de Ciencias Económicas y Administrativas de la UNAS; un 4% para el sitio web del Hotel Oro Verde; un 20% para el sitio web del Hotel Natural Green y un 4% para la cámara de Comercio de Canadá Perú. Además del impacto del protocolo TLS versión 1.2 en el rendimiento de los sitios web.

Asimismo, el resultado de las pruebas de nivel de seguridad del sitio web con la herramienta Qualys SSL Labs indican que los cinco sitios web obtienen una puntuación de entre A y B lo cual se consideran configuraciones optimas, teniendo un impacto positivo en la seguridad de la información trasmitida durante la interacción del sitio web con el usuario final.

Sin embargo, se debe considerar que desde la perspectiva del usuario promedio es posible que no se perciba las diferencias encontradas como poco significativas debido a la potencia de hardware actualmente disponible.

VI. CONCLUSIONES

El uso del protocolo TLS versión 1.2 para el cifrado de sitios web (HTTPS) es altamente recomendable, debido a los riesgos que representa el transferir información en texto plano con protocolos no cifrados como HTTP. Aunque el uso de protocolos como TLS generan mayor consumo de recursos computacionales afectando mínimamente el rendimiento de los sitios web, expresados en tiempo de respuesta o carga (time taken), la percepción negativa del usuario promedio es posible que no sea significativa.

Se ha podido comprobar que mientras más componentes (imágenes, archivos css, archivos java script, videos, entre otros) tenga un sitio web, el número de solicitudes HTTP o HTTPS se incrementaran, reflejándose en un mayor tiempo de carga. Se recomienda reducir en lo más mínimo estos componentes ya sea combinando archivos y script en archivos únicos, o eliminando y reduciendo el peso de componentes innecesarios, así mismo empleando el guardado en cache.

Asimismo, se puede demostrar que el uso del protocolo SSL/TLS influye de manera positiva en la seguridad de los sitios web y esto se puede comprobar mediante la herramienta Qualys SSL Labs obteniendo una puntuación (A-F) respecto a las configuraciones habilitadas en el servidor web, se debe considerar que si la configuración de este protocolo es incorrecta será igual de vulnerable como si la navegación fuera por HTTP.

Además del impacto del protocolo TLS versión 1.2 en el rendimiento de los sitios web, es importante considerar los tipos de algoritmos de cifrado y la combinación de uso para garantizar la mejor protección durante una sesión e intercambio de información a nivel de la web.

TRABAJOS FUTUROS

Realizar evaluaciones incluyendo otros servidores Web como IIS de Microsoft y GlasFish, además de considerar sitios web mas complejos que realicen transacciones con bases de datos.

Finalmente, complementar la evaluación de este tipo de protocolos en los sitios web, poniendo a prueba su fortaleza y robustez con adecuadas técnicas de pruebas de penetración de forma controlada.

Comparar el rendimiento de sitios web entre el uso del protocolo TLSv1.2 y TLSv1.3.

AGRADECIMIENTOS

A la empresa Web-Out por permitir analizar cinco de sus sitos web desarrollados y administrados.

REFERENCIAS

[1] J. D. Irwin y C.-H. Wu, «Introduction to Computer Networks and Cybersecurity,» 2013.

[2] IETF, «Who we are,» [En línea]. Available: https://www.ietf.org/about/who/. [Último acceso: 15 Noviembre 2018].

[3] E. Rescorla, «The Transport Layer Security (TLS) Protocol,» Agosto 2008. [En línea]. Available: https://www.ietf.org/rfc/rfc5246.txt.

[4] E. Rescorla, «HTTP Over TLS,» Network Working Group, 2000. [En línea]. Available: https://tools.ietf.org/html/rfc2818.

[5] D. Holmes, «The 2017 TLS Telemetry Report,» 23 Abril 2018. [En línea]. Available: https://www.f5.com/labs/articles/threat-intelligence/the-2017-tls-telemetry-report.

