**UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA**

**FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS**


**TESIS PARA TITULO PROFESIONAL**

# CIFRADO CON EL PROTOCOLO SSL/TLS Y EL RENDIMIENTO DE SITIOS WEB. CASO: EMPRESA WEB-OUT, 2018 – 2019

**PARA OBTENER EL TITULO PROFESIONAL DE**

**INGENIERO EN INFORMÁTICA Y SISTEMAS**

**ELABORADO POR:**

**EDGAR ETSON RUEDA LIBERATO**

**ASESOR:**

**MG. WILLIAM ROGELIO MARCHAND NIÑO**

**TINGO MARÍA – PERÚ**

**2019**

| Universidad Nacional Agraria de la Selva<br>Facultad de Ingeniería en Informática y Sistemas | **ACTA DE SUSTENTACIÓN DE TESIS N.° 03-2019** | **COMISION DE GRADOS Y TITULOS**<br>**Fecha:** 09/Agosto/2019 |
|---|---|---|

## PARTE 1. FASE INICIAL

Siendo las 09:25 horas del día viernes 09 de Agosto de 2019; en la Sala de Grados de la FIIS, se instala el jurado calificador conformado por:

Jurado 1: Ing. Pedro Crisólogo TRUJILLO NATIVIDAD (Presidente)

Jurado 2: Ing. José Martín SANTILLAN RUIZ

Jurado 3: Mg. Gardyn OLIVERA RUIZ

Oficializado mediante **Resolución N.° 0103-2019-D-FIIS-UNAS** del 01 de julio de 2019, para el proceso de sustentación del informe final de Tesis del bachiller **Edgar Etson RUEDA LIBERATO,** titulado: **"CIFRADO CON EL PROTOCOLO SSL/TLS Y EL RENDIMIENTO DE SITIOS WEB. CASO: EMPRESA WEB-OUT, 2018-2019".** ASESOR: **Mg. William Rogelio MARCHAND NIÑO.** Se manifiesta que el bachiller cumple con los requisitos exigidos de Ley y se le invita a disertar su Tesis por espacio de 30 minutos, asimismo se dispondrá de igual tiempo para la absolver preguntas y sugerencias.

## PARTE 2. FASE DE PREGUNTAS Y RESULTADO

Culminada la exposición se inicia la fase de preguntas por parte del jurado calificador; también se invita a los asistentes a formular preguntas sobre el tema de Tesis.

Absueltas todas las peticiones, el jurado calificador procede a deliberar en privado la calificación y resultado.

Concluida la deliberación y en presencia del público asistente, el jurado calificador anuncia que el resultado de la Sustentación de Tesis es: APROBADO POR UNANIMIDAD

(NOTA: consignar una de la siguientes: DESAPROBADO, APROBADO POR MAYORIA o APROBADO POR UNANIMIDAD)

Con calificativo de: MUY BUENO

(NOTA: consignar una de la siguientes: EXCELENTE, MUY BUENO, BUENO, DEFICIENTE, MUY DEFICIENTE)

Por lo que se comunicará a las instancias correspondientes para el trámite respectivo.

## PARTE 3. CONFORMIDAD

De todo lo mencionado se firma al pie en señal de conformidad, siendo las ..... horas se da por finalizada la ceremonia de Sustentación de Tesis.

| Firma: | Firma: | Firma: |
|---|---|---|
| Jurado 1: Pedro C. Trujillo Natividad | Jurado 2: Jose M. Santillan Ruiz | Jurado 3: Gardyn Olivera Ruiz |

| Firma: | |
|---|---|
| Sustentante: Rueda Liberato, Edgar Etson | Asesor: William MARCHAND NIÑO |

## DEDICATORIA

A Dios, por brindarme sabiduría y fuerzas para culminar esa etapa académica muy importante.

A mis padres Jesus Rueda Marin y Francisca Liberato Castillo quienes fueron fuente de inspiración para lograr culminar satisfactoriamente la presente tesis. Gracias por su sacrificio, enseñanzas y amor brindado de manera incondicional.

A mis hermanos Linder Rueda Liberato, Cerilo Rueda Liberato y Nilton Rueda Liberato quienes gracias a sus consejos, enseñanzas y momentos felices me han enseñado a seguir adelante. Gracias por su paciencia, por preocuparse como hermanos y por estar siempre presente en estos momentos tan importantes.

## AGRADECIMIENTO

Un especial agradecimiento al Mg. William R. Marchand Niño por sus orientaciones, consejos, confianza, y conocimiento impartido como asesor en la elaboración de esta Tesis, estoy muy agradecido con su persona.

A Milko Rivera S. y Williams Acuña C. socios de la empresa Web-Out S.A. y a todo su equipo de trabajo, por ser grandes personas y por la confianza brindada durante el desarrollo de este trabajo de investigación. A Moises Rios R. por todos los consejos brindados y Graciela Ruth R. por la motivación a continuar con esta aventura, estando siempre pendientes con los continuos avances.

A Nathaly Atencio S. por estar siempre a mi lado en los malos y buenos momentos, por motivarme, por su cariño, por su alegría y por su paciencia brindada durante el desarrollo de esta tesis.

A Einstein Ortiz M. por sus consejos y apoyo durante el periodo de este proyecto, brindándome sugerencias que permitieron un mayor compromiso con el trabajo de investigación.

A la Universidad Nacional Agraria de la Selva y a la Facultad de Ingeniería en Informática y Sistemas, por ser casa de estudio en la que he aprendido mucho de las virtudes y experiencias de los docentes y compañeros de clase; un agradecimiento muy grande por formar parte de mi formación académica y personal.

Y a las personas más cercanas, amigos y familiares que siempre me han apoyado en esta labor con sus palabras y consejos.

## ABREVIATURAS

| | |
|---|---|
| **AC** | Autoridad Certificadora. |
| **CMS** | Sistema Gestor de Contenidos. |
| **HTTP** | Protocolo de Transferencia de Hipertexto. |
| **HTTPS** | Protocolo Seguro de Transferencia de Hipertexto. |
| **IETF** | Grupo de Trabajo de Ingeniería de Internet. |
| **OSI** | Interconexión de Sistemas Abiertos. |
| **RFC** | Petición de Comentarios (*Request for Comments*). |
| **SSL** | Capa de Puerto Seguro. |
| **TLS** | Seguridad de Capa de Transporte. |
| **URL** | Localizador Uniforme de Recursos. |
| **VPS** | Servidor Virtual Privado. |

## ÍNDICE

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

## RESUMEN

La presente tesis está enfocada en determinar el impacto que genera el uso del protocolo SSL/TLS (Secure Sockets Layer/Transport Layer Security) en los sitios web; para ello se ha tomado como caso de estudio a cinco sitios web desarrollados y administrados por la empresa Web-Out. S.A., periodo 2018 - 2019. Este estudio identifica la problemática de conocer el impacto que el cifrado con el protocolo SSL/TLS produce en el rendimiento de los sitios web, de acuerdo con la metodología propuesta es: la planificación y diseño, pruebas, análisis de resultados y conclusiones. Para la determinación del impacto generado por el uso del protocolo SSL/TLS se utilizó herramientas para la obtención de información como: Apache Bench, OpenSSL, Wireshark, Qualys SSL Labs, entre otros. Entre los principales resultados, se encuentra que el protocolo SSL/TLS no influye significativamente en el rendimiento de los sitios web, generando un tiempo de carga no mayor a 15% a comparación de una web no cifrada, y verificando que un sitio web por medio de HTTPS (HTTP sobre SSL/TLS) es mínimamente afectado al rendimiento ante peticiones concurrentes, y que además gracias a los algoritmos de cifrado, uso de certificados digitales y uso de algoritmos de hash brindan una capa de seguridad a la información transmitida entre cliente y servidor. Así también se realizó un análisis previo del protocolo TLS versión 1.3 y versión 1.2 logrando determinar que el protocolo TLS versión 1.3 es mucho más eficiente que su predecesora durante el proceso de negociación (Protocolo handshake).



**Palabras clave:** SSL/TLS, cifrado, HTTP, HTTPS, rendimiento, sitios web.

## ABSTRACT

The present thesis is focused on determining the impact generated on websites from the use of the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocol; to do this, five websites that were developed and are administrated by the company Web-Out. S.A. were used for the case study, 2018 – 2019 period. This study identifies the problem of understanding the impact that the SSL/TLS protocol coding produces on the output of the websites, according to the proposed methodology, which is: the planning and design, tests, results analysis and the conclusion. In order to determine the impact generated by the use of the SSL/TLS protocol, tools for obtaining the information such as: Apache Bench, OpenSSL, Wireshark and Qualys SSL Labs, among others, were used to obtain the information. Among the principal results, it is found that the SSL/TLS protocol does not significantly influence the output of the websites, generating a loading no more than 15% greater when compared to a uncoded website and verifying that the yield of an HTTPS (HTTP with SSL/TLS) website is minimally affected by concurring requests and that moreover, thanks to coding algorithms, the use of digital certificates and the use of hash algorithms, it offers a layer of security for the information transmitted between the client and the server. At the same time, an analysis was done ahead of time of the TLS protocol, version 1.3 and 1.2, it was determined that the TLS protocol, version 1.3, is much more efficient than its predecessor during the negotiation process (handshake protocol).



**Keywords:** SSL/TLS, coding, HTTP, HTTPS, output, website.

# INTRODUCCIÓN

El protocolo SSL/TLS es cada vez más empleado por las compañías y organizaciones, los cuales cuentan con sitios web y quieren brindar una comunicación segura entre cliente (navegador) y servidor, estos sitios web pueden estar alojados en sus propios servidores o en VPS adquiridos como servicio de hosting. Siendo la principal característica de este protocolo brindar una comunicación cifrada entre cliente y servidor web, por medio de certificados digitales, algoritmos de cifrado y hash; asegurando la autenticación, confidencialidad e integridad de la información.

El protocolo HTTPS es HTTP sobre SSL/TLS, caracterizándose también por emplear el puerto 443 para las conexiones seguras. Para ello todos los sitios web necesitan de un servidor web para que pueda funcionar correctamente de entre las cuales el más utilizado mundialmente es apache, caracterizado por ser estable, multiplataforma y altamente configurable.

La presente investigación se refiere a la problemática de evaluar el impacto del cifrado con el protocolo SSL/TLS en el rendimiento de los sitios web, para tener conocimiento y demostrar que el protocolo SSL/TLS no afecta negativamente en el rendimiento, más por el contrario brinda mejoras en aspectos de seguridad para la comunicación HTTP a un costo mínimo del rendimiento; para ello se ha tomado como caso de estudio a cinco sitios web de la empresa Web-Out. S.A.

Para analizar la problemática se han determinado las siguientes dimensiones; el tiempo de procesamiento del sitio web, el nivel de solicitudes de clientes en la que por medio de la herramienta Apache Bench (ab) se puede simular

conexiones múltiples de clientes saturando al servidor con el objetivo de obtener datos del comportamiento cuando la comunicación es cifrada y no cifrada por SSL/TLS, la transferencia de la información en la que es segmentada por tipo de contenido (sea CSS, HTML, JavaScript, Imágenes, Videos, etc) y finalmente medir el nivel de seguridad de los sitios web el cual están estrechamente ligados con las versiones de SSL/TLS, así también con las suites de cifrado, y los tamaños de clave empleados por los algoritmos de cifrado. Siendo definido en los archivos de configuración de apache con el módulo mod_ssl, y analizados teniendo habilitado y deshabilitado el protocolo SSL/TLS con la finalidad de realizar una comparación y llegar a una conclusión.

El contenido de esta tesis consta de cuatro capítulos: En el CAPÍTULO I, se describe la formulación del problema, la justificación y los objetivos tanto general como específicas en relación con el uso del protocolo SSL/TLS. El CAPÍTULO II, se refiere a la revisión de la bibliografía, trabajos de investigación que guardan similitud, las bases teóricas, el marco conceptual y las hipótesis planteadas. En el CAPÍTULO III, se describe los materiales y métodos, describiendo el tipo y nivel de investigación, la población y metodología propuesta que permitieron mantener una secuencia de pasos para la investigación. En el CAPÍTULO IV, se expone la aplicación de la metodología propuesta en sus 4 fases**:** Planificación, se describe y define las herramientas empleadas para obtener información del protocolo SSL/TLS, por mencionar algunas: Openssl, Qualys SSL Labs, Apache Bench, Wireshark; en la segunda etapa de Diseño, se describió el escenario y elementos que lo conforman para definir bajo qué características se están obteniendo dichos resultados; en la etapa de Pruebas, se realizaron las diversas pruebas empleando las herramientas

descritas en la etapa 1; y en la última etapa de Análisis de resultados se realizó la interpretación de la información encontrada en base a una navegación por medio de HTTP y HTTPS. Finalmente se describe las conclusiones, recomendaciones y un glosario de los términos más importantes para la presente tesis.

# CAPITULO I

## PROBLEMA DE INVESTIGACIÓN

Aproximadamente hace 5 años era la excepción navegar por medio de “HTTPS” siendo común la navegación por medio de “HTTP” (Schechter, 2017); El uso de “HTTPS” (HTTP sobre SSL/TLS) era necesario en las transacciones y acceso a cuentas bancarias y todo lo enfocado a la industria de las finanzas donde la información tenía que ser cifrada, actualmente esto ha cambiado existiendo un mayor uso de la navegación segura por “HTTPS” y todo gracias a empresas como Google que anuncio en agosto de 2014 que los sitios bajo “HTTPS” serán mejor posicionados en su buscador (Google, 2014), y Let’s Encrypt que proporciona certificados gratuitos con validación de dominio para cualquier sitio web.

El uso del protocolo SSL/TLS en la web brinda conexiones seguras de extremo a extremo entre cliente y servidor. Según se detalla en el reporte del 03 de Mayo del 2019 de (Qualys SSL Labs, 2019) a cargo de Ivan Ristic, existe un aproximado de 67.4% de sitios seguros en base a 150 000 sitios web según la lista de los sitios más populares por “*The Top Alexa*” (Anexo 8).

El protocolo SSL/TLS desde sus inicios, en el año 1994, hasta la fecha, ha seguido una serie de actualizaciones y mejoras en aspectos de seguridad; al principio el protocolo se definió como SSL (*Secure Socket Layer*) y años más tarde por la intervención de la IETF (*Internet Engineering Task Force*) paso a llamarse TLS (*Transport Layer Security*) (Navarro, Ubilla, & Tejeda, 2014). Durante el periodo

de 1994 a 2018 se desarrolló y se precisó en diversos RFC (*Request for Comments*) como TLS versión 1 (RFC 2246) en 1999, TLS versión 1.1 (RFC 4346) en 2006, TLS versión 1.2 (RFC 5246) en 2008 y TLS versión 1.3 (RFC 8446) en el 2018.

Actualmente TLS 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 del mes de Mayo por (Qualys SSL Labs, 2019), existe un 94.5% de sitios web seguros por TLS versión 1.2. Es así, como este protocolo desarrollado por la empresa Netscape e implementado en sus inicios en Netscape Navigator versión 1.1 llega a ser uno de los más importantes en cuando al acceso seguro a la web por medio de un navegador. Es de vital importancia su implementación para todas las empresas los cuales tienen sitios web alojados en Internet y visibles a nivel mundial.

Las características que brinda el protocolo SSL/TLS son: confidencialidad, integridad y autenticación; por medio del uso de algoritmos de cifrado, intercambio de claves simétricas y asimétricas e incluyendo el uso de certificados digitales bajo el estándar x.509.

Esta investigación consta de los cinco sitios web desarrollados y administrados durante el periodo 2018-2019 por la empresa Web-Out. S.A., los cuales tienen configurado el protocolo SSL/TLS para la navegación segura por medio de certificados digitales; el objetivo para esta investigación es conocer el impacto generado por dicho protocolo hacia los sitios web, teniendo habilitado y deshabilitado el SSL/TLS.

Esta investigación aportará en comprender si existe un impacto en el rendimiento de los sitios web cuando se tiene habilitado el protocolo TLS en su

versión 1.2. Ese impacto será medido mediante las dimensiones como: tiempo de procesamiento, nivel de concurrencia, transferencia de información y nivel de seguridad que brinda este protocolo para asegurar un correcto funcionamiento y no verse afectado en brindar una mala experiencia para el usuario final.

## 1.1 Marco referencial del problema

En la actualidad existen muchas actividades donde se hace uso del navegador web, desde que ingresamos a las redes sociales, sitios web de la institución donde trabajamos, sitios del Gobierno o del Estado para realizar consultas o trámites, y más aún cuando realizamos una transacción bancaria. Todos estos son realizados por medio de Internet y un navegador (Google Chrome, Internet Explorer, Edge, Firefox, Opera, Safari, etc.) y en muchas ocasiones los usuarios no se percatan si en la URL (Localizador Uniforme de Recursos) existe el identificador del protocolo “HTTPS” haciendo referencia a una navegación segura.

Los certificados digitales están inmersos en el protocolo SSL/TLS que permite a los navegadores estar seguros con cual servidor web deben establecer comunicación (visualizamos “HTTPS” en la URL), gracias a que internamente manejan un intercambio de llaves para posteriormente formar un canal seguro. Estos certificados digitales ayudan al usuario final a tener la certeza de que se encuentra ante el sitio web original y no uno FALSO (*Phishing*) logrando ser verificado; estos certificados son administrados por las Autoridades Certificadoras (en inglés *Certificación Authority* - CA) siendo empresas reconocidas a nivel internacional encargadas de emitir y revocar los certificados según sea el caso.

Cuando se desarrolla un sitio web muchas veces no se toma en cuenta si la aplicación esta optimizada para que pueda tener un impacto mínimo en el costo

computacional cuando este ya se encuentre en producción. En algunos casos el administrador web, conoce de herramientas alojadas en Internet que permiten realizar un diagnóstico y logra obtener datos técnicos los cuales permiten mejorar el tiempo de respuesta, reducir el peso (cantidad de Kilobytes) y encontrar errores del sitio web; indistintamente si el sitio tiene o no implementado el uso de la navegación segura por “HTTPS”.

Según el informe de Telemetría del año 2017 (Holmes, 2018) elaborado por David Holmes y publicado 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.

El uso de este protocolo seguro no es ajeno a la empresa Web-Out S.A. el cual es caso de estudio en esta investigación. La empresa cuenta con un listado de sitios web seguros detallados en la Tabla 1. que fueron desarrollados y actualmente administrados (periodo 2018-2019) por la empresa; esta investigación tiene como objetivo medir ese impacto del protocolo SSL/TLS en el rendimiento de los sitios web sabiendo que emplear algoritmos de cifrado implica un costo computacional para los servidores web.

**Tabla 1.** Listado de Sitios Web desarrollados y administrados por Web-Out S.A.

| SITIO WEB | PLATAFORMA | URL DE ACCESO | SSL/TLS |
|---|---|---|---|
| Web-Out S.A. | Drupal 7.60 | https://www.web-out.com | Si |
| Facultad de Ciencias Económicas y Administrativas de la UNAS | Drupal 8.5.6 | https://www.fceaunas.edu.pe | Si |
| Hotel Oro Verde | Drupal 7.60 | https://www.hotel-oroverde.com | Si |
| Hotel Natural Green | Drupal 7.60 | https://www.hotelnaturalgreen.com | Si |
| Cámara de Comercio Canadá - Perú | Drupal 7.00 | https://www.canadaperu.org | Si |

**Fuente:** Empresa Web-Out S.A.

## 1.2 Planteamiento del problema

La seguridad con la que viaja nuestra información a través de la red de Internet se ha vuelto cada vez más importante y delicado a la vez, por ende, el uso de los certificados digitales por medio del protocolo SSL/TLS se ha vuelto indispensable y mucho más accesible para las medianas y pequeñas empresas.

Cada vez son más los administradores que configuran los certificados digitales emitidos por autoridades certificadoras por medio de un pago y por opciones gratuitas como Let's Encrypt; actualmente Let’s Encrypt tiene como patrocinadores a empresas reconocidas como Mozilla, Cisco, Chrome, Facebook, GitHub, entre otros, ofreciendo mayor tiempo de validez, renovación ilimitada, facilidad de instalación y configuración de los certificados. Esta autoridad certificadora va sirviendo hasta el 31 de diciembre del 2018 con un aproximado de 150 millones de dominios activos y 90 millones de certificados activos según (Aas, 2018) siendo una cantidad muy elevada haciendo que más personas y empresas confíen en su uso.

Según manifiesta el Gerente General de Web-Out S.A., como empresa administran sitios web por medio de un Panel de Control (acrónimo cPanel) siendo la administración de los certificados digitales x.509 mucho más fácil e intuitiva, generando beneficios para sus clientes logrando mantener segura la información cuando estas acceden al sitio web, evitando ser fácilmente interceptada por un tercero de manera malintencionada.

Las versiones iniciales del protocolo SSL/TLS presentan fallos de seguridad los cuales son prohibidos su uso actualmente, como SSL versión 2 (se prohíbe su

uso por la IETF en la RFC 6176 por graves fallos de seguridad entre ellas el ataque DROWN) y la versión 3 (no suficientemente seguro descrito en la RFC 7568); así como también TLS versión 1.0 (vulnerable a ataques como BEAST y POODLE, no recomendable por manejar una criptografía débil). Existen estudios respecto al tipo de cifrado como RC2, SHA-1, IDEA, RC4 y DES que actualmente ya no son recomendables para su uso debido a graves fallos de privacidad, seguridad y vulnerabilidades encontradas. Así mismo se realizaron estudios internacionales por la PCI SSC en un informe de título “Migrar de SSL y TLS temprana” (PCI Security Standards Council, 2016) respecto a TLS versión 1.1 el cual menciona que no todas las implementaciones se consideran seguras, debido a que no ofrece características modernas de cifrado descritos así mismo en la RFC 5246 sección 1.2.

En vista de no existir investigación respecto a TLS versión 1.2 enfocado al impacto que genera en el rendimiento de los sitios web, en esta investigación se consideró como caso de estudio, cinco sitios web de la empresa Web-Out S.A., en el cual se analiza los tiempos de carga por HTTP y HTTPS; describiendo el escenario de pruebas, así como también el análisis de las nuevas suites de cifrado que han sido implementados; teniendo en consideración que ambas versiones son actualmente recomendadas por la IETF para su uso y configuración, este estudio será importante para poder determinar el nivel de impacto que implica el uso de este protocolo en un entorno real y con sitios web que actualmente se encuentran en producción.

## 1.3 Formulación del problema

### 1.3.1 Problema general

¿Cuál es el impacto que el cifrado con el protocolo SSL/TLS produce en el rendimiento de los sitios web, caso empresa Web-Out S.A.?

### 1.3.2 Problemas específicos

A. ¿De qué manera influye el cifrado mediante el protocolo SSL/TLS en el tiempo de procesamiento de los sitios web?

B. ¿De qué manera influye el cifrado mediante el protocolo SSL/TLS en el nivel de solicitudes de usuario que puede soportar un sitio web?

C. ¿De qué manera influye el cifrado mediante el protocolo SSL/TLS en la transferencia de información que existe cuando se ingresa a un sitio web?

D. ¿De qué manera influye el cifrado mediante el protocolo SSL/TLS en el nivel de seguridad del sitio web?

## 1.4 Justificación

El creciente interés por resguardar y hacer más segura la transmisión de la información entre dos personas haciendo uso de canales computacionales ha sido cada vez mayor, en consecuencia se han ido desarrollando diversos protocolos que hacen uso de certificados digitales por medio del protocolo SSL/TLS para finalmente lograr una interacción de manera segura entre emisor y receptor; algunos de estos protocolos son: IPSec (Protocolo de seguridad de Internet), SFTP (Protocolo de transferencia de archivos SSH, puerto 22), SMTPS (Protocolo simple de transferencia de correo seguro, puerto 465), HTTPS (Protocolo de transferencia de hipertexto seguro, puerto 443), IMAPS (Protocolo Seguro de acceso a mensajes de Internet, puerto 993), entre otros.

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 hace uso del algoritmo de cifrado simétrico y asimétrico en el proceso de intercambio de llaves entre navegador y servidor para establecer un canal seguro por donde transmitir la información.

Actualmente el uso de SSL/TLS en el protocolo HTTP se va haciendo cada vez más importante, debido a las constantes vulnerabilidades encontradas por los ciberdelincuentes al momento de extraer información cuando se intercepta una comunicación en Internet, es por ende que existieron nuevas mejoras con el objetivo de cubrir todas estas brechas de inseguridad.

El uso de versiones más actuales del protocolo SSL/TLS hace que también estas empleen suites de cifrado más complejas para brindar una mayor seguridad en las comunicaciones. En la que muchas veces las organizaciones desconocen del

funcionamiento y de buenas prácticas para una buena configuración, mejorando la seguridad y el tiempo de respuesta a peticiones de clientes web.

A **nivel técnico**, el análisis del uso del protocolo SSL/TLS y de las suites de cifrado empleado en su versión TLS 1.2 para los sitios web, permitirá entender si genera un impacto negativo en el rendimiento de los sitios web asegurando la confidencialidad, integridad y autenticación de la información. Generando de esta manera conocimiento validado respecto al impacto que genera a los sitios web, y ayudando a conocer las buenas prácticas en la configuración de dicho protocolo.

A **nivel social**, el estudio de este protocolo permitirá a los administradores web y usuarios finales los cuales hacen uso de un navegador web, comprender la importancia y la influencia que genera el uso del protocolo SSL/TLS cuando se navega en Internet. Del mismo modo se espera generar confianza en los administradores web a nivel de rendimiento y seguridad de la información como también para los usuarios consumidores de los sitios web garantizando que la navegación sea cada vez más segura y confiable.

A **nivel organizacional**, para la empresa Web-Out S.A. tomado como caso de estudio para el análisis de este protocolo, les permitirá tener un mayor conocimiento respecto a cómo funciona y que nivel de seguridad poseen sus sitios web respecto al uso del protocolo SSL/TLS. En base a este entorno real con sitios web que se encuentran en producción, permitirá validar algunas recomendaciones respecto al uso y adecuada configuración del protocolo SSL/TLS, que bien otras organizaciones y empresas que administran sitios web puedan tomarlas como referencia.

A **nivel teórico**, esta investigación se realiza con el propósito de generar un aporte al conocimiento existente respecto al uso del protocolo SSL/TLS, cuyas características y suites de cifrado actualizadas permitirán obtener resultados que pueda ser favorables y posteriormente incorporado en el conocimiento en temas de servidores y sitios web bajo navegación segura.

Según lo descrito anteriormente, este estudio da a conocer el impacto del protocolo SSL/TLS en el rendimiento de los sitios web desarrollados y administrados en el periodo 2018-2019, caso empresa Web-Out. S.A. que permitirá conocer el funcionamiento de dicho protocolo y su impacto generado hacia los sitios web asegurando la confidencialidad, integridad y autenticación.

También es importante detallar que permitirá a los administradores web de las pequeñas y medianas empresas conocer cuál es el impacto generado por el protocolo SSL/TLS en su versión TLS 1.2 actualmente recomendada por las empresas como Mozilla, Qualys SSL Labs y Google, cuyo objetivo es tener un ambiente seguro en Internet.

## 1.5 Objetivos

### 1.5.1 Objetivo general

Evaluar el impacto del cifrado con el protocolo SSL/TLS en el rendimiento de los sitios web de la empresa Web-Out. S.A. para conocer si dicho protocolo genera un impacto negativo en la carga de los sitios web, con el fin de brindar recomendaciones respecto a la configuración y uso correcto del protocolo para mejorar el rendimiento y seguridad del sitio web.

### 1.5.2 Objetivos específicos

A. Determinar la influencia del cifrado mediante el protocolo SSL/TLS en el tiempo de procesamiento de los sitios web.

B. Determinar la influencia del cifrado con SSL/TLS en el nivel de solicitudes de usuarios que puede soportar un sitio web.

C. Determinar la influencia del cifrado con el protocolo SSL/TLS en el nivel de transferencia de información que existe cuando se ingresa a un sitio web.

D. Determinar la influencia del cifrado con el protocolo SSL/TLS en el nivel de seguridad del sitio web.

# CAPITULO II

# REVISIÓN DE LA LITERATURA

## 2.1. Antecedentes

Existen diversas investigaciones que se enfocan en la implementación del protocolo SSL/TLS en las comunicaciones entre cliente y servidor principalmente en la capa de transporte del modelo OSI y TCP/IP.

A continuación, se hace una descripción detallada de las investigaciones encontradas de ámbito nacional e internacional relacionadas con la investigación que se está realizando.

(López Fernández, 2015) En su trabajo de fin de Máster que lleva por título: "**Caracterización y medida pasiva del rendimiento para conexiones web seguras HTTPS**" realizado en la Universidad Pública de Navarra – España, 2015. Esta investigación consistió en obtener toda la información posible de una conexión HTTPS y HTTP con el fin de caracterizarla y observar el rendimiento que ofrece el servidor web seguro. Se probaron distintos algoritmos de cifrado para analizar la sobrecarga generada, todo esto en un ambiente de pruebas que estaba compuesto por 2 equipos, uno como servidor web y el segundo como cliente. Se realizó el análisis de distintos sistemas de cifrado (AES, 3DES, Camellia, SEED y RC4), sobrecarga de datos y el tiempo de procesamiento que generan los algoritmos criptográficos con el objetivo de establecer una regla o función que permita caracterizar cualquier conexión HTTPS. Llegando a la conclusión que para tener

una comunicación segura haciendo uso del protocolo SSL será necesario sacrificar parte del rendimiento, y elegir el algoritmo criptográfico que más se adapte a las condiciones y ambiente de trabajo.

(Coarfa, Druschel, & Wallach, 2006) En el artículo científico de Título: "***Performance Analysis of TLS Web Servers***" realizado en la Universidad William Marsh Rice - EE.UU, 2006. Llega a la conclusión que se realizó un análisis en servidores web donde tenían configurado el módulo "mod_ssl" en apache para la entrega segura por medio de TLS versión 1.0, 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. Por lo que invertir en CPU más rápidas o adicionales parece ser una estrategia preferible para maximizar el rendimiento del servidor web TLS. Así mismo sugieren que para optimizar el rendimiento del servidor TLS se deben de enfocar en reducir los costos de CPU de la fase de configuración de la conexión de TLS.

(Shen, Nahum, Schulzrinne, & Wright, 2009) En el artículo científico de título: "***The Impact of TLS on SIP Server Performance***" realizado en la Universidad de Columbia – EE.UU, 2009. El estudio evalúa el impacto en el rendimiento del uso de TLS como protocolo de transporte para servidores SIP. Así mismo, 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 púbica, 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.

(Kuo, Tschofenig, & Meyer, 2006) En su artículo científico de título: "***Comparison Studies between Pre-Shared and Public Key Exchange Mechanisms for Transport Layer Security***" realizado en *National Institute of Informatics* – Japón, 2006. El estudio consistía en la evitación o reducción de las operaciones criptográficas utilizadas en los mecanismos basados en claves publicas estándar en TLS, se realizó un análisis sistemático y una comparación del rendimiento entre los mecanismos de intercambio de claves pre-compartidos y los mecanismos de intercambio de claves públicas. Las métricas de rendimiento fue el tiempo de procesamiento y la cantidad de datos transmitida para un establecimiento de protocolo de enlace. Además, se evaluó la interacción entre la duración global del handshake de TLS y el entorno de red. Llegando a la conclusión que cuando se compara 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.

(Li & Zhao, 2012) En su artículo científico de título: "***Improving Secure Server Performance By EAMRSA SSL Handshakes***" realizado en *Nanyang Institute of Technology* – China, 2012. Llegan a la siguiente conclusión, que en "vista que los servidores SSL a menudo están sobrecargados con muchas solicitudes simultaneas, se propuso 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".

(Granda & Saquicela Parra, 2017) En su tesis de pregrado titulada: "**Análisis de vulnerabilidades del protocolo SSL/TLS en las páginas web gubernamentales del ecuador más usadas en la carrera de ingeniería en Networking y Telecomunicaciones**" realizado en Guayaquil – Ecuador, 2017; tiene como objetivo general "Analizar las vulnerabilidades del protocolo SSL/TLS en el transporte de la información en las páginas gubernamentales del Ecuador más utilizadas en la Carrera de Ingeniería en Networking y Telecomunicaciones y proponer medidas de seguridad para reducir el impacto de las vulnerabilidades". Obteniendo como conclusiones que se tomaron 39 páginas gubernamentales de las cuales como resultado de una encuesta realizadas se llegó a solo 26, que vendrían a ser las más concurrentes. De esta muestra el 54% no tenían implementado ningún protocolo de seguridad y el 23% tuvo una puntuación de entre "B" y "F", y un 23% una puntuación "A" según los parámetros establecidos por Qualys haciendo un equivalente de esta última puntuación a una seguridad aproximada al 80%. Esta herramienta también logro identificar 15 vulnerabilidades de las cuales 10 fueron los más repetitivos. Asimismo, recomienda el uso de diversas herramientas para

analizar vulnerabilidades de las páginas web para poder recolectar más información para un mejor estudio en investigaciones a futuro.

(Ordoñez Calero, 2013) En su tesis de pregrado de título: "**Desarrollo del módulo de gestión de información técnica para TELALCA S.A. e implementación de seguridad mediante cifrado SSL del protocolo HTTPS**" realizado en Quito - Ecuador, 2013; tiene como objetivo general: "Desarrollar un módulo de gestión de información técnica para TELALCA S.A. e implantación de seguridad mediante cifrado SSL del Protocolo HTTPS". De la cual podemos rescatar la siguiente conclusión de que: "gracias a la implementación del protocolo de seguridad HTTPS en el acceso, la transmisión de la información se realizara mediante un canal cifrado".

(Ariansen Moncada & Rojas Diaz) En su tesis de pregrado de título: "**Implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte 2016**" realizado en Chiclayo – Perú, 2016; tiene como objetivo principal: "Implementar el protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte", llegando a la conclusión de que las versiones más actuales del protocolo SSL/TLS ya sea en su versión TLS versión 1.1 y TLS versión 1.2 ya son compatibles con los navegadores más actuales y usados por la gran mayoría de usuarios en la web.

(Alvarado Sarango, 2016) En su tesis de pregrado de título: "**Implementación de seguridad en la capa de transporte del modelo TCP/IP en los servidores web y de aplicación de la Universidad Nacional de Loja**". Realizado en Loja – Ecuador, 2016; tiene como objetivo principal: "Implementar

seguridad en la capa de transporte del modelo TCP/IP, en los servidores web y de aplicación de la Universidad Nacional de Loja; para lo cual se emplea los certificados digitales SSL/TLS" de la cual en la investigación se pasó a realizar un análisis de las vulnerabilidades que presentaban los servidores y páginas web que eran propiedad de la universidad de Loja con la finalidad de corregir dichas vulnerabilidades, así también se pasó a estudiar diversos certificados SSL para posteriormente realizar una actualización de dichos certificados con las que estaban actualmente. Llegando a la siguiente conclusión: "Al usar certificados SSL/TLS contrarresta ataques como: Hombre en el medio, Phishing, lo que proporciona a los servidores confidencialidad, integridad y autenticidad. SSL/TLS no ofrece seguridad en la disponibilidad del servidor especialmente en ataques de negación de servicio (DoS) y otros ataques como XSS Cross-Site Scripting, Backdoor." En la cual recomienda el uso de certificados digitales gratuitos (emitidos por una CA) en ambientes donde manejan información académica; como colegios, institutos y PYMES; las cuales no tienen un presupuesto para dichos gastos que pueda generar adquirir un certificado de pago con soporte técnico y mejores características en cuanto a seguridad.

