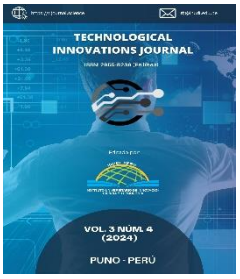
Technol. innov. j. (2024). Vol. 3 Núm. 4 págs. 25-37

Technological Innovations Journal

www.tijournal.science

ISSN 2955-8239 (En línea)

Editada por: Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú



ARTÍCULO DE REVISIÓN

Análisis de Protocolos Transport Layer Security y Secure Socket Layer como mecanismos de seguridad y competitividad en las organizaciones digitales

Analysis of Transport Layer Security and Secure Socket Layer protocols as security and competitiveness mechanisms in digital organizations

Análise dos protocolos Transport Layer Security e Secure Socket Layer como mecanismos de segurança e competitividade nas organizações digitais

Antonio Flores-Vargas[1]
Universidad Nacional del Altiplano, Puno – Puno, Perú
https://orcid.org/0000-0002-5966-865X
72919423@epg.unap.edu.pe (correspondencia)

Marvin Llerena
Universidad Nacional del Altiplano, Puno – Puno, Perú
https://orcid.org/0009-0001-3289-5502
70238041@epg.unap.edu.pe

DOI: https://doi.org/10.35622/j.ti.2024.04.002

Recibido: 09/09/2024 Aceptado: 25/11/2024 Publicado: 03/12/2024

PALABRAS CLAVE

cibercomercio, cibergobierno, cibernética, protección de datos.

RESUMEN. El crecimiento y competitividad de las organizaciones dependen en gran medida de la digitalización, lo que plantea nuevos retos en ciberseguridad. Este artículo tiene por objetivo identificar la importancia de los protocolos SSL y TLS en sectores clave del entorno organizacional. Se siguió un enfoque cualitativo, de revisión sistemática bajo la metodología PRISMA, se realizó una búsqueda en las bases de Google Schoolar, Dialnet y La Referencia, se utilizaron los descriptores "protocolo, SSL, seguridad, TSL, ciberseguridad" en inglés y español, considerando artículos y tesis de grado publicados en el periodo 2014-2024, para la revisión final se seleccionaron 14 trabajos. La revisión mostró que ambos protocolos aseguran la confidencialidad, integridad y autenticación de comunicaciones en sistemas y aplicativos previniendo principalmente ataques como *phishing, man in the middle*, diccionario de datos e interrupciones con los sitios web legítimos. En conclusión, los protocolos son el primer paso en medidas de seguridad de infraestructura web en un entorno digital fluctuante y altamente competitivo, con influencia en sectores como el financiero, comercio electrónico, servicios e incluso el gobierno digital, es importante que toda organización establezca medidas, áreas, departamentos y recursos en su propia seguridad web para asegurar su confiabilidad, prestigio y mantener seguros datos comerciales y la de sus usuarios y clientes.

[1] Doctorando en Administración en la Universidad Nacional del Altiplano, Perú.

KEYWORDS

cyber commerce, cyber government, cybernetics, data protection.

ABSTRACT. The growth and competitiveness of organizations largely depend on digitalization, which poses new challenges in cybersecurity. This article aims to identify the importance of SSL and TLS protocols in key sectors of the organizational environment. A qualitative approach was followed, using a systematic review under the PRISMA methodology. A search was conducted in the Google Scholar, Dialnet, and La Referencia databases, using the descriptors "protocol, SSL, security, TSL, cybersecurity" in both English and Spanish. Articles and thesis papers published between 2014 and 2024 were considered, and 14 works were selected for the final review. The review showed that both protocols ensure the confidentiality, integrity, and authentication of communications in systems and applications, mainly preventing attacks such as phishing, man-in-the-middle, data dictionary, and interruptions with legitimate websites. In conclusion, protocols are the first step in security measures for web infrastructure in a fluctuating and highly competitive digital environment, with influence in sectors such as finance, e-commerce, services, and even digital government. It is important that every organization establishes measures, areas, departments, and resources for its own web security to ensure reliability, prestige, and to keep business and user/customer data secure.

PALAVRAS-CHAVE

cibercomércio, cibergoverno, cibernética, proteção de dados.

RESUMO. O crescimento e a competitividade das organizações dependem em grande parte da digitalização, o que apresenta novos desafios em cibersegurança. Este artigo tem como objetivo identificar a importância dos protocolos SSL e TLS em setores chave do ambiente organizacional. Seguiu-se uma abordagem qualitativa, com uma revisão sistemática sob a metodologia PRISMA. Foi realizada uma busca nas bases de dados Google Scholar, Dialnet e La Referencia, utilizando os descritores "protocolo, SSL, segurança, TSL, cibersegurança" em inglês e espanhol. Foram considerados artigos e teses de graduação publicados no período de 2014-2024, sendo selecionados 14 trabalhos para a revisão final. A revisão mostrou que ambos os protocolos garantem a confidencialidade, integridade e autenticação das comunicações em sistemas e aplicativos, prevenindo principalmente ataques como phishing, man-in-the-middle, dicionário de dados e interrupções com sites legítimos. Em conclusão, os protocolos são o primeiro passo nas medidas de segurança da infraestrutura web em um ambiente digital flutuante e altamente competitivo, com influência em setores como o financeiro, comércio eletrônico, serviços e até mesmo o governo digital. É importante que toda organização estabeleça medidas, áreas, departamentos e recursos para a sua própria segurança web, garantindo sua confiabilidade, prestígio e mantendo os dados comerciais e os dados de seus usuários e clientes seguros.