[6] Qualys Inc., «SSL Labs,» 09 Abril 2019. [En línea]. Available: https://www.ssllabs.com/ssl-pulse/. [Último acceso: abril 2019].

[7] OpenSSL, «TLS/SSL and crypto library,» [En línea]. Available: https://github.com/openssl/openssl. [Último acceso: Octubre 2018].

[8] C. Coarfa, P. Druschel y D. Wallach, «Performance Analysis of TLS Web Servers,» *IEEE Xplore Digital Library,* pp. 39-69, 2006.

[9] C. Shen, E. Nahum, H. Schulzrinne y C. Wright, «The Impact of TLS on SIP Server Performance,» 2009.

[10] F.-C. Kuo, H. Tschofenig y F. Meyer, «Comparison Studies between Pre-Shared and Public Key Exchange Mechanisms for Transport Layer Security,» *IEEE Xplore Digital Library,* 2006.

[11] H. Li y G. Zhao, «Improving Secure Server Performance By EAMRSA SSLHandshakes,» *IEEE Xplore Digital Library,* 2012.

[12] IETF, *The TLS Protocol version 1.0,* vol. RFC 2246, IETF, 1999.

[13] R. Oppliger, SSL and TLS Theory and Practice, London: Artech House, 2016.

[14] M. López Fernández, «Caracterización y medida pasiva del rendimiento para conexiones Web seguras HTTPS,» España, 2015.

[15] C. Mateu, Desarrollo de Aplicaciones Web, Barcelona, 2004.

[16] F. Carvajal Palomares, «Administración y Auditoría de los servicios web,» Editorial CEP, S.L., 2017.

[17] J. L. Villada Romero, Instalación y configuración del software de servidor web (UF1271), IC Editorial, 2015, p. 403.

[18] J. Sabogal Rosas, «Modelamiento de una plataforma virtual para la gestión de avisos normativos y de trámite legal,» 2015.

[19] A. O. Pallmall, Demografía, un problema global, 2014.

[20] R. A. Ariansen Moncada y J. I. Rojas Diaz, «Implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte 2016,» Chiclayo, 2016.

[21] Apache, «Apache Modulo mod_ssl,» [En línea]. Available: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslprotocol.

[22] IETF, « The Transport Layer Security (TLS) Protocol version 1.2,» agosto 2008. [En línea]. Available: https://tools.ietf.org/html/rfc5246.

[23] M. Driscoll, «The Illustrated TLS Connection v1.2,» diciembre 2018. [En línea]. Available: https://tls.ulfheim.net/.

[24] M. Driscoll, «The New Illustrated TLS Connection v1.3,» diciembre 2018. [En línea]. Available: https://tls13.ulfheim.net/.

[25] G. Escrivá Gascó, R. Romero Serrano, D. Jorge Ramada y R. Onrubia Pérez, Seguridad Informática, Madrid, 2013.

[26] I. Ristic, Bulletproof SSL and TLS: The Complete Guide to Deploying Secure Servers and Web Applications, 2014.

William-Rogelio Marchand-Niño, Ingeniero de Sistemas otorgado por la Universidad Nacional del Centro del Perú, con maestría en Dirección Estratégica de TI de la Universidad de Piura, con 18 años de experiencia académica en UNAS, UDH, UPLA. Desde el año 2004 es profesor asociado en la UNAS. Ha impartido más de 90 cursos de pregrado en diferentes universidades. Instructor CISCO por 12 años. Posee múltiples certificaciones de la Industria como PMP, ITIL Foundation, CCNA, MTA. Director del Centro de Tecnologías de Información y Comunicación de la Universidad Nacional Agraria de la Selva. Miembro Senior de la IEEE.

Edgar Etson Rueda Liberato, Bachiller en Ingeniería en Informática y Sistemas de la Universidad Nacional Agraria de la Selva (UNAS). Miembro del Grupo de Investigación de Redes y Seguridad de la Facultad de Ingeniería en Informática y Sistemas (FIIS-UNAS)