(Oporto Guzmán, 2016) En su tesis de pregrado de título: "**Optimización del tiempo de respuesta en el cifrado de datos utilizando computación de alto desempeño por GPGPU**" realizado en Arequipa – Perú, 2015; Su objetivo principal de su investigación es: "Optimización del tiempo de respuesta en el cifrado de datos utilizando computación de alto desempeño por GPGPU, logrando acelerar el proceso de codificación y decodificación de algoritmos de encriptación obteniendo mejores tiempos de respuesta para este tipo de proceso." Donde llega a la

recomendación que si lo que se quiere es aumentar el nivel de seguridad de los algoritmos configurados es necesario utilizar el algoritmo RSA con un tamaño de llave muy alto.

(Sánchez Vallejos, 2017) En su tesis de pregrado de título: "**Técnicas de encriptación para mejorar la seguridad en la transferencia de archivos en un entorno fiable**" realizado en la Universidad Señor de Sipán, Pimentel – Perú, 2017. En la cual tiene como objetivo principal "Implementar técnicas de encriptación, para mejorar la seguridad en la transferencia de archivos en un entorno fiable". Llegando a la conclusión de que el análisis de los algoritmos de encriptación como RSA y AES se caracterizaron por su gran velocidad, seguridad y fácil entendimiento.

(Haro Montero & Gavilanes Sagñay, 2009) En su tesis de pregrado de título: "**Análisis de funciones criptográficas de código libre en los protocolos SSL y TLS aplicado al portal web de la jefatura provincial de tránsito de Chimborazo.**", realizado en Riobamba – Ecuador, 2009; en la cual tiene como objetivo principal:" Analizar y comparar las herramientas de código libre para la administración de funciones criptográficas en los protocolos SSL y TLS aplicado al desarrollo del portal web de la Jefatura Provincial de Tránsito de Chimborazo" de la cual nos quedamos con la conclusión que la herramienta OpenSSL presenta una mejor organización en la generación de claves públicas y privadas, así también tiene una gran cantidad de información documental respecto al funcionamiento y enfoque en el protocolo SSL/TLS.

## 2.2 Bases Teóricas

### 2.2.1 Cifrado Web mediante el Protocolo SSL/TLS

El cifrado web mediante el protocolo SSL/TLS permite que la información que es enviada de un nodo a otro, viaje como un texto no legible para usuarios no involucrados en la comunicación. De esta manera se mantiene segura y de acceso solo por el personal autorizado. Estos protocolos protegen el enlace de comunicación o la capa de transporte, que es de donde proviene el nombre de TLS (Ristic, 2014, pág. 1).

El protocolo SSL/TLS ha ido evolucionando desde su creación en el año 1994. Las diversas versiones de SSL y TLS brindan ciertos servicios de seguridad, como la confidencialidad, autenticación de la entidad y la integridad. Asimismo, dichos protocolos se han diseñado teniendo presente características como la eficiencia y extensibilidad (López Fernández, 2015, pág. 12).

Esta eficiencia se ve con mayor impacto en las versiones finales de TLS, como por ejemplo en la versión 1.2 descrita en la RFC 5246 en Agosto (2008) y la versión 1.3 descrito en la RFC 8446 aprobado en agosto de 2018 (Rescorla, 2018). Los navegadores más comunes ya tienen habilitado estas últimas versiones del TLS, se debe tener en cuenta respecto a esta última versión que aún se están realizando pruebas e implementaciones en los diversos servidores web como Apache, Nginx, IIS y otros; mostrando muchas mejoras en cuanto a su funcionalidad, eficiencia y seguridad.

El protocolo SSL/TLS para poder establecer el canal seguro antes de iniciar con el intercambio de información, hace uso del algoritmo de cifrado simétrico y

asimétrico. En un principio se hará uso del algoritmo asimétrico (también conocido como sistema de clave pública) que será generado por parte del servidor para intercambiar de manera segura la clave que servirá para posteriormente hacer uso del algoritmo simétrico (IBM, s.f.); mediante este último será que la información se estará cifrando en la comunicación, caracterizándose por ser más rápido y eficiente para el intercambio de datos (Roa Buendia, 2013, pág. 39).

### 2.2.2 Rendimiento de un sitio web

Carles Mateu (Mateu, 2004) menciona “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.”, para el cual esta tesis está enfocado a conocer el impacto generado por el protocolo SSL/TLS; si genera retrasos en los tiempos de respuesta afectando positiva o negativamente en la experiencia del usuario.

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 (Mateu, 2004). 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 costo computacional 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.

El intercambio y flujo de mensajes entre el cliente y servidor en el protocolo TLS versión 1.2 se muestra en la siguiente Figura 1, y se precisa en detalle en la RFC 5246.

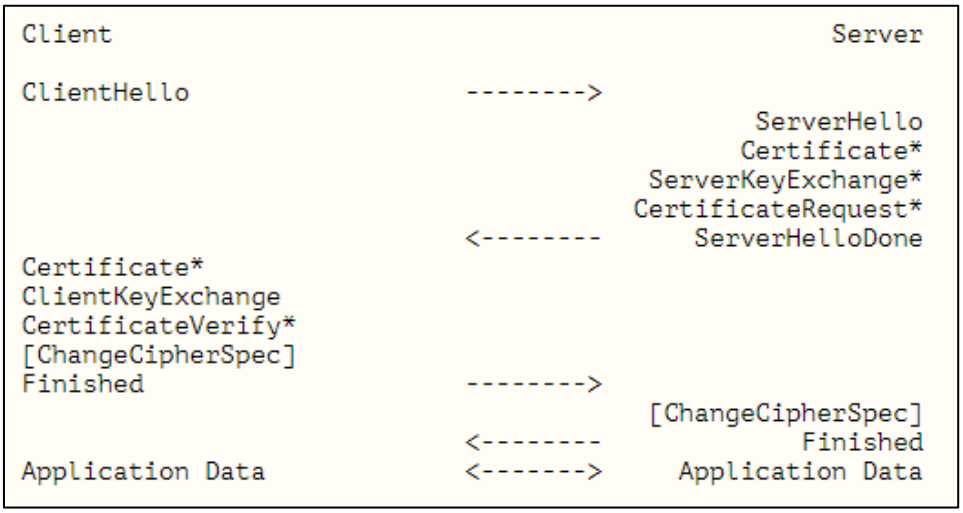



**Figura 1.** Flujo de mensajes entre Cliente y Servidor en TLS v1.2
**Fuente**: (T. Dierks, 2008)

Este intercambio de mensajes se realiza en cuestión de milisegundos antes de iniciar con el proceso de transmisión de información, lo que provoca que el tiempo sea superior a 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 por parte del servidor; distinto a como si la comunicación viajase haciendo uso del Protocolo SSL/TLS. Con la investigación podremos conocer cuánto es este tiempo de diferencia y en cuanto puede influir en el rendimiento del sitio web.

Según (Villada Romero, 2015, pág. 94), la cantidad total de clientes que pueden ser atendidos en simultaneo por un Servidor Web está dada por la siguiente formula.

$$\boldsymbol{Max\ Clientes} = (\boldsymbol{Total\ RAM}) / (\boldsymbol{Max\ tamaño\ del\ proceso\ hijo})$$

Aunque esta fórmula pueda parecer muy simple, existen múltiples factores y herramientas que puedan ayudarnos a conocer el rendimiento de un servidor web, en esta investigación nos apoyaremos de algunas herramientas que funcionan de

manera online y otros que se ejecutan desde la línea de comandos de un terminal en Linux.

Empresas como Google y Mozilla proporcionan herramientas 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 tomada con mucha consideración ya que evidencia el rendimiento que pueda tener el sitio web cuando es accedido por un cliente.

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

### 2.2.3 Seguridad en SSL/TLS

(Ristic, 2014) menciona que Internet en sus inicios, fue diseñado sin pensar en brindar una comunicación segura a sus clientes. Actualmente, hubiera presentado graves problemas de no ser por los protocolos que aseguran esta comunicación, SSL/TLS es uno de esos protocolos; fue diseñado para brindar seguridad sobre una infraestructura insegura e implementado en la capa de Transporte, de ahí es donde proviene el nombre de TLS.

La seguridad no es el único objetivo de TLS, menciona (Ristic, 2014, pág. 2), sino que tienen 4 objetivos, que se describen a continuación:

- **Seguridad criptográfica:** Este es el problema principal, habilitar la comunicación segura entre cualquiera de las dos partes que se desea intercambiar información.
- **Interoperabilidad:** Los programadores independientes deben poder desarrollar programas y bibliotecas que sean capaces de comunicarse entre sí utilizando parámetros criptográficos comunes.
- **Extensibilidad:** TLS es efectivamente un marco para el desarrollo y despliegue de los protocolos criptográficos. Su objetivo importante es ser independiente de las primitivas criptográficas reales (por ejemplo, las cifras y las funciones de hash) utilizadas, lo que permite la migración de una primitiva a otra sin la necesidad de crear nuevos protocolos.
- **Eficiencia:** El objetivo final es lograr todos los objetivos anteriores a un costo de rendimiento aceptable, reduciendo al mínimo las costosas operaciones criptográficas y proporcionando un esquema de almacenamiento en caché de sesión para evitarlas en conexiones posteriores.

### 2.2.4 Criptografía

(Ristic, 2014, pág. 49) describe que una suite de cifrado es una selección de algoritmos de cifrado, funciones hash y otros parámetros que definen exactamente como se implementara la seguridad, en la Figura 2, se puede visualizar los atributos el cual está contenida una suite de cifrado.

Cuando accedemos a un sitio web que tiene habilitado el protocolo SSL/TLS, nos encontramos con los dos tipos de algoritmos de cifrado, el simétrico y el asimétrico, acompañado del protocolo y algoritmo hash empleado. Esto puede ser visto desde el navegador ingresando en la configuración de seguridad de la conexión (Anexo 2.), mostrando del siguiente formato para la conexión cifrada al sitio web:

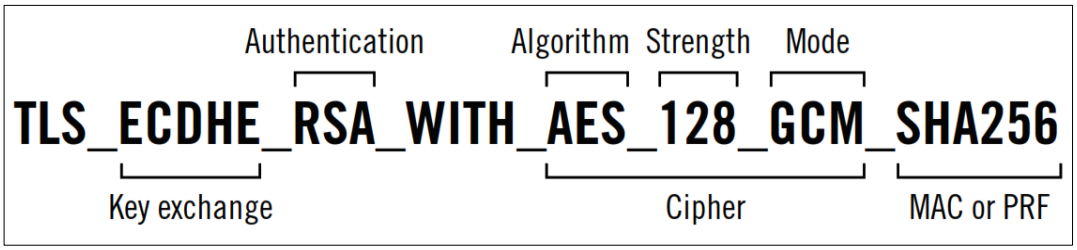



**Figura 2.** Atributos de una Suite de Cifrado
**Fuente**: (Ristic, 2014)

Podemos encontrar un listado completo y actualizado de las Suite de Cifrado empleado en conexiones SSL/TLS, publicada por la (Internet Assigned Numbers Authority, 2019) en su sitio web, y actualizado hasta el 22 de abril de 2019.

En ella podremos encontrar distintas secciones relacionadas al Protocolo SSL/TLS; nos enfocaremos en la sección "*TLS Cipher Suites*" que es donde describe por medio de la Figura 3 la suite de cifrado existente. En esta figura es posible encontrar información de cumplimiento de DTLS (*Datagram Transport Layer*

*Security*), así como también indica si es recomendable para su uso y finalmente nos muestra la RFC de referencia para más información.

| Value | Description | DTLS-OK | Recommended | Reference |
|---|---|---|---|---|
| 0x00,0x00 | TLS_NULL_WITH_NULL_NULL | Y | N | [RFC5246] |
| 0x00,0x01 | TLS_RSA_WITH_NULL_MD5 | Y | N | [RFC5246] |
| 0x00,0x02 | TLS_RSA_WITH_NULL_SHA | Y | N | [RFC5246] |
| 0x00,0x03 | TLS_RSA_EXPORT_WITH_RC4_40_MD5 | N | N | [RFC4346][RFC6347] |
| 0x00,0x04 | TLS_RSA_WITH_RC4_128_MD5 | N | N | [RFC5246][RFC6347] |
| 0x00,0x05 | TLS_RSA_WITH_RC4_128_SHA | N | N | [RFC5246][RFC6347] |
| 0x00,0x06 | TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 | Y | N | [RFC4346] |
| 0x00,0x07 | TLS_RSA_WITH_IDEA_CBC_SHA | Y | N | [RFC5469] |
| 0x00,0x08 | TLS_RSA_EXPORT_WITH_DES40_CBC_SHA | Y | N | [RFC4346] |
| 0x00,0x09 | TLS_RSA_WITH_DES_CBC_SHA | Y | N | [RFC5469] |
| 0x00,0x0A | TLS_RSA_WITH_3DES_EDE_CBC_SHA | Y | N | [RFC5246] |
| 0x00,0x0B | TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA | Y | N | [RFC4346] |
| 0x00,0x0C | TLS_DH_DSS_WITH_DES_CBC_SHA | Y | N | [RFC5469] |
| 0x00,0x0D | TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA | Y | N | [RFC5246] |
| 0x00,0x0E | TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA | Y | N | [RFC4346] |
| 0x00,0x0F | TLS_DH_RSA_WITH_DES_CBC_SHA | Y | N | [RFC5469] |

**Figura 3.** Reporte de Suites de Cifrado de SSL/TLS por la IANA
**Fuente:** (Internet Assigned Numbers Authority, 2019)

## 2.3 Marco Conceptual

### 2.3.1 Algoritmos de Cifrado

El algoritmo de cifrado está inmerso dentro de la criptografía, consiste en tomar un documento original y aplicarle un algoritmo para obtener como resultado un nuevo documento el cual no se puede entender al leerlo directamente. El receptor podrá descifrarlo siempre en cuando aplique el algoritmo utilizado por el emisor (Roa Buendia, 2013). La complejidad del algoritmo de cifrado está vinculada con el tamaño de clave en bytes que puede ser: 512, 1024, 2048, 4096 u otro.

- **Algoritmo de cifrado simétrico:** La explicación realizada por (Roa Buendia, 2013, pág. 30) en su libro "*Seguridad Informatica*", es que este algoritmo utiliza la misma clave para el proceso de cifrado y descifrado, son sencillos de utilizar y se caracterizan por ser muy eficientes (tardan poco en cifrar y descifrar). Existen

diversos algoritmos simétricos solo por mencionar algunos: AES, DES, 3-DES, RC2, RC4, RC5, IDEA.

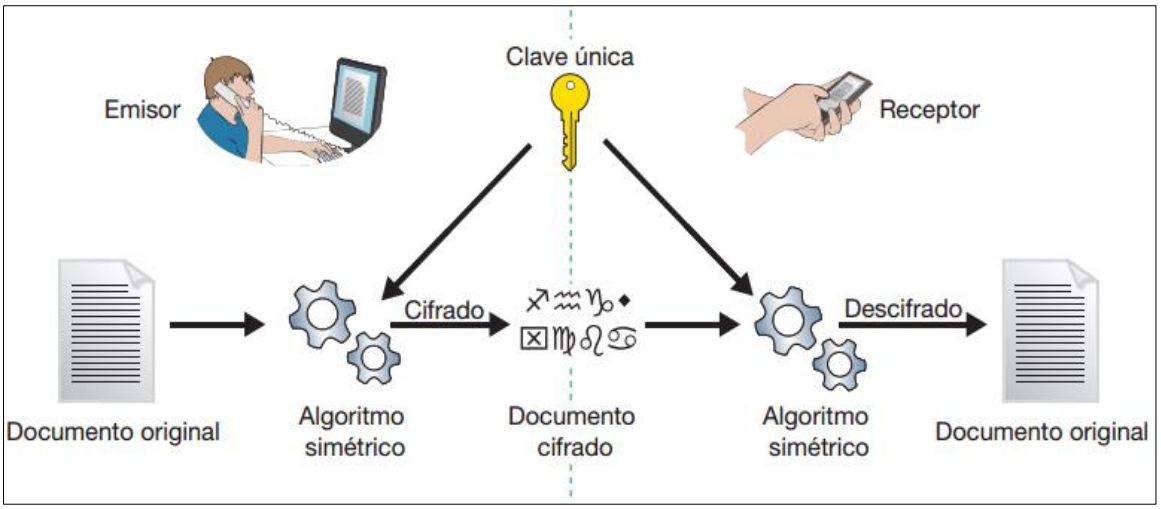



**Figura 4.** Proceso de cifrado y descifrado del algoritmo simétrico.
**Fuente**: (Roa Buendia, 2013, pág. 30)

En la Figura 4. se puede visualizar como el emisor envía un documento para luego ser cifrado con la clave única mediante el algoritmo simétrico, como resultado se obtiene el documento cifrado; el receptor para poder ver la información original es necesario que aplique el algoritmo simétrico con la misma clave que se utilizó para cifrar el documento por parte del emisor.

- **Algoritmo de cifrado asimétrico:** El algoritmo utiliza dos claves (pública y privada) que se encuentran relacionadas desde el momento de su creación. Lo que se cifra utilizando la clave pública, se descifra con la clave privada; esta última clave nunca es compartida siendo matemáticamente imposible obtener a partir de la clave pública (Roa Buendia, 2013). Adicionalmente, cuando el usuario cifra la información con su clave privada, se le conoce como una información firmada digitalmente, siendo posible verificar su identidad por medio de su clave pública;

este es un aspecto muy interesante ya que según se cifre con la clave pública del destino o la clave privada del emisor, se consigue bien la confidencialidad o bien la autenticidad del emisor (Muñoz Muñoz & Ramió Aguirre, 2013, pág. 121).

En la Figura 5 se detalla el proceso de cifrado de un documento original haciendo uso de la clave pública del receptor, se emplea el algoritmo asimétrico al documento pasando de ser legible a ininteligible, finalmente el receptor para obtener el documento original debe hacer uso de su clave privada.

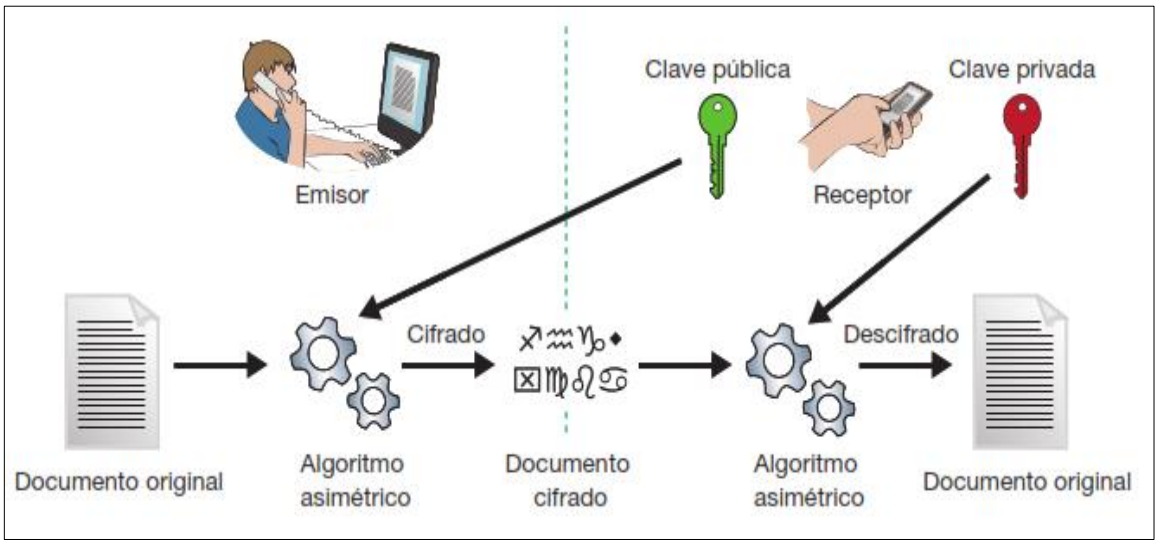



**Figura 5.** Proceso de cifrado y descifrado del algoritmo asimétrico
**Fuente:** (Roa Buendia, 2013)

El protocolo SSL/TLS en el proceso de negociación hace uso del algoritmo simétrico y asimétrico, (Roa Buendia, 2013, pág. 39) hace mención que el algoritmo de cifrado asimétrico es usado en el inicio de la conversación entre el cliente y servidor para establecer una comunicación cifrada. Una vez que la comunicación cifrada ha sido establecida se hace uso del cifrado simétrico para el intercambio de todos los paquetes, esta clave tiene un tiempo límite en minutos, y vuelve a ser generado para evitar que una persona malintencionada intercepte la comunicación habiendo obtenido la clave de cifrado.

### 2.3.2 Protocolo SSL/TLS

El protocolo SSL/TLS ha sido diseñado e implementado por la empresa Netscape en el año 1994, para transferir información segura a través de Internet. La autorización SSL del servidor es vital para transacciones seguras de comercio electrónico en las cuales, por ejemplo, los/as usuarios/as envían números de tarjetas de crédito y antes desean verificar la identidad del servidor. Una vez autorizado SSL se podrán habilitar conexiones HTTPS a ese dominio o incluso forzar a que las conexiones sean exclusivamente por HTTPS. El puerto por defecto para el protocolo HTTPS es el 443 (Villada Romero, 2015, pág. 92).

Otra definición de la empresa GlobalSign es: “El SSL … y el TLS … son los protocolos de seguridad de uso común que establecen un canal seguro entre dos ordenadores conectados a través de Internet o de una red interna” (GlobalSign, 2018).

Cuando se implementa el protocolo SSL/TLS en una infraestructura de servidor web, la comunicación viaja de manera cifrada accediendo desde la URL ya no como “http://” sino como “https://”. También hace uso de certificados digitales emitidos por una autoridad certificadora (A.C.) que es verificado por el navegador, de no ser válido estaría mostrando un mensaje diciendo que el sitio web no es seguro.

En la Figura 6 se puede apreciar el acceso al sitio web de la Empresa Web-Out. S.A. (www.web-out.com) mediante HTTP y HTTPS, haciendo uso de los navegadores como Google Chrome, Mozilla Firefox, Opera y Internet Explorer; siendo en su mayoría los más utilizados a nivel nacional e internacional como

navegadores de escritorio (Anexo 7). Cuando se accede a un sitio web el cual tienen habilitado SSL/TLS el símbolo característico es un “candado” casi siempre de color verde, representando la seguridad del sitio web y la correcta instalación y configuración del certificado digital.

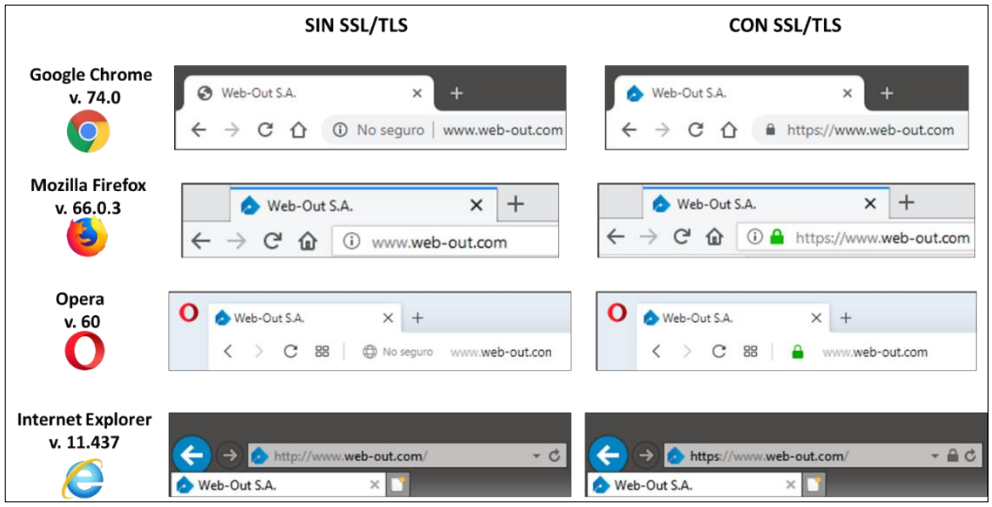



**Figura 6.** Navegación por HTTP y HTTPS en los navegadores más comunes.
**Fuente:** Elaboración propia.

Se puede apreciar en la Figura 7, el proceso de verificación de una comunicación vía HTTPS es aspectos generales, definida por Villa Romero en su Libro “Instalación y configuración del software de servidor web (UF1271)”.

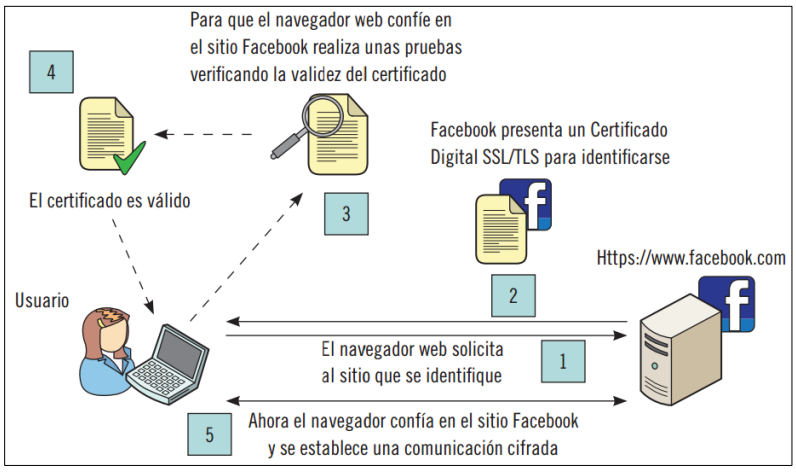



**Figura 7.** Secuencia de pasos en la comunicación vía HTTPS.
**Fuente**: (Villada Romero, 2015, pág. 362)

Según la RFC 4346 de (Dierks & Rescorla, 2006) menciona que: “*El protocolo TLS proporciona seguridad de comunicaciones a través de Internet. El*

*protocolo permite que las aplicaciones cliente/servidor se comuniquen de una manera que esté diseñada para evitar el espionaje, la manipulación o la falsificación de mensajes."*

A lo largo de los años el protocolo SSL/TLS ha pasado por una serie de versiones, cada versión superior trae mejoras en comparación con la anterior; mejoras a nivel de funcionalidad, seguridad, velocidad, entre otros. A continuación, se detallan esas versiones en orden cronológico.

- **SSL versión 1:** Fue la primera versión del SSL originado en 1994, nunca fue publicada.
- **SSL versión 2:** Esta segunda versión fue publicada en el año 1995, y fue utilizado por el navegador Netscape Navigator v1.1.
- **SSL versión 3:** Esta versión fue publicada en 1996, presentaba mejoras en seguridad con respecto a sus versiones anteriores.
- **TLS versión 1.0:** Según el autor (Herrera Joancomartí, García Alfaro, & Perramón Tornil, 2004, pág. 58) considera que el protocolo TLS versión 1.0 es equivalente al SSL versión 3.0 con mínimos cambios, por lo que en ciertos contextos consideran la versión TLS versión 1.0 como si fuera SSL versión 3.1.
- **TLS versión 1.1:** Esta versión fue definida por la RFC 4346 en abril del 2006, es una actualización de TLS versión 1.0, entre las mejoras y diferencias más significativas están:
  - ✓ El vector de inicialización (IV) que es el bloque de bits requerido para permitir un cifrado de flujo o por bloques, fue reemplazado por un IV

explicito el cual permite protegerse del ataque de texto plano que se da en TLS que implicaba conocer el IV para un registro anterior.

- ✓ Se realizaron cambios en el manejo de los errores de relleno.
- ✓ Se agrego soporte para el registro de parámetros de IANA.

- **TLS versión 1.2:** Esta versión de TLS fue definida en el RFC 5246 en agosto del 2008 (T. Dierks, 2008), posteriormente en marzo del 2011 fue redefinido con la RFC 6176 (S. & T. Polk, 2011) redactando su compatibilidad con versiones anteriores.

Esta versión superior a la anterior, de TLS versión 1.1 trae consigo las siguientes mejoras.

- ✓ Mejoras en la habilidad de clientes y servidores para establecer el algoritmo de hash y de firma que van a hacer uso.
- ✓ La combinación MD5-SHA-1 fue reemplazada tanto en la función pseudoaleatoria, y en el mensaje terminado por SHA-256, y en el elemento digitalmente por el hash simple negociado durante el handshake (SHA-1).

- **TLS versión 1.3:** Esta en la versión más actualizada del protocolo TLS, definido en el RFC 8446 en agosto de 2018. Entre las principales mejoras en comparación con TLS versión 1.2 son:

- ✓ Retiro de la hora GTM.
- ✓ Fusiona soporte de ECC del RFC 4492 pero sin curvas explícitas.
- ✓ Retira el campo de longitud innecesaria de la entrada de AD a cifras AEAD.

- ✓ Cambiar el nombre de {Cliente, Servidor} KeyExchange a {Cliente, Servidor} KeyShare.
- ✓ Añade un HelloRetryRequest explícita para rechazar el del cliente.
- ✓ Handshake revisado a fin de proporcionar el modo 1-RTT.
- ✓ Retiro de grupos DHE personalizados.
- ✓ Eliminado el soporte para la compresión.
- ✓ Eliminado el soporte para el intercambio de claves RSA estática y DH.
- ✓ Eliminado el soporte para sistemas de cifrado no AEAD.

Para verificar si el navegador soporta esta última versión la empresa Qualys SSL Labs cuenta con una herramienta online (https://www.ssllabs.com/ssltest/viewMyClient.html) que permite obtener información de las versiones SSL/TLS que soporta nuestro navegador; hay que tener presente que al ser la última versión fue aprobada hace 1 año aproximadamente (en agosto del 2018) y para que los navegadores puedan hacer uso es necesario que se encuentre actualizado.

### 2.3.3 Fortaleza del Algoritmo de Cifrado

La fortaleza del algoritmo de cifrado SSL/TLS pertenece a la dimensión de la variable Independiente. La fortaleza del algoritmo de cifrado tanto simétrico como asimétrico forman parte de una comunicación por medio de HTTPS. (Ristic, 2014, pág. 18) menciona que la seguridad y la fuerza del algoritmo de cifrado está relacionada con el tiempo, cada vez más las computadoras son mucho más rápidas a accesibles a un menor costo. Permitiendo que los algoritmos de cifrado de mayor complejidad puedan ser procesados con mucha facilidad en comunicaciones por HTTPS.

Ivan Ristic menciona: “Una clave de tamaño pequeño podría ser imposible de romper para una persona, pero hacerlo podría estar al alcance de una agencia” (Ristic, 2014, pág. 18); es por eso que la fortaleza está vinculada con el tamaño de la clave utilizada y por los recursos computacionales con el cual puede ser vulnerado.

En la Figura 8 es posible ver una comparación de tamaños de bits entre los algoritmos simétricos, asimétricos (RSA, DSA, DH), algoritmos con curva elíptica y hash, el cual nos permite convertir de un conjunto de bits a otro conociendo la fortaleza con el cual se está trabajando.

| Symmetric | RSA / DSA / DH | Elliptic curve crypto | Hash |
|---|---|---|---|
| 80 | 1,024 | 160 | 160 |
| 112 | 2,048 | 224 | 224 |
| 128 | 3,072 | 256 | 256 |
| 256 | 15,360 | 512 | 512 |

**Figura 8.** Asignación de la intensidad de cifrado para los tamaños de clave de uso común.
**Fuente:** (Ristic, 2014)

### 2.3.4 Rendimiento frente a ataques

El rendimiento frente a ataques del protocolo SSL/TLS pertenece a una de las dimensiones de la variable independiente, donde Ivan Ristic (Ristic, 2014, pág. 16) en su Libro ”*Bulletproof SSL and TLS: The Complete Guide to Deploying Secure Servers and Web Applications*” detalla que la fuerza de un algoritmo criptográfico está representada por bits de seguridad. El uso de claves más grandes implementara un nivel de seguridad más alto. Usas 128 bits de seguridad (Equivale a $2^{128}$ operaciones) siendo suficiente para las mayorías de las implementaciones; el hacer uso de 256 bits brindara un mayor margen de seguridad.

El romper un algoritmo de encriptación consiste en encontrar la clave para acceder a la información encriptada en texto plano.

### 2.3.5 Tiempo de Procesamiento

El tiempo de procesamiento como una de las dimensiones de la variable dependiente consiste en detallar cuando demora en cargar un sitio web, teniendo en cuenta que el sitio web está contenida por elementos como: imágenes, archivos css, archivos java Script, videos, etc.

### 2.3.6 Nivel de concurrencia de usuarios

El nivel de concurrencia descrito como una de las dimensiones de la variable dependiente, trata de explicar la cantidad de solicitudes de clientes que puede soportar el servidor web cuando se tiene habilitado y deshabilitado el protocolo SSL/TLS; para el cual se hará uso de la herramienta apache Bench desarrollada por la empresa Apache, el cual permite simular una gran cantidad de peticiones a un servidor web.

### 2.3.7 Transferencia de Información

La transferencia de la información como una de las dimensiones de la variable dependiente trata de explicar un aspecto importante en el intercambio de información entre el cliente y servidor, que es conocer la cantidad de bytes intercambiados y la cantidad de peticiones que realiza el cliente ante el servidor web.

El autor (Cardador Cabello, 2014) en su libro “Desarrollo de aplicaciones web distribuidas” menciona:

“Los sistemas en red Cliente/Servidor o protocolos son sistemas que se diseñan para que un cliente realice peticiones a otro programa servidor que da respuesta. Estos sistemas se basan en una arquitectura Cliente/Servidor que es un modelo de aplicación distribuida la cual reparte las tareas entre los recursos o servicios (servidores) y los demandantes de estos (clientes).”

### 2.3.8 Nivel de Seguridad

El nivel de seguridad como una de las dimensiones de la variable dependiente consiste en comprobar si el protocolo SSL/TLS agrega un nivel de seguridad de un sitio web; para lo cual se empleará herramientas Open Source para comprobar que se esté realizando la confidencialidad, integridad, autenticación.

En Internet es cada vez más común encontrar casos donde por medio de un sitio web se ha obtenido información confidencial, mas es el riesgo si es que estos involucran grandes cantidades de dinero de miles y miles de personas.

La creatividad de los ciberdelincuentes cada vez es mayor, por el cual estarán en constante búsqueda de agujeros y vulnerabilidades de los sitios web. En ese sentido es importante conocer las diversas herramientas y protocolos que ayudaran a mejorar la seguridad en este aspecto. (Matute, Cuervo, Salazar , & Santos , 2012)

Teniendo presente que el protocolo HTTPS utiliza un cifrado basado en los protocolos de Capa de Conexiones Seguras (SSL - en ingles *Secure Sockets Layer*) que es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet y que fue sustituido por el protocolo de Capa de Transporte Segura (TLS – en ingles *Transport Layer Security*) que es un

protocolo que se basa en el protocolo SSL y consiste en establecer una conexión segura a través de un canal cifrado entre el cliente y servidor. (Sabogal Rosas, 2015, pág. 7)

Sabogal Rosas en su Tesis de máster, en 2015, ha citado a Naylor, Finamore, Leontiadis, Grunenberger, Mellia, Munafò, Papagiannaki & Steenkiste en su investigación de título "*The Secure Hypertext Transfer Protocol*" lo siguiente:

"El protocolo SSL/TLS hace uso del cifrado que fue establecido entre cliente (navegador) y servidor web. Así, se consigue que la información sensible del usuario como son sus datos personales y claves de acceso, no puedan ser usadas por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendría sería un flujo de datos cifrados que le resultará imposible de descifrar".