1. INTRODUCCIÓN

El protocolo *Secure Socket Layer* (SSL) fue desarrollado por *Netscape Communications* en la década de 1990 como una solución para garantizar la seguridad en las comunicaciones a través de la web, siendo su principal función es proporcionar una capa de seguridad entre el servidor web y el navegador del cliente, garantizando que los datos transmitidos no puedan ser interceptados o modificados por terceros no autorizados. El SSL actúa cifrando la información en tránsito, de modo que, si alguien accede a los datos, no podrá interpretarlos sin la clave de descifrado adecuada. Este enfoque transformó radicalmente la seguridad en internet, permitiendo a las empresas confiar en la transmisión segura de información sensible como datos personales, contraseñas y detalles de tarjetas de crédito (Cardenas Urrea et al., 2016).

Para Ortega Martorell y Canino Gutiérrez (2006) el protocolo SSL y su sucesor, *Transport Layer Security* (TLS), actúan como una capa de protección que garantiza que la información transmitida no pueda ser interceptada o alterada por actores maliciosos, ya que se utilizan protocolos criptográficos que trabajan por debajo de la capa de aplicación y facilitan el cifrado de extremo a extremo a la protección de una gran cantidad de protocolos, incluidos HTTPS, IMAPS (Ordean & Giurgiu, 2010).

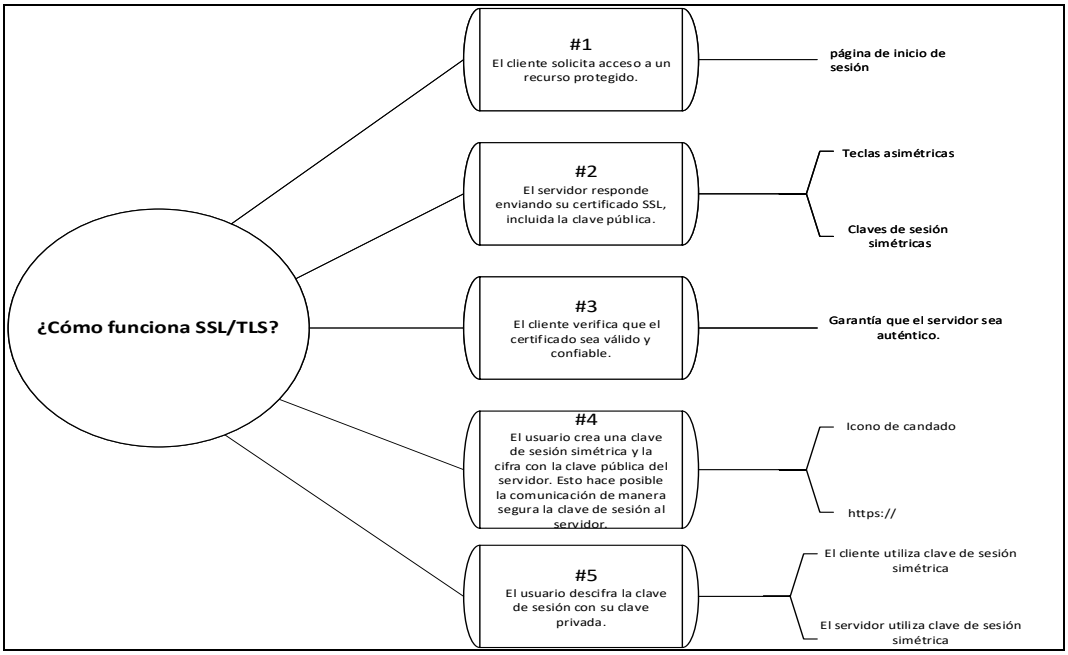
Con el tiempo, las primeras versiones de SSL presentaron varias vulnerabilidades de seguridad que dieron lugar a la creación de nuevas versiones mejoradas. Sin embargo, las vulnerabilidades críticas detectadas en SSL 2.0 y SSL 3.0 llevaron a la necesidad de desarrollar una versión más segura, conocida como *Transport Layer Security* (TLS), que desde entonces ha reemplazado gradualmente a SSL. TLS 1.0, introducido en 1999, fue la primera iteración de este protocolo mejorado, manteniendo muchas de las funciones esenciales de SSL pero con importantes mejoras en la seguridad, como el uso de algoritmos de cifrado más sólidos y mecanismos avanzados para evitar ataques de intermediario, a su vez el TLS es el modelo de la industria para proteger y asegurar la confiabilidad de las comunicaciones en internet, siendo usado con frecuencia en aplicaciones como la navegación web, correo electrónico y las transferencias de archivos (Cloudflare., *s.f.*).

Es así que, Angulo Castro y Henao Leiva (2017) mencionan que a pesar de la evolución tecnológica y la aparición de amenazas cada vez más sofisticadas, SSL sigue siendo una de las herramientas más robustas para garantizar la seguridad de las páginas empresariales. Cabe precisar que el SSL es independiente de la aplicación que lo utilice, ya que, no solo puede ser empleado para dar seguridad en las comunicaciones HTTP, sino también en aplicaciones como Telnet, FTP y IMAP (Ortega Martorell & Canino Gutiérrez, 2006).