## 2.4 Hipótesis

### 2.4.1 Hipótesis general

El cifrado con el uso del protocolo SSL/TLS tiene un impacto poco significativo en el rendimiento de los sitios web de la empresa Web-Out S.A.

### 2.4.2 Hipótesis específicas

A. El cifrado mediante el protocolo SSL/TLS no influye significativamente en el tiempo de procesamiento de los sitios web.

B. El cifrado mediante el protocolo SSL/TLS no influye significativamente en el nivel de solicitudes de usuario que pueda soportar un sitio web.

C. El cifrado mediante el protocolo SSL/TLS no influye significativamente en el nivel de transferencia de información que provoca el acceder a un sitio web.

D. El cifrado mediante el protocolo SSL/TLS influye significativamente en el nivel de seguridad del sitio web.

# CAPITULO III

# MATERIALES Y MÉTODOS

## 3.1 Tipo de investigación

El tipo de investigación es aplicada, Caballero Romero (2014) quien ha citado, en su libro: "*Metodología integral innovadora para planes y tesis*", una idea publicada por Hayman en 1969, donde se menciona que "*la investigación aplicada es aquella cuyo propósito fundamental es dar solución a problemas prácticos*". Otra definición, que argumenta (Luis Com, Ernesto Ackerman, & Alvin Postolski, 2013) es *"… las ciencias aplicadas apuntan a la resolución de problemas prácticos, concretos, en un área específica. Por lo general se ligan a lo productivo y tienen por fin aumentar las utilidades empresariales.*"

## 3.2 Nivel de investigación

El nivel de investigación es Cuasi Experimental, tomando como referencia lo descrito por (Mejía Mejía, 2005, págs. 34,180), menciona que en las investigaciones cuasi experimentales el investigador ya encuentra grupos formados y que no tiene oportunidad de formar grupos experimentales y de control. Este nivel de investigación se caracteriza por la manipulación de la variable independiente (Cifrado con protocolo SSL/TLS - X) para los sujetos o unidades experimentales (cinco sitios web) y ver los resultados obtenidos. También coincide con lo que define Sampieri (2014): "*El diseño incorpora la administración de un pretest y un post test a los grupos que componen el experimento"* donde existirá un grupo de control

(Sitios Web sin SSL/TLS) y un grupo Experimental (Sitios Web con SSL/TLS), donde al final se tendrá que comparar los resultados en ambos grupos.

## 3.3 Población

Los cinco sitios web desarrollados y administrados en el año 2018 - 2019 por la empresa Web-Out S.A.

## 3.4 Muestra

En este proyecto de tesis no se determina una muestra, ya que se trabajará con toda la población de estudio que para el caso son los cinco sitios web desarrollados y administrados por la empresa Web-Out S.A. en el año 2018 - 2019.

## 3.5 Variables de la investigación

### 3.5.1 Variable dependiente

- **Rendimiento de sitios web (Y).**

El rendimiento de los sitios web está definida por el tiempo que demora en cargar todos los componentes conformados para la vista hacia el navegante o visitante de determinado sitio web.

### 3.5.2 Variable independiente

- **Cifrado con protocolo SSL/TLS (X).**

En una comunicación por medio de HTTPS, se emplea el protocolo SSL/TLS el cual genera una comunicación cifrada entre cliente y servidor web empleando certificados digitales, algoritmos de cifrado y algoritmos de hash; asegurando la autenticación, confidencialidad e integridad.

## 3.6 Operacionalización de variables

**Tabla 2.** Matriz de Operacionalización de variables.

| VARIABLE | DIMENSIONES | INDICADORES | TÉCNICAS / INSTRUMENTOS DE RECOLECCIÓN INFORMACIÓN | UNIDAD DE MEDIDA |
|---|---|---|---|---|
| **Variable Independiente "X"** Cifrado con protocolo SSL/TLS | **Dim. 1:** Fortaleza del algoritmo de cifrado | - Tiempo de procesamiento del algoritmo de cifrado, firmado y verificación de la firma.<br>- Velocidad de cifrado de algoritmos simétricos.<br>- Costo computacional. | - Observación.<br>- Sniffer (wireshark).<br>- Herramienta<br>- OpenSSL.<br>- HTOP.<br>- SSLRobot. | - Segundos<br>- KBytes/Segundo<br>- Porcentaje (%) |
| | **Dim. 2** Rendimiento frente a ataques | - Fortaleza de clave de cifrado.<br>- Fortaleza de algoritmos de cifrado. | - Observación.<br>- Sniffer (wireshark).<br>- A2SV Auto Scanning SSL Vulnerability.<br>- Navegadores Web. | - Nro. de versiones de TLS soportadas y algoritmos empleados. |
| **Variable Dependiente "Y"** Rendimiento de sitios web | **Dim. 1:** Tiempo de procesamiento | - Latencia<br>- Tiempo de carga de cada sitio web.<br>- Tiempo de descarga de elemento web desde el servidor al cliente (solicitudes web). | - Observación<br>- Sniffer (wireshark)<br>- Apache Bench.<br>- Ping<br>- Navegadores. | - Milisegundos.<br>- Segundos.<br>- Nro. de solicitudes al servidor. |
| | **Dim. 2:** Nivel de solicitudes de usuarios | - Número de usuarios concurrentes que pueden ser procesados simultáneamente.<br>- Número total de paquetes intercambiados. | - Observación.<br>- Apache Bench. | - Nro. Solicitudes atendidas y fallidas<br>- Nro. de usuarios concurrentes.<br>- Nro. de solicitudes al servidor. |
| | **Dim 3:** Transferencia de información | - Cantidad de bytes descargados.<br>- Número de solicitudes por tipo de contenido.<br>- Tamaño de las solicitudes por tipo de contenido. | - Sniffer (wireshark).<br>- Observación.<br>- Navegador.<br>- Pingdom Tools. | -Tamaño (KBytes ó MBytes) por tipo de contenido.<br>- Nro. de solicitudes por Tipo de contenido. |
| | **Dim 4:** Nivel de seguridad | - Datos sin cifrar y datos cifrados (contenido mixto).<br>- Soporte del Protocolo SSL/TLS.<br>- Intercambio de llaves.<br>- Fuerza de cifrado.<br>- Vulnerabilidades al protocolo SSL/TLS. | - Sniffer (wireshark).<br>- Observación.<br>- Registro de resultados.<br>- TestSSL<br>- Qualys. SSL Labs. | - Nro. versiones habilitadas y deshabilitadas.<br>- Puntuación de A - F por Qualys SSL Labs.<br>- Nro. vulnerabilidades encontradas. |

**Fuente:** Elaboración propia.

### 3.7 Metodología

En esta investigación con el objetivo de tener una secuencia ordenada de procesos, se hará uso de cinco fases; no existiendo una metodología para realizar una auditoria respecto al impacto causado por el protocolo SSL/TLS en el rendimiento los sitios web, se pasó a definir las siguientes fases:

A. **Planificación.-** En esta primera fase se responde diversas interrogantes sobre los sitios web caso de estudio y que herramienta se utilizaron para obtener la información técnica respecto al protocolo SSL/TLS, así como también conocer las versiones que soportan los sitios web.

B. **Diseño**.- En esta fase se establecerán y se describirán los escenarios en el cual se han realizado las pruebas para medir el impacto en el rendimiento de los sitios web. Así también se especificarán las características tanto de hardware como de software de cada escenario, para comprender que los resultados fueron obtenidos en base a esos escenarios y con las características especificadas.

C. **Pruebas**.- Se realizarán diversas pruebas de rendimiento hacia los sitios web teniendo habilitado y deshabilitado el protocolo SSL/TLS, con la finalidad de validar las hipótesis planteadas en un inicio. Las pruebas se realizarán haciendo uso de diversas herramientas detalladas en la fase de planificación y en relación con los escenarios establecidos en la fase de diseño.

D. **Análisis de Resultados.-** En esta etapa se describen los resultados obtenidos en forma de tablas y gráficos, donde se podrá distinguir la diferencia del

rendimiento de los sitios web cuando se tiene habilitado y deshabilitado dicho protocolo.

Dentro de esta fase nos guiaremos de las definiciones que da Qualys SSL Labs, Pingdom Tools, OpenSSL y Mozilla respecto al rendimiento de un sitio web, estas organizaciones están alineadas en el tema de seguridad e impacto del protocolo SSL/TLS en los sitios web.

E. **Recomendaciones.-** En esta fase se detallarán las recomendaciones en base a la experiencia obtenida en esta investigación sobre el rendimiento de los sitios web respecto al protocolo SSL/TLS. Así como también se agregarán buenas prácticas y recomendaciones brindadas por entidades dedicadas al rubro de la seguridad y rendimiento de los sitios web.

# CAPITULO IV

# METODOLOGÍA

Este capítulo se centra en presentar la metodología empleada durante la ejecución de esta investigación. Es una secuencia de fases que está conformada por: planificación y diseño, posteriormente las pruebas y finalmente el análisis de los resultados obtenidos.

## 4.1 Planificación y Diseño

En esta primera fase se define y establece con claridad las siguientes interrogantes: ¿De qué elementos está conformado el escenario de estudio?, ¿Los sitios web están en producción?, ¿En qué consistirán las pruebas a realizar?, ¿Existen algunas falencias o restricciones para esta investigación?, entre otros.

Al responder estas interrogantes será mucho más fácil y comprensible el escenario y pruebas que se tienen que realizar en esta investigación, y así llegar a obtener los resultados esperados en el menor tiempo posible gracias a una buena planificación y diseño.

### A. ¿De qué elementos está conformado el escenario de estudio?

El estudio es realizado a cinco sitios web desarrollados bajo el CMS Drupal (versión 7 y 8). Alojados en dos servidores virtuales adquiridos como un servicio de la empresa “Inmotion Hosting”, siendo una de las mejores opciones del mercado para la empresa Web-Out S.A. respecto a la adquisición de VPS.

El servicio web está ejecutándose bajo una infraestructura de Linux, con el servidor web Apache, base de datos Mysql y Php. Tiene configurada la dirección IP pública 173.231.212.158 para VPS 1 como se detalla en la Tabla 3, y IP Pública 69.167.175.211 para el VPS 2 como se detalla en la Tabla 4. En ambas tablas es posible ver las características tanto de Hardware y Software que tienen instalado, perteneciendo al escenario de pruebas para esta Tesis.

**Tabla 3.** 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 |
| | Herramienta de Criptografía | OpenSSL versión 1.0.2k-fips (26 Jan 2017) |
| | PHP | versión 7.1.28 |
| | Mysql | 10.2.24-MariaDB |

**Fuente:** Elaboración Propia.

**Tabla 4.** 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 |
| | Herramienta de Criptografía | OpenSSL versión 1.0.2k-fips |
| | PHP | versión 5.6 |
| | Mysql | 5.6 |

**Fuente:** Elaboración Propia.

La Figura 9. muestra de una manera gráfica el escenario de pruebas para la medición del rendimiento de los cinco sitios web alojados en el Servidor Web perteneciente a la empresa Web-Out S.A. Por el lado del cliente en estas pruebas se ha hecho uso de Windows 10 como anfitrión y como máquinas virtuales a Centos 7 minimalista y Ubuntu 19; para la virtualización se ha empleado la herramienta Virtual Box en su versión 6.0.6.

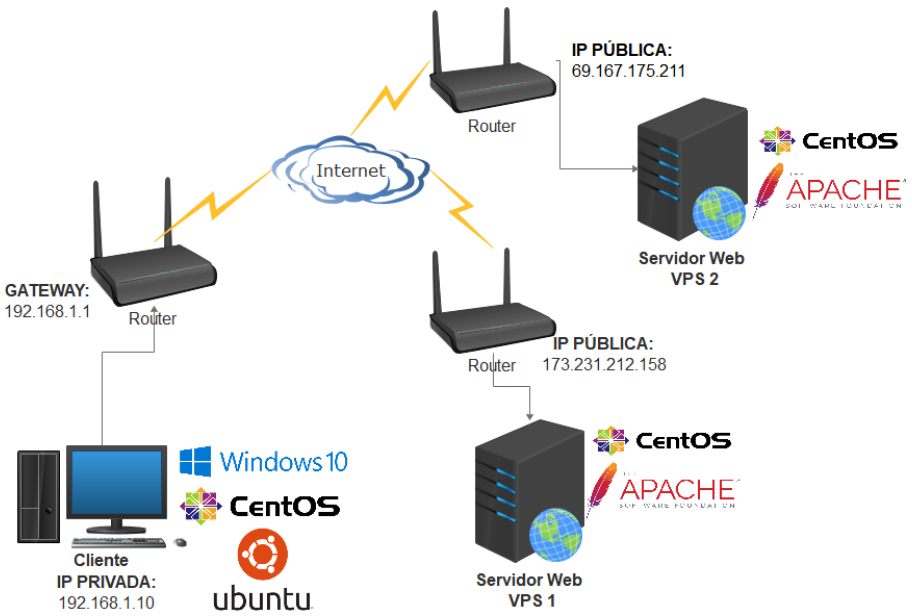



**Figura 9.** Escenario de pruebas para medir el Rendimiento de los cinco sitios web.
**Fuente:** Elaboración Propia.

### B. ¿Los Sitios Web están en Producción?

Los cinco sitios web actualmente se encuentran en producción. A continuación, en la Tabla 5. se detalla el nombre, la dirección URL de cada sitio web, y el VPS donde se encuentra ubicado cada sitio web que son caso de estudio.

**Tabla 5.** Sitios Web, URL de Acceso y ubicación en el VPS de cada sitio web.

| NOMBRE SITIO WEB | URL DE ACCESO | VPS |
|---|---|---|
| Web-Out S.A. | https://www.web-out.com | VPS 1 |
| Facultad de Ciencias Económicas y Administrativas de la UNAS | https://www.fceaunas.edu.pe | VPS 1 |
| Hotel Oro Verde | https://www.hotel-oroverde.com | VPS 2 |
| Hotel Natural Green | https://www.hotelnaturalgreen.com | VPS 1 |
| Cámara de Comercio Canadá - Perú | https://www.canadaperu.org | VPS 1 |

**Fuente:** Elaboración Propia.

### C. ¿Qué pruebas se realizaron para medir el rendimiento?

Se realizo la simulación de una gran cantidad de peticiones al sitio web con la finalidad de obtener los tiempos de carga y velocidad de respuesta de las solicitudes cuando se tiene habilitado y deshabilitado el protocolo SSL/TLS. El tiempo de carga de un sitio web está vinculado a muchos factores, pero en esta investigación nos trataremos de enfocar en el uso del protocolo SSL/TLS.

Se realizarán varias pruebas y con diversas herramientas para poder constatar que la información sea la correcta en todas las mediciones de tiempo de carga, tamaño del sitio web, número de solicitudes del sitio web, vulnerabilidades del sitio web, etc.

**D. ¿Qué herramientas se emplearon para llegar al objetivo?**

Se emplearon herramientas Open Source que permiten realizar test desde un equipo local hasta herramientas en línea el cual puede ser accedido desde Internet; que permitan obtener información respecto al protocolo SSL/TLS, haciendo lo posible de obtener toda la información necesaria desde que un cliente ingresa al sitio web hasta que el sitio termine de cargar con todos los componentes de su vista principal.

- **Wireshark:** Analizar paquetes del Protocolo HTTP y HTTPS de un Sitio Web.
- **Apache Bench:** Herramienta Open Source desarrollada por Apache sirve para realizar pruebas de carga de Sitios Web bajo HTTP o HTTPS. Permite conocer cuantas solicitudes por segundo pueden ser atendidas por el servidor web. Se debe de tener precaución ya que un mal uso puede causar un ataque de Denegación de Servicio.
- **Cipherscan y Analyze.py:** Es una herramienta desarrollada por Mozilla, alojado en el repositorio de GitHub. Permite obtener el orden de cifrado de SSL/TLS de un determinado sitio web teniendo en consideración todas las versiones de SSL/TLS y Analyze.py que permite obtener una serie de recomendaciones divididas en niveles (antiguo, intermedio, moderno) respecto al uso de SSL/TLS.
- **Qualys SSL Labs:** Herramienta creada por Ivan Ristic (investigador especializado en temas de seguridad de aplicaciones web, creador del módulo: modsecurity y apasionado por el protocolo SSL/TLS siendo autor de libros como “Apache Security”, “ModSecurity Handbook”, “Bulletproof SSL and TLS”). Esta herramienta puede ser probado con tan solo tener acceso a Internet, es gratuito y

nos muestra un reporte completo sobre un sitio web, indicando una valoración del sitio respecto a su configuración y características enfocadas en el protocolo SSL/TLS.

- **Open SSL:** es un proyecto desarrollado por Eric Young y Tim Hudson, es software libre y está compuesto por bibliotecas relacionadas a la criptografía siendo pieza clave para el funcionamiento del protocolo SSL/TLS en sus últimas versiones, brindando funciones criptográficas a los navegadores web (para acceso seguro a sitios web por HTTPS). Permite obtener información sobre algoritmos de cifrado, certificados SSL/TLS de los sitios web y validación de un correcto funcionamiento del HTTPS.

- **Pingdom Tools:** Herramienta en línea que permite obtener información de la velocidad de carga de un sitio web, mostrando un detalle del peso por tipo de contenido, número de solicitudes al servidor, puntaje asignado por la herramienta, sugerencias para mejorar el rendimiento, entre otros.

- **A2SV Auto Scanning SSL Vulnerability:** Herramienta que permite obtener vulnerabilidades de un sitio web en relación con el uso del protocolo SSL/TLS.

- **TestSSL:** Herramienta de línea de comandos que permite obtener información de los protocolos y defectos criptográficos que presenta un servidor web respecto al uso del protocolo SSL/TLS.

- **SSLyze:** Herramienta en Python que se ejecuta por la línea de comandos que sirve para analizar las configuraciones del protocolo SSL/TLS conectándose al servidor y probando distintos aspectos de seguridad como ataques a los sitios web con HTTPS.

**E. ¿Qué herramientas se han empleado en cada Sistema Operativo para realizar las diversas pruebas para medir el rendimiento de los sitios web?**

A continuación, se muestra la Tabla 6. el detalle de los Sistemas Operativos junto con la información de hardware y software que se están empleando para las diversas pruebas.

**Tabla 6.** Información técnica de las características de hardware y software empleado para las pruebas de rendimiento.

| | | |
|---|---|---|
| **WINDOWS 10** | **HARDWARE** | |
| | Disco Duro | 1 TB |
| | Memoria RAM | 16 GB |
| | Procesador | x64 |
| | **SOFTWARE** | |
| | SSL Robot versión 1.2.19 | |
| | Nmap 7.70 | |
| | Wireshark versión 3.0.1 | |
| | Qualys. SSL Labs (Online) | |
| **CENTOS 7.6.1810** MINIMALISTA | **HARDWARE** | |
| | Disco Duro | 100 GB |
| | Memoria RAM | 4 GB |
| | Procesador | x64 |
| | **SOFTWARE** | |
| | Apache Bench (AB) versión 2.3 | |
| | OpenSSL 1.1.1 | |
| | Curl 7.64.1 | |
| **UBUNTU 19** GRAFICO | **HARDWARE** | |
| | Disco Duro | 100 GB |
| | Memoria RAM | 4 GB |
| | Procesador | x64 |
| | **SOFTWARE** | |
| | Apache Bench (AB) versión 2.3 | |
| | Tcpdump | |
| | Cipherscan y Analyze.py | |
| | Test SSL | |
| | Curl 7.64.1 | |
| | SSLyze | |

**Fuente:** Elaboración propia.

**F. ¿Qué versiones del Protocolo son los más probables que estén habilitados?**

El soporte a las diversas versiones del protocolo SSL/TLS está estrechamente vinculado con la configuración del servidor, el cual está a cargo del

Administrador Web. Ya que es en la configuración del servidor donde se establecen las versiones de SSL/TLS y suites de cifrado que deben ser soportados cuando accedemos al sitio web; aparte de diversas configuraciones de seguridad que se pueden realizar para brindar una mayor seguridad en la navegación a los clientes. Las versiones más probables que se puedan encontrar son: TLS versión 1.0, TLS versión 1.1, TLS versión 1.2.

## 4.2 Pruebas

### 4.2.1 Fortaleza del Algoritmo de cifrado

La seguridad de las comunicaciones por medio de HTTPS es gracias a la suite de cifrado (compuesta por algoritmos de cifrado simétrica y asimétrica) que se tiene configurado en el Servidor Web, así que realizamos un primer análisis con la herramienta “SSL Robot” para obtener información técnica de los algoritmos empleados durante la conexión a los sitios web.

La herramienta SSL Robot nos permite obtener información valiosa, tales son: IP pública, puerto del servidor, protocolos SSL/TLS habilitados y deshabilitados, validez del certificado, suite de cifrado, entre otros. Esta información será valiosa para poder conocer cuáles son los algoritmos de cifrado que existe en la comunicación y en base a eso poder realizar un análisis de la fortaleza.

A continuación, se detalla en la Tabla 7 la información obtenida con la herramienta SSL Robot, encontrando dos direcciones IP Publicas: 173.231.212.158 (perteneciente al VPS 1) y 69.167.175.211 (perteneciente al VPS 2) debido a que se encuentran en distintos equipos físicos; según lo manifestado por el Webmaster responsable de Web-Out. S.A. para el VPS 2 no es posible realizar instalaciones o

verificación de consumo de memoria debido a que no se tiene control total como en el VPS 1; por ese motivo no es posible ver el consumo de memoria cuando se realizan las pruebas de rendimiento.

**Tabla 7.** Información técnica del lado del servidor obtenida con la herramienta SSL Robot accediendo por medio de HTTPS a los cinco sitios web**.**

| | **Web-Out** | **Facultad de ciencias económicas y administrativas de la UNAS** | **Hotel oro verde** | **Hotel Natural Green** | **Camara 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<br>TLS 1.1<br>TLS 1.0 | TLS 1.2<br>TLS 1.1<br>TLS 1.0 | TLS 1.2<br>TLS 1.1<br>TLS 1.0 | TLS 1.2<br>TLS 1.1<br>TLS 1.0 | TLS 1.2<br>TLS 1.1<br>TLS 1.0 |
| **Protocolos Deshabilitados** | SSL 3.0<br>SSL 2.0 | SSL 3.0<br>SSL 2.0 | SSL 3.0<br>SSL 2.0 | SSL 3.0<br>SSL 2.0 | SSL 3.0<br>SSL 2.0 |
| **Nombre común**<br><br>**Nombre alternativo** | web-out.com<br><br>www.web-out.com | www.fceaunas.edu.pe<br><br>faceaunas.edu.pe | hotel-oroverde.com<br><br>www.hotel-oroverde.com | www.hotelnaturalgreen.com<br><br>hotelnaturalgreen.com | www.canadaperu.org<br><br>canadaperu.org |
| **Periodo de validez del Certificado Digital** | 12/03/2020<br><br>13/03/2017 | 12/07/2019<br><br>12/07/2018 | 06/05/2019<br><br>05/02/2019 | 10/08/2019<br><br>10/08/2018 | 30/08/2019<br><br>30/08/2018 |

**Fuente:** Elaboración propia.

Cuando nos conectamos por medio de HTTPS a los cinco sitios web, lo hace por medio del puerto por defecto 443. Así mismo, todas las versiones de TLS se encuentran habilitados (excepto TLS versión 1.3) y para los de SSL se encuentran deshabilitados en sus versiones: 2.0 y 3.0. Esta información es obtenida en base a la configuración que existe en los servidores web. Finalmente podemos visualizar en la tabla el periodo de validez del certificado digital emitido en formato X.509, siendo generado con nombre común y nombre alternativo para cada sitio web.

En una comunicación mediante HTTP (sin SSL/TLS) no existe ningún proceso de cifrado entre cliente y servidor, siendo totalmente legible y transparente la comunicación (ver Figura 10) encontrándose vulnerable a la captura de paquetes por usuarios malintencionados mediante herramientas de sniffer como Wireshark, Microsoft Message Analyzer, Tcpdump, Windump, etc.

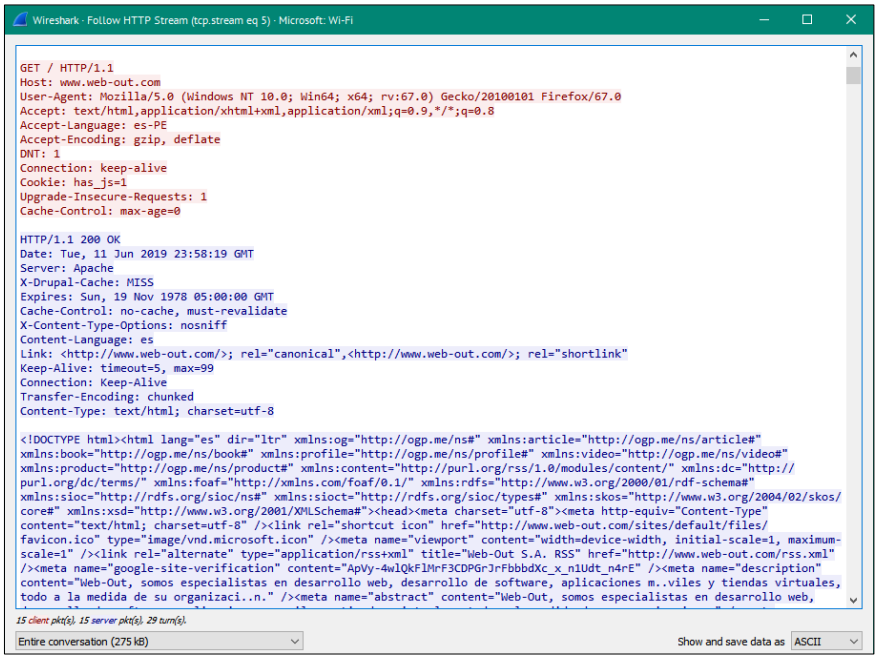



**Figura 10.** Paquetes interceptados cuando se accede al sitio web de Web-Out por HTTP.
**Fuente:** Elaboración propia.

En la Tabla 8 se detalla información del certificado digital de los cinco sitios web, indicando el tipo y tamaño de clave publica, la autoridad certificadora por sus siglas en ingles CA - *Certification Authority* y el algoritmo de firma del Certificado Digital generado para cada sitio web.

Se puede apreciar una similitud de que los cinco sitios web emplean el algoritmo RSA con un tamaño de clave de 2048 bits, la autoridad certificadora raíz para todos es Comodo excepto para el sitio web del Hotel Oro Verde; el tipo de certificado es por validación de dominio para todos los casos, 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 8.** Información del Certificado Digital empleado en la conexión con los cinco sitios web por HTTPS mediante la herramienta SSL Robot.

| | 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 de la UNAS** | 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 |

**Fuente:** Elaboración propia.

Para conocer las preferencias de la suite de cifrado de parte del cliente (navegador Mozilla Firefox) y del servidor; ha sido necesario emplear la herramienta Wireshark (ver Figura 11) y SSL Robot (ver Figura 12). Los resultados de la suite de cifrado se muestran en la Tabla 9. ordenados de manera ascendente según la prioridad de uso por el cliente y por el servidor web. Así mismo, se ha resaltado de negrita la suite de cifrado empleado en la conexión a cada sitio web, después de haber realizado el proceso de negociación conocido como el Protocolo Handshake.

**Tabla 9.** Suite de Cifrado en orden de prioridad del lado del Cliente (Wireshark versión 3.0.1) y Servidor (SSL Robot) en una conexión por HTTPS.

| | PRIORIDAD | SERVIDOR WEB (Suite de Cifrado) | CLIENTE – MOZILLA QUANTUM (Suite de Cifrado) |
|---|---|---|---|
| Web-Out | 1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_AES_128_GCM_SHA256 |
| | **2** | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** | TLS_CHACHA20_POLY1305_SHA256 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | TLS_AES_256_GCM_SHA384 |
| | 4 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 |
| | 5 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** |
| | 6 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 7 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 8 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 |
| | 9 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
| | 10 | TLS_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA |
| Facultad de Ciencias Económicas y Administrativas – UNAS | 1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_AES_128_GCM_SHA256 |
| | **2** | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** | TLS_CHACHA20_POLY1305_SHA256 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | TLS_AES_256_GCM_SHA384 |
| | 4 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 |
| | 5 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** |
| | 6 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 7 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 8 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 |
| | 9 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
| | 10 | TLS_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA |
| Hotel Oro Verde | **1** | **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** | TLS_AES_128_GCM_SHA256 |
| | 2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | TLS_CHACHA20_POLY1305_SHA256 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | TLS_AES_256_GCM_SHA384 |
| | 4 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 |
| | 5 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 |
| | 6 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 7 | TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 8 | TLS_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 |

| | | | |
|---|---|---|---|
| | 9 | TLS_RSA_WITH_AES_256_CBC_SHA256 | **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** |
| | 10 | TLS_RSA_WITH_AES_256_CBC_SHA | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA |
| Hotel Natural Green | 1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_AES_128_GCM_SHA256 |
| | **2** | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** | TLS_CHACHA20_POLY1305_SHA256 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | TLS_AES_256_GCM_SHA384 |
| | 4 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 |
| | 5 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** |
| | 6 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 7 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 8 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 |
| | 9 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
| | 10 | TLS_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA |
| Cámara de Comercio Canadá - Perú | 1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_AES_128_GCM_SHA256 |
| | **2** | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** | TLS_CHACHA20_POLY1305_SHA256 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | TLS_AES_256_GCM_SHA384 |
| | 4 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 |
| | 5 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** |
| | 6 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 7 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
| | 8 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 |
| | 9 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
| | 10 | TLS_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA |

**Fuente:** Elaboración propia.

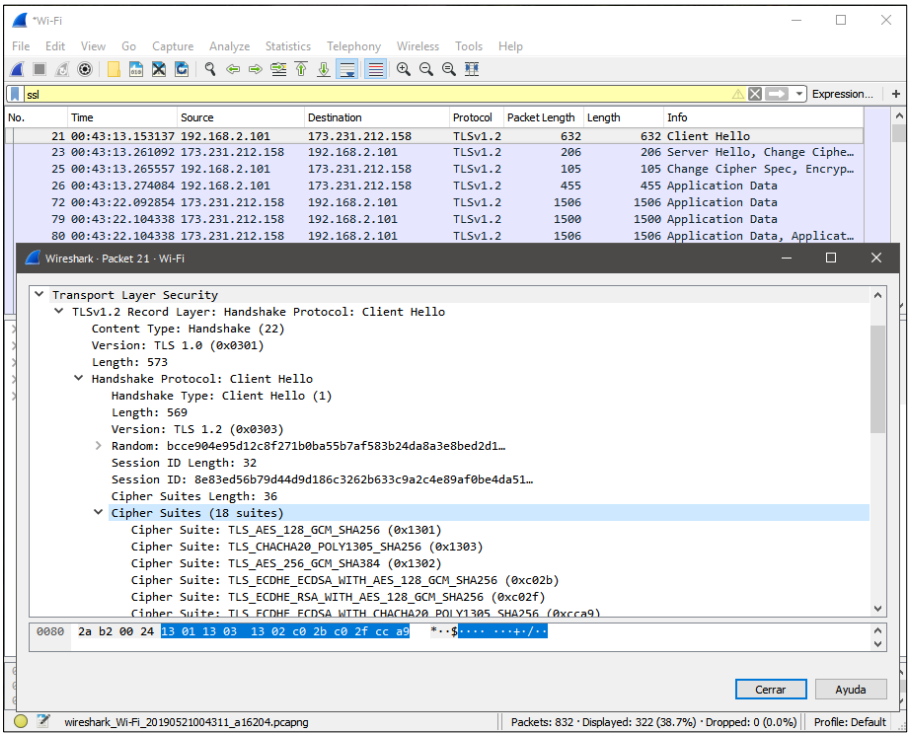



**Figura 11.** Prioridad de Suite de Cifrado de lado del Cliente (Mozilla Firefox) con la herramienta Wireshark versión 3.0.1.
**Fuente:** Elaboración propia.

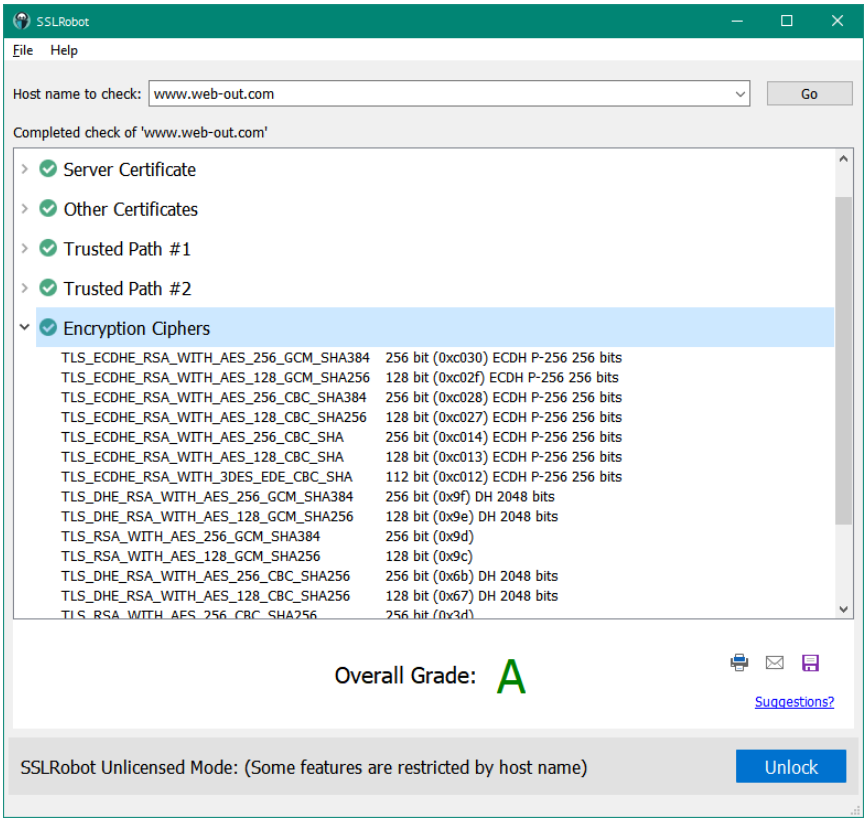



**Figura 12.** Prioridad de Suite de Cifrado de lado del Servidor con la herramienta SSL Robot.
**Fuente:** Elaboración propia.

Realizando un análisis de la suite de cifrado empleado para la conexión a cada sitio web, para todos los casos hace uso del algoritmo de cifrado asimétrico ECDHE, para la firma digital emplea RSA y como cifrado simétrico AES con un tamaño de 128 bits, a continuación, se medirá el tiempo de procesamiento de estos algoritmos.

Mediante la herramienta OpenSSL versión 1.1.1 se ha realizado la prueba de rendimiento de los algoritmos de cifrados ya mencionados, empleados en la comunicación HTTPS a cada sitio web.

En la Tabla 10 se puede visualizar que el algoritmo RSA conforme aumenta la longitud de clave, el proceso de firmado es mucho mas lento que el proceso de verificación de la firma. Asi mismo tambien nos indica que el servidor mediante el algoritmo RSA 2048 bits es posible realizar 331.8 firmas/segundo, en otras palabras puede manejar 331 conexiones TLS nuevas por segundo. Y con el algoritmo ECDSA 256 bits es posible 3572 conexiones TLS por segundo con un proceso de verificación mucho mas lento que el de RSA.

**Tabla 10.** Rendimiento del Algoritmo de firma RSA, DSA Y ECDSA en una comunicación HTTPS obtenido mediante la herramienta OpenSSL v 1.1.1

| 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 |

**Fuente**: Elaboración Propia.

De igual forma, se pasó a realizar un análisis del tiempo de procesamiento del algoritmo AES, Camellia y 3DES de tamaño 128 y 256 bits que son los empleados durante la conexión entre cliente y servidor descritos anteriormente en la Tabla 9.

**Tabla 11.** Tiempo de procesamiento del algoritmo de cifrado simétrico AES, CAMELLIA y 3DES con tamaños de clave 128 y 256.

| | **Tamaño de bloque de entrada** | | | | | |
|---|---|---|---|---|---|---|
| **Tipo de Algoritmo** | **16 bytes** | **64 bytes** | **256 bytes** | **1024 bytes** | **8192 bytes** | **16384 bytes** |
| **AES-128-GCM** | 63230.27k | 185203.67k | 680727.13k | 1131852.5k | 2348395.18k | 2566580.91k |
| **AES-256-GCM** | 46684.71k | 138681.79k | 597250.22k | 926964.05k | 1370298.43k | 1675083.78k |
| **AES-128-CBC** | 80533.2k | 181946.67k | 273705.9k | 297036.46k | 290832.38k | 264820.05k |
| **AES-256-CBC** | 59940.45k | 113123.09k | 156944.47k | 162634.07k | 175289.69k | 170442.75k |
| **CAMELLIA-128-CBC** | 34696.31k | 74764.14k | 107442.09k | 125709.99k | 126118.57k | 130995.54k |
| **CAMELLIA-256-CBC** | 30991.05k | 65137.86k | 88524.80k | 99908.27k | 104240.47k | 105207.13k |
| **DES-EDE3-CBC** | 12319.26k | 13417.86k | 16051.37k | 17309.70k | 17298.77k | 18453.85k |

**Fuente:** Elaboración propia.

En la Tabla 11, se muestra el resumen generado por la herramienta OpenSSL (empleando el comando *openssl speed*), indicando el tipo de algoritmo simétrico empleado con diferentes tamaños de clave (128 y 256), así también se encuentran campos con distintos tamaños de bloque de entrada que se emplean durante el proceso de cifrado y finalmente en la parte central los valores están en Kilobytes por segundo.

En la Figura 13 se evidencia la diferencia de los algoritmos simétricos AES, Camellia y 3DES. En base a las pruebas realizadas, AES-128-GCM obtiene el mayor rendimiento en comparación con los otros algoritmos de cifrado, explicando

un mejor desempeño y observando porque es el más utilizado en la mayoría de las comunicaciones con los 5 sitios web.

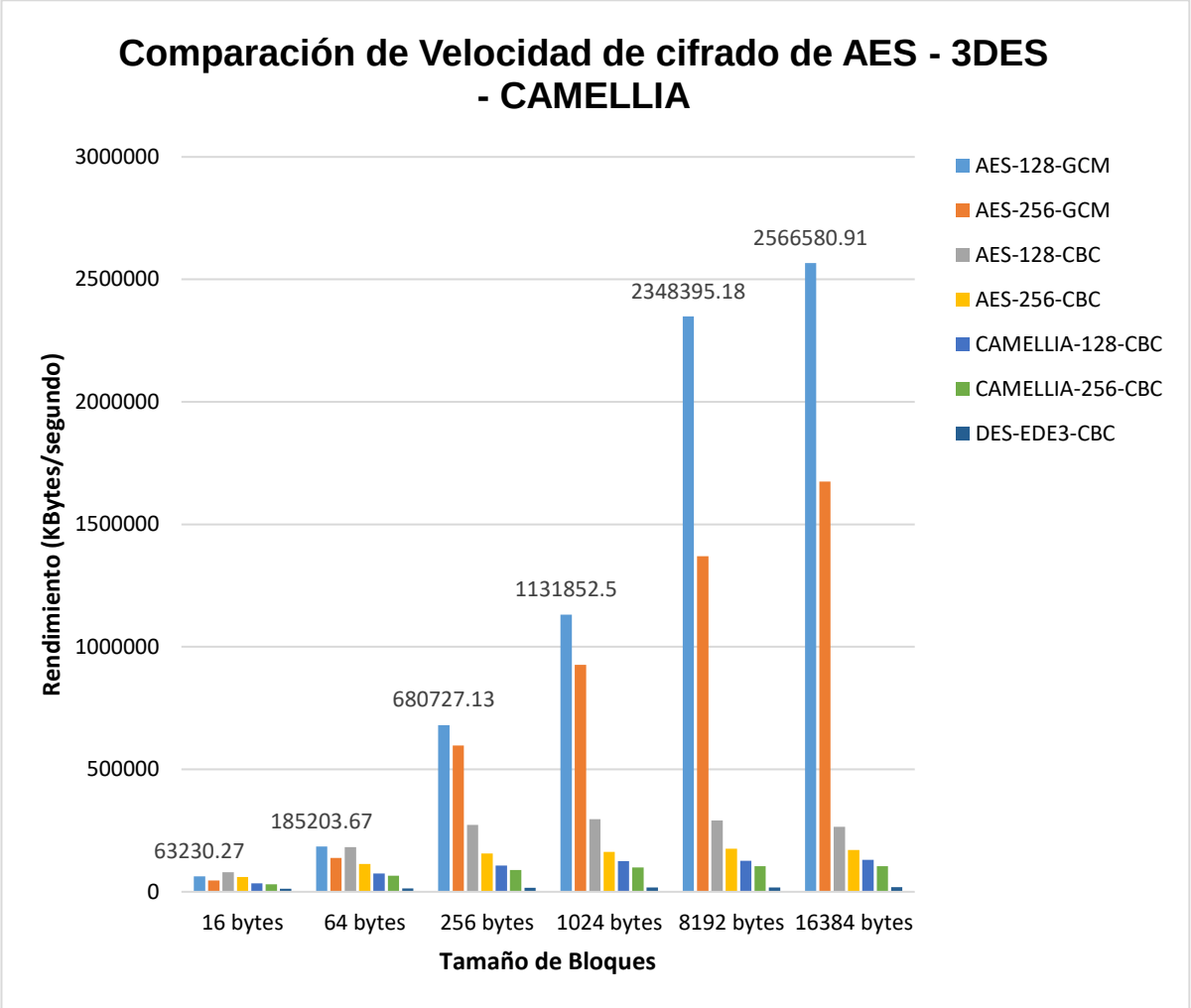



**Figura 13.** Comparación de velocidad de los algoritmos de cifrado AES, Camellia y 3DES.
**Fuente:** Elaboración propia.

## A. Costo Computacional

El costo computacional del VPS 1 ha sido analizado mediante la herramienta HTOP, conocido como una herramienta para la monitorización, administración y visor de procesos interactivo para los sistemas vasados en Unix (ver Figura 14), obteniéndose como resultado lo descrito en la Tabla 12.

Para el VPS 2 que es donde se encuentra alojado el sitio web Hotel Oro Verde, no ha sido posible obtener el costo computacional porque no se cuenta con la administración del servidor (acceso al terminal).

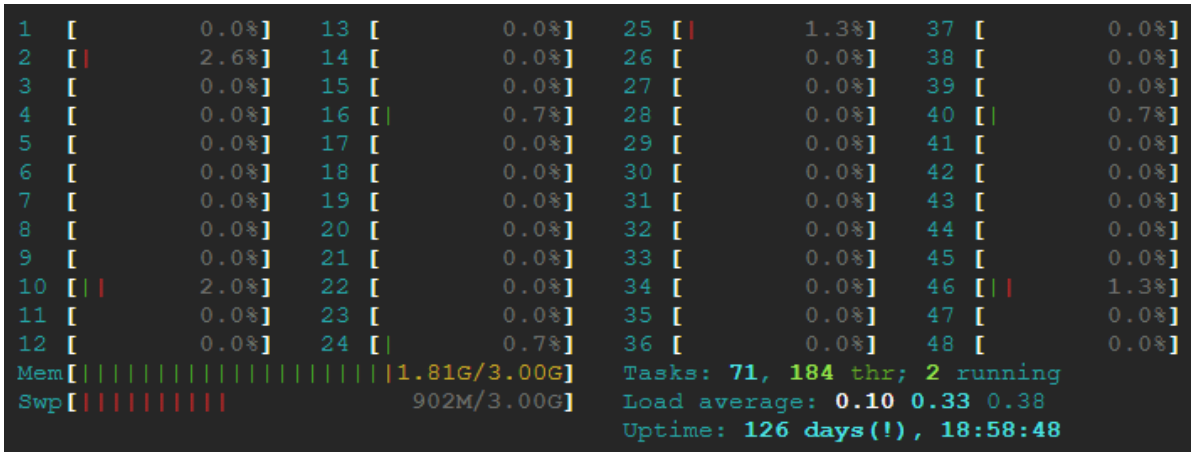



**Figura 14.** Costo computacional del Servidor Web (VPS 1).
**Fuente:** Elaboración propia.

En la Tabla 12 se puede apreciar el costo computacional que exige el acceder a los cinco sitios web con 500 solicitudes y una concurrencia de 20 peticiones (test realizado con Apache Bench desde máquina Ubuntu detallado en la Tabla 6), por medio de HTTP y HTTPS. El campo de sitios web corresponde a los cinco sitios web que son caso de estudio, seguido de la información del costo computacional que se obtiene cuando: no se realizan solicitudes al servidor web, cuando existe solicitudes al servidor web por HTTP y cuando las solicitudes al servidor son por HTTPS.

**Tabla 12.** Costo computacional del servidor Web con 500 solicitudes y 20 peticiones concurrentes con acceso a HTTP y HTTPS.

| Sitios Web | Servidor Web Sin Solicitudes Web | | | | | Servidor Web con 500 solicitudes (20 concurrencia) accedido por HTTP | | | | | Servidor Web con 500 solicitudes (20 concurrencia) accedido por HTTPS | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Mem. RAM (3 GB) | Mem. SWAP (3 GB) | N° Procesos | N° Max. Hilos corriendo | Max. Promedio de Carga | Mem. RAM (3 GB) | Mem. SWAP (3 GB) | N° Procesos | N° Max. Hilos corriendo | Max. Promedio de Carga | Mem. RAM (3 GB) | Mem. SWAP (3 GB) | N° Procesos | N° Max. Hilos corriendo | Max. Promedio de Carga |
| **Web-Out** | 1.85 GB | 840 MB | 66 | 1 | 0.10 | 1.89 GB | 880 MB | 73 | 8 | 3.01 | 1.82 GB | 909 MB | 77 | 8 | 3.70 |
| **Facultad de Ciencias Económicas y Administrativas de la UNAS** | 1.85 GB | 840 MB | 66 | 1 | 0.10 | 1.80 GB | 920 MB | 75 | 2 | 0.49 | 1.81 G | 922 MB | 80 | 5 | 0.59 |
| **Hotel Oro Verde** | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| **Hotel Natural Green** | 1.85 GB | 840 MB | 66 | 1 | 0.10 | 1.88 GB | 893 MB | 76 | 6 | 3.20 | 1.94 GB | 890 MB | 75 | 6 | 3.46 |
| **Cámara de comercio Canadá - Perú** | 1.85 GM | 840 MB | 66 | 1 | 0.10 | 1.57 GB | 1.10 GB | 74 | 5 | 4.13 | 1.89 GB | 918 MB | 78 | 6 | 3.87 |

**Fuente:** Elaboración propia.

## B. Análisis de Resultados

Se ha podido identificar que el algoritmo de firma empleado por los cinco sitios web en su mayoría es RSA, este algoritmo se caracteriza por ser seguro y eficiente llegando a 331 firmas/segundo, representando 331 conexiones TLS por segundo. Así mismo, el algoritmo ECDSA también es una buena opción apareciendo en algunas suites de cifrado. ECDSA tiene una velocidad de firmado mucho mayor que el de RSA, pero el proceso de verificación de la firma es mucho más lento que RSA, así como se muestra en la Figura 15**.**

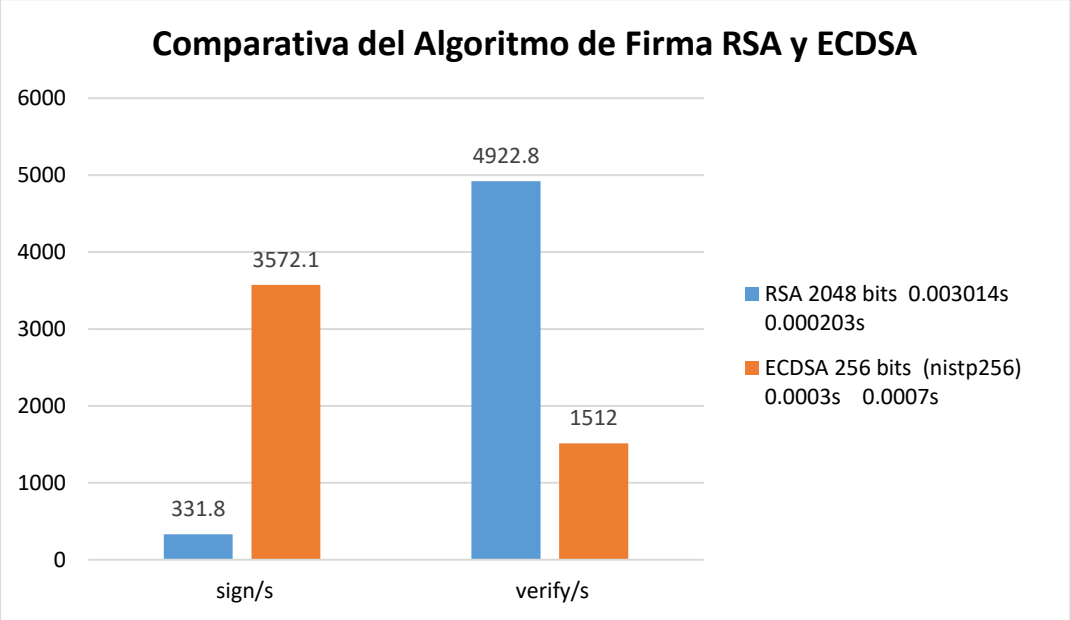



**Figura 15.** Velocidad de Firmado y verificación de la Firma de RSA y ECDSA.
**Fuente:** Elaboración propia.

Las pruebas realizadas para el algoritmo simétrico fueron realizadas satisfactoriamente, donde el algoritmo de cifrado simétrico AES-128-GCM y AES-256-GCM son los más eficientes en comparación con CAMELLIA y 3DES, siendo uno de los motivos por el cual se utiliza en las cinco suites de cifrado elegidas al conectarse a los 5 sitios web.

Finalmente se realizó la medición del costo computacional del servidor cuando realiza 500 solicitudes con 20 peticiones concurrentes, de las cuales el rendimiento no varía significativamente, así como se muestra en la Tabla 13.

**Tabla 13.** Resumen del costo computacional por HTTP y HTTPS con 500 solicitudes y una concurrencia de 20 peticiones.

| | **Servidor sin Solicitudes** | **Servidor con solicitudes HTTP** | **Servidor con Solicitudes HTTPS** | **Diferencia del costo computacional entre HTTP y HTTPS** |
|---|---|---|---|---|
| Mem. RAM (3GB) | 1.85 GB | 1.785 GB | 1.865 GB | 4% |
| Mem. SWAP (3 GB) | 840 GB | 673.525 GB | 909.75 GB | 35% |
| N° Procesos | 66 | 74.5 | 77.5 | 4% |
| N° Max. Hilos corriendo | 1 | 5.25 | 6.25 | 19% |
| Max. Promedio de Carga | 0.1 | 2.7075 | 2.905 | 7% |

**Fuente:** Elaboración propia.

En la Tabla 13 se puede apreciar que el consumo de memoria RAM aumenta en un 4%, el uso de la memoria de intercambio (SWAP) aumenta en un 35%, el número de procesos se incrementan en un 4%, y respecto al número máximo de hilos corriendo se incrementa en 19%, para todos los casos cuando se accede por medio de HTTPS. Los valores son más altos cuando el acceso es por HTTPS que cuando se accede por medio de HTTP.

### 4.2.2 Rendimiento frente a ataques

Las vulnerabilidades que se puedan encontrar en un Sitio Web van de la mano con los archivos de configuración del protocolo SSL/TLS, en Apache el archivo es ssl.conf el cual se agrega gracias a la instalación del módulo de nombre mod_ssl. En este archivo ssl.conf es donde se configura las características de seguridad enfocados al protocolo SSL/TLS que cumplirá cuando se accede al sitio web.

En la Figura 16 se muestra un reporte realizado con la herramienta “A2SV Auto Scanning SSL Vulnerability” alojado en GitHub e instalado en Ubuntu 19, obteniendo como resultado las vulnerabilidades de “Cifrado Anónimo” y CRIME (SPDY) en base a la configuración del servidor web (VPS 1).

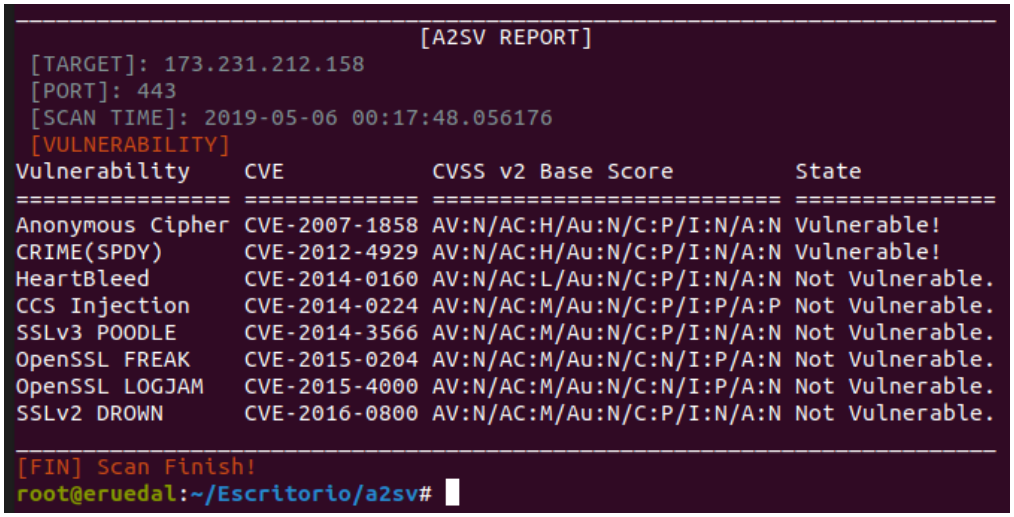



**Figura 16.** Reporte de vulnerabilidades encontradas al Servidor web con la herramienta A2SV Auto Scanning SSL Vulnerability.
**Fuente**: Elaboración propia.

La importancia de contar con un navegador actualizado hace que soporte las suites de cifrado más actuales y por ende emplee una clave de cifrado mucho más segura (fortaleza de la clave de cifrado), a diferencia de un navegador desactualizado.

A continuación, en la Tabla 14 se describe la suite de cifrado empleado por cada navegador cuando es accedido a los cinco sitios web. Así también, se muestra el tamaño de clave empleado y la versión del Protocolo SSL/TLS acordado entre cliente y servidor.

**Tabla 14.** Suite de cifrado, tamaño de clave y versión de TLS empleado en la comunicación con el sitio web.

| Sitios Web/ Navegador | Suite de Cifrado Elegido | Tamaño de Clave | Versión de TLS |
|---|---|---|---|
| **Web-Out** | | | |
| Google Chrome | ECDHE_RSA, AES_128_GCM | P-256 | TLS 1.2 |
| Mozilla v. 66.0.3 | ECDHE_RSA_WITH_AES_128_GCM_SHA256 | 128 bits | TLS 1.2 |
| Opera v. 60 | ECDHE_RSA, AES_128_GCM | P-256 | TLS 1.2 |
| Internet Explorer versión 11 | AES 256, ECDH 256 | 256 | TLS 1.2 |
| **Facultad de Ciencias Económicas y Administrativas de la UNAS** | | | |
| Google Chrome v. 74 | ECDHE_RSA, AES_128_GCM | P-256 | TLS 1.2 |
| Mozilla v. 66.0.3 | ECDHE_RSA_WITH_AES_128_GCM_SHA256 | 128 bits | TLS 1.2 |
| Opera v. 60 | ECDHE_RSA, AES_128_GCM | P-256 | TLS 1.2 |
| Internet Explorer v. 11 | AES 256, ECDH 256 | 256 | TLS 1.2 |
| **Hotel Oro verde** | | | |
| Google Chrome v. 74 | ECDHE_RSA, AES_256_GCM | P-256 | TLS 1.2 |
| Mozilla v. 66.0.3 | ECDHE_RSA_WITH_AES_256_GCM_SHA384 | 256 bits | TLS 1.2 |
| Opera v. 60 | ECDHE_RSA, AES_256_GCM | P-256 | TLS 1.2 |
| Internet Explorer v. 11 | AES 256, ECDH 256 | 256 | TLS 1.2 |
| **Hotel Natural Green** | | | |
| Google Chrome v. 74 | ECDHE_RSA, AES_128_GCM | P-256 | TLS 1.2 |
| Mozilla v. 66.0.3 | ECDHE_RSA_WITH_AES_128_GCM_SHA256 | 128 bits | TLS 1.2 |
| Opera v. 60 | ECDHE_RSA, AES_128_GCM | P-256 | TLS 1.2 |
| Internet Explorer v. 11 | AES 256, ECDH 256 | 256 | TLS 1.2 |
| **Cámara de Comercio Canadá - Perú** | | | |
| Google Chrome v. 74 | ECDHE_RSA, AES_128_GCM | P-256 | TLS 1.2 |
| Mozilla v. 66.0.3 | ECDHE_RSA_WITH_AES_128_GCM_SHA256 | 128 bits | TLS 1.2 |
| Opera v. 60 | ECDHE_RSA, AES_128_GCM | P-256 | TLS 1.2 |
| Internet Explorer v. 11 | AES 256, ECDH 256 | 256 | TLS 1.2 |

**Fuente:** Elaboración propia.

- **Análisis de Resultados**

El tamaño de las claves empleadas en la comunicación por medio de SSL/TLS con los cinco sitios web son de 128 y de 256 bits, encontrándose en un rango intermedio. La versión del protocolo TLS versión 1.2 es establecida para la conexión con los cinco sitios web, permitiendo protección frente a ataques que son comunes en sus versiones anteriores.

Los algoritmos de cifrado simétrico, asimétrico, algoritmo de firma y de hash poseen tamaños que brindan una protección aceptable frente a las diversas vulnerabilidades encontradas en sus versiones anteriores.

### 4.2.3 Tiempo de procesamiento

El tiempo de procesamiento es medido desde que el cliente solicita el servicio web al servidor y hasta que este devuelva con éxito lo solicitado, para esto se ha dividido en dos indicadores, siendo el tiempo de carga y la velocidad de atención de solicitudes por segundo.

Aparte de existir sobrecarga por medio de las operaciones criptográficas realizadas en el protocolo SSL/TLS por cada sitio web, también otro síntoma es la latencia, ya que el tener un alto valor de latencia es síntoma de que el rendimiento no es muy bueno.

Tener un alto valor de latencia aparte de perjudicar en el rendimiento podría estar perjudicando en los beneficios para la empresa, (Ristic, 2014) ha citado una idea publicada por Make Data en 2006. Según esta cita, para la empresa Amazon el tener un aumento de 100 ms en la latencia le cuesta 1% de sus ingresos. En la Figura 17 se muestra los tiempos aproximados de latencia existentes en una comunicación por HTTPS.

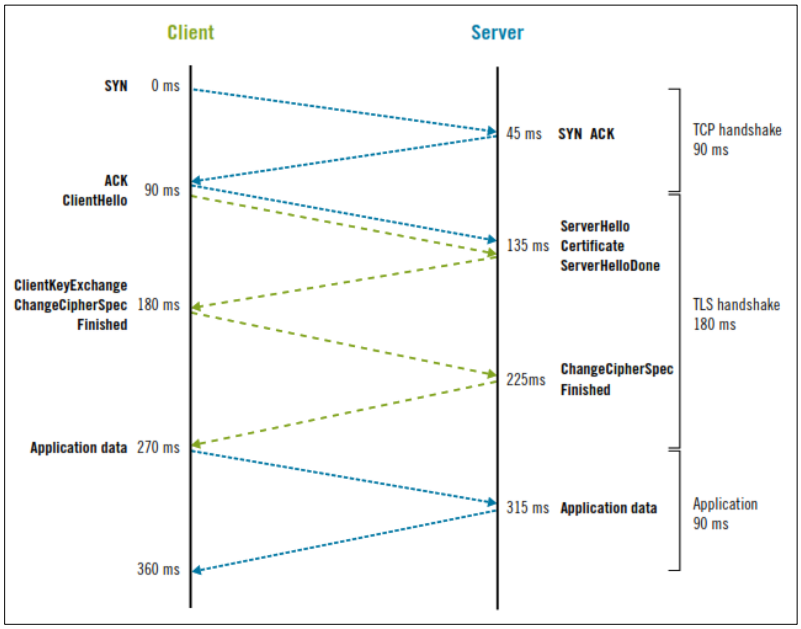



**Figura 17.** Latencias de TCP Handshake y TLS Handshake.
**Fuente:** (Ristic, 2014, pág. 271).

La latencia ha sido medida haciendo uso de la herramienta Ping, el cual lo encontramos en los distintos sistemas operativos. Se realizaron 10 pruebas de latencia para cada sitio web habilitado con el protocolo SSL/TLS así como se detalla en la Tabla 15 mostrado a continuación.

**Tabla 15.** Tiempos de Latencia en milisegundos (ms) de los cinco sitios web con HTTPS.

| HTTPS | Latencia - Milisegundos (Herramienta Ping) | | | | | | | | | | Promedio: |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Web-Out** | 114 | 114 | 114 | 113 | 112 | 114 | 113 | 115 | 114 | 114 | 114 ms |
| **Facultad de Ciencias Económicas y Administrativas de la UNAS** | 113 | 114 | 114 | 114 | 115 | 115 | 114 | 114 | 114 | 113 | 114 ms |
| **Hotel Oro Verde** | 123 | 122 | 124 | 124 | 129 | 123 | 123 | 123 | 122 | 122 | 124 ms |
| **Hotel Natural Green** | 114 | 113 | 115 | 114 | 114 | 115 | 114 | 114 | 115 | 114 | 114 ms |
| **Camara de comercio Canadá - Perú** | 114 | 114 | 115 | 114 | 113 | 113 | 112 | 115 | 114 | 114 | 114 ms |

**Fuente:** Elaboración Propia.

En la Tabla 15, se obtuvo el promedio de latencia de 114 ms para los sitios web de Web-Out, Facultad de Ciencias Económicas y Administrativas-UNAS, Hotel Natural Green y Cámara de Comercio de Canadá; el cual representa el tiempo que tarda en recibir un paquete del servidor (VPS 1). Y para el sitio web Hotel Oro Verde se obtiene una latencia de 124 ms.

- **Tiempo de carga de cada sitio web.**

La Tabla 16. está conformada por un resumen de 5 pruebas realizadas a cada sitio web (Anexo 5) administrados por la empresa Web-Out, la herramienta empleada fue el navegador Mozilla Quantum v.66.0.3 con el cual se ha podido recabar dicha información.

Se segmentaron las pruebas cuando se emplea HTTP y HTTPS, así también se especificó la versión del protocolo siendo para todos HTTP/1.1. Para los campos de número de solicitudes y tiempos de carga de todas las solicitudes vienen a ser el promedio de 5 pruebas realizadas a cada sitio web, esto con el objetivo de obtener una mayor precisión en los resultados. También se puede apreciar en el campo de servidor, que en todos los casos el servidor web empleado es Apache.

Entre las configuraciones que favorecen a un mejor rendimiento de los sitios web se puede visualizar que existen conexiones persistentes (*Keep alive*) habilitadas en el servidor, que permite la atención de múltiples sesiones por una sola conexión. Así también se encuentra habilitado en el servidor para el sitio web del Hotel Oro Verde la compresión gzip para los contenidos que son transmitidos por el servido mejorando el rendimiento de los sitios web, en los demás sitios esta característica se encuentra deshabilitada; y finalmente si se está utilizando la navegación estricta por HSTS el cual obliga a usar una conexión por HTTPS sin pasar por una redirección desde HTTP.

**Tabla 16.** Resumen de la información técnica y promedio de tiempo de carga de cinco sitios web realizado con el navegador Mozilla Quantum v. 66.0.5.

| Sitio Web: | HTTP/HTTPS | Versión de Protocolo HTTP | Número de Solicitudes | Tiempo en Cargar todas las Solicitudes | Servidor | Conexiones Persistentes (*Keep Alive*) | Codificación del contenido | Seguridad de Transporte Estricto (*HSTS*) |
|---|---|---|---|---|---|---|---|---|
| www.web-out.com | HTTP | HTTP/1.1 | 86 | 8.784 segundos | Apache | timeout=5 max= 100 | - | NO |
| www.fceaunas.edu.pe | HTTP | HTTP/1.1 | 106 | 6.386 segundos | Apache | timeout=5 max= 100 | - | NO |
| www.hotel-oroverde.com | HTTP | HTTP/1.1 | 94 | 18.692 segundos | Apache | - | gzip | NO |
| www.hotelnaturalgreen.com | HTTP | HTTP/1.1 | 107 | 9.572 segundos | Apache | timeout=5 max= 100 | - | NO |
| www.canadaperu.org | HTTP | HTTP/1.1 | 146 | 20.234 segundos | Apache | timeout=5 max= 100 | - | NO |
| www.web-out.com | HTTPS | HTTP/1.1 | 86 | 10.644 segundos | Apache | timeout=5 max= 100 | - | NO |
| www.fceaunas.edu.pe | HTTPS | HTTP/1.1 | 106 | 6.5 segundos | Apache | timeout=5 max= 100 | - | NO |
| www.hotel-oroverde.com | HTTPS | HTTP/1.1 | 94 | 19.842 segundos | Apache | - | gzip | NO |
| www.hotelnaturalgreen.com | HTTPS | HTTP/1.1 | 107 | 9.906 segundos | Apache | timeout=5 max= 100 | - | NO |
| www.canadaperu.org | HTTPS | HTTP/1.1 | 146 | 21.324 segundos | Apache | timeout=5 max= 100 | - | NO |

**Fuente:** Elaboración Propia.

- **Análisis de Resultados**

Se ha podido obtener un promedio de la latencia a cada sitio web cuando es accedido desde una red local, teniendo un promedio de 114 milisegundos y 124 milisegundos.

Asimismo, se ha logrado obtener el tiempo de carga de cada sitio web obteniendo el porcentaje de incremento del tiempo de carga de cada sitio web cuando es accedido por HTTPS y HTTP. En la Tabla 17 y el campo de título "% de Incremento del tiempo de cada sitio web", se ha empleado la siguiente formula de nombre tasa de crecimiento (Pallmall, 2014).

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

***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 caga total por HTTP" para el mismo sitio web, el cual nos permitió calcular el incremento porcentual existente entre estos dos tiempos.

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

Como antecedente, dicha fórmula también fue empleada en la tesis de Título "Implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte 2016" (Ariansen Moncada & Rojas Diaz, pág. 111), 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.

**Tabla 17.** Diferencia de Número de solicitudes y Tiempo de carga total del Sitio Web.

| Sitio Web | Núm. de Solicitudes HTTP | Núm. 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 segundos | 10.300 segundos | 15% |
| fceaunas.edu.pe | 106 | 106 | 6.386 segundos | 6.500 segundos | 2% |
| hotel-oroverde.com | 94 | 94 | 18.692 segundos | 19.842 segundos | 6% |
| hotelnaturalgreen.com | 107 | 107 | 9.572 segundos | 9.906 segundos | 3% |
| canadaperu.org | 146 | 146 | 20.234 segundos | 21.324 segundos | 5% |

**Fuente:** Elaboración Propia.

Se ha podido determinar que el tiempo de carga de los sitios web cuando tienen habilitado el protocolo SSL/TLS (HTTPS) es mayor que cuando se accede por HTTP. Existiendo una variación del tiempo de carga de: 15% (aprox. 1.37 segundos) para el Sitio Web de la empresa Web-Out. S.A., un 2% (aprox.0.2 segundos) para el sitio web de la FCEA-UNAS, un 6% (aprox. 1.5 segundos) para el sitio web del Hotel Oro Verde, un 3% (aprox. 0.334 segundos) para el sitio web del Hotel Natural Green y un 5% (aprox. 1.09 segundos) para el sitio web de la Cámara de Comercio de Canadá - Perú.

### 4.2.4 Nivel de solicitudes de usuarios

Para medir el tiempo de carga de cada sitio web, se ha hecho uso de la herramienta Apache Bench, el cual es una herramienta que viene junto con la instalación de apache dentro de un servidor web, o se puede instalar de manera independiente como una herramienta de pruebas dentro de los sistemas operativos como Windows y Linux.

Se realizaron 5 pruebas de rendimiento a cada sitio web (Anexo 4) con la finalidad de obtener un valor promedio con mayor precisión, obteniendo tiempo de la prueba (*Time Taken*) y media de peticiones por segundo (*Request per Second - mean*) por parte del servidor, el resumen de estas cinco pruebas por cada sitio web se describen a continuación.

**Tabla 18.** Resumen de pruebas de rendimiento de 1,100 y 500 solicitudes con peticiones concurrentes de 1, 20, 40, 60, 80 y 100 al sitio web de Web-Out S.A.

| **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** |

**Fuente:** Elaboración Propia.

En la Tabla 18, se aprecia el resumen de la duración de la prueba y la Media de peticiones atendidas por segundo realizadas al sitio web de Web-Out S.A. (*www.web-out.com*) alojado en el servidor web del VPS 1. La duración de la prueba con 1, 100 y 500 solicitudes habiendo una concurrencia de peticiones de 1, 20, 40,

60, 80 y 100 fueron realizados sin complicaciones, no existiendo error de solicitudes (*failed requests*) durante las pruebas realizadas.

Así mismo también podemos ver la diferencia de los valores de duración de la prueba cuando se accede al sitio web por HTTP y HTTPS, existiendo un promedio de 0.7 segundos mayor cuando la prueba es al sitio web habilitado por HTTPS y un promedio de 2.277 solicitudes/segundos atendidas mucho más rápido cuando se accede al sitio web por medio de HTTP.

En la Tabla 19, se aprecia el resumen de la duración de la prueba y la Media de peticiones atendidas por segundo realizadas al sitio web de la Facultad de Ciencias Económicas y Administrativas de la UNAS (*www.fceaunas.edu.pe*) alojado en el servidor web del VPS 1. La duración de la prueba con 1, 100 y 500 solicitudes habiendo una concurrencia de peticiones de 1, 20, 40, 60, 80 y 100 fueron realizados sin complicaciones, no existiendo error de solicitudes (*failed requests*) durante las pruebas realizadas.