Los protocolos funcionan protegiendo las comunicaciones entre un cliente y un servidor mediante cifrado. El proceso comienza con la autenticación del servidor, donde este envía su certificado digital, que contiene su clave pública, para que el usuario verifique su autenticidad a través de una Autoridad de Certificación (CA). Una vez autenticado, se lleva a cabo un intercambio de claves, en el cual cliente y servidor acuerdan una clave secreta para cifrar y descifrar los datos durante la sesión. Finalmente, los datos son cifrados y enviados, asegurando que solo las partes autorizadas pueden acceder a ellos, protegiendo así la información contra ataques de intermediario y otras amenazas cibernéticas. Además, estos protocolos garantizan el cumplimiento de normativas como el GDPR, que protege la privacidad de los datos personales (Flórez et al., 2021).

Figura 1

Funcionamiento de SSL/TLS



Nota. Adaptado de Cueva Hurtado y Alvarado Sarango (2017).

En el contexto digital en el que las organizaciones de los diferentes sectores económicos realizan sus actividades a través del ciberespacio, estas se ven vulneradas por potenciales ataques cibernéticos los mismos que pueden perjudicar tanto, teléfonos móviles, equipos de cómputo y redes informáticas inalámbricas (Machín & Gazapo, 2016); así mismo; los ciberataques vulneran las medidas de seguridad utilizadas en las TIC para borrar , copiar, y/o sustraer la información del usuario, y de esa manera beneficiarse de las falencias que presentan la mayor parte de las estructuras cibernéticas como, las redes sociales, comercio electrónico la banca móvil (Casar Corredera, 2012).

De acuerdo con Machín y Gazapo (2016) La cantidad y diversidad de los ciberataques puede llegar a ser excesivamente alto, ello provocado por la constante evolución y cambios de los dispositivos informáticos cuya complejidad es cada vez más elevada, es así que se tiene a las siguientes amenazas que puedan vulnerar la ciberseguridad:

Tabla 1

Amenazas que vulneran la ciberseguridad

Amenaza	Descripción
Código dañino:	Conocida como la amenaza más usual dentro del ciberespacio. Es llamado también código malicioso o malware, cuyo fin primordial es causar daño en la operatividad de distintos equipos informáticos, haciendo inservible el sistema operativo
Gusano:	Son códigos maliciosos categorizados como aislados, los cuales fueron creados para multiplicarse por sí solos, esto quiere decir, que este código malicioso puede reproducirse y dañar a los equipos conectados a través de la red común.
Virus:	Son programas que fueron creados para multiplicarse por sí solos con el único propósito de contaminar otros programas o ficheros.
Troyano:	Es un software que aparenta ser confiable, realizando funciones relevantes para el cliente, ocultando su verdadero objetivo el cual es el robo y pérdida de la información contenida en el equipo.
Botnet:	Grupo de software que interviene a través de la anulación de denegación de fraudes, sustracción de información, haciendo que los sistemas de antivirus sean ineficaces
Bomba lógica:	Considerados como ciberataques cuyo propósito es actuar en un tiempo establecido por el atacante, en donde su duración depende del tiempo en el que ejecuta sus funciones maliciosas.

Nota. Adaptado de Machín y Gazapo (2016).

Es por ello que, en la era digital, según Navia y Zambrano-Romero (2021) la seguridad en las comunicaciones web se ha convertido en una prioridad fundamental para las empresas que manejan información sensible, ya sea de clientes, transacciones financieras o datos confidenciales, por otro lado, Casar Corredera (2012) indica que el uso de protocolos de seguridad son utilizados para asegurar la integridad, disponibilidad y confidencialidad de la información que se comparte a través de redes públicas o privadas, siendo la

confidencialidad, integridad y autenticación un factor indispensable para la seguridad; a través de la utilización de algoritmos de cifrado, intercambiando claves simétricas y asimétricas a través de la utilización de certificados digitales que estén en el estándar x.509, siendo una de las características más relevantes que brinda el protocolo SSL/TLS (Qualys SSL Labs, *s.f.*).

De acuerdo a Angulo Castro y Henao Leiva (2017), la evolución tecnológica y la aparición de amenazas cada vez más sofisticadas, SSL sigue siendo una de las herramientas más robustas para garantizar la seguridad de las páginas empresariales.

La creciente dependencia de internet para las operaciones diarias y el comercio electrónico ha puesto de manifiesto la necesidad de garantizar que las comunicaciones entre usuarios y servidores sean seguras, confiables y privadas. En este contexto, el protocolo *Secure Socket Layer* (SSL) ha surgido como una tecnología clave para asegurar la transferencia de datos a través de la web, al proporcionar autenticación, integridad y cifrado de la información intercambiada entre el servidor y el cliente (Ortega Martorell & Canino Gutiérrez, 2006). Por medio del uso de cifrado que aseguren la confiabilidad y confidencialidad de la información compartida. Esto quiere decir que solo los usuarios autorizados pueden acceder a la información, previniendo la interceptación o la sustracción de datos; así mismo, los protocolos SSL y TLS comprueban la integridad de la información compartida, lo que hace posible la detección y así evitar cualquier modificación no autorizada de los datos (Cruz Lucas et al., 2022).

En el entorno empresarial, donde se cuenta con un gran número de datos sensibles, la implementación de SSL no solo es una medida de seguridad recomendada, sino también un estándar esencial para proteger la confianza del cliente y cumplir con las normativas de protección de datos. De hecho, la adopción de SSL se ha convertido en un factor crítico en la reputación y operatividad de las empresas en línea, ya que los navegadores modernos penalizan a los sitios web que no cuentan con esta capa de seguridad, advirtiendo a los usuarios sobre los riesgos potenciales (Cruz Lucas et al., 2022), un claro ejemplo es la empresa *Netscape Communication*, reconocida por el diseño del navegador web *Netscape Navigator*, obtuvo con el protocolo SSL una homogeneización de sus procedimientos para producir transmisiones confiables en la red (Clark & Van Oorschot, 2013).