**Tabla 19.** Resumen de pruebas de rendimiento de 1, 100 y 500 solicitudes con peticiones concurrentes de 1, 20, 40, 60, 80 y 100 al sitio web de la Facultad de Ciencias Económicas y Administrativas de la UNAS.

| **WEB2 - (www.fceaunas.edu.pe/) - 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** | 0.056 | 18.182 | 0.037 | 27.680 | **0.02** | **9.50** |
| **100** | **20** | 0.880 | 114.286 | 0.845 | 119.144 | **0.04** | **4.86** |
| | **40** | 0.904 | 110.960 | 0.892 | 112.376 | **0.01** | **1.42** |
| | **60** | 1.039 | 104.644 | 0.790 | 126.730 | **0.25** | **22.09** |
| | **80** | 0.998 | 100.850 | 0.722 | 139.420 | **0.28** | **38.57** |
| | **100** | 0.833 | 121.150 | 0.706 | 142.168 | **0.13** | **21.02** |
| **500** | **20** | 5.136 | 97.498 | 4.111 | 124.744 | **1.02** | **27.25** |
| **PROMEDIO:** | | | | | | **0.25** | **17.82** |

**Fuente:** Elaboración Propia.

Así mismo también podemos ver la diferencia de los valores de duración de la prueba cuando se accede al sitio web por HTTP y HTTPS, existiendo un promedio de 0.25 segundos mayor cuando la prueba es al sitio web habilitado por HTTPS y un promedio de 17.82 de solicitudes/segundos atendidas mucho más rápido cuando se accede al sitio web por medio de HTTP.

En la Tabla 20, se aprecia el resumen de la duración de la prueba y la Media de peticiones atendidas por segundo realizadas al sitio web de Hotel Oro Verde (*www.hotel-oroverde.com*) alojado en el servidor web del VPS 2. La duración de la prueba con 1, 100 y 500 solicitudes habiendo una concurrencia de peticiones de 1, 20, 40, 60, 80 y 100 fueron realizados con algunas complicaciones, existiendo error de solicitudes (*failed requests*) durante las pruebas realizadas a causa de que el tamaño del sitio web era variable y el servidor no era posible responder a todas las solicitudes.

Así mismo también podemos ver la diferencia de los valores de duración de la prueba cuando se accede al sitio web por HTTP y HTTPS, existiendo un promedio de 1.41 segundos mayor cuando la prueba es al sitio web habilitado por HTTPS y un promedio de 3.97 de solicitudes/segundos mucho más rápido cuando se accede al sitio web por medio de HTTP.

**Tabla 20.** Resumen de pruebas de rendimiento de 1, 100 y 500 solicitudes con peticiones concurrentes de 1, 20, 40, 60, 80 y 100 al sitio web Hotel Oro Verde.

| WEB3 - (www.hotel-oroverde.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** | 0.3604 | 2.784 | 0.2812 | 3.568 | **0.08** | **0.78** |
| **100** | **20** | 10.0042 | 10.162 | 9.3436 | 10.73 | **0.66** | **0.57** |
| | **40** | 5.8286 | 23.704 | 4.9756 | 27.006 | **0.85** | **3.30** |
| | **60** | 5.092 | 24.33 | 4.523 | 32.966 | **0.57** | **8.64** |
| | **80** | 6.1134 | 25.37 | 5.3 | 28.894 | **0.81** | **3.52** |
| | **100** | 4.7168 | 27.61 | 2.6666 | 37.496 | **2.05** | **9.89** |
| **500** | **20** | 48.9132 | 10.258 | 44.083 | 11.346 | **4.83** | **1.09** |
| **PROMEDIO** | | | | | | **1.41** | **3.97** |

**Fuente:** Elaboración Propia.

En la Tabla 21, se aprecia el resumen de la duración de la prueba y la Media de peticiones atendidas por segundo realizadas al sitio web del Hotel Natural Green (*www.hotelnaturalgreen.com*) alojado en el servidor web del VPS 1. La duración de la prueba con 1, 100 y 500 solicitudes habiendo una concurrencia de peticiones de 1, 20, 40, 60, 80 y 100 fueron realizados sin complicaciones, no existiendo error de solicitudes (*failed requests*) durante las pruebas realizadas.

Así mismo también podemos ver la diferencia de los valores de duración de la prueba cuando se accede al sitio web por HTTP y HTTPS, existiendo un promedio de 0.52 segundos mayor cuando la prueba es al sitio web habilitado por HTTPS y un promedio de 0.24 de solicitudes/segundos mucho más rápido cuando se accede al sitio web por medio de HTTP.

**Tabla 21.** Resumen de pruebas de rendimiento de 1, 100 y 500 solicitudes con peticiones concurrentes de 1, 20, 40, 60, 80 y 100 al sitio web Hotel Natural Green.

| WEB4 - (www.hotelnaturalgreen.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** | 0.515 | 1.952 | 0.477 | 2.104 | **0.04** | **0.15** |
| **100** | **20** | 13.048 | 7.680 | 12.507 | 8.088 | **0.54** | **0.41** |
| | **40** | 14.388 | 7.296 | 13.766 | 7.638 | **0.62** | **0.34** |
| | **60** | 12.131 | 8.370 | 11.450 | 8.870 | **0.68** | **0.50** |
| | **80** | 13.213 | 7.642 | 12.747 | 7.896 | **0.47** | **0.25** |
| | **100** | 12.674 | 7.960 | 12.401 | 8.072 | **0.27** | **0.11** |
| **500** | **20** | 128.676 | 3.996 | 127.688 | 3.936 | **0.99** | **-0.06** |
| **PROMEDIO** | | | | | | **0.52** | **0.24** |

**Fuente:** Elaboración Propia.

En la Tabla 22, se aprecia el resumen de la duración de la prueba y la Media de peticiones atendidas por segundo realizadas al sitio web de la Cámara de comercio Canadá - Perú (*www.canadaperu.org*) alojado en el servidor web del VPS 1. La duración de la prueba con 1, 100 y 500 solicitudes habiendo una concurrencia de peticiones de 1, 20, 40, 60, 80 y 100 fueron realizados sin complicaciones, no existiendo error de solicitudes (failed requests) durante las pruebas realizadas.

Así mismo también podemos ver la diferencia de los valores de duración de la prueba cuando se accede al sitio web por HTTP y HTTPS, existiendo un promedio de 1.08 segundos mayor cuando la prueba es al sitio web habilitado por HTTPS y un promedio de 0.12 de solicitudes/segundos mucho más rápido cuando se accede al sitio web por medio de HTTP.

**Tabla 22.** Resumen de pruebas de rendimiento de 1, 100 y 500 solicitudes con peticiones concurrentes de 1, 20, 40, 60, 80 y 100 al sitio web Cámara de Comercio Canadá - Perú.

| WEB5 - (www.canadaperu.org) - 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** | 1.135 | 0.890 | 1.090 | 0.920 | **0.04** | **0.03** |
| **100** | **20** | 28.132 | 3.578 | 26.016 | 3.846 | **2.12** | **0.27** |
| | **40** | 27.609 | 3.662 | 27.035 | 3.716 | **0.57** | **0.05** |
| | **60** | 26.405 | 3.796 | 25.095 | 3.998 | **1.31** | **0.20** |
| | **80** | 22.909 | 4.400 | 21.923 | 4.588 | **0.99** | **0.19** |
| | **100** | 25.639 | 3.984 | 25.045 | 4.020 | **0.59** | **0.04** |
| **500** | **20** | 135.782 | 3.688 | 133.857 | 3.758 | **1.93** | **0.07** |
| **PROMEDIO** | | | | | | **1.08** | **0.12** |

**Fuente:** Elaboración Propia.

- **Análisis de Resultados**

Con relación al tiempo de carga de las diversas pruebas realizadas mediante la herramienta Apache Bench la diferencia del tiempo promedio de carga entre HTTPS (conectándose por TLS versión 1.2) y HTTP para cada sitio web es:

- Existe 0.7 segundos de diferencia de tiempo de carga para el sitio Web-Out. S.A. equivalente a un incremento de 11% para una conexión por HTTPS.
- Existe 0.25 segundos de diferencia para el sitio web de la FCEA – UNAS equivalente a un incremento de 18% para una conexión por HTTPS.
- Existe 1.41 segundos de diferencia para el sitio web Hotel Oro Verde equivalente a un incremento de 4% para una conexión por HTTPS.
- Existe 0.52 segundos para el sitio web Hotel Natural Green equivalente a un incremento de 17% para una conexión por HTTPS.

- Existe 1.08 segundos para el sitio web de la Cámara de comercio Canadá-Perú; siendo en todos los casos mayor el tiempo de carga cuando se accede por HTTPS.

**Tabla 23.** Duración del Test (*Time taken*) y Media de peticiones por segundo (*Request per Second*) atendidas por el servidor entre HTTP y HTTPS

| Sitio Web | Diferencia de Duración del Test entre HTTP y HTTPS | % de diferencia de Duración del Test entre HTTP y HTTPS | Diferencia de Peticiones atendidas entre HTTP y HTTPS | % de diferencia de Peticiones atendidas entre HTTP y HTTPS |
|---|---|---|---|---|
| Web-Out | 0.7 segundos | 11% | 2.227 #/s | 11% |
| Facultad de Ciencias Económicas y Administrativas de la UNAS | 0.25 segundos | 18% | 17.82 #/s | 23% |
| Hotel Oro Verde | 1.41 segundos | 4% | 3.97 #/s | 4% |
| Hotel Natural Green | 0.52 segundos | 17% | 0.24 #/s | 20% |
| Cámara de comercio Canadá - Perú | 1.08 segundos | 4% | 0.12 #/s | 4% |

**Fuente:** Elaboración propia.

Asimismo, se puede apreciar en la Tabla 23, la velocidad de diferencia de peticiones atendidas por el servidor cuando accedemos por HTTPS y HTTP, y el porcentaje de diferencia de la velocidad de respuesta por parte del Servidor (*Request per Second*); existiendo una mayor velocidad de respuesta ante las peticiones cuando se accede por HTTP (sin SSL/TLS).

### 4.2.5 Transferencia de Información

Existen diversos tipos de contenido que son intercambiados entre el cliente (navegador) y el servidor web; como imágenes, videos, archivos CSS, archivos JavaScript, archivos HTML, entre otros.

A continuación, se muestra un resumen del número de solicitudes y el porcentaje del tipo de contenido que es solicitado al servidor por el navegador cuando accedemos a los cinco sitios web.

#### A. Web-Out S.A.

El peso del sitio web cuando ingresamos a Web - Out S.A. es de 1.4 MB, en la que el 52.33% son ocupados por imágenes, seguido de un 25.93% de archivos Script, y un 12.97% para los archivos de fuente, un 5.45% para archivos CSS y finalmente un 3.32% para el archivo HTML (ver Figura 18).

| CONTENT TYPE | PERCENT | SIZE |
|---|---|---|
| Image | 52.33% | 716.0 KB |
| Script | 25.93% | 354.8 KB |
| Font | 12.97% | 177.5 KB |
| CSS | 5.45% | 74.6 KB |
| HTML | 3.32% | 45.4 KB |
| Total | 100.00% | 1.4 MB |

**Figura 18.** Tamaño del contenido por tipo de contenido del sitio web de Web-Out. S.A.
**Fuente:** Pingdom Tools.

Respecto al número de solicitudes por tipo de contenido, tal como se detalla en la Figura 19 existe 42 solicitudes al tipo de contenido imagen (42 imágenes que se cargan), seguido de los archivos script, luego los archivos CSS con 10

solicitudes, para los archivos de fuentes 4 solicitudes y finalmente para los archivos HTML 1 solicitud.

| CONTENT TYPE | PERCENT | REQUESTS |
|---|---|---|
| Image | 50.60% | 42 |
| Script | 31.33% | 26 |
| CSS | 12.05% | 10 |
| Font | 4.82% | 4 |
| HTML | 1.20% | 1 |
| Total | 100.00% | 83 |

**Figura 19.** número de solicitudes por tipo de contenido del sitio web de Web-Out. S.A.
**Fuente:** Pingdom Tools.

### B. Facultad de Ciencias Económicas y Administrativas - UNAS

El peso total del sitio web es de 2.1 MB, donde el uso de imágenes en la vista principal ocupa un 29.88% con un tamaño de 632.0 KB logrando ser el tipo de archivo más pesado, luego sigue los archivos Java Script ocupando un 26.30%, seguido de los archivos de fuente ocupando un 24.04%, los archivos CSS con un 18.19%, y finalmente archivos HTML ocupando un 1.60% del peso total del sitio web. Así como se puede visualizar en la Figura 20.

| CONTENT TYPE | PERCENT | SIZE |
|---|---|---|
| Image | 29.88% | 632.0 KB |
| Script | 26.30% | 556.1 KB |
| Font | 24.04% | 508.3 KB |
| CSS | 18.19% | 384.6 KB |
| HTML | 1.60% | 33.8 KB |
| Total | 100.00% | 2.1 MB |

**Figura 20.** Tamaño del contenido por tipo de contenido del sitio web de la Facultad de Ciencias Economías y Administrativas de la UNAS.
**Fuente:** Pingdom Tools.

En la Figura 21 se detalla el número de solicitudes por tipo de contenido que existe cuando accedemos al sitio web, teniendo como máximo 37 solicitudes para archivos CSS siendo un 34.26% del total de solicitudes. Para los archivos Script existen 36 solicitudes con un 33.33%, seguido de las imágenes teniendo 25 solicitudes con un 23.15 %. Para las fuentes existen 9 solicitudes ocupando un 8.33% y finalmente los archivos HTML con 1 solicitud ocupando un 0.93%.

| CONTENT TYPE | PERCENT | REQUESTS |
|---|---|---|
| { } CSS | 34.26% | 37 |
| JS Script | 33.33% | 36 |
| Image | 23.15% | 25 |
| Font | 8.33% | 9 |
| HTML | 0.93% | 1 |
| Total | 100.00% | 108 |

**Figura 21.** Solicitudes por tipo de contenido del sitio web de la Facultad de Ciencias Economías y Administrativas de la UNAS.
**Fuente:** Pingdom Tools.

### C. Hotel Oro Verde

En la Figura 22 se aprecia el tamaño total del sitio web del Hotel Oro Verde es de 5.0 MB. Existiendo un mayor porcentaje en el tipo de contenido de imágenes ocupando 3.8 MB (75.31% del peso del sitio web). Ocupando en segundo lugar los archivos Script con un 17.03%, seguido de los archivos de fuentes con un 3.39%, los archivos CSS con un 2.04% y finalmente los archivos HTML y solicitudes redireccionadas con un 2.03% y un 0.04% respectivamente.

| CONTENT TYPE | PERCENT | SIZE |
|---|---|---|
| Image | 75.31% | 3.8 MB |
| Script | 17.03% | 855.2 KB |
| Font | 3.39% | 170.1 KB |
| CSS | 2.04% | 102.3 KB |
| HTML | 2.03% | 102.1 KB |
| XHR | 0.17% | 8.7 KB |
| Redirect | 0.04% | 1.8 KB |
| Total | 100.00% | 5.0 MB |

**Figura 22.** Tamaño del contenido por tipo de contenido del sitio web del Hotel Oro Verde.
**Fuente:** Pingdom Tools.

En la Figura 23. se puede apreciar que el número total de solicitudes al sitio web del Hotel Oro Verde es de 129. Existiendo 51 solicitudes (39.53%) para el tipo de contenido Script siendo el más alto, seguido de las imágenes con 37 solicitudes (28.68%), para los archivos CSS con 13 solicitudes (10.08%), para los archivos XHR 12 solicitudes, los archivos de Fuentes 8 solicitudes, y finalmente para los archivos HTML y solicitudes redireccionados 6 y 2 respectivamente.

| CONTENT TYPE | PERCENT | REQUESTS |
|---|---|---|
| Script | 39.53% | 51 |
| Image | 28.68% | 37 |
| CSS | 10.08% | 13 |
| XHR | 9.30% | 12 |
| Font | 6.20% | 8 |
| HTML | 4.65% | 6 |
| Redirect | 1.55% | 2 |
| Total | 100.00% | 129 |

**Figura 23.** Solicitudes por tipo de contenido del sitio web del Sitio Web Oro Verde
**Fuente:** Pingdom Tools.

### D. Hotel Natural Green

En la Figura 24 se puede visualizar el tamaño y porcentaje por tipo de contenido cuando ingresamos al sitio web del hotel Natural Green. Teniendo como peso total de 2.1 MB; ocupando en un 49.86% para las imágenes y teniendo un peso de 1.1 MB, seguido por el tipo de archivo Script con 628.6 KB (equivalente a 29.61%), posteriormente los archivos CSS y fuentes, y finalmente el archivo HTML junto con solicitudes Redireccionadas (código de respuesta del servidor – 3XX) ocupando un 3.29% y 0.03% respectivamente.

| CONTENT TYPE | PERCENT | SIZE |
|---|---|---|
| Image | 49.86% | 1.1 MB |
| Script | 29.61% | 628.6 KB |
| CSS | 11.48% | 243.8 KB |
| Font | 5.73% | 121.6 KB |
| HTML | 3.29% | 69.9 KB |
| Redirect | 0.03% | 576.0 B |
| Total | 100.00% | 2.1 MB |

**Figura 24.** Tamaño del contenido por tipo de contenido del sitio web del Hotel Natural Green.
**Fuente:** Pingdom Tools.

En la Figura 25 se puede visualizar que el número total de solicitudes al servidor cuando se accede al sitio web del Hotel Natural Green es de 106, existiendo un mayor número en el tipo de contenido como Script (34.91%), posteriormente para los archivos CSS existe 34 solicitudes, seguido para las imágenes en 28 solicitudes, para las fuentes 4 solicitudes siendo equivalente a 3.77% y finalmente para el archivo HTML y las solicitudes redireccionadas existiendo 2 y 1 solicitud respectivamente.

| CONTENT TYPE | PERCENT | REQUESTS |
|---|---|---|
| Script | 34.91% | 37 |
| CSS | 32.08% | 34 |
| Image | 26.42% | 28 |
| Font | 3.77% | 4 |
| HTML | 1.89% | 2 |
| Redirect | 0.94% | 1 |
| Total | 100.00% | 106 |

Content Type

**Figura 25.** Solicitudes por tipo de contenido del sitio web del Hotel Natural Green.
**Fuente:** Pingdom Tools.

### E. Cámara de Comercio Canadá - Perú

En la Figura 26 se puede apreciar, que el tamaño total del sitio web de la Cámara de Comercio Canadá - Perú es de 9.4 MB, de la cual un 75.87% es parte del contenido de tipo Imagen, seguido del tipo de contenido Script con un 13.42%, un 6.51% del tipo de contenido CSS, y para el tipo de contenido HTML un 2.09%, para las Fuentes un 1.98%, y para el tipo XHR un 0.10% y finalmente para las solicitudes con redireccionadas un 0.03%.

| CONTENT TYPE | PERCENT | SIZE |
|---|---|---|
| Image | 75.87% | 7.2 MB |
| Script | 13.42% | 1.3 MB |
| CSS | 6.51% | 615.5 KB |
| HTML | 2.09% | 197.1 KB |
| Font | 1.98% | 187.5 KB |
| XHR | 0.10% | 9.5 KB |
| Redirect | 0.03% | 2.7 KB |
| Total | 100.00% | 9.4 MB |

**Figura 26.** Tamaño del contenido por tipo de contenido del sitio web del Hotel Oro Verde.
**Fuente:** Pingdom Tools.

En la Figura 27 se puede apreciar el número total de solicitudes al servidor cuando accedemos al sitio web del Hotel Oro Verde. Existiendo en total 179 solicitudes, donde el 34.64% de solicitudes pertenecen al contenido de Imagen, un 29.05% pertenece al tipo de contenido de Script, un 18.99% pertenece a los archivos CSS. Un 4.47% pertenece a los archivos de fuentes, y finalmente un 3.91% y 2.23% al tipo de contenido HTML y solicitudes redireccionadas respectivamente.

| CONTENT TYPE | PERCENT | REQUESTS |
|---|---|---|
| Image | 34.64% | 62 |
| Script | 29.05% | 52 |
| CSS | 18.99% | 34 |
| XHR | 6.70% | 12 |
| Font | 4.47% | 8 |
| HTML | 3.91% | 7 |
| Redirect | 2.23% | 4 |
| Total | 100.00% | 179 |

**Figura 27.** Solicitudes por tipo de contenido del sitio web del Hotel Oro Verde.
**Fuente:** Pingdom Tools.

- **Transferencia de información y empleo de Cache**

Se ha empleado la herramienta Mozilla Firefox para obtener la cantidad de solicitudes y conocer el tamaño de la información que está siendo almacenado en cache, las pruebas realizadas se detallan en el Anexo 10.

En la Tabla 24 se detalla los cinco sitios web, con información del número de solicitudes que fueron almacenados en cache, la cantidad total de solicitudes realizadas al servidor, el tamaño de la información que se ha solicitado y el tamaño trasferido en relación con el tiempo de carga, mostrando finalmente el porcentaje de diferencia del tamaño del sitio web.

**Tabla 24.** Rendimiento de sitios web empleado almacenado en cache con el navegador Mozilla Firefox Quantum v. 66.0.3.

| Sitios Web | Estado | Respuestas en Cache | Total de Solicitudes | Tamaño | Tamaño transferido | Tiempo | Diferencia del Tamaño |
|---|---|---|---|---|---|---|---|
| Web-Out | Usando Cache | 57 | 90 | 359.09 KB | 235.38 KB | 4.59 segundos | 0.93 MB |
| | Sin usar Cache | 0 | 90 | 1319.62 KB | 3722.99 KB | 18.19 segundos | |
| Facultad de Ciencias Económicas y Administrativas de la UNAS | Usando Cache | 71 | 102 | 218.70 KB | 1966.46 KB | 4.19 segundos | 0.94 MB |
| | Sin usar Cache | 0 | 102 | 1181.73 KB | 4045.83 KB | 35.81 segundos | |
| Hotel Oro Verde | Usando Cache | 44 | 86 | 2351.93 KB | 9436.97 KB | 23.73 segundos | 3.25 MB |
| | Sin usar Cache | 0 | 86 | 5678.19 KB | 13529.01 KB | 89.03 segundos | |
| Hotel Natural Green | Usando Cache | 102 | 112 | 552.00 KB | 554.83 KB | 3.35 segundos | 3.83 MB |
| | Sin usar Cache | 0 | 112 | 4469.08 KB | 4493.04 KB | 84.98 segundos | |
| Cámara de comercio Canadá - Perú | Usando Cache | 59 | 135 | 2908.56 KB | 10003.53 KB | 46.34 segundos | 5.83 MB |
| | Sin usar Cache | 0 | 135 | 8883.15 KB | 18265.59 KB | 81.91 segundos | |

**Fuente:** Elaboración propia.

- **Análisis de Resultados**

En la Tabla 25 se describe el peso por tipo de contenido y número de solicitudes que hay por cada sitio web obtenidas con la herramienta Pingdom Tools. Existiendo una relación entre el tamaño del sitio web y el número de solicitudes; expresando que a mayor tamaño del sitio web, el número de solicitudes tiende a incrementarse.

Así mismo, podemos relacionar el número de solicitudes de la Tabla 25, guardan relación con el tiempo de carga del Sitio Web cuando se accede por HTTP y HTTPS detallado anteriormente en la Tabla 17.

**Tabla 25.** Resumen de tamaño y número de solicitudes por Sitio Web obtenido con la herramienta Pingdom Tools.

| Sitio Web | Tamaño del Sitio Web | Número total de Solicitudes |
|---|---|---|
| Web-Out | 1.4 MB | 83 |
| Facultad de Ciencias Económicas y Administrativas de la UNAS | 2.1 MB | 108 |
| Hotel Oro Verde | 5.0 MB | 129 |
| Hotel Natural Green | 2.1 MB | 106 |
| Camara de comercio Canadá - Perú | 9.4 MB | 179 |

**Fuente:** Elaboración propia.

Si el sitio web y el servidor tienen configurado el almacenamiento en cache, esto brinda una ventaja en el tamaño de transferencia de información que tiene que enviar el servidor a los sitios web, así como se muestra en la Tabla 24. Haciendo que el tiempo de carga de los sitios web sea mucho más rápido, y las solicitudes enviadas al servidor disminuyan. Si los sitios web tienen habilitado el almacenamiento en cache reduce en más del 50% del tamaño de componentes solicitados al servidor. Así mismo el tiempo de carga se ve influida en más del 50%, siendo mucho más rápido cuando se tiene habilitado el almacenamiento en cache.

### 4.2.6 Nivel de Seguridad

- **Compatibilidad con el Protocolo SSL/TLS:** Los sitios web, pueden ser compatibles con diversas versiones del protocolo SSL/TLS, algunas con vulnerabilidades (todas las versiones SSL y TLS versión 1.0); siendo las versiones actuales mucho más seguras y eficientes que sus predecesores. En la Tabla 26, se detalla los cinco sitios web con las versiones de SSL/TLS habilitados y deshabilitados en la configuración del servidor web, en el cual están alojados.

**Tabla 26.** Protocolos SSL/TLS soportados por el servidor Web de cada sitio web.

| | **Web-Out** | **Facultad de ciencias económicas y administrativas de la UNAS** | **Hotel oro verde** | **Hotel Natural Green** | **Cámara de Comercio Canadá - Perú** |
|---|---|---|---|---|---|
| **Protocolos Habilitados** | TLS 1.2<br>TLS 1.1<br>TLS 1.0 | TLS 1.2<br>TLS 1.1<br>TLS 1.0 | TLS 1.2<br>TLS 1.1<br>TLS 1.0 | TLS 1.2<br>TLS 1.1<br>TLS 1.0 | TLS 1.2<br>TLS 1.1<br>TLS 1.0 |
| **Protocolos Deshabilitados** | SSL 3.0<br>SSL 2.0 | SSL 3.0<br>SSL 2.0 | SSL 3.0<br>SSL 2.0 | SSL 3.0<br>SSL 2.0 | SSL 3.0<br>SSL 2.0 |

**Fuente:** Elaboración propia.

- **Vulnerabilidades del Protocolo SSL/TLS:** Por medio de la herramienta SSLyze se realizó un análisis de la seguridad de los cinco sitios web. En la Tabla 27, se puede ver el detalle de la prueba realizada. En la primera columna se definen las diversas pruebas que fueron comprobadas para la configuración de los cinco sitios web, coincidiendo en el soporte y vulnerabilidad para los cinco.

**Tabla 27.** Análisis de seguridad del Protocolo SSL/TLS a los cinco sitios web con SSLyze.

| | **Los 5 sitios web caso de estudio** |
|---|---|
| **OpenSSL Heartbleed** | No vulnerable a Heartbleed |
| **OpenSSL CCS Injection** | No vulnerable a inyección OpenSSL CCS |
| **Downgrade Attacks** | TLS_FALLBACK_SCSV (Soportado) |
| **Deflate Compression** | OK – compresión deshabilitada |
| **Robot Attack** | OK – No vulnerable |
| **Session Renegotiation:** | Client-initiated Renegotiation: OK - Rechazado<br>Secure Renegotiation: OK - Soportado |
| **SSL versión 2, 3 y TLS versión 1.3** | Servidor rechaza todas las suites de cifrado |
| **TLS versión 1.0, 1.1 y 1.2** | Forward Secrecy: OK – soportado<br>RC4: OK – No soportado |
| **Plugins Disponibles** | CertificateInfoPlugin<br>CompressionPlugin<br>FallbackScsvPlugin<br>HeartbleedPlugin<br>HttpHeadersPlugin<br>OpenSslCcsInjectionPlugin<br>OpenSslCipherSuitesPlugin<br>RobotPlugin<br>SessionRenegotiationPlugin<br>SessionResumptionPlugin |

**Fuente:** Elaboración Propia.

***OpenSSL Heartbleed*:** Vulnerabilidad encontrada en la herramienta Openssl en las siguientes versiones: 1.0.1, 1.0.1f, 1.0.2-beta, 1.0.2-beta1. La mitigación a esta vulnerabilidad es emplear una versión distinta a las mencionadas.

***OpenSSL CCS Injection*:** Es una vulnerabilidad de la herramienta de OpenSSL; para su mitigación es recomendable no utilizar las siguientes versiones: anteriores a 0.9.8za, de la version 1.0.0 hasta 1.0.0.m, y de la versión 1.0.1 hasta 1.0.1.h.

***Downgrade Attacks*:** Es un ataque criptográfico, que consiste en reducir la versión de SSL/TLS en una comunicación por HTTPS, con el fin de aprovechar las vulnerabilidades de las versiones más antiguas.

***Deflate Compression*:** Ataque provechado por la compresión de paquetes en una comunicación HTTPS. Para su mitigación debemos de agregar la siguiente línea (*SSLCompression off*) en la configuración del servidor apache.

***Robot Attack*:** Vulnerabilidad que permite que mediante un ataque *Man-In-the-Middle* llevar a cabo un descifrado de RSA.

***Session Renegotiation*:** Propiedad que permite retomar una sesión anteriormente abierta. Lo recomendable es tener habilitado una renegociación segura.

**SSL versión 2, 3 y TLS versión 1.3:** Al no encontrarse habilitado en los servidores web de cada sitio web, no es posible obtener la suite de cifrado establecida por el servidor para estas versiones.

**TLS versión 1.0, 1.1 y 1.2:** Hace referencia a que dentro de la configuración del servidor se ha deshabilitado el algoritmo RC4 y *Forward Secrecy* siendo una propiedad de los sistemas criptográficos que garantiza que el sistema es seguro-adelante (la clave usada para generar una trasmisión segura de información no se puede usar para generar una nueva clave adicional).

***Plugins* Disponibles:** Vienen a ser los *Plugins* que están instalados en el servidor web de los cinco sitios web.

Así mismo se ha empleado la herramienta Qualys SSL Labs obteniéndose el siguiente resultado descrito en la Tabla 28. En esta tabla se puede visualizar una calificación obtenida por cada sitio web, existiendo un intervalo de calificación de A – F; siendo A la nota más alta y F la nota más baja en base de diversos indicadores descritos más adelante en la Figura 29.

**Tabla 28.** 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 |

**Fuente:** Elaboración Propia.

Los indicadores por el cual Qualys SSL Labs asigna determinada calificación de la A - F, es en base a una escala de puntuación detallado en la Figura 28.

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

**Figura 28.** Equivalencia del puntaje número en la calificación asignada por Qualys SSL Labs.
**Fuente**: (Qualys SSL Labs, 2019)

El puntaje numérico es la suma en base a tres categorías de evaluación siendo el Protocolo Soportado, que va desde SSL versión 2.0 hasta TLS versión 1.2; Intercambio de llaves**,** que viene a ser los tamaños de llave que se emplean en la comunicación por medio de HTTPS, y finalmente la fuerza de cifrado; en la Figura 29 se puede visualizar la puntuación asignada para cada categoría.

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

**Figura 29.** Puntuación a las categorías para SSL Labs.
**Fuente**: (Qualys SSL Labs, 2019)

Para la primera categoría que vendría a ser el “Soporte de Protocolo” se maneja en base a las calificaciones detallas en la Figura 30. Dentro de los protocolos no se incluye a TLS versión 1.3.

| Protocolo | Puntuación |
|---|---|
| SSL 2.0 | 0% |
| SSL 3.0 | 80% |
| TLS 1.0 | 90% |
| TLS 1.1 | 95% |
| TLS 1.2 | 100% |

**Figura 30.** Puntuación por soporte de Protocolo SSL/TLS.
**Fuente**: (Qualys SSL Labs, 2019)

Para la segunda categoría de nombre “Intercambio de llaves” se maneja en base a las Puntuaciones detalladas en la Figura 31.

| Aspecto clave de intercambio | Puntuación |
|---|---|
| Clave débil (defecto Debian OpenSSL) | 0% |
| Intercambio de claves anónimas (sin autenticación) | 0% |
| Clave o fuerza del parámetro DH <512 bits | 20% |
| Intercambio de claves exportables (limitado a 512 bits) | 40% |
| Clave o intensidad del parámetro DH <1024 bits (por ejemplo, 512) | 40% |
| Clave o intensidad del parámetro DH <2048 bits (por ejemplo, 1024) | 80% |
| Clave o intensidad del parámetro DH <4096 bits (por ejemplo, 2048) | 90% |
| Clave o intensidad del parámetro DH> = 4096 bits (por ejemplo, 4096) | 100% |

**Figura 31.** Guía de calificación de intercambio de claves.
**Fuente**: (Qualys SSL Labs, 2019)

Para la última categoría de nombre “Fuerza de Cifrado”, se maneja en base a las calificaciones detalladas en la Figura 32.

| Fuerza de cifrado | Puntuación |
|---|---|
| 0 bits (sin cifrado) | 0% |
| <128 bits (por ejemplo, 40, 56) | 20% |
| <256 bits (por ejemplo, 128, 168) | 80% |
| > = 256 bits (por ejemplo, 256) | 100% |

**Figura 32.** Guía de clasificación de intensidad de cifrado.
**Fuente**: (Qualys SSL Labs, 2019)

**Tabla 29.** Análisis de los cinco sitios web con la herramienta Qualys SSL Labs.

| Detalles del Protocolo | Web-Out | Facultad de Ciencias Económicas y Administrativas - UNAS | Hotel Oro Verde | Hotel Natural Green | Cámara de Comercio Canadá - Perú |
|---|---|---|---|---|---|
| **Ataque DROWN** | No vulnerable. SSL versión 2 no soportado. | No vulnerable. SSL versión 2 no soportado. | No vulnerable. SSL versión 2 no soportado. | No vulnerable. SSL versión 2 no soportado. | No vulnerable. SSL versión 2 no soportado. |
| **Renegociación Segura** | Soportado | Soportado | Soportado | Soportado | Soportado |
| **Asegura la renegociación iniciada por el cliente** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |
| **Insegura renegociación iniciada por el cliente** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |
| **Ataque BEAST** | No mitigado por el lado del servidor por TLS versión 1.0 | No mitigado por el lado del servidor por TLS versión 1.0 | No mitigado por el lado del servidor por TLS versión 1.0 | No mitigado por el lado del servidor por TLS versión 1.0 | No mitigado por el lado del servidor por TLS versión 1.0 |
| **Ataque POODLE en SSL** | No vulnerable. SSL version 3 no soportado. | No vulnerable. SSL version 3 no soportado. | No vulnerable. SSL version 3 no soportado. | No vulnerable. SSL version 3 no soportado. | No vulnerable. SSL version 3 no soportado. |
| **Ataque POODLE en TLS** | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. |
| **Ataque GOLDENDOODLE** | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. |
| **Ataque OpenSSL 0-Length** | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. |
| **Ataque Sleeping POODLE** | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. |
| **Prevención a ataques Downgrade** | Soportado. | Soportado. | Soportado. | Soportado. | Soportado. |
| **Compresión SSL/TLS** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |
| **Cifrado RC4** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |
| **Extensión Heartbeat** | Si soportado. | Si soportado. | Si soportado. | Si soportado. | Si soportado. |
| **Vulnerable Heartbleed** | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. |
| **Vulnerable Ticketbleed** | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. |

| | | | | | |
|---|---|---|---|---|---|
| **Vulnerabilidad OpenSSL CCS (CVE-2014-0224)** | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. |
| **Vulnerabilidad OpenSSL Padding Oracle (CVE-2014-0224)** | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. |
| **Vulnerabilidad ROBOT** | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. | No vulnerable. |
| **Secreto perfecto hacia adelante.** | Con algunos navegadores | Con algunos navegadores | Con la mayoría de los navegadores | Con algunos navegadores | Con algunos navegadores |
| **Negociación de protocolo de capa de aplicación (ALPN)** | Soportado, http/1.1 | Soportado, http/1.1 | Soportado, http/1.1 | Soportado, http/1.1 | Soportado, http/1.1 |
| **NPN** | No | No | No | No | No |
| **OCSP stapling** | Yes | Yes | Yes | Yes | Yes |
| **Seguridad de Transporte Estricto (HSTS)** | No habilitado | No habilitado | No habilitado | No habilitado | No habilitado |
| **Precargado HSTS** | No habilitado en Chrome, Edge, Firefox y Internet Explorer | No habilitado en Chrome, Edge, Firefox y Internet Explorer | No habilitado en Chrome, Edge, Firefox y Internet Explorer | No habilitado en Chrome, Edge, Firefox y Internet Explorer | No habilitado en Chrome, Edge, Firefox y Internet Explorer |
| **Fijación de clave Publica (HPKP)** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |
| **Intolerancia al apretón de manos largo** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |
| **Intolerancia a la extension TLS** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |
| **Intolerancia a la versión TLS** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |
| **Utiliza primos DH comunes** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |
| **Servidor Público con parámetro de reutilización ECDH** | No soportado. | No soportado. | No soportado. | No soportado. | No soportado. |

**Fuente:** Elaboración Propia

El orden y los algoritmos de cifrado por parte del navegador no cambian, ya que la prueba se realiza desde un mismo navegador (Mozilla), pero por el lado del servidor si existe variación debido a que la suite de cifrado puede configurarse de una manera distinta para cada sitio Web a pesar de que se encuentren en el mismo servidor.