Este artículo explora la relevancia del protocolo SSL en la protección de los datos empresariales, destacando su importancia en la preservación de la integridad y la privacidad de las comunicaciones en un entorno digital cada vez más amenazante. Además, se discuten las ventajas, limitaciones y mejores prácticas para su implementación en sitios web corporativos, con el fin de asegurar una experiencia de usuario segura y confiable.

2. MÉTODO

El estudio partió de un paradigma hermenéutico, enfoque cualitativo, de tipo revisión sistemática siguiendo los lineamientos de Page et al. (2021), aplicando la metodología PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). La revisión se tomó de agosto a octubre de 2024, aplicando criterios de inclusión y selección (Tabla 1) para la selección final de trabajos.

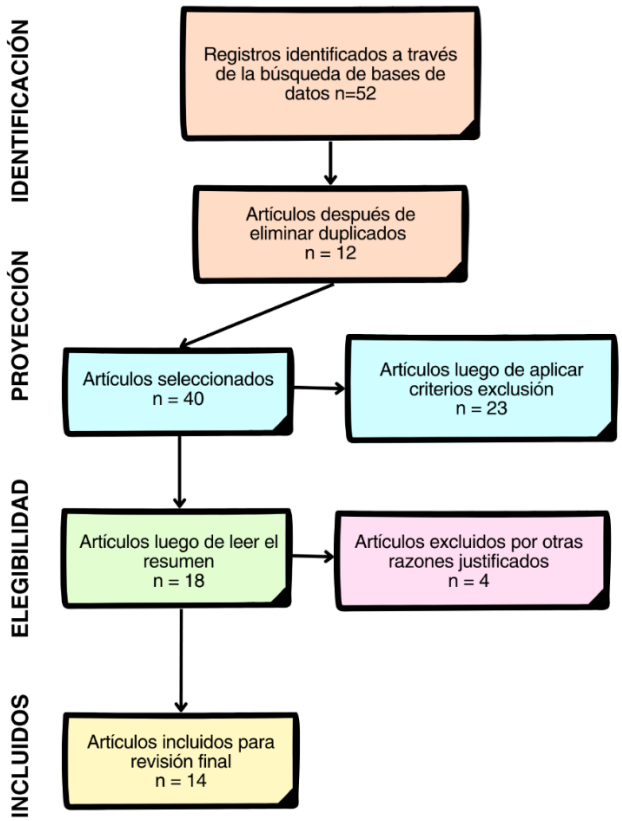
Tabla 1

Criterios de búsqueda y de exclusión en la investigación

Criterios de búsqueda	Criterios de exclusión
• Bases de datos: Google Schoolar, Dialnet, La Referencia. • Rango: últimos 10 años (2014-2024) • Idiomas: inglés y español. • Área del conocimiento: informática, tecnología, administración, ciencias empresariales. • Descriptores: protocolo, SSL, seguridad, TSL, ciberseguridad. • Tipo de documento: artículo científico, tesis de pregrado y maestría. • Acceso: abierto - Full text.	• Documentos en idiomas y periodos diferentes. • Pre prints. • Trabajos que no detallan aplicaciones de los protocolos de seguridad.

Figura 2

Flujograma PRISMA del proceso de selección de trabajos



La búsqueda se realizó en las bases de Google Schoolar y Dialnet estableciendo el periodo de búsqueda de 2014 - 2024, al no encontrar demasiados artículos con la información necesaria, se decidió incluir tesis de grado en la base de datos "La Referencia", entre artículos y tesis con menciones a protocolos SSL y TSL se

encontraron 51 documentos, luego se revisó el abstract y se comprobó si el documento completo era de acceso abierto, eliminando así los duplicados y aquellos que no eran visibles. Finalmente se excluyeron documentos debido a que sus resultados no presentaban evidencias concretas o de carácter solamente teórico, excluyendo además 4 archivos que no tenían datos completos para referenciación, obteniendo 14 documentos finales.

3. RESULTADOS

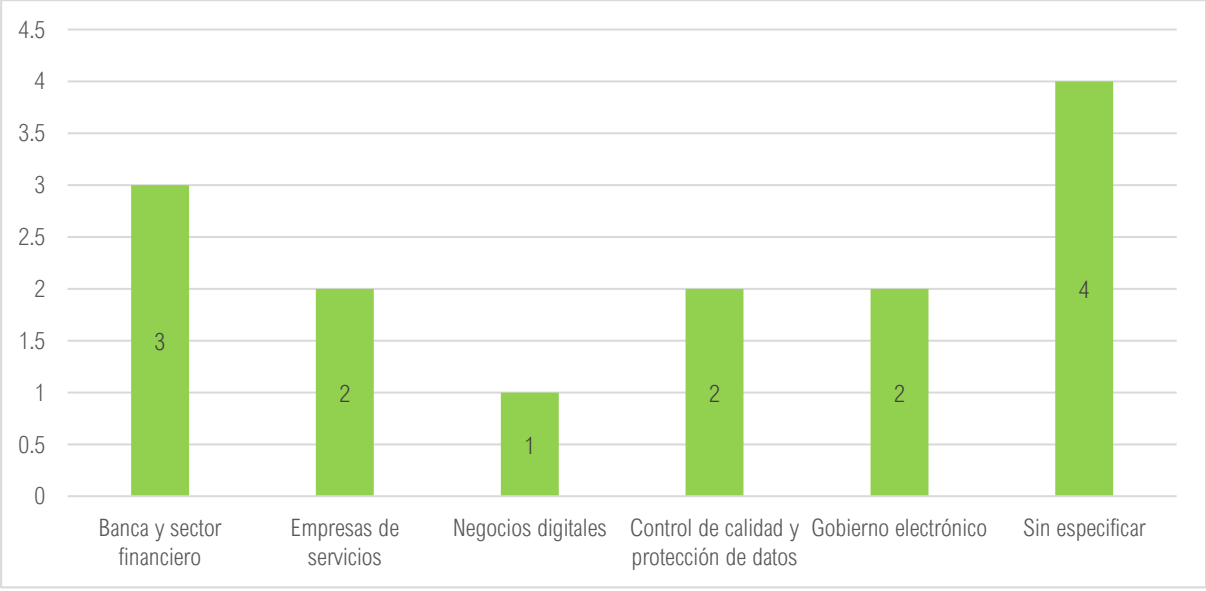
Los resultados denotan la relevancia de los protocolos de seguridad web, tales como el SSL y TSL en la mitigación de riesgos y la protección de los sistemas en todo tipo de organizaciones. Teniendo en cuenta que el entorno global los organismos públicos y empresas están forzadas a contar con presencia digital para su visibilidad, operaciones y prestación de servicios. Es así que la seguridad de la información se ha convertido en un pilar fundamental para garantizar la confianza de los usuarios y la integridad de los procesos operativos. Estos protocolos son de las primeras medidas para la reducción de vulnerabilidades, integridad y disponibilidad de los datos, esenciales en servicios críticos, como, por ejemplo, la banca en línea (Bravo Zambrano, 2021).

A partir de la revisión se identificó que la seguridad web va más allá que una configuración o protección técnica, que requiere de altos estándares, componentes físicos y lógicos (Figueroa-Suárez, 2017). La seguridad es estandarizable, pero requiere de ciertas particularidades en el manejo de datos de la actividad a la que se involucra la organización, esto es importante para la escalabilidad de los protocolos (Movilla-Jiménez et al., 2023). Esto refuerza la idea de que, en un entorno donde las amenazas a la seguridad son constantes y evolutivas, las empresas que implementan esquemas robustos y adaptables están mejor preparadas para mitigar ataques y garantizar la continuidad de sus operaciones, especialmente cuando sus actividades involucran el uso de aplicaciones (Coronel Suárez & Quirumbay Yagual, 2023).

Se identificaron 14 trabajos que ahondan en la seguridad y aplicación de protocolos en sectores como el financiero, empresas de servicios, negocios digitales, calidad, gobierno electrónico, y generales, su distribución se muestra en la figura 2:

Figura 3

Distribución temática de trabajos analizados



En la tabla 2 se describen los principales resultados y usos de los protocolos en sectores específicos:

Tabla 2

Detalle de trabajos analizados

Ámbito	Riesgo	Aplicación del protocolo	Fuente
Banca y sector financiero	Robo de información sensible (datos bancarios, contraseñas), ataques de intermediario (MITM), phishing, fraudes financieros.	Los protocolos cifran las transacciones financieras, protegiendo los datos bancarios, datos de usuarios y garantizando la autenticación del servidor para evitar fraudes.	Bravo Zambrano (2021) Figueroa-Suárez (2017) Fajardo et al. (2024)
Empresas de servicios	Exposición de datos de clientes, robo de identidad, acceso no autorizado a redes internas.	El SSL/TLS asegura las conexiones a las plataformas de servicio, protegiendo la información del cliente y autenticando los accesos a la red corporativa.	Movilla-Jiménez et al. (2023) Rueda Liberato (2019)
Negocios digitales	Interceptación de datos de usuarios, ataques de phishing, vulnerabilidades en transacciones de comercio electrónico.	Los protocolos generan confianza a los clientes de negocios digitales al mostrar el candado de seguridad en el navegador, lo que genera accesibilidad y seguridad al momento de interactuar o realizar transacciones en páginas comerciales.	Angulo Castro y Henao Leiva (2017)
Control de calidad y protección de datos	Violaciones de datos confidenciales, manipulación de información sensible, acceso no autorizado a bases de datos.	SSL/TLS garantiza que la información transmitida entre servidores y usuarios esté cifrada, preservando la integridad y confidencialidad de los datos.	Molina Marin y Orozco Nott (2020) Vigil (2018)
Gobierno electrónico	Ataques de espionaje, manipulación de datos gubernamentales, robo de información clasificada.	Se cifran las comunicaciones y protege los portales web gubernamentales, impidiendo el acceso no autorizado a información clasificada.	Filio Aguilar (2014) Fontalvo Fajardo (2016)
Otros (Sin especificar)	Las bases de dato alojadas en servidores sin cifrado, son vulnerables la información como contraseñas, datos personales, pueden manipularse o interferirse las interacciones del usuario con el servidor.	Los protocolos reducen el riesgo de inyección de código malicioso al cifrar y autenticar las comunicaciones entre el usuario y el servidor.	Toaza Moran (2023) Priego García (2018) Niño Benítez y Silega Martínez (2018) Jáuregui Sanabria (2021)