Las suites de cifrado se dividen en un conjunto de partes, así como se detalla a continuación:

**Tabla 30.** Propiedades de seguridad de las Suites de cifrado del servidor web

| | N°. | SERVIDOR WEB | FIRMA | INTER. DE CLAVE | CIFRADO | HASH |
|---|---|---|---|---|---|---|
| Web-Out | 1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | ECDHE | AES-256-GCM | SHA384 |
| | 2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | RSA | ECDHE | AES-128-FCM | SHA256 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | RSA | ECDHE | AES-256-CBC | SHA384 |
| | 4 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | RSA | ECDHE | AES-128-CBC | SHA256 |
| | 5 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | RSA | ECDHE | AES-256-CBC | SHA1 |
| | 6 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | RSA | ECDHE | AES-128-CBC | SHA1 |
| | 7 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | RSA | ECDHE | 3DES-EDE-CBC | SHA1 |
| | 8 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | DHE | AES-256-GCM | SHA384 |
| | 9 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | RSA | DHE | AES-128-GCM | SHA256 |
| | 10 | TLS_RSA_WITH_AES_256_GCM_SHA384 | RSA | RSA | AES-256-GCM | SHA384 |
| Facultad de Ciencias Económicas y Administrativas de la UNAS | 1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | ECDHE | AES-256-GCM | SHA384 |
| | 2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | RSA | ECDHE | AES-128-GCM | SHA256 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | RSA | ECDHE | AES-256-CBC | SHA384 |
| | 4 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | RSA | ECDHE | AES-128-CBC | SHA256 |
| | 5 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | RSA | ECDHE | AES-256-CBC | SHA1 |
| | 6 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | RSA | ECDHE | AES-128-CBC | SHA1 |
| | 7 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | RSA | ECDHE | 3DES-EDE-CBC | SHA1 |
| | 8 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | DHE | AES-256-GCM | SHA384 |
| | 9 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | RSA | DHE | AES-128-GCM | SHA256 |
| | 10 | TLS_RSA_WITH_AES_256_GCM_SHA384 | RSA | RSA | AES-256-GCM | SHA384 |
| Cámara de Comercio Canadá - Perú | 1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | ECDHE | AES-256-GCM | SHA384 |
| | 2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | RSA | ECDHE | AES-128-GCM | SHA256 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | RSA | ECDHE | AES-256-CBC | SHA384 |
| | 4 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | RSA | ECDHE | AES-128-CBC | SHA256 |
| | 5 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | RSA | ECDHE | AES-256-CBC | SHA1 |
| | 6 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | RSA | ECDHE | AES-128-CBC | SHA1 |
| | 7 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | RSA | ECDHE | 3DES-EDE-CBC | SHA1 |
| | 8 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | DHE | AES-256-GCM | SHA384 |
| | 9 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | RSA | DHE | AES-128-GCM | SHA256 |
| | 10 | TLS_RSA_WITH_AES_256_GCM_SHA384 | RSA | RSA | AES-256-GCM | SHA384 |
| Hotel Oro Verde | 1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | ECDHE | AES-256-GCM | SHA384 |
| | 2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | RSA | ECDHE | AES-256-CBC | SHA384 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | RSA | ECDHE | AES-256-CBC | SHA1 |
| | 4 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | DHE | AES-256-CBC | SHA384 |
| | 5 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 | RSA | DHE | AES-256-CBC | SHA256 |
| | 6 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA | RSA | DHE | AES-256-CBC | SHA1 |
| | 7 | TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA | RSA | DHE | CAMELLIA-256-CBC | SHA1 |
| | 8 | TLS_RSA_WITH_AES_256_GCM_SHA384 | RSA | RSA | AES-256-GCM | SHA384 |
| | 9 | TLS_RSA_WITH_AES_256_CBC_SHA256 | RSA | RSA | AES-256-CBC | SHA256 |
| | 10 | TLS_RSA_WITH_AES_256_CBC_SHA | RSA | RSA | AES-256-CBC | SHA1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Hotel Natural Green** | 1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | ECDHE | AES-256-GCM | SHA384 |
| | 2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | RSA | ECDHE | AES-128-GCM | SHA256 |
| | 3 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | RSA | ECDHE | AES-256-CBC | SHA384 |
| | 4 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | RSA | ECDHE | AES-128-CBC | SHA256 |
| | 5 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | RSA | ECDHE | AES-256-CBC | SHA1 |
| | 6 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | RSA | ECDHE | AES-128-CBC | SHA1 |
| | 7 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | RSA | ECDHE | EDES-EDE-CBC | SHA1 |
| | 8 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | RSA | DHE | AES-256-GCM | SHA384 |
| | 9 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | RSA | DHE | AES-128-GCM | SHA256 |
| | 10 | TLS_RSA_WITH_AES_256_GCM_SHA384 | RSA | RSA | AES-256-GCM | SHA384 |

**Fuente:** Elaboración propia.

- **Análisis de Resultados**

Se ha podido conocer que existe diversas vulnerabilidades; el cual con una correcta configuración del archivo ssl.conf se puede cubrir la mayoría de las vulnerabilidades que afectan a este protocolo. Las calificaciones asignadas por la herramienta Qualys SSL Labs son muy buenos siendo entre A y B, el cual hace mención que cumple con los requerimientos de seguridad que un sitio web debe de tener en base a los estándares de Qualys SSL Labs, gracias al uso del Protocolo SSL/TLS.

### 4.2.7 Rendimiento con el protocolo TLS versión 1.3

Se realizó un escenario de prueba haciendo uso de máquinas virtuales utilizando la herramienta de VirtualBox versión 6.0.8, para poder demostrar que es posible configurar el protocolo TLS versión 1.3 y a la vez demostrar que es mucho más rápido en relación con la versión 1.2. Con el objetivo de no hacer muy repetitiva las pruebas y a manera de demostración, solo se ha empleado 2 sitios web (Sitio web de la empresa Web-Out. S.A. y el sitio del Hotel Natural Green).

Los requerimientos mínimos para que soporte el protocolo TLS versión 1.3 en los servidores Web Apache y Nginx se detallan en la Tabla 31, siendo ambos con mayor cuota de mercado de todos los sitios web a nivel mundial según el reporte de (Netcraft, 2019) actualizado hasta el 10 de Mayo del 2019.

**Tabla 31.** Versiones mínimas con soporte para el protocolo TLS versión 1.3.

| | **Servidor Web** | | **Herramienta Criptográfica** |
|---|---|---|---|
| | **Apache** | **Nginx** | **OpenSSL** |
| **Versión Mínima:** | 2.4.36 (10 octubre 2018) | 1.13 (02 octubre 2018) | 1.1.1 (11 setiembre 2018) |
| **Versión Estable:** | 2.4.37 (23 octubre 2018) | 1.16 (23 abril 2019) | 1.1.1b (26 febrero 2019) |

**Fuente:** Elaboración propia

Se ha realizado la instalación y configuración del servidor web y servidor de base de datos en máquinas virtuales diferentes, así mismo se desplego los 2 sitios web sin ningún inconveniente. Las características técnicas de ambos equipos se describen en la Tabla 32.

**Tabla 32.** Características del servidor Web y base de datos virtualizado como escenario de pruebas.

| | | |
|---|---|---|
| **SERVIDOR WEB**<br><br>Centos 7.6 Minimalista | **HARDWARE** | |
| | Disco Duro | 80 Gb |
| | Memoria RAM | 4 Gb |
| | Dirección IP local | 192.168.1.60 |
| | **SOFTWARE** | |
| | Servidor Web | Apache 2.4.39 |
| | Modulo SSL/TLS | mod_ssl |
| | Herramienta de Criptografía | OpenSSL v. 1.1.1 (03 Abril 2019) |
| | PHP | versión 7.1.27 |
| **SERVIDOR DE BASE DE DATOS**<br><br>Ubuntu Server | **HARDWARE** | |
| | Disco Duro | 80 Gb |
| | Memoria RAM | 4 Gb |
| | Dirección IP local | 192.168.1.60 |
| | **SOFTWARE** | |
| | Servidor Web | Apache 2.4.39 |
| | Modulo SSL/TLS | mod_ssl |
| | Herramienta de Criptografía | OpenSSL v. 1.1.1 (03 Abril 2019) |
| | PHP | versión 7.1.27 |

**Fuente:** Elaboración propia.

Ambos sitios web fueron configurados en el servidor web, haciendo uso de un Certificado Auto firmado generado con la herramienta OpenSSL versión 1.1.1. El certificado tiene 1 año de validez, generado con fines académicos para ambientes de prueba.

Las pruebas serán realizadas desde la maquina anfitrión, teniendo como Sistema Operativo Windows 10, con 16 Gigabytes RAM, Disco duro de 1 Terabyte, Procesador: Intel (R) Core I7 - 4510U y CPU 2.00 GHz de 64 Bits.

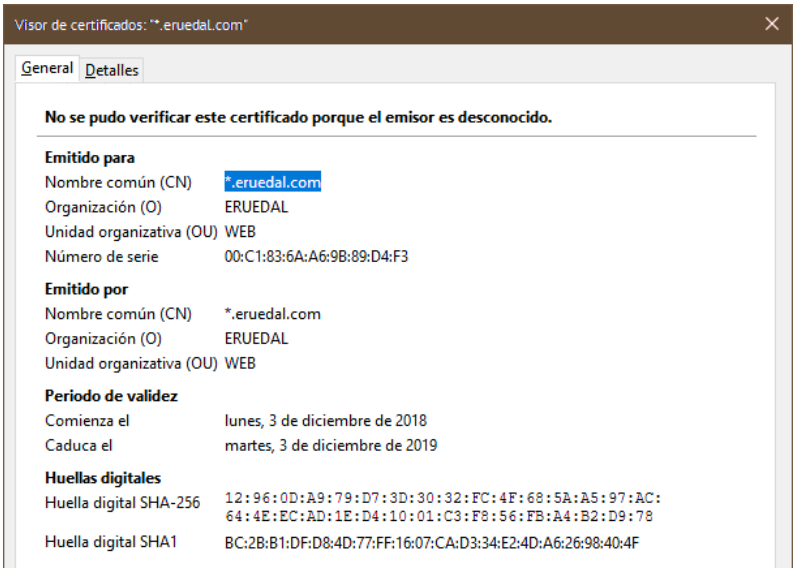



**Figura 33.** Detalles del Certificado Auto firmado generado con la herramienta OpenSSL v.1.1.1
**Fuente:** Elaboración propia.

Cuando accedemos a ambos sitios web, es posible verificar que la conexión con el servidor se realiza mediante el protocolo TLS versión 1.3, y si accedemos con el navegador Mozilla Firefox, nos detallara la Suite de Cifrado que está empleando en la comunicación con el servidor, así como se muestra en la Figura 34.

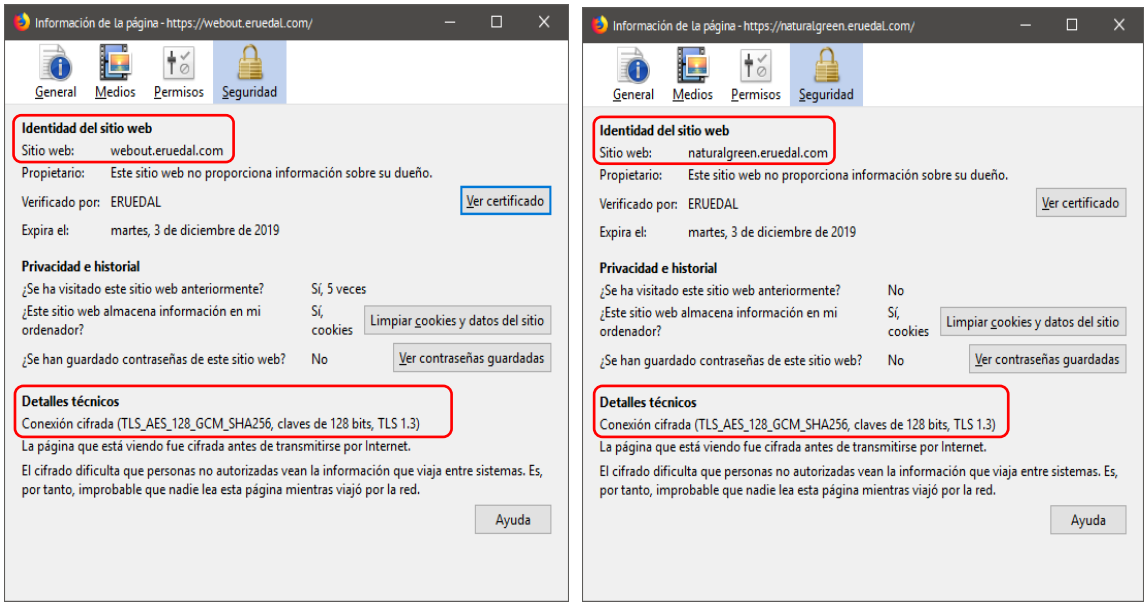
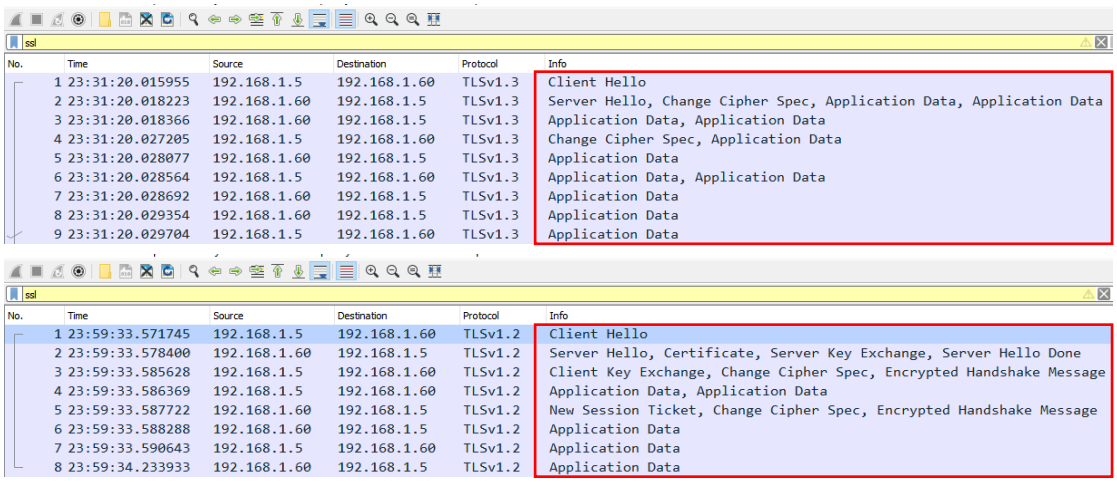



**Figura 34.** Información de la conexión por HTTPS al sitio web de Web-Out S.A. y Hotel Natural Green.
**Fuente:** Elaboración propia.

En la Figura 35, se visualiza la captura de paquetes cuando se accede al servidor web (máquina virtual) por medio del sitio web https://webout.eruedal.com/ (URL Local) habilitando el protocolo TLS versión 1.3 y TLS versión 1.2. Existiendo diferencias en la Información generada por los paquetes trasmitidos en ambas versiones.



ssl

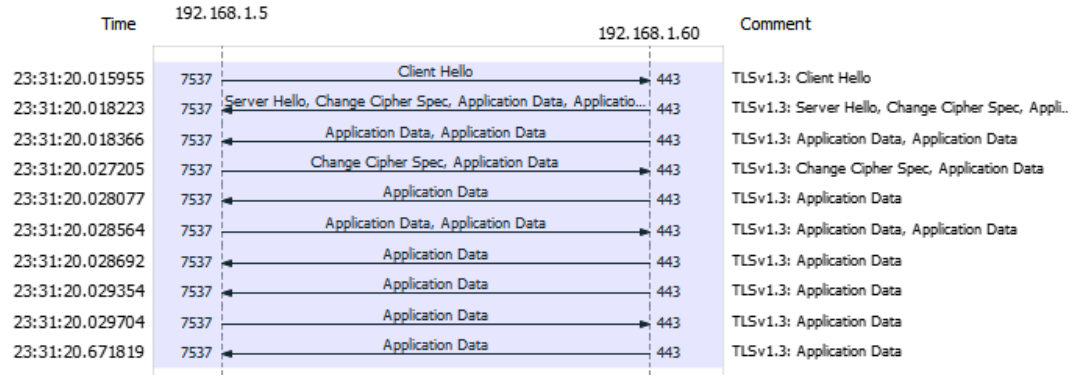
| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 23:31:20.015955 | 192.168.1.5 | 192.168.1.60 | TLSv1.3 | Client Hello |
| 2 | 23:31:20.018223 | 192.168.1.60 | 192.168.1.5 | TLSv1.3 | Server Hello, Change Cipher Spec, Application Data, Application Data |
| 3 | 23:31:20.018366 | 192.168.1.60 | 192.168.1.5 | TLSv1.3 | Application Data, Application Data |
| 4 | 23:31:20.027205 | 192.168.1.5 | 192.168.1.60 | TLSv1.3 | Change Cipher Spec, Application Data |
| 5 | 23:31:20.028077 | 192.168.1.60 | 192.168.1.5 | TLSv1.3 | Application Data |
| 6 | 23:31:20.028564 | 192.168.1.5 | 192.168.1.60 | TLSv1.3 | Application Data, Application Data |
| 7 | 23:31:20.028692 | 192.168.1.60 | 192.168.1.5 | TLSv1.3 | Application Data |
| 8 | 23:31:20.029354 | 192.168.1.60 | 192.168.1.5 | TLSv1.3 | Application Data |
| 9 | 23:31:20.029704 | 192.168.1.5 | 192.168.1.60 | TLSv1.3 | Application Data |

ssl

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 23:59:33.571745 | 192.168.1.5 | 192.168.1.60 | TLSv1.2 | Client Hello |
| 2 | 23:59:33.578400 | 192.168.1.60 | 192.168.1.5 | TLSv1.2 | Server Hello, Certificate, Server Key Exchange, Server Hello Done |
| 3 | 23:59:33.585628 | 192.168.1.5 | 192.168.1.60 | TLSv1.2 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 4 | 23:59:33.586369 | 192.168.1.5 | 192.168.1.60 | TLSv1.2 | Application Data, Application Data |
| 5 | 23:59:33.587722 | 192.168.1.60 | 192.168.1.5 | TLSv1.2 | New Session Ticket, Change Cipher Spec, Encrypted Handshake Message |
| 6 | 23:59:33.588288 | 192.168.1.60 | 192.168.1.5 | TLSv1.2 | Application Data |
| 7 | 23:59:33.590643 | 192.168.1.5 | 192.168.1.60 | TLSv1.2 | Application Data |
| 8 | 23:59:34.233933 | 192.168.1.60 | 192.168.1.5 | TLSv1.2 | Application Data |

**Figura 35.** Diferencia entre TLS versión 1.2 y TLS versión 1.3.
**Fuente:** Elaboración propia.

En la Figura 36, se visualiza el flujo de paquetes que existe cuando se realiza la conexión al sitio web de Web-Out alojado en el servidor web de prueba, mostrando información como el tiempo empleado para cada paquete en milisegundos (ms), puerto por defecto 443; asi como tambien la columna de comentarios donde es posible ver la información de cada paquete.



| Time | 192.168.1.5 | | 192.168.1.60 | Comment |
|---|---|---|---|---|
| 23:31:20.015955 | 7537 | Client Hello → | 443 | TLSv1.3: Client Hello |
| 23:31:20.018223 | 7537 | ← Server Hello, Change Cipher Spec, Application Data, Applicatio... | 443 | TLSv1.3: Server Hello, Change Cipher Spec, Appli.. |
| 23:31:20.018366 | 7537 | ← Application Data, Application Data | 443 | TLSv1.3: Application Data, Application Data |
| 23:31:20.027205 | 7537 | Change Cipher Spec, Application Data → | 443 | TLSv1.3: Change Cipher Spec, Application Data |
| 23:31:20.028077 | 7537 | ← Application Data | 443 | TLSv1.3: Application Data |
| 23:31:20.028564 | 7537 | Application Data, Application Data → | 443 | TLSv1.3: Application Data, Application Data |
| 23:31:20.028692 | 7537 | ← Application Data | 443 | TLSv1.3: Application Data |
| 23:31:20.029354 | 7537 | ← Application Data | 443 | TLSv1.3: Application Data |
| 23:31:20.029704 | 7537 | Application Data → | 443 | TLSv1.3: Application Data |
| 23:31:20.671819 | 7537 | ← Application Data | 443 | TLSv1.3: Application Data |

**Figura 36.** Flujo de paquetes en TLS versión 1.3 para el sitio web Web-Out. S.A. alojado en servidor virtual Centos 7.
**Fuente:** Elaboración propia.

La Figura 37, describe el flujo de paquetes que existe en TLS v.1.2, indicando el tiempo, IP Origen, IP destino, puerto y comentario por cada paquete trasmitido.

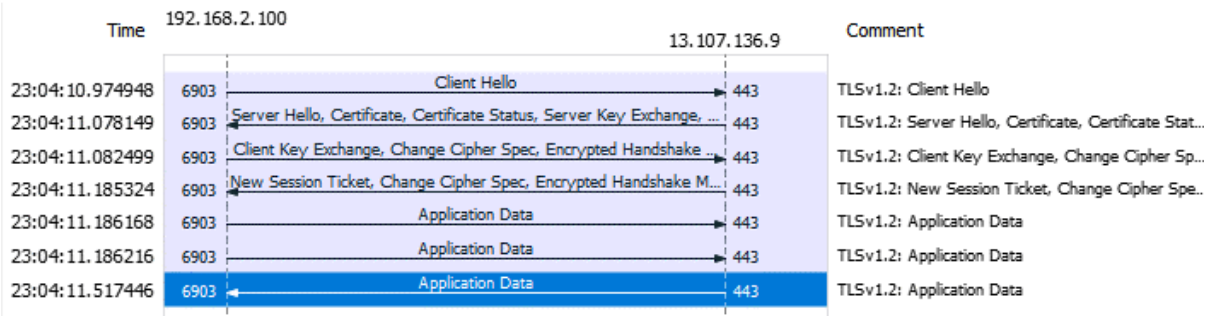



**Figura 37.** Flujo de paquetes en TLS versión 1.2 para el sitio web Web-Out. S.A. alojado en el VPS 1
**Fuente:** Elaboración propia.

Se paso a medir el rendimiento con la herramienta Wireshark v. 3.0.1 de los paquetes transmitidos, tomando en consideración el tiempo en milisegundos desde que se envía el primer paquete (*Client Hello*) hasta el último paquete (*Application Data*) que indica que el proceso de negociación entre cliente y servidor termina y se empiezan a transmitir los contenidos del sitio web por medio de un canal cifrado, así como se muestra en la Tabla 33.

**Tabla 33.** Rendimiento de TLS versión 1.2 y TLS versión 1.3 en el proceso de negociación entre Cliente y Servidor (Handshake).

| | **TLS versión 1.3** | | **TLS versión 1.2** | |
|---|---|---|---|---|
| **Sitios Web** | Paquete *Client Hello* | Paquete *Application Data* | Paquete *Client Hello* | Paquete *Application Data* |
| **Web-Out. S.A.** | 20.015955 ms. | 20.028077 ms. | 33.571745 ms. | 33.588288 ms. |
| Tiempo promedio | 0.012122 ms. | | 0.016543 ms. | |
| **Hotel Natural Green** | 3.843528 ms. | 3.858782 ms. | 18.61337 ms. | 20.040162 ms. |
| Tiempo promedio | 0.015254 ms. | | 1.426792 ms. | |

**Fuente:** Elaboración propia.

Por otra parte, también es importante conocer que versiones del protocolo SSL/TLS y que suite de cifrado son los empleados por los clientes web cuando acceden a los sitios web, para ello se ha realizado un análisis en un entorno de prueba en la que se ha agregado un formato de Logs personalizado en el archivo ssl.conf de Apache, con el principal objetivo de conocer que versiones y cuáles son las suites de cifrado más empleadas en nuestros sitios web, esto nos permitirá mejorar la configuración del protocolo SSL/TLS permitiendo deshabilitar las versiones inseguras evitando así posibles ataques.

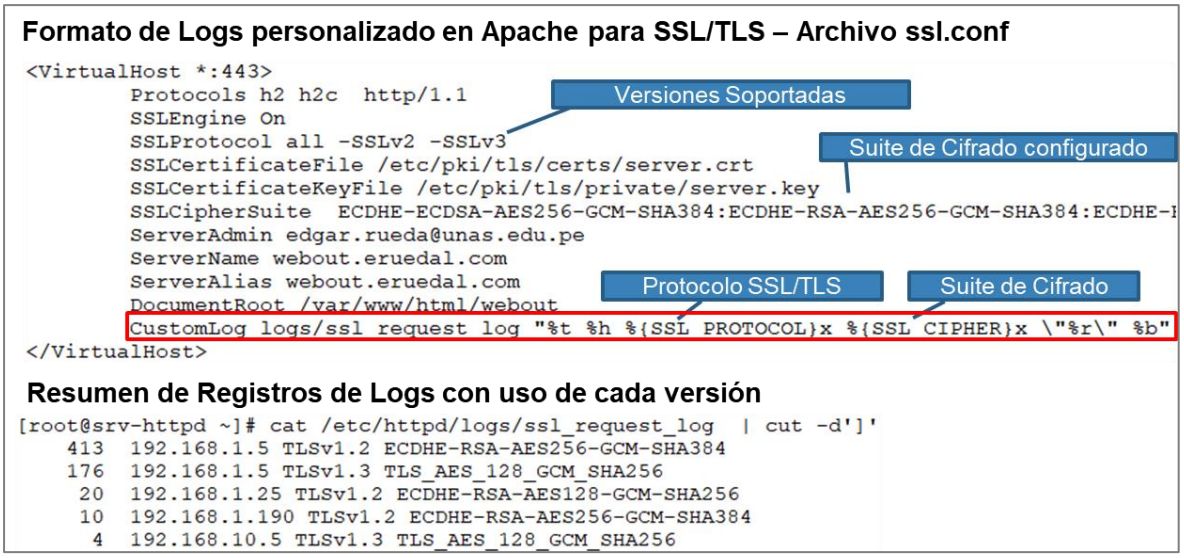



**Figura 38.** Registro de Logs en Apache, con versión del Protocolo y Suite de Cifrado empleado en las conexiones web.
**Fuente:** Elaboración propia.

En la Figura 38, se puede visualizar la configuración realizada en el servidor apache, agregándose un VirtualHost del sitio web de Web-Out. S.A. desplegado en un entorno de prueba. En la cual se ha agregado un registro de Log “CustomLog” el cual nos permite obtener el protocolo SSL y la Suite de Cifrado negociados con el cliente web, en la parte inferior se muestra un resumen del número de clientes que han empleado determinada versión, dirección IP del cliente y suite de cifrado, existiendo una mayoría de conexiones por medio de TLS versión 1.2 y con la suite

de cifrado ECDHE-RSA-AES256-GCM-SHA384, seguido de TLS Versión 1.3 y suite de cifrado TLS_AES_128_GCM_SHA256.

- **Análisis de Resultados**

El tiempo de negociación entre el cliente y servidor cuando se conecta por medio de TLS versión 1.2 es de 0.016543 ms. y 1.426792 ms. para los sitios web de Web-Out y Hotel Natural Green respectivamente. Estos tiempos son relativamente mayor en comparación del tiempo de negociación del protocolo TLS versión 1.3, siendo 0.012122 ms. para el sitio Web-Out y 0.015254 ms. para el sitio web Hotel Natural Green en el ambiente de prueba. Llegando a la conclusión que el protocolo TLS versión 1.3 es relativamente más rápido que TLS versión 1.2

Estos resultados concuerdan con las características de la versión TLS versión 1.3, ya que se caracterizan por ser mucho más eficientes y seguros en el proceso de negociación (Rescorla, 2018). Se recomienda su uso tanto de ambas versiones siendo las más actuales y eficientes en cuando a la conexión de equipos cliente – servidor por medio del protocolo SSL/TLS.

## 4.3 Discusión

El estudio del “Cifrado con el Protocolo SSL/TLS y el rendimiento de los sitios web. Caso Empresa Web-Out., 2018-2019” permitió cumplir con los objetivos de esta investigación.

La hipótesis general de la investigación responde positivamente respecto a las diversas pruebas realizadas en las que se ha podido comprobar que el uso del protocolo SSL/TLS genera un impacto poco significativo en el rendimiento de los cinco sitios web que son caso de estudio de esta investigación. En la Tabla 34 se describe la discusión por cada antecedente.

**Tabla 34.** Comparación de los antecedentes de la investigación con la presente tesis.

| Antecedente | Discusión |
|---|---|
| “Caracterización y medida pasiva del rendimiento para conexiones web seguras HTTPS” | Este antecedente tiene cierta similitud con la presente investigación ya que el objetivo fue el análisis de la sobrecarga de los algoritmos de cifrado como AES, 3DES, CAMELLIA, SEED Y RC4 con el objetivo de determinar si existía un gran consumo de recursos computacionales; lo cual para esta investigación también ha sido necesario conocer el rendimiento de los algoritmo de cifrado empleados en las conexiones HTTPS con los sitios web, a diferencia de los algoritmos estudiados en esta investigación fue la que utilizó el cliente(navegador) y el servidor para la comunicación por HTTPS. En ambas investigaciones se concluye que es necesario emplear los algoritmos que se adapten mejor al entorno y ambientes de trabajo, conociendo que el cifrado si implica un costo computacional. |

| | |
|---|---|
| “Performance Analysis of TLS Web Servers” | En ambas investigaciones se realizaron un estudio del rendimiento del protocolo SSL/TLS, a diferencia que las pruebas realizadas en el antecedente fueron de la versión 1.0 en la que los algoritmos de cifrado y las características de los servidores web son diferentes o inferiores respecto de las últimas versiones; para esta investigación se utilizó la versión 1.2 de TLS y una pequeña prueba de una conexión a dos sitios web por TLS versión 1.3. La investigación del antecedente llega a la conclusión que el algoritmo RSA es una operación costosa hablando en términos de rendimiento para el proceso de cifrado y descifrado consumiendo entre un 13% a 58%. Para la presente investigación se realizó una medición del rendimiento para el proceso de firmado y verificación de la firma siendo mucho más rápido el proceso de firmado que la de verificación de la firma cuando el tamaño de clave es de 2048 bits. |
| “Análisis de vulnerabilidades del protocolo SSL/TLS en las páginas web gubernamentales del ecuador más usadas en la carrera de ingeniería en Networking y Telecomunicaciones” | En este trabajo de investigación de realizo un análisis de las vulnerabilidades del protocolo SSL/TLS ubicado en el transporte de la información a paginas gubernamentales del Ecuador empleando la herramienta Qualys SSL Labs. En esta investigación también se ha empleado esta herramienta Online que además de evaluar el nivel de seguridad de los sitios web, también se analizó el tiempo de carga cuando se realizan diversas peticiones al servidor de manera simultánea, visualizar cómo influye en tamaño del sitio web y el número de solicitudes que se emplean para la conexión a los sitios web por medio de HTTP y HTTPS. |
| “Implementación de protocolo de cifrado TLS para mejorar la | Esta tesis como antecedente se basó en la implementación del protocolo SSL/TLS en sus versiones TLS versión 1.1 y 1.2 llegando a la |

| | |
|---|---|
| seguridad de las comunicaciones en la capa de transporte 2016” | conclusión que se ha logrado implementar correctamente y que los navegadores más comunes soportan ya estas versiones. Mantiene una similitud respecto al protocolo TLS v 1.2 pero solo aborda el la instalación y configuración mas no el tema del rendimiento de dicho protocolo en los sitios web. |
| “Técnicas de encriptación para mejorar la seguridad en la transferencia de archivos en un entorno fiable” | En este trabajo de investigación se realizaron diversas pruebas de encriptación con los algoritmos RSA y AES, guardando una relación con esta investigación en que dichos algoritmos fueron parte del estudio llegando ambos a la conclusión que RSA y AES brindan una gran velocidad de procesamiento, y seguridad a la información cifrada. |

**Fuente:** Elaboración propia.

## CONCLUSIONES

Al evaluar el rendimiento de los sitios web, teniendo habilitado y deshabilitado el protocolo SSL/TLS se ha podido conocer y medir el impacto generado afirmando que brinda una navegación segura entre en cliente y servidor, siendo cada vez más utilizado por los sitios web a nivel mundial; por lo que la presente tesis se enfocó en medir el rendimiento de dicho protocolo en los cinco sitios web creados y administrados por la Empresa Web-Out S.A. como caso de estudio; con base en las pruebas y análisis de resultados alineados al objetivo general y los objetivos específicos de la investigación, se llegó a las siguientes conclusiones:

1. Se comprobó que el cifrado mediante el protocolo SSL/TLS en su versión 1.2 de TLS no influye significativamente en el tiempo de procesamiento de los cinco sitios web, debido a que el número de solicitudes es el mismo cuando el sitio web es accedido por HTTP y HTTPS, así mismo el porcentaje del incremento del tiempo de carga de cada sitio web no sobrepasan del 7% para los sitios web de la Facultad de Ciencias Económicas y Administrativas de la UNAS, Hotel Oro Verde, Hotel Natural Green y la Cámara de Comercio Canadá - Perú a excepción del sitio web de Web-Out. S.A. existiendo un 15% lo que demuestra que el tiempo de carga del sitio web no se ve significativamente afectado por el proceso de cifrado y descifrado, demostrando que es favorablemente beneficiado asegurando una comunicación segura con un incremento mínimo de tiempo de procesamiento.

2. Se comprobó que el cifrado mediante el protocolo SSL/TLS no influye significativamente en el nivel de solicitudes que pueda atender un servidor web, resultando favorable para el rendimiento del sitio web, ya que se realizaron 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 las cuales albergan a los cinco sitios web caso de estudio de esta investigación. 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 25% para la cámara de Comercio de Canadá Perú.

3. Se comprobó que el cifrado mediante el protocolo SSL/TLS no influye significativamente en el nivel de transferencia de información generando beneficios para el sitio web, debido a que cada vez es mayor el rendimiento de los ordenadores haciendo que el proceso de cifrado y descifrado de dicha información no influya significativamente en el tiempo de carga de los sitios web, se ha podido conocer el tamaño del sitio web y de manera específica el tamaño por tipo de contenido el cual está estrechamente relacionado con el número de solicitudes que es necesario enviar al servidor para que el sitio web cargue en su totalidad. Asimismo, se ha podido conocer que si los sitios web y la configuración del servidor permiten el

guardado en cache de manera temporal ayuda significativamente en reducir los Kilobytes transferidos desde el servidor al cliente en más del 50% y de la misma forma existe una reducción del tiempo de carga en más del 50% para dichos sitios web.