El impacto del uso de los protocolos de seguridad como SSL y TLS en las empresas es fundamental para garantizar la protección de la información que se transmite a través de sus sitios web y aplicativos (Niño Benítez & Silega Martínez, 2018). Estos protocolos emplean métodos de cifrado avanzados que protegen la privacidad de los datos, asegurando que solo las partes autorizadas puedan acceder a la información. Esto es especialmente relevante en el ámbito empresarial, donde el manejo de datos sensibles como transacciones financieras, información personal de clientes o detalles internos de la empresa es común. Gracias a estas medidas de seguridad se mitiga significativamente el riesgo de que esta información sea interceptada por ciberdelincuentes (Coronel Suárez & Quirumbay Yagual, 2023), igualmente los protocolos resultan efectivos con el uso de aplicaciones de banca móvil a través de QR (Fajardo et al., 2024).

Uno de los factores relevantes en ciberseguridad es la autenticación, que es una de los *features* principales que incluyen estos protocolos, utilizando certificados digitales que verifican la identidad del servidor con el que el usuario está interactuando. Esto permite a las empresas proporcionar a sus clientes un nivel adicional de confianza, ya que el protocolo confirma que los usuarios se están comunicando con el sitio web legítimo de la empresa, lo que reduce el riesgo de ataques de suplantación de identidad (phishing) (Priego García, 2018), además de ataques como hombre en el medio (*man in the middle*) y ataques con diccionario de datos (Cueva Hurtado & Alvarado Sarango, 2017).

Se menciona también que la seguridad no es solo un factor diferenciador, es un requisito legal en contextos como el europeo, donde existe el Reglamento General de Protección de Datos (RGPD) que establece directrices estrictas para la protección y privacidad de los datos personales de los ciudadanos de la UE, se exige que las empresas y organizaciones manejen los datos de manera transparente, segura y con el consentimiento explícito de los usuarios (European Commission, 2016). Así, la implementación de estos protocolos contribuye a una mejor experiencia del usuario y a un entorno digital más seguro para las operaciones empresariales evitando problemas como el malware y spyware (Castillo-Perez et al., 2010).

Recientemente, según Ortega Martorell y Canino Gutiérrez (2006) las nuevas versiones mejoradas y estables de SSL, aseguran mediante la utilización de protocolos como medios para garantizar la seguridad en la transmisión de información entre cliente y servidor en la web. Por lo cual se ha convertido en uno de los mecanismos de seguridad más usados en la actualidad, los mismos que se vienen utilizando en la mayoría de los navegadores. Mientras que el protocolo TLS ha evidenciado ser un enfoque más sólido en cuanto a la privacidad y protección de datos, descartando opciones de cifrado tenues y desarrollando un cifrado perfecto hacia adelante de forma predeterminada en TLS 1.3., el cual permitirá garantizar una mayor confidencialidad de la información compartida con cada nueva versión (Toaza Moran, 2023).

En sus versiones recientes los protocolos SSL (versión 3.0) y TLS (versión 1.0 o posterior) añaden una capa extra de seguridad mediante la validación del código de autenticación del usuario a través de una matriz de plantillas. Esta matriz es seleccionada por el usuario durante el registro y almacenada de forma segura en el servidor. Al intentar conectarse, el usuario debe elegir el código correcto de entre las plantillas mostradas por el servidor legítimo. Este mecanismo, al estar ligado exclusivamente al conocimiento del usuario, bloquea intentos de ataques cibernéticos ya que un atacante no puede replicar correctamente la matriz de plantillas sin acceso a la selección original del usuario (Razumov et al., 2023).

4. DISCUSIÓN

La literatura analizada confirma que la seguridad web va más allá de un cumplimiento de especificaciones técnicas; la inclusión de medidas, protocolos y procesos de seguridad han permitido a las organizaciones enfrentar un panorama de amenazas cibernéticas mejorando su imagen ante el entorno y sus usuarios/clientes.

El impacto positivo de los protocolos SSL y TLS, en la experiencia del usuario, es considerable. Su uso ha permitido a las organizaciones proporcionar entornos digitales confiables, especialmente en sectores donde la protección de información crítica, como las transacciones financieras y los datos personales, es una prioridad (Bravo Zambrano, 2021; Figueroa-Suárez, 2017; Fajardo et al., 2024). Esta capacidad de garantizar que el usuario está interactuando con el servidor correcto es esencial para combatir ataques como el *phishing* y *man in the middle*, que continúan siendo amenazas significativas en el panorama cibernético actual (Niño Benítez & Silega Martínez, 2018).

En cuanto a la diferencia de protocolos, los estudios sugieren que tanto SSL como TLS en sus distintas versiones resultan efectivos para la autenticación, cifrado y capas de protección para evitar la intromisión de malwares, cortes de comunicación, interacción de servidores e integridad de los datos (Toaza Moran, 2023). El uso de SSL y TLS, con su capacidad para cifrar y autenticar, también fortalece la resiliencia organizacional ante el creciente número de amenazas cibernéticas (Rueda Liberato, 2019).

Por otro lado, la integración de métodos de autenticación más avanzados, como sugiere Priego García (2018) con las matrices de plantillas, señala que SSL y TSL, son de momento, la opción más básica de protección, aunque no todos los sectores son comparables ni tienen el mismo nivel de riesgo (Niño Benítez & Silega Martínez, 2018). Esto implica que las estrategias de ciberseguridad no deben ser genéricas, sino adaptadas a las necesidades particulares de cada empresa y sus usuarios, la generación, importancia y amplitud de las bases de datos tendrán implicancias en la medida de seguridad seleccionada (Jáuregui Sanabria, 2021).