4. Se comprobó que el protocolo SSL/TLS influye de manera positiva en el nivel de seguridad de los sitios web, ya que sin ello la navegación por medio de HTTP es totalmente legible y puede ser fácilmente interceptado. Para mantener seguro nuestros sitios web es necesario tener deshabilitado las versiones SSL versión 2, 3 y TLS versión 1.0, porque se han identificado diversas vulnerabilidades y graves fallos de seguridad en los algoritmos de cifrado, asimismo el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI Security Standards Council, 2016) prohíbe el uso de todas las versiones SSL y de TLS versión 1.0 y TLS versión 1.1 asegurando que en esta última existen implementaciones no seguras. Es importante el uso de TLS versión 1.2 y TLS versión 1.3, encontrándose habilitado en la configuración del servidor siendo las versiones más modernas y seguras. Se logró realizar la comprobación de vulnerabilidades mediante diversas herramientas como: Analyze.py, TestSSL, SSLyze, Qualys SSL Labs, obteniéndose de este último una calificación de entre A y B a los cinco sitios web tal como se muestra en la Tabla 28 resultando ser positivo para los sitios web, demostrando la seguridad que brindan cuando se accede a los sitios web por medio del protocolo SSL/TLS.

## RECOMENDACIONES

Se ha podido comprobar que mientras más componentes (imágenes, archivos css, archivos java script, videos, etc) 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.

Se recomienda que para el uso de TLS versión 1.1, se debe de realizar un previo estudio y análisis, identificando si esta versión es empleado por un gran porcentaje de clientes web cuando acceden a determinado sitio web, y dependiendo de este porcentaje se deberá de tomar una decisión si debe de mantenerse habilitado o deshabilitarlo por completo, para conocer si esta Versión es empleada en la comunicación por HTTPS debemos de agregar un registro de Log para cada sitio web.

Como trabajo futuro se recomienda utilizar el protocolo TLS versión 1.3 para el análisis del rendimiento, en esta investigación se realizó un análisis preliminar del tiempo que emplea durante el proceso de negociación utilizando la herramienta Wireshark versión 3.0.1, se plantea utilizar herramientas más completas y desarrolladas principalmente para medir el tiempo de carga de los sitios web cuando hacen uso de esta versión de protocolo.

Si bien el mantener seguro nuestras aplicaciones con el protocolo SSL/TLS involucra realizar pruebas respecto a la seguridad y rendimiento, se recomienda elaborar un segundo ambiente muy similar al ambiente de producción donde se puedan realizar pruebas, actualización de requerimientos como Apache y OpenSSL que soporten TLS versión 1.3, de manera que no impida el correcto funcionamiento de los sitios web que se encuentran activos y en producción.

Se recomienda realizar futuras investigaciones sobre el rendimiento del protocolo SSL/TLS haciendo uso de la versión TLS versión 1.3 y la versión del protocolo HTTP/2; que según la documentación encontrada en diversos sitios web, brindan una mayor velocidad y seguridad a las conexiones HTTPS.

# GLOSARIO

- **Algoritmo**

  Una secuencia ordenada y finita de pasos u operaciones que contribuyen a resolver un problema.

- **Confidencialidad**

  (Roa Buendia, 2013, pág. 15) en su libro “Seguridad Informática” menciona que la confidencialidad consiste en que el acceso a la información por personas o equipos computacionales sea solamente siempre en cuando estos pasaron por un mecanismo de autentificación, autorización y cifrado.

- **Integridad**

  La descripción que da Roa Buendía (Roa Buendia, 2013), es que la integridad consiste en que “los datos queden almacenados (pág. 15)

- **Autenticidad**

  Tanto el emisor como el receptor debe de confirmar su identificación.

- **Autoridad Certificadora**

  Es la entidad de confianza que se encarga de emitir y revocar/eliminar los certificados digitales brindando confianza ante validaciones de terceros.

- **Certificado Digital**

  Es el medio digital que permite identificar la información de una entidad, así como brindar a su vez una información extra. Estos son emitidos por la autoridad certificadora y tiene un periodo de validez que es un factor que asegura la confiabilidad de esta.

- **Cifrado**

  En el diccionario de la Real Academia Española (RAE) el término “cifrado” proviene del adjetivo cifrar, que se refiere a transcribir en guarismos, letras o símbolos, de acuerdo con una clave cuyo contenido se quiere proteger.

- **Servidor Web**

  Programa que atiende a peticiones realizadas por un navegador proporcionando los recursos vía http o https.

- **Sitio Web**

  La definición que Mozilla MDN Web Docs establece para “sitio web” (Marcos & Narvaez, 2018) es la siguiente: “*Un sitio web es una colección de páginas web vinculadas (más sus recursos asociados) que comparten un único nombre de dominio. Cada página web de un sitio web determinado proporciona enlaces explícitos - la mayoría del tiempo en forma de parte del texto que se puede hacer clic - que permite al usuario moverse de una página del sitio a otra”.*

## REFERENCIAS BIBLIOGRÁFICAS


Aas, J. (Diciembre de 2018). *Looking Forward to 2019*. Obtenido de Let's Encrypt: https://letsencrypt.org/2018/12/31/looking-forward-to-2019.html

Adrián, P. (2011). *Algoritmo de cifrado simétrico AES. Aceleración de tiempo de Computo sobre arquitecturas multicore.* La Plata, Argentina. Obtenido de http://sedici.unlp.edu.ar/handle/10915/4210

Alvarado Sarango, D. J. (2016). *Implementación de seguridad en la capa de transporte del modelo TCP/IP en los servidores web y de aplicación de la Universidad Nacional de Loja.* Loja, Ecuador. Obtenido de http://dspace.unl.edu.ec/jspui/handle/123456789/18533

Ariansen Moncada, R. A., & Rojas Diaz, J. (s.f.). *Implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte 2016.* Chiclayo, Perú. Obtenido de http://renati.sunedu.gob.pe/handle/sunedu/115095

Bellovin, S. M. (2018). Understanding Flaws in the Deployment and Implementation of Web Encryption. New York, Estados Unidos. Obtenido de https://academiccommons.columbia.edu/doi/10.7916/D8001JJ6

Burnside, M., & Keromytis , A. (Octubre de 2003). Accelerating Application - Level Security Protocols. *IEEE Xplore Digital Library*. Obtenido de https://academiccommons.columbia.edu/doi/10.7916/D8TH8X2R

Caballero Romero, A. (2014). *Metodología integral innovadora para planes y tesis.* México.

Cardador Cabello, A. L. (Julio de 2014). Desarrollo de aplicaciones web distribuidas (UF1846). IC Editorial. Obtenido de https://ebookcentral.proquest.com/lib/bibliotecaunassp/detail.action?docID=4184019&query=Desarrollo+de+aplicaciones#

Carvajal Palomares, F. (Enero de 2017). Administración y Auditoría de los servicios web. Editorial CEP, S.L. Obtenido de https://ebookcentral.proquest.com/lib/bibliotecaunassp/detail.action?docID=5213972&query=administracion+y+auditoria+de+los+servidores#

Chapaca Garzón, J., & Rojas Bustamante, J. D. (2013). *Análisis, Diseño y desarrollo de un prototipo de Protocolo de transporte basado en comunicación TCP con capacidad de cubrir las necesidades de transferencia de datos seguros, confiables y de alta disponibilidad.* Quito, Ecuador. Obtenido de https://dspace.ups.edu.ec/handle/123456789/6354

Coarfa, C., Druschel, P., & Wallach, D. (2006). Performance Analysis of TLS Web Servers. *IEEE Xplore Digital Library*, 39-69. Obtenido de https://www.cs.rice.edu/~dwallach/pub/tls-tocs.pdf

Dierks, T., & Rescorla, E. (Abril de 2006). *The Transport Layer Security (TLS) Protocol Versión 1.1*. Obtenido de RFC 4346: https://www.ietf.org/rfc/rfc4346.txt

Escrivá Gascó, G., Romero Serrano, R. M., Jorge Ramada, D., & Onrubia Pérez, R. (2013). *Seguridad Informática.* Macmillan Iberia, S.A. Obtenido de https://ebookcentral.proquest.com/lib/bibliotecaunassp/detail.action?docID=3217398

GlobalSign. (2018). *¿Qué es SSL?* Obtenido de GlobalSign: https://www.globalsign.com/es/centro-de-informacion-ssl/que-es-ssl/

Google. (07 de Agosto de 2014). *El Blog para Webmasters*. Obtenido de HTTPS como señal del ranking: https://webmaster-es.googleblog.com/2014/08/https-como-senal-del-ranking.html

Granda, K., & Saquicela Parra, L. (2017). *Análisis de vulnerabilidades del protocolo SSL/TLS en las paginas web gubernamentales del ecuador mas usadas en la carrera de ingeniería en Networking y Telecomunicaciones.* Guayaquil, Ecuador. Obtenido de http://repositorio.ug.edu.ec/handle/redug/24303

Haro Montero, M. A., & Gavilanes Sagñay, F. M. (2009). *Análisis de funciones criptográficas de código libre en los protocolos SSL y TLS aplicado al portal web de la jefatura provincial de tránsito de Chimborazo.* Riobamba, Ecuador. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/55

Hernández Encinas, L. (01 de Enero de 2016). La criptografía. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la Investigación* (Sexta ed.). México: McGRAW-HILL.

Herrera Joancomartí, J., García Alfaro, J., & Perramón Tornil, X. (2004). *Aspectos avanzados de Seguridad en Redes.* Barcelona. Obtenido de http://www.sw-computacion.f2s.com/Linux/012.1-Aspectos_avanzados_en_seguridad_en_redes_modulos.pdf

Holmes, D. (23 de Abril de 2018). *The 2017 TLS Telemetry Report.* Obtenido de F5 Labs: https://www.f5.com/labs/articles/threat-intelligence/the-2017-tls-telemetry-report

IBM. (s.f.). *Cómo SSL y TLS proporcionan la identificación, la autenticación, la confidencialidad y la integridad*. Recuperado el 22 de Mayo de 2019, de IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_8.0.0/com.ibm.mq.sec.doc/q009940_.htm

Internet Assigned Numbers Authority. (22 de Abril de 2019). *Transport Layer Security (TLS) Parameters*. Obtenido de https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Kuo, F.-C., Tschofenig, H., & Meyer, F. (2006). Comparison Studies between Pre-Shared and Public Key Exchange Mechanisms for Transport Layer Security. *IEEE Xplore Digital Library*. Obtenido de https://ieeexplore.ieee.org/document/4146705/

Li, H., & Zhao, G. (2012). Improving Secure Server Performance By EAMRSA SSLHandshakes. *IEEE Xplore Digital Library*. Obtenido de https://ieeexplore.ieee.org/document/6322794/

López Fernández, M. (18 de Setiembre de 2015). Caracterización y medida pasiva del rendimiento para conexiones Web seguras HTTPS. España. Obtenido de http://academica-e.unavarra.es/handle/2454/18683

Luis Com, S., Ernesto Ackerman, S., & Alvin Postolski, G. (2013). *Metodología de la Investigación.* Buenos Aires, Argentina.

Marcos, & Narvaez, D. (16 de Enero de 2018). *¿Cuál es la diferencia entre la página web, el sitio web, el servidor web y el motor de búsqueda?* Obtenido de https://developer.mozilla.org/es/docs/Learn/Common_questions/Pages_sites_servers_and_search_engines

Mateu, C. (2004). *Desarrollo de Aplicaciones Web.* Barcelona.

Matute, G., Cuervo, S., Salazar , S., & Santos , B. (Mayo de 2012). Del consumidor convencional al consumidor digital El caso de las tiendas por departamento. (1). Lima: Cecosami Preprensa e Impresión Digital S. A.

Mejía Mejía, E. (Julio de 2005). *Investigación Educativa.* Obtenido de Revistas de investigación UNMSM: https://es.scribd.com/document/312926678/Libro-Metodologia-de-La-Investigacion-Cientifica-Elias-Mejia-Mejia-UNSM

Muñoz Muñoz, A., & Ramió Aguirre, J. (2013). *Cifrado de las comunicaciones digitales de la cifra clásica al algoritmo* (Segunda ed.). Madrid. Obtenido de https://0xword.com/es/libros/36-libro-cifrado-comunicaciones-rsa.html

Navarro, J., Ubilla, G., & Tejeda, M. (2014). *Protocolo TLS.* Valparaíso - Chile.

Netcraft. (10 de Mayo de 2019). *May 2019 Web Server Survey*. Obtenido de https://news.netcraft.com/archives/2019/05/10/may-2019-web-server-survey.html

NIGNX. (Julio de 2014). NGINX SSL Performance. San Francisco. Obtenido de https://www.nginx.com/wp-content/uploads/2014/07/NGINX-SSL-Performance.pdf

Oporto Guzmán, A. M. (2016). *Optimización del tiempo de respuesta en el cifrado de datos utilizando computación de alto desempeño por GPGPU.* Arequipa, Perú. Obtenido de http://tesis.ucsm.edu.pe/repositorio/handle/UCSM/2169

Ordoñez Calero, H. D. (2013). *Desarrollo del módulo de gestión de información técnica para TELALCA S.A e implementación de Seguridad mediante Cifrado SSL del protocolo https.* Quito, Ecuador. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/7211

Pallmall, A. (2014). *Demografía, un problema global.* Obtenido de https://ebookcentral.proquest.com

PCI Security Standards Council. (2016). Migrar de SSL y TLS temprana. *Suplemento Informativo*, 9. Obtenido de https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Info_Supp_v1-1_es-LA.pdf

Qualys SSL Labs. (03 de Mayo de 2019). *SSL Pulse*. Obtenido de https://www.ssllabs.com/ssl-pulse/

Qualys SSL Labs. (Mayo de 2019). *SSL Server Rating Guide*. Obtenido de https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

Rescorla, E. (Agosto de 2018). The Transport Layer Security (TLS) Protocol Version 1.3. *Request for Comments: 8446*. doi:10.17487/RFC8446

Ristic, I. (2014). *Bulletproof SSL and TLS: The Complete Guide to Deploying Secure Servers and Web Applications.* Obtenido de https://www.feistyduck.com/books/bulletproof-ssl-and-tls/

Ristić, I. (03 de Mayo de 2019). *Qualys SSL Labs*. Obtenido de SSL Pulse: https://www.ssllabs.com/ssl-pulse/

Roa Buendia, J. F. (2013). *Seguridad Informática.* España: McGraw-Hill España. Recuperado el 20 de 07 de 2018, de https://ebookcentral.proquest.com/lib/bibliotecaunassp/detail.action?docID=3211239

S., T., & T. Polk. (Marzo de 2011). *Prohibiting Secure Sockets Layer (SSL) Version 2.0*. Obtenido de Internet Engineering Task Force (IETF): https://tools.ietf.org/html/rfc6176

Sabogal Rosas, J. (Julio de 2015). Modelamiento de una plataforma virtual para la gestión de avisos normativos y de trámite legal. Piura.

Sánchez Vallejos, J. M. (2017). *Técnicas de encriptación para mejorar la seguridad en la transferencia de archivos en un entorno fiable.* Pimentel, Perú. Obtenido de http://renati.sunedu.gob.pe/handle/sunedu/160635

Schechter, E. (Octubre de 2017). *Say "yes" to HTTPS: Chrome secures thee web, one site at a time*. Obtenido de Safety and Security: https://www.blog.google/technology/safety-security/say-yes-https-chrome-secures-web-one-site-time/

Shen, C., Nahum, E., Schulzrinne, H., & Wright, C. (2009). The Impact of TLS on SIP Server Performance.

StatCounter. (Abril de 2019). *Cuota de Mercado por navegador a nivel Mundial*. Obtenido de http://gs.statcounter.com/

T. Dierks, E. R. (Agosto de 2008). The Transport Layer Security (TLS) Protocol - Version 1.2. *Request for Comments: 5246*. doi:10.17487/RFC5246

Valdiviezo Echeverria, T. A. (2012). *Análisis de la tecnología PKI y su aplicación en el aseguramiento de los servicios corporativos www, ftp y http.* Riobamba, Ecuador. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/2915

Villada Romero, J. L. (2015). *Instalación y configuración del software de servidor web (UF1271).* IC Editorial. Obtenido de https://ebookcentral.proquest.com/lib/bibliotecaunassp/detail.action?docID=4310544

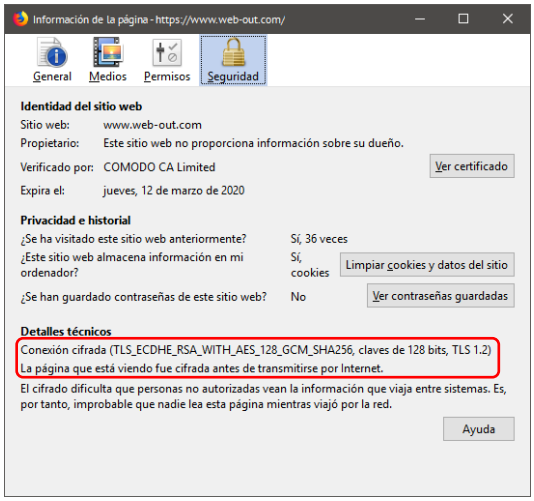
# ANEXOS

**ANEXO 1.** Matriz de Consistencia.

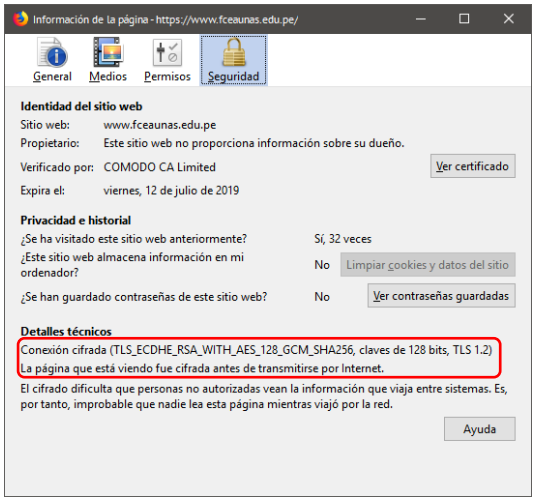
| PROBLEMA | OBJETIVOS | HIPÓTESIS | VARIABLE | DIMENSIONES | INDICADORES | METODOLOGÍA |
|---|---|---|---|---|---|---|
| **General.**<br>¿Cuál es el impacto que el cifrado con el protocolo SSL/TLS produce en el rendimiento de los sitios web, caso empresa Web-Out S.A.?<br><br>**Específicos**<br>**1.** ¿De qué manera influye el cifrado mediante el protocolo SSL/TLS en el tiempo de procesamiento de los sitios web?<br><br>**2.** ¿De qué manera influye el cifrado mediante el protocolo SSL/TLS en el nivel de solicitudes de usuarios que puede soportar un sitio web?<br><br>**3.** ¿De qué manera influye el cifrado mediante el protocolo SSL/TLS en la transferencia de información que existe cuando se ingresa a un sitio web?<br><br>**4.** ¿De qué manera influye el cifrado mediante el protocolo SSL/TLS en el nivel de seguridad del sitio web? | **General.**<br>Evaluar el impacto del cifrado con el protocolo SSL/TLS en el rendimiento de los sitios web de la empresa Web-Out. S.A. para conocer si dicho protocolo genera un impacto negativo en la carga de los sitios web, con el fin de brindar recomendaciones respecto a la configuración y uso correcto del protocolo para mejorar el rendimiento y seguridad del sitio web.<br><br>**Específicos**<br>**1.** Determinar el nivel de influencia del Cifrado mediante el protocolo SSL/TLS en el tiempo de procesamiento de los sitios web.<br>**2.** Determinar la influencia del cifrado con SSL/TLS en el nivel de solicitudes de usuarios que puede soportar un sitio web.<br>**3.** Determinar la influencia del cifrado con el protocolo SSL/TLS en el nivel de transferencia de información que existe cuando se ingresa a un sitio web.<br>**4.** Determinar la influencia del cifrado con el protocolo SSL/TLS en el nivel de seguridad del sitio web? | **General.**<br>El cifrado con el uso del protocolo SSL/TLS tiene un impacto poco significativo en el rendimiento de los sitios web de la Web-Out S.A.<br><br>**Específicos**<br>**1.** El cifrado mediante el protocolo SSL/TLS no influye significativamente en el tiempo de procesamiento de los sitios web.<br><br>**2.** El cifrado mediante el protocolo SSL/TLS no influye significativamente en el nivel de solicitudes de usuario que pueda soportar un sitio web.<br><br>**3.** El cifrado mediante el protocolo SSL/TLS no influye significativamente en el nivel de transferencia de información que provoca el acceder a un sitio web.<br><br>**4.** El cifrado mediante el protocolo SSL/TLS influye significativamente en el nivel de seguridad del sitio web. | **Variable Independiente "X"**<br>Cifrado mediante el protocolo SSL/TLS | **Dim. 1:**<br>Fortaleza del algoritmo de cifrado. | - Tiempo de procesamiento del algoritmo de cifrado, firmado y verificación de la firma.<br>- Velocidad de cifrado de algoritmos simétricos.<br>- Costo computacional. | **Tipo de Investigación:**<br>Aplicada<br><br>**Método de investigación:**<br>Cuasi Experimental.<br><br>**Población: cinco**<br>Sitios web administrado por la empresa Web-Out S.A.<br><br>**Muestra:** Para este estudio se trabajará con toda la población.<br><br>**Instrumentos de Recolección de información:**<br>**-** Observación.<br>- Sniffer (wireshark).<br>- OpenSSL.<br>- Htop.<br>- SSLRobot.<br>- Qualys SSL Labs<br>- PingDom Tools<br>- SSLyze. |
| | | | | **Dim. 2**<br>Rendimiento frente a ataques. | - Fortaleza de clave de cifrado.<br>- Fortaleza de algoritmos de cifrado. | |
| | | | **Variable Dependiente "Y"**<br>Rendimiento de sitios web | **Dim. 1:**<br>Tiempo de procesamiento. | - Latencia.<br>- Tiempo de carga de cada sitio web.<br>- Tiempo de descarga de elemento web desde el servidor al cliente (solicitudes web). | |
| | | | | **Dim. 2:**<br>Nivel de solicitudes de usuarios. | - Número de usuarios concurrentes que pueden ser procesados simultáneamente.<br>- Número total de paquetes intercambiados. | |
| | | | | **Dim 3:**<br>Transferencia de información. | - Cantidad de bytes descargados.<br>- Número de solicitudes por tipo de contenido.<br>- Tamaño de las solicitudes por tipo de contenido. | |
| | | | | **Dim 4:**<br>Nivel de seguridad. | - Datos sin cifrar y datos cifrados (contenido mixto).<br>- Soporte del Protocolo SSL/TLS.<br>- Intercambio de llaves.<br>- Fuerza de cifrado.<br>- Vulnerabilidades al protocolo SSL/TLS. | |

**Fuente:** Elaboración propia.

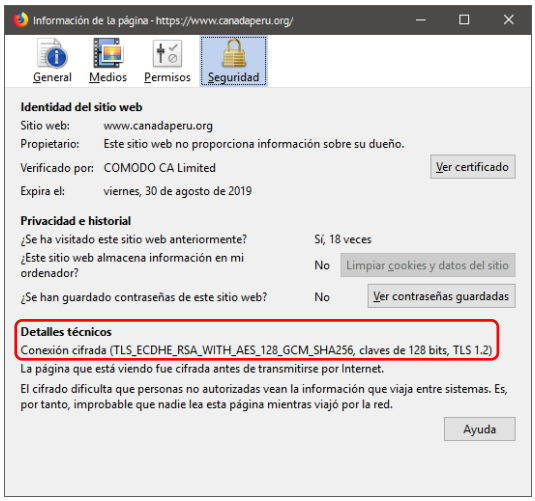
**ANEXO 2.** Detalles de la conexión cifrada por el Protocolo SSL/TLS.



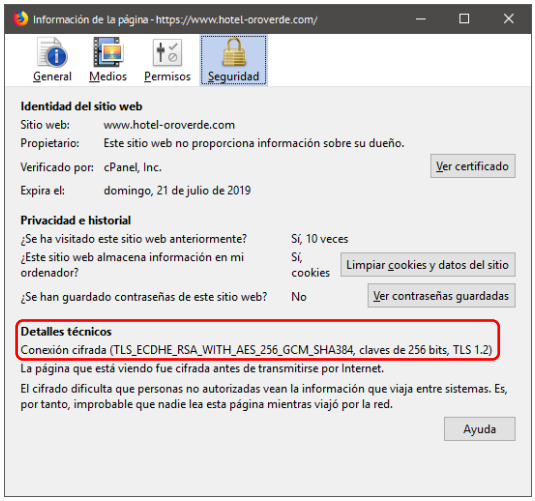

**Sitio web de Web-Out**



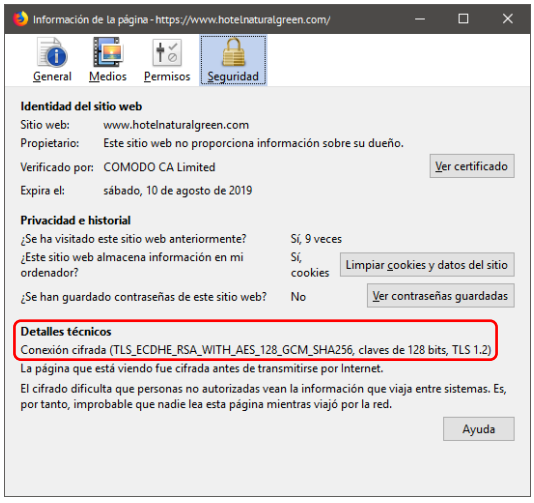

**Sitio web FCEA de la UNAS**




**Sitio web Cámara de Comercio Canadá - Perú**




**Sitio web Hotel Oro Verde**




**Sitio web Hotel Natural Green**

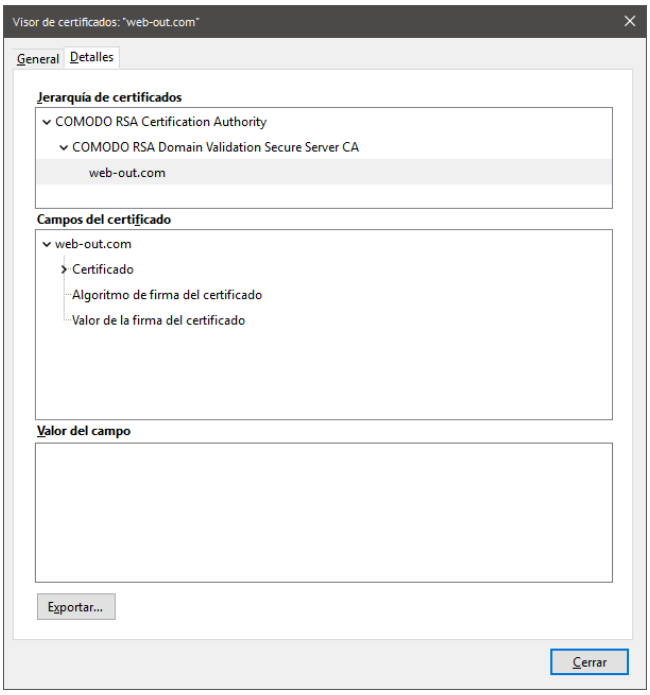
**ANEXO 3.** Ver cadena de certificado de un sitio web.

Para ver cadena completa del certificado de un sitio web podemos hacerlo mediante la herramienta OpenSSL.

```
openssl s_client -showcerts -host www.web-out.com -port 443 </dev/null
```

Existen herramientas la línea, incluso el propio navegador nos muestra como es la cadena de certificados.


**Fuente**: Digicert - www.digicert.com/help




**Fuente:** Elaboración Propia.
**Herramienta:** Mozilla Firefox Quantum v. 66.0.3

**ANEXO 4.** Pruebas de rendimiento de los cinco sitios web de la empresa Web-Out S.A.

**Web de Web-Out**

| Solicitudes | Concurrencia | PRUEBA 1 | | | | PRUEBA 2 | | | | PRUEBA 3 | | | | PRUEBA 4 | | | | PRUEBA 5 | | | | PROMEDIO | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | |
| | | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken (segundos) | Request per Second |
| 1 | 1 | 0.504 | 1.98 | 0.242 | 4.13 | 0.243 | 4.11 | 0.263 | 3.8 | 0.206 | 4.84 | 0.285 | 3.51 | 0.219 | 4.58 | 0.217 | 4.6 | 0.216 | 4.63 | 0.245 | 4.08 | 0.278 | 4.028 | 0.250 | 4.024 |
| 100 | 20 | 3.862 | 25.9 | 3.531 | 28.32 | 4.221 | 23.69 | 4.017 | 24.89 | 4.736 | 21.11 | 3.935 | 25.41 | 3.875 | 25.81 | 3.714 | 26.93 | 4.072 | 24.56 | 3.808 | 26.26 | 4.153 | 24.214 | 3.801 | 26.362 |
| | 40 | 3.978 | 25.14 | 3.836 | 26.07 | 3.544 | 28.22 | 4.283 | 23.35 | 6.706 | 14.91 | 4.057 | 24.65 | 5.165 | 19.36 | 3.463 | 28.88 | 5.844 | 17.11 | 4.696 | 21.29 | 5.047 | 20.948 | 4.067 | 24.848 |
| | 60 | 5.017 | 19.93 | 3.238 | 30.88 | 3.773 | 26.5 | 4.863 | 20.57 | 3.59 | 27.85 | 4.392 | 22.77 | 3.944 | 25.36 | 3.493 | 28.63 | 4.445 | 22.5 | 3.55 | 28.17 | 4.154 | 24.428 | 3.907 | 26.204 |
| | 80 | 7.376 | 13.56 | 5.649 | 17.7 | 7.284 | 13.73 | 5.811 | 17.21 | 6.862 | 14.57 | 3.405 | 29.37 | 3.949 | 25.32 | 3.337 | 29.97 | 3.82 | 26.18 | 3.559 | 28.1 | 5.858 | 18.672 | 4.352 | 24.470 |
| | 100 | 3.822 | 26.17 | 3.575 | 27.97 | 3.949 | 25.33 | 3.849 | 25.98 | 3.615 | 27.66 | 3.829 | 26.12 | 3.995 | 25.03 | 3.602 | 27.76 | 3.765 | 26.56 | 3.438 | 29.09 | 3.829 | 26.150 | 3.659 | 27.384 |
| 500 | 20 | 30.702 | 16.29 | 22.913 | 21.82 | 21.525 | 23.23 | 23.857 | 20.96 | 19.88 | 25.15 | 19.286 | 25.93 | 22.503 | 22.22 | 24.349 | 20.53 | 27.087 | 18.46 | 23.267 | 21.49 | 24.339 | 21.070 | 22.734 | 22.146 |

**Facultad de Ciencias Económicas y Administrativas de la UNAS**

| Solicitudes | Concurrencia | PRUEBA 1 | | | | PRUEBA 2 | | | | PRUEBA 3 | | | | PRUEBA 4 | | | | PRUEBA 5 | | | | PROMEDIO | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | |
| | | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second |
| 1 | 1 | 0.072 | 13.92 | 0.034 | 29.58 | 0.062 | 16.13 | 0.043 | 23.3 | 0.051 | 19.45 | 0.039 | 25.82 | 0.048 | 20.96 | 0.039 | 25.49 | 0.049 | 20.45 | 0.029 | 34.21 | 0.056 | 18.182 | 0.037 | 27.680 |
| 100 | 20 | 0.97 | 103.12 | 0.905 | 110.51 | 0.902 | 110.84 | 0.747 | 133.95 | 0.824 | 121.34 | 0.926 | 108 | 0.922 | 108.4 | 0.815 | 122.71 | 0.783 | 127.73 | 0.83 | 120.55 | 0.880 | 114.286 | 0.845 | 119.144 |
| | 40 | 0.956 | 104.63 | 0.962 | 103.9 | 0.953 | 104.91 | 0.923 | 108.28 | 0.848 | 117.97 | 0.895 | 111.7 | 0.931 | 107.41 | 0.871 | 114.77 | 0.834 | 119.88 | 0.811 | 123.23 | 0.904 | 110.960 | 0.892 | 112.376 |
| | 60 | 1.072 | 93.26 | 0.79 | 126.63 | 0.797 | 125.54 | 0.766 | 130.54 | 0.763 | 131.13 | 0.833 | 120.05 | 1.686 | 59.3 | 0.761 | 131.34 | 0.877 | 113.99 | 0.799 | 125.09 | 1.039 | 104.644 | 0.790 | 126.730 |
| | 80 | 0.935 | 106.9 | 0.74 | 135.09 | 1.075 | 93.01 | 0.783 | 127.64 | 1.112 | 89.92 | 0.771 | 129.75 | 0.91 | 109.83 | 0.634 | 157.63 | 0.956 | 104.59 | 0.68 | 146.99 | 0.998 | 100.850 | 0.722 | 139.420 |
| | 100 | 0.792 | 126.25 | 0.748 | 133.73 | 0.908 | 110.14 | 0.738 | 135.46 | 0.86 | 116.32 | 0.727 | 137.62 | 0.905 | 110.48 | 0.658 | 152.07 | 0.701 | 142.56 | 0.658 | 151.96 | 0.833 | 121.150 | 0.706 | 142.168 |
| 500 | 20 | 4.973 | 100.54 | 3.646 | 137.13 | 5.028 | 99.44 | 3.586 | 139.45 | 5.365 | 93.19 | 3.7 | 135.13 | 5.395 | 92.68 | 4.133 | 120.97 | 4.919 | 101.64 | 5.492 | 91.04 | 5.136 | 97.498 | 4.111 | 124.744 |