Finalmente, se advierte una implicancia regulatoria importante en términos de seguridad web, con los avances tecnológicos venideros. El cumplimiento con normativas como el RGPD (European Commission, 2016), tarde o temprano, terminará abarcando todas las operaciones digitales y protección de datos, por lo que resulta como una oportunidad para las organizaciones de mejorar sus sistemas de gestión de datos y fortalecer sus relaciones con los clientes/usuarios, consolidando la transparencia y seguridad como valores clave en sus operaciones (Castillo-Perez et al., 2010; Ortega Martorell & Canino Gutiérrez, 2006).

A modo de síntesis, los estudios concuerdan con que ambos protocolos son medidas importantes de seguridad, gracias a su autenticación y cifrado, fortaleciendo la resiliencia organizacional y la confianza del usuario. Sin embargo, estos protocolos son solamente el primer nivel en términos de ciberseguridad, por lo que cada organización debe buscar medidas más avanzadas para salvaguardar sus datos y los de sus clientes, en el contexto actual es impensable que una página web no tenga alguna de estas medidas. Es importante ahondar en el desarrollo de nuevas versiones de protocolos de seguridad que continúen elevando el nivel de protección y que incluyan mejoras específicas para diversos sectores empresariales y de gobierno con el fin de crear clústeres de seguridad web.

5. CONCLUSIONES

Los protocolos son esenciales para garantizar la seguridad en las comunicaciones digitales, protegiendo la integridad y confidencialidad de la información transmitida, particularmente en entornos empresariales y organizaciones de gobierno. Ello debido a su capacidad para mitigar amenazas cibernéticas, como ataques de suplantación de identidad y robo de datos; a su vez, refuerza su rol crucial en la protección de los sistemas, especialmente en sectores donde la seguridad de la información es crítica.

La implementación de SSL y TLS es una necesidad estratégica más que un requisito técnico web. El hecho de que estos protocolos ofrezcan una solución robusta y adaptable a las necesidades empresariales refuerza la importancia de un enfoque integral de ciberseguridad. Este análisis invita a reflexionar sobre la creciente sofisticación de las amenazas y la necesidad de adoptar medidas de seguridad que no solo se adapten a las exigencias actuales, sino que también anticipen futuros riesgos. Cabe precisar que en el contexto legal y normativo también juega un papel relevante, ya que el cumplimiento con regulaciones internacionales fortalece la confianza de los usuarios y mejora la reputación corporativa.

Conflicto de intereses / Competing interests:

Los autores declaran que no incurre en conflictos de intereses.

Rol de los autores / Authors Roles:

Antonio Flores-Vargas: Conceptualización, metodología, análisis formal, investigación, escritura – borrador original, escritura – revisión y edición, visualización, supervisión, administración del proyecto.

Marvin Llerena: Conceptualización, análisis formal, investigación, escritura revisión y edición, recursos, visualización

Fuentes de financiamiento / Funding:

Los autores declaran que no recibieron un fondo específico para esta investigación.

Aspectos éticos / legales; Ethics / legals:

Los autores declaran no haber incurrido en aspectos antiéticos, ni haber omitido aspectos legales en la realización de la investigación.

REFERENCIAS

Angulo Castro, D. & Henao Leiva, J. (2017). Análisis de herramientas de interceptación para el control de ataques reales de suplantación con certificados SSL. *Redes de Ingeniería*, *20*(20), 1-19. http://hdl.handle.net/11349/7812

Bravo Zambrano, L. (2021). *Riesgo percibido, confianza electrónica y la intención de usar los servicios de la banca en línea, Chiclayo 2021* [Tesis de maestría, Universidad Católica Santo Toribio de Mogrovejo]. http://hdl.handle.net/20.500.12423/3939

Cardenas Urrea, S. E., Navarro Núñez, W., Sarmiento Osorio, H. E., Forero Paez, N. A., & Bareño Gutierrez, R. (2016). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. *Revista UIS Ingenierías, 16*(1), 75-84. https://doi.org/10.18273/revuin.v16n1-2017008

Casar Corredera, J. R. (2012). *El ciberespacio: nuevo escenario de confrontación.* Centro Superior de Estudios de Defensa Nacional.

Castillo-Perez, S., Murcia Andres, J., & Garcia-Alfaro, J. (2010). *El Spyware como amenaza contra navegadores web* [Conferencia]. XI Reunión Española sobre Criptología y Seguridad de la Información (RECSI), 277-281, Tarragona, España.

Clark, J., & Van Oorschot, P. C. (2013). SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. *Proceedings* [Simposio]. EEE Symposium on Security and Privacy, 511–525. http://doi.org/10.1109/SP.2013.41

Cloudflare. (*s.f.*). *¿Qué es TLS (Transport Layer Security)?* https://cutt.ly/NeKTZWQi

Coronel Suárez, I. A., & Quirumbay Yagual, D. I. (2023). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE, 9*(12), 97-109. https://doi.org/10.26423/rctu.v9i2.672

Cruz Lucas, G. I., Galarza Espinoza, R. E., Delgado De La Cruz, R. S., & Marcillo Merino, M. J. (2022). Aplicación de protocolos SSL y TSL para él envió de información. *Journal TechInnovation, 1*(2), 4–9. https://doi.org/10.47230/journal.techinnovation.v1.n2.2022.4-9

Cueva Hurtado, M. E., & Alvarado Sarango, D. J. (2017). Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación. *Enfoque UTE, 8*(1), 273-286. https://doi.org/10.29019/enfoqueute.v8n1.128

European Commission (2016). *How will the data protection reform help fight international crime?* https://cutt.ly/deKYsLFj

Fajardo, C., Yamba-Yugsi, M., & Campaña Ortega, E. M. (2024). Evaluación de vulnerabilidades informáticas en códigos QR de la aplicación de Banca Móvil "Wallink". *Religación, 9*(41), 1-11. https://doi.org/10.46652/rgn.v9i41.1287

Figueroa-Suárez, J., Rodríguez-Andrade, R., Bone-Obando, C., & Saltos-Gómez, J. (2017). La seguridad informática y la seguridad de la información. *Polo del Conocimiento, 2*(12), 145-155. https://doi.org/10.23857/pc.v2i12.420

Filio Aguilar, P. D. (2014). *Propuesta de inclusión del criptosistema triple des 96en SSL/TLS record protocol*. [Tesis de grado, Universidad Autónoma del Estado de México]. http://hdl.handle.net/20.500.11799/49976

Flórez, A. S., Chacón, J. G., Chía, R. A., Flórez, A. E., & Rodriguez, J. E. (2021). Política de seguridad HSTS o seguridad de transporte HTTP estricta y su implementación en entornos web. *Ingeniería e Innovación*, 169-183. https://doi.org/10.21897/23460466.2643

Fontalvo Fajardo, A. E. (2016). *Análisis de la importancia de la seguridad electrónica en la sociedad portuaria regional de Cartagena* [Trabajo de grado, Universidad Militar Nueva Granada]. http://hdl.handle.net/10654/15449

Jáuregui Sanabria, J. (2021). *Impacto de la seguridad electrónica en tiempos de pandemia, adaptación a las edificaciones del futuro "inteligentes"* [Trabajo de grado, Universidad Militar Nueva Granada]. http://hdl.handle.net/10654/40353

Machín, N., & Gazapo, M. (2016). Cybersecurity as a critical factor for the security of the European Union. *Revista UNISCI* (42), 47–68. https://doi.org/10.5209/RUNI.53786

Molina Marin, Y., & Orozco Nott, L. G. (2020). *Vulnerabilidades de los Sistemas de Información: una revisión.* [Trabajo de grado, Tecnológico de Antioquia]. https://dspace.tdea.edu.co/handle/tdea/1398

Movilla-Jiménez, C., Torra-Bou, J. E., & García-Fernández, F. P. (2023). Políticas sobre seguridad del paciente y lesiones por presión: información publicada en las páginas web institucionales de España. *Gerokomos, 34*(1), 61-67.

Navia, M., & Zambrano-Romero, W. (2021). Instrumento para la auditoría técnica de seguridad informática en pequeños proveedores de Internet. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Telecomunicaciones, 5*(2), 119-128. https://doi.org/10.33936/isrtic.v5i2.3952.

Niño Benítez, Y., & Silega Martínez, N. (2018). Requisitos de seguridad para aplicaciones web. *Revista Cubana de Ciencias Informáticas, 12*(1), 205-221.

Ordean, M., & Giurgiu, M. (10-12 de noviembre de 2010). *Implementation of a security layer for the SSL/TLS protocol* [Simposio]. 9th International Symposium on Electronics and Telecommunications, Timisoara, Rumania, 209–2012. http://doi.org/10.1109/ISETC.2010.5679350

Ortega Martorell, S., & Canino Gutiérrez, L. (2006). Protocolo de seguridad SSL. *Ingeniería Industrial, 27*(2-3), 57-62. https://www.redalyc.org/articulo.oa?id=360433561012

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., & Moher, D. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Revista Española de Cardiología, 74*(9), 790–799. https://doi.org/10.1016/j.recesp.2021.06.016

Priego García, L. (2018). *Estudio del protocolo TLS (Transport Layer Security)* [Trabajo de grado, Universitat Oberta de Catalunya]. http://hdl.handle.net/10609/81045

Qualys SSL Labs. (*s.f.*). *SSL Pulse*. Recuperado el 03 de mayo de 2019 de https://cutt.ly/zeKT5v5T

Razumov, P., Cherckesova, L., Revyakina, E., Morozov, S., Medvedev, D., & Lobodenko, A. (2023). *Ensuring the security of web applications operating on the basis of the SSL/TLS protocol* [Conferencia]. International Scientific Siberian Transport Forum - TransSiberia 2023, Novosibirsk, Russia. https://doi.org/10.1051/e3sconf/202340203028

Rueda Liberato, E. (2019). *Cifrado con el protocolo SSL/TLS y el rendimiento de sitios web. caso: empresa Web-Out, 2018 – 2019*. [Tesis de grado, Universidad Nacional Agraria de la Selva]. https://hdl.handle.net/20.500.14292/1535

Toaza Moran, A. (2023). *Análisis de diferencias y mejoras entre SSL y TLS en términos de seguridad y protección* [Trabajo de grado, Universidad Técnica de Babahoyo]. http://dspace.utb.edu.ec/handle/49000/15139

Vigil, A. (2018). Implementación de mecanismos de seguridad en las comunicaciones de un sistema de gestión de edificios dedicado a tareas de oficina. *Revista Tecnología y Ciencia*, (29), 75–84. https://rtyc.utn.edu.ar/index.php/rtyc/article/view/191