**Camara de Comercio Canadá-Perú**

| Solicitudes | Concurrencia | PRUEBA 1 | | | | PRUEBA 2 | | | | PRUEBA 3 | | | | PRUEBA 4 | | | | PRUEBA 5 | | | | PROMEDIO | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | |
| | | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second |
| 1 | 1 | 1.274 | 0.79 | 1.016 | 0.98 | 1.085 | 0.92 | 1.156 | 0.87 | 1.064 | 0.94 | 1.11 | 0.9 | 0.986 | 1.01 | 1.045 | 0.96 | 1.264 | 0.79 | 1.122 | 0.89 | 1.135 | 0.890 | 1.090 | 0.920 |
| 100 | 20 | 25.538 | 3.92 | 25.24 | 3.96 | 28.383 | 3.52 | 26.109 | 3.83 | 31.957 | 3.13 | 25.639 | 3.9 | 28.441 | 3.52 | 26.416 | 3.79 | 26.341 | 3.8 | 26.677 | 3.75 | 28.132 | 3.578 | 26.016 | 3.846 |
| | 40 | 32.38 | 3.09 | 24.176 | 4.14 | 25.174 | 3.97 | 27.305 | 3.66 | 29.748 | 3.36 | 28.337 | 3.53 | 24.361 | 4.1 | 29.303 | 3.41 | 26.381 | 3.79 | 26.052 | 3.84 | 27.609 | 3.662 | 27.035 | 3.716 |
| | 60 | 24.854 | 4.02 | 23.663 | 4.23 | 26.79 | 3.73 | 24.489 | 4.08 | 26.005 | 3.85 | 24.842 | 4.03 | 25.568 | 3.91 | 24.693 | 4.05 | 28.806 | 3.47 | 27.787 | 3.6 | 26.405 | 3.796 | 25.095 | 3.998 |
| | 80 | 24.678 | 4.05 | 20.711 | 4.83 | 22.032 | 4.54 | 24.369 | 4.1 | 25.603 | 3.91 | 20.077 | 4.98 | 22.279 | 4.49 | 20.929 | 4.78 | 19.951 | 5.01 | 23.531 | 4.25 | 22.909 | 4.400 | 21.923 | 4.588 |
| | 100 | 23.442 | 4.27 | 27.828 | 3.59 | 33.847 | 2.95 | 26.335 | 3.8 | 24.163 | 4.14 | 25.456 | 3.93 | 22.984 | 4.35 | 23.59 | 4.24 | 23.758 | 4.21 | 22.018 | 4.54 | 25.639 | 3.984 | 25.045 | 4.020 |
| 500 | 20 | 140.09 | 3.57 | 147.413 | 3.39 | 130.36 | 3.84 | 137.729 | 3.63 | 142.977 | 3.5 | 128.234 | 3.9 | 133.667 | 3.74 | 117.713 | 4.25 | 131.816 | 3.79 | 138.194 | 3.62 | 135.782 | 3.688 | 133.857 | 3.758 |

| Hotel Oro Verde | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Solicitudes | Concurrencia | PRUEBA 1 | | | | PRUEBA 2 | | | | PRUEBA 3 | | | | PRUEBA 4 | | | | PRUEBA 5 | | | | PROMEDIO | | | |
| | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | |
| | | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second |
| 1 | 1 | 0.391 | 2.56 | 0.293 | 3.42 | 0.321 | 3.11 | 0.259 | 3.87 | 0.372 | 2.68 | 0.283 | 3.53 | 0.362 | 2.76 | 0.27 | 3.7 | 0.356 | 2.81 | 0.301 | 3.32 | 0.360 | 2.784 | 0.281 | 3.568 |
| 100 | 20 | 12.452 | 8.03 | 9.96 | 10.04 | 9.201 | 10.87 | 8.531 | 11.72 | 8.481 | 11.79 | 9.554 | 10.47 | 10.13 | 9.87 | 9.4 | 10.64 | 9.757 | 10.25 | 9.273 | 10.78 | 10.004 | 10.162 | 9.344 | 10.730 |
| | 40 | 9.062 | 10.41 | 9.09 | 11 | 5.466 | 18.3 | 2.233 | 44.78 | 9.574 | 10.45 | 5.688 | 17.58 | 2.547 | 39.26 | 5.581 | 17.92 | 2.494 | 40.1 | 2.286 | 43.75 | 5.829 | 23.704 | 4.976 | 27.006 |
| | 60 | 10.056 | 9.94 | 8.684 | 11.52 | 5.747 | 17.4 | 1.928 | 51.86 | 2.826 | 35.39 | 7.459 | 13.41 | 3.686 | 27.13 | 2.239 | 44.66 | 3.145 | 31.79 | 2.305 | 43.38 | 5.092 | 24.330 | 4.523 | 32.966 |
| | 80 | 8.678 | 11.52 | 2.192 | 45.61 | 2.211 | 45.23 | 2.179 | 45.9 | 2.114 | 47.31 | 3.135 | 31.9 | 8.54 | 11.71 | 9.537 | 10.49 | 9.024 | 11.08 | 9.457 | 10.57 | 6.113 | 25.370 | 5.300 | 28.894 |
| | 100 | 11.03 | 9.07 | 2.938 | 34.04 | 3.584 | 27.9 | 2.608 | 38.34 | 2.872 | 34.81 | 2.36 | 42.38 | 2.741 | 36.48 | 2.684 | 37.26 | 3.357 | 29.79 | 2.743 | 35.46 | 4.717 | 27.610 | 2.667 | 37.496 |
| 500 | 20 | 48.34 | 10.34 | 43.689 | 11.44 | 51.348 | 9.74 | 43.387 | 11.52 | 46.721 | 10.7 | 42.808 | 11.68 | 53.071 | 9.42 | 45.359 | 11.02 | 45.086 | 11.09 | 45.172 | 11.07 | 48.913 | 10.258 | 44.083 | 11.346 |

| Hotel Natural Green | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Solicitudes | Concurrencia | PRUEBA 1 | | | | PRUEBA 2 | | | | PRUEBA 3 | | | | PRUEBA 4 | | | | PRUEBA 5 | | | | PROMEDIO | | | |
| | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | | HTTPS | | HTTP | |
| | | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second | Time Taken | Request per Second |
| 1 | 1 | 0.493 | 2.03 | 0.488 | 2.05 | 0.507 | 1.97 | 0.507 | 1.97 | 0.46 | 2.17 | 0.486 | 2.06 | 0.587 | 1.7 | 0.466 | 2.15 | 0.529 | 1.89 | 0.436 | 2.29 | 0.515 | 1.952 | 0.477 | 2.104 |
| 100 | 20 | 13.287 | 7.53 | 10.12 | 9.88 | 12.711 | 7.87 | 13.829 | 7.23 | 13.801 | 7.25 | 12.534 | 7.98 | 13.312 | 7.51 | 13.071 | 7.65 | 12.131 | 8.24 | 12.981 | 7.7 | 13.048 | 7.680 | 12.507 | 8.088 |
| | 40 | 21.347 | 4.68 | 20.662 | 4.84 | 13.298 | 7.52 | 11.489 | 8.7 | 12.021 | 8.32 | 11.568 | 8.64 | 13.759 | 7.27 | 11.659 | 8.58 | 11.513 | 8.69 | 13.451 | 7.43 | 14.388 | 7.296 | 13.766 | 7.638 |
| | 60 | 13.288 | 7.53 | 9.86 | 10.14 | 12.87 | 7.77 | 13.446 | 7.44 | 13.73 | 7.28 | 12.803 | 7.81 | 10.529 | 9.5 | 11.093 | 9.01 | 10.24 | 9.77 | 10.049 | 9.95 | 12.131 | 8.370 | 11.450 | 8.870 |
| | 80 | 14.89 | 6.72 | 13.643 | 7.33 | 14.524 | 6.88 | 12.668 | 7.89 | 13.033 | 7.67 | 12.322 | 8.12 | 11.979 | 8.35 | 13.979 | 7.15 | 11.64 | 8.59 | 11.125 | 8.99 | 13.213 | 7.642 | 12.747 | 7.896 |
| | 100 | 14.381 | 6.95 | 11.923 | 8.39 | 11.809 | 8.47 | 12.66 | 7.9 | 13.749 | 7.27 | 13.014 | 7.68 | 12.241 | 8.17 | 12.195 | 8.2 | 11.188 | 8.94 | 12.214 | 8.19 | 12.674 | 7.960 | 12.401 | 8.072 |
| 500 | 20 | 122.488 | 4.08 | 122.235 | 4.09 | 99.607 | 5.02 | 115.959 | 4.31 | 115.697 | 4.32 | 123.463 | 4.05 | 143.505 | 3.48 | 139.072 | 3.6 | 162.085 | 3.08 | 137.712 | 3.63 | 128.676 | 3.996 | 127.688 | 3.936 |

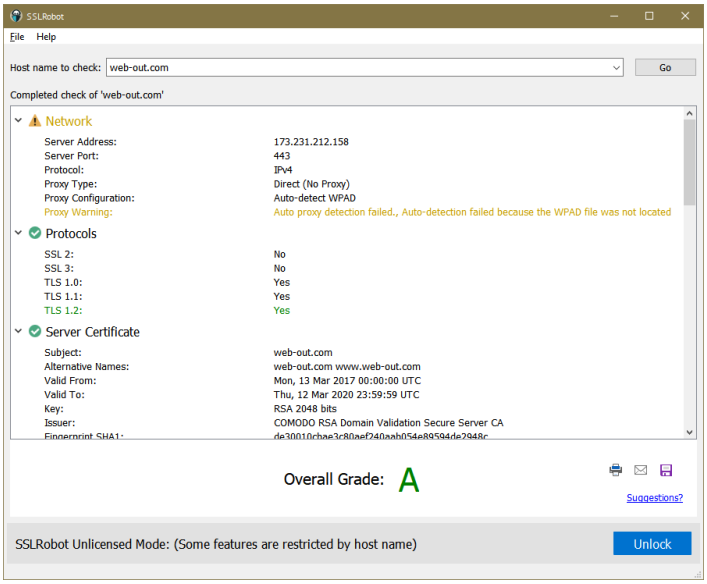
**Fuente:** Elaboración propia.

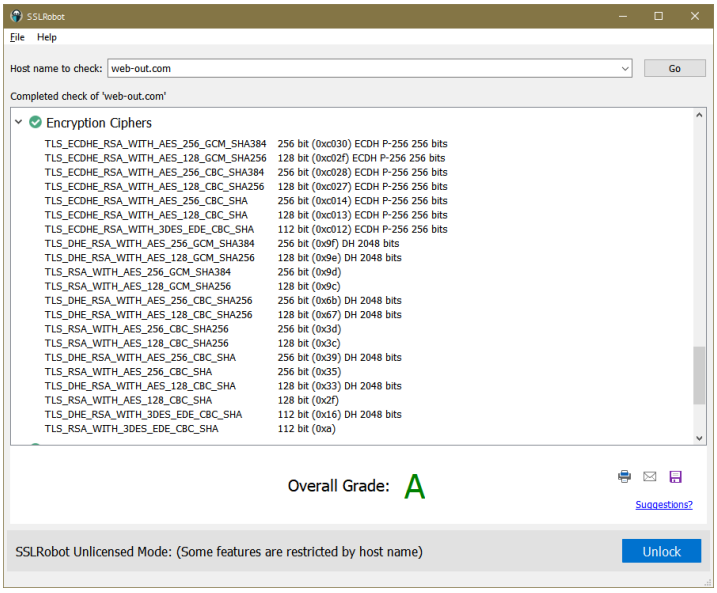
**ANEXO 5.** Test de carga de los cinco sitios web, indicando versión del protocolo http, servidor web, tipo de *encoding*, presencia de HSTS**.**

| Sitio Web | HTTP/HTTS | Versión | N° Solicitudes | Tiempo en Cargar todas las Solicitudes | Servidor | Keep Alive | Content-Encoding (Server) | Strict-Transport-Security (HSTS) |
|---|---|---|---|---|---|---|---|---|
| .www.web-out.com | HTTP | HTTP/1.1 | 86 | 9.45 | Apache | timeout=5 max= 100 | - | NO |
| .www.web-out.com | HTTP | HTTP/1.1 | 86 | 9.8 | Apache | timeout=5 max= 100 | - | NO |
| .www.web-out.com | HTTP | HTTP/1.1 | 86 | 8.64 | Apache | timeout=5 max= 100 | - | NO |
| .www.web-out.com | HTTP | HTTP/1.1 | 86 | 8.12 | Apache | timeout=5 max= 100 | - | NO |
| .www.web-out.com | HTTP | HTTP/1.1 | 86 | 8.63 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTP | HTTP/1.1 | 106 | 6.96 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTP | HTTP/1.1 | 106 | 6.26 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTP | HTTP/1.1 | 106 | 5.73 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTP | HTTP/1.1 | 106 | 6.43 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTP | HTTP/1.1 | 106 | 6.55 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTP | HTTP/1.1 | 146 | 19.87 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTP | HTTP/1.1 | 146 | 20.05 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTP | HTTP/1.1 | 146 | 20.01 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTP | HTTP/1.1 | 146 | 20.95 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTP | HTTP/1.1 | 146 | 20.29 | Apache | timeout=5 max= 100 | - | NO |
| .www.hotel-oroverde.com | HTTP | HTTP/1.1 | 94 | 18.79 | Apache | - | gzip | |
| .www.hotel-oroverde.com | HTTP | HTTP/1.1 | 94 | 18.63 | Apache | - | gzip | |
| .www.hotel-oroverde.com | HTTP | HTTP/1.1 | 94 | 18.85 | Apache | - | gzip | |
| .www.hotel-oroverde.com | HTTP | HTTP/1.1 | 94 | 18.34 | Apache | - | gzip | |
| .www.hotel-oroverde.com | HTTP | HTTP/1.1 | 94 | 18.85 | Apache | - | gzip | |
| .www.hotelnaturalgreen.com | HTTP | HTTP/1.1 | 107 | 9.7 | Apache | timeout=5 max= 100 | - | |
| .www.hotelnaturalgreen.com | HTTP | HTTP/1.1 | 107 | 9.34 | Apache | timeout=5 max= 100 | - | |
| .www.hotelnaturalgreen.com | HTTP | HTTP/1.1 | 107 | 9.89 | Apache | timeout=5 max= 100 | - | |
| .www.hotelnaturalgreen.com | HTTP | HTTP/1.1 | 107 | 9.22 | Apache | timeout=5 max= 100 | - | |
| .www.hotelnaturalgreen.com | HTTP | HTTP/1.1 | 107 | 9.71 | Apache | timeout=5 max= 100 | - | |
| .www.web-out.com | HTTPS | HTTP/1.1 | 86 | 11.06 | Apache | timeout=5 max= 100 | - | NO |
| .www.web-out.com | HTTPS | HTTP/1.1 | 86 | 10.17 | Apache | timeout=5 max= 100 | - | NO |
| .www.web-out.com | HTTPS | HTTP/1.1 | 86 | 10.48 | Apache | timeout=5 max= 100 | - | NO |
| .www.web-out.com | HTTPS | HTTP/1.1 | 86 | 11.39 | Apache | timeout=5 max= 100 | - | NO |
| .www.web-out.com | HTTPS | HTTP/1.1 | 86 | 8.4 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTPS | HTTP/1.1 | 106 | 6.25 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTPS | HTTP/1.1 | 105 | 6.21 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTPS | HTTP/1.1 | 106 | 6.53 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTPS | HTTP/1.1 | 106 | 6.47 | Apache | timeout=5 max= 100 | - | NO |
| .www.fceaunas.edu.pe | HTTPS | HTTP/1.1 | 106 | 7.04 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTPS | HTTP/1.1 | 146 | 21.86 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTPS | HTTP/1.1 | 146 | 20.37 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTPS | HTTP/1.1 | 146 | 21.04 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTPS | HTTP/1.1 | 146 | 22.9 | Apache | timeout=5 max= 100 | - | NO |
| .www.canadaperu.org | HTTPS | HTTP/1.1 | 146 | 20.45 | Apache | timeout=5 max= 100 | - | NO |
| .www.hotel-oroverde.com | HTTPS | HTTP/1.1 | 94 | 20.85 | Apache | - | gzip | NO |
| .www.hotel-oroverde.com | HTTPS | HTTP/1.1 | 94 | 20.07 | Apache | - | gzip | NO |
| .www.hotel-oroverde.com | HTTPS | HTTP/1.1 | 94 | 19.93 | Apache | - | gzip | NO |
| .www.hotel-oroverde.com | HTTPS | HTTP/1.1 | 94 | 19.15 | Apache | - | gzip | NO |
| .www.hotel-oroverde.com | HTTPS | HTTP/1.1 | 94 | 19.21 | Apache | - | gzip | NO |
| .www.hotelnaturalgreen.com | HTTPS | HTTP/1.1 | 107 | 10.18 | Apache | timeout=5 max= 100 | - | NO |
| .www.hotelnaturalgreen.com | HTTPS | HTTP/1.1 | 107 | 9.37 | Apache | timeout=5 max= 100 | - | NO |
| .www.hotelnaturalgreen.com | HTTPS | HTTP/1.1 | 107 | 10 | Apache | timeout=5 max= 100 | - | NO |
| .www.hotelnaturalgreen.com | HTTPS | HTTP/1.1 | 107 | 9.37 | Apache | timeout=5 max= 100 | - | NO |
| .www.hotelnaturalgreen.com | HTTPS | HTTP/1.1 | 107 | 10.61 | Apache | timeout=5 max= 100 | - | NO |

**Fuente:** Elaboración Propia.

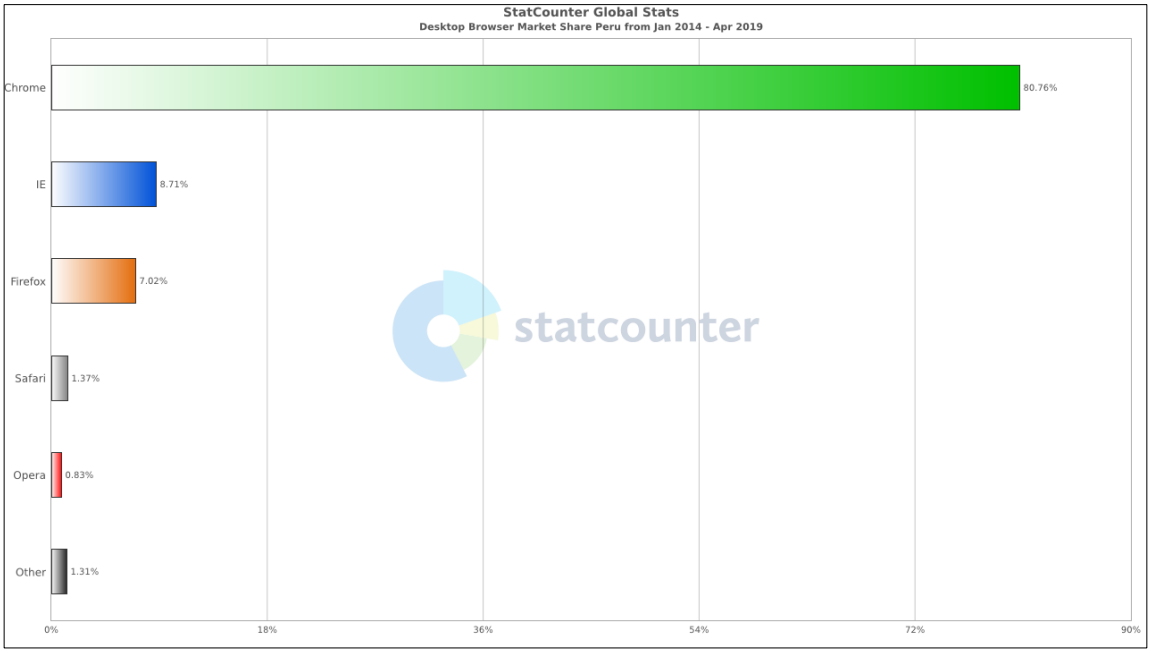
**ANEXO 6.** Análisis del cifrado mediante la herramienta SSL Robot.

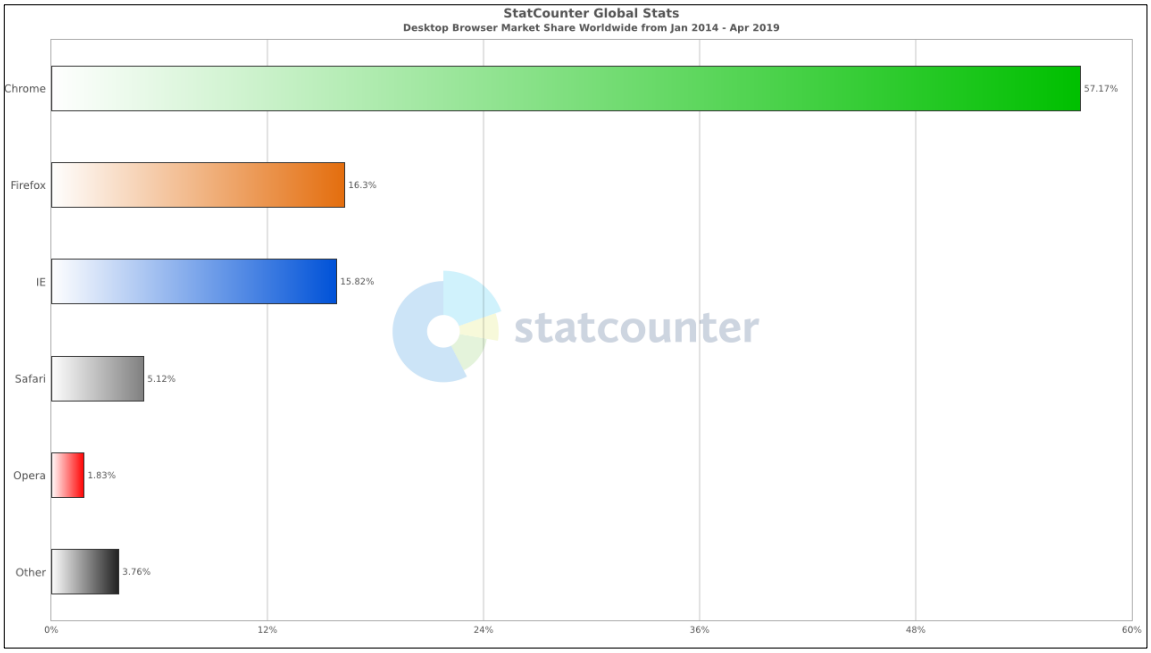



**Fuente:** Elaboración Propia

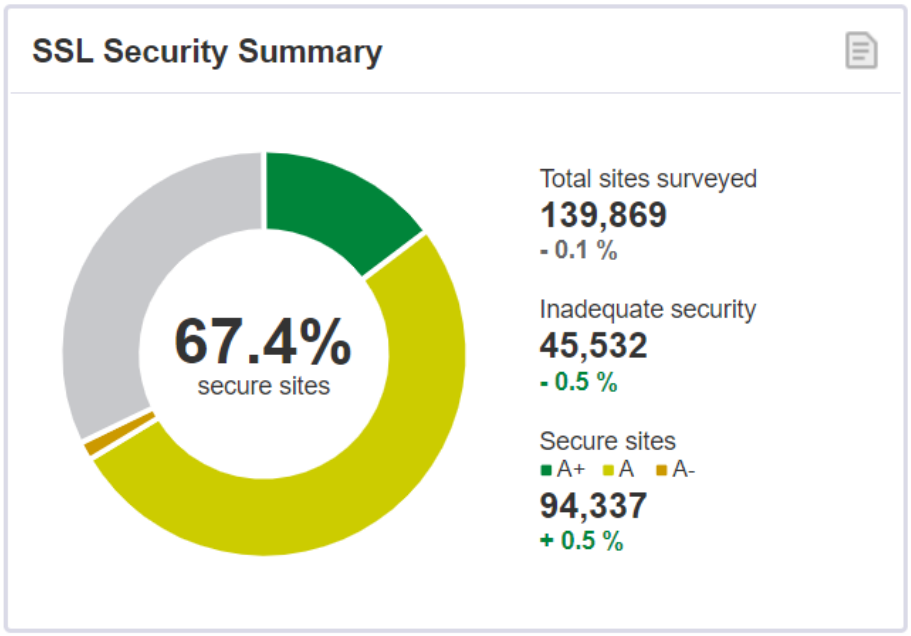
**ANEXO 7.** Navegadores de escritorio más utilizados a nivel nacional (imagen superior) e internacional (imagen inferior) desde enero del 2014 a abril del 2019 según reporte de Statcounter.



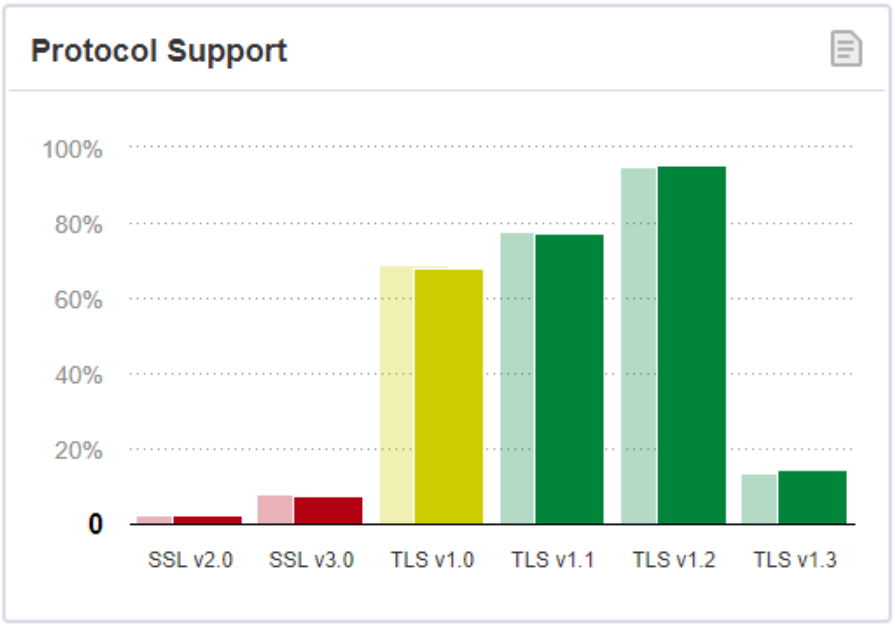




**Fuente:** (StatCounter, 2019)

**ANEXO 8.** Resumen de Sitios Seguros con SSL/TLS en base a 150 000 sitios web según la lista de Alexa de los sitios más populares del mundo.




**Fuente:** (Qualys SSL Labs, 2019)




**Fuente:** (Qualys SSL Labs, 2019)

**ANEXO 9.** Top 10 de los navegadores más utilizados para acceder a los 5 sitios web administrados por la empresa Web-Out. S.A.

## Web-Out. S.A.

| Navegadores (Top 10) | | | | |
|---|---|---|---|---|
| Navegadores | Páginas | Porcentaje | Solicitudes | Porcentaje |
| Desconocido | 20,960 | 90.20% | 22,303 | 45.80% |
| Google Chrome | 1,575 | 6.70% | 24,438 | 50.20% |
| MS Internet Explorer | 249 | 1% | 411 | 0.80% |
| Firefox | 154 | 0.60% | 701 | 1.40% |
| Opera | 93 | 0.40% | 134 | 0.20% |
| Safari | 59 | 0.20% | 241 | 0.40% |
| Mozilla | 54 | 0.20% | 54 | 0.10% |
| Edge | 37 | 0.10% | 333 | 0.60% |
| Netscape | 20 | 0% | 20 | 0% |
| Android browser (Phone browser) | 20 | 0% | 20 | 0% |

**Fuente:** AwStats - cPanel

## Facultad de Ciencias Económicas y Administrativas de la UNAS

| Navegadores (Top 10) | | | | |
|---|---|---|---|---|
| Navegadores | Páginas | Porcentaje | Solicitudes | Porcentaje |
| Desconocido | 17,003 | 98.10% | 17,177 | 85.40% |
| Google Chrome | 225 | 1.20% | 2,247 | 11.10% |
| Firefox | 66 | 0.30% | 608 | 3% |
| MS Internet Explorer | 23 | 0.10% | 46 | 0.20% |
| Mozilla | 1 | 0% | 1 | 0% |
| Safari | 1 | 0% | 22 | 0.10% |
| Opera | 0 | 0% | 1 | 0% |

**Fuente:** AwStats - cPanel

## Hotel Natural Green

| Navegadores (Top 10) | | | | |
|---|---|---|---|---|
| Navegadores | Páginas | Porcentaje | Solicitudes | Porcentaje |
| Desconocido | 11,612 | 91.30% | 11,921 | 49% |
| Google Chrome | 968 | 7.60% | 10,199 | 41.90% |
| Safari | 82 | 0.60% | 1,655 | 6.80% |
| Firefox | 32 | 0.20% | 264 | 1% |
| Edge | 11 | 0% | 222 | 0.90% |
| Mozilla | 5 | 0% | 5 | 0% |
| MS Internet Explorer | 2 | 0% | 4 | 0% |
| Opera | 2 | 0% | 41 | 0.10% |

**Fuente:** AwStats - cPanel

## Hotel Oro Verde

| Navegadores (Top 10) | | | | |
|---|---|---|---|---|
| Navegadores | Páginas | Porcentaje | Solicitudes | Porcentaje |
| Google Chrome | 12,248 | 45.60% | 173,094 | 77.90% |
| Desconocido | 9,935 | 37% | 10,292 | 4.60% |
| Firefox | 2,218 | 8.20% | 7,640 | 3.40% |
| Safari | 1,533 | 5.70% | 13,961 | 6.20% |
| MS Internet Explorer | 321 | 1.10% | 11,271 | 5% |
| Netscape | 283 | 1% | 301 | 0.10% |
| Edge | 92 | 0.30% | 2,289 | 1% |
| Opera | 81 | 0.30% | 725 | 0.30% |
| IPhone (PDA/Phone browser) | 55 | 0.20% | 1,124 | 0.50% |
| Mozilla | 33 | 0.10% | 504 | 0.20% |
| Otros | 31 | 0.10% | 924 | 0.40% |

**Fuente:** AwStats - cPanel

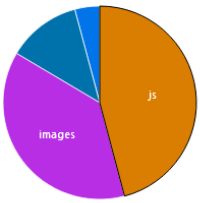
## Cámara de Comercio Canadá - Perú

| Navegadores (Top 10) | | | | |
|---|---|---|---|---|
| Navegadores | Páginas | Porcentaje | Solicitudes | Porcentaje |
| Desconocido | 14,718 | 99% | 15,042 | 79.80% |
| Google Chrome | 118 | 0.70% | 3,441 | 18.20% |
| Safari | 10 | 0% | 180 | 0.90% |
| Mozilla | 5 | 0% | 5 | 0% |
| Firefox | 2 | 0% | 100 | 0.50% |
| MS Internet Explorer | 1 | 0% | 4 | 0% |
| IPhone (PDA/Phone browser) | 1 | 0% | 72 | 0.30% |
| Android browser (PDA/Phone browser) | 0 | 0% | 1 | 0% |

**Fuente:** AwStats - cPanel

**ANEXO 10.** Transferencia de Información de los cinco sitios web caso de estudio.

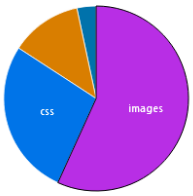
- **Sitio web de Web-Out. S.A.**




Usando caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 25 js | 164,70 KB | 43,34 KB |
| 53 images | 135,22 KB | 145,62 KB |
| 1 html | 44,24 KB | 44,68 KB |
| 11 css | 14,94 KB | 1,74 KB |

Respuestas cacheadas: 57
Solicitudes totales: 90
Tamaño: 359,09 KB
Tamaño transferido: 235,38 KB
Tiempo: 4,59 segundos
Tiempo no bloqueante: 4,58 segundos

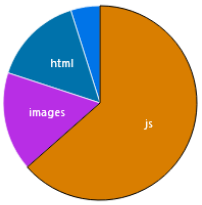



Sin usar caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 53 images | 749,46 KB | 766,65 KB |
| 11 css | 361,22 KB | 75,94 KB |
| 25 js | 164,70 KB | 2.835,72 KB |
| 1 html | 44,24 KB | 44,68 KB |

Respuestas cacheadas: 0
Solicitudes totales: 90
Tamaño: 1.319,62 KB
Tamaño transferido: 3.722,99 KB
Tiempo: 18,19 segundos
Tiempo no bloqueante: 11,91 segundos

- **Sitio web de Facultad de Ciencias Económicas y Administrativas de la UNAS**




Usando caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 34 js | 138,93 KB | 1.890,00 KB |
| 30 images | 36,07 KB | 42,03 KB |
| 1 html | 33,02 KB | 33,67 KB |
| 37 css | 10,68 KB | 0,76 KB |

Respuestas cacheadas: 71
Solicitudes totales: 102
Tamaño: 218,70 KB
Tamaño transferido: 1.966,46 KB
Tiempo: 4,19 segundos
Tiempo no bloqueante: 2,46 segundos


Sin usar caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 30 images | 626,48 KB | 636,98 KB |
| 37 css | 382,40 KB | 379,83 KB |
| 34 js | 139,83 KB | 2.995,35 KB |
| 1 html | 33,02 KB | 33,67 KB |

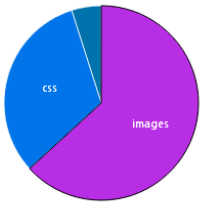
Respuestas cacheadas: 0
Solicitudes totales: 102
Tamaño: 1.181,73 KB
Tamaño transferido: 4.045,83 KB
Tiempo: 35,81 segundos
Tiempo no bloqueante: 10,70 segundos

- **Sitio web de Hotel Oro Verde**


Usando caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 13 css | 1.533,99 KB | 258,84 KB |
| 23 images | 580,11 KB | 583,17 KB |
| 6 html | 237,83 KB | 89,36 KB |
| 44 js | 0 KB | 8.505,60 KB |

Respuestas cacheadas: 44
Solicitudes totales: 86
Tamaño: 2.351,93 KB
Tamaño transferido: 9.436,97 KB
Tiempo: 23,73 segundos
Tiempo no bloqueante: 9,55 segundos

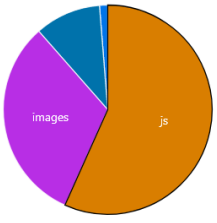



Sin usar caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 23 images | 3.588,73 KB | 3.593,82 KB |
| 13 css | 1.809,83 KB | 305,94 KB |
| 6 html | 279,33 KB | 97,82 KB |
| 44 js | 0,29 KB | 9.531,43 KB |

Respuestas cacheadas: 0
Solicitudes totales: 86
Tamaño: 5.678,19 KB
Tamaño transferido: 13.529,01 KB
Tiempo: 89,03 segundos
Tiempo no bloqueante: 30,23 segundos

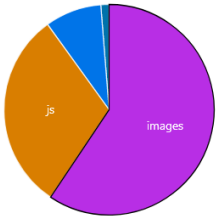
- **Sitio web de Hotel Natural Green**




Usando caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 36 js | 313,10 KB | 313,85 KB |
| 40 images | 175,47 KB | 176,15 KB |
| 2 html | 56,47 KB | 57,40 KB |
| 34 css | 6,96 KB | 7,43 KB |

Respuestas cacheadas: 102
Solicitudes totales: 112
Tamaño: 552,00 KB
Tamaño transferido: 554,83 KB
Tiempo: 3,35 segundos
Tiempo no bloqueante: 3,33 segundos

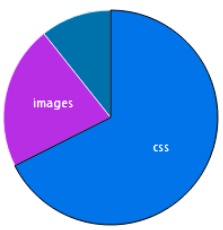



Sin usar caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 40 images | 2.654,34 KB | 2.662,59 KB |
| 36 js | 1.369,42 KB | 1.376,79 KB |
| 34 css | 388,84 KB | 396,26 KB |
| 2 html | 56,47 KB | 57,40 KB |

Respuestas cacheadas: 0
Solicitudes totales: 112
Tamaño: 4.469,08 KB
Tamaño transferido: 4.493,04 KB
Tiempo: 84,98 segundos
Tiempo no bloqueante: 23,43 segundos

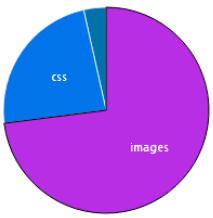
- **Sitio web de Cámara de Comercio Canadá –**




Usando caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 34 css | 1.965,31 KB | 687,67 KB |
| 52 images | 631,82 KB | 640,67 KB |
| 6 html | 311,43 KB | 169,59 KB |
| 43 js | 0 KB | 8.505,60 KB |

Respuestas cacheadas: 59
Solicitudes totales: 135
Tamaño: 2.908,56 KB
Tamaño transferido: 10.003,53 KB
Tiempo: 46,34 segundos
Tiempo no bloqueante: 12,83 segundos




Sin usar caché

| Tipo | Tamaño | Transferido |
|---|---|---|
| 52 images | 6.482,37 KB | 6.496,32 KB |
| 34 css | 2.088,55 KB | 813,16 KB |
| 6 html | 311,43 KB | 169,59 KB |
| 43 js | 0,80 KB | 10.786,52 KB |

Respuestas cacheadas: 0
Solicitudes totales: 135
Tamaño: 8.883,15 KB
Tamaño transferido: 18.265,59 KB
Tiempo: 81,91 segundos
Tiempo no bloqueante: 22,62 segundos