VOLUMEN 5, N°2 / JULIO - DICIEMBRE 2023 / e - ISSN: 2661

EXPLORACIÓN INTEGRAL DE LA SEGURIDAD EN REDES DE PROVEEDORES DE SERVICIOS DE INTERNET: UNA REVISIÓN SISTEMÁTICA DE LITERATURA

Comprehensive security exploration in internet service providers networks: A systematic literature review

Chrystian Viteri-Hernández *	cpviteri@pucesa.edu.ec
Diego Avila-Pesantez†	davila@espoch.edu.ec

* Pontifícia Universidad Católica del Ecuador, sede Ambato. Departamento de Posgrado, Ambato, Ecuador
†Escuela Superior Politécnica de Chimborazo (ESPOCH), Grupo de Investigación en Innovación Científica y Tecnológica (GIICYT), Riobamba, Ecuador

RESUMEN

La seguridad en las redes de los Proveedores de Servicios de Internet (ISP) es crucial para proteger la información y servicios esenciales en línea, especialmente hoy en día cuando nuestra dependencia del internet es mayor. Con el aumento de ataques cibernéticos más sofisticados, los ISPs necesitan implementar medidas de seguridad eficaces. Este trabajo ofrece una visión integral de la seguridad en las redes de los ISP, basada en una revisión sistemática de 57 documentos de SpringerLink, Scopus y Web of Science, utilizando la metodología de Kitchenham. Se descubrió que los ISPs usan diversos mecanismos de seguridad como firewalls, sistemas de detección y prevención de intrusiones, y pruebas de penetración. Estos enfoques son fundamentales para contrarrestar eficazmente los ataques cibernéticos. La investigación concluye que una estrategia de seguridad integral, combinando varias medidas como firewalls avanzados, cifrado de datos y pruebas de penetración regulares, es vital en la infraestructura de los ISPs.

Palabras Clave: Detección de amenazas, proveedores de internet, seguridad en redes, revisión sistemática de literatura.

ABSTRACT

Network security in Internet Service Providers (ISPs) is paramount for safeguarding essential online information and services, particularly in an era where reliance on the internet is more pronounced than ever. In response to increasingly sophisticated cyber-attacks, ISPs must implement effective security measures. This study provides a comprehensive insight into ISP network security, grounded in a systematic review of 57 documents from SpringerLink, Scopus, and Web of Science, employing Kitchenham's methodology. It was found that ISPs deploy a variety of security mechanisms, including firewalls, intrusion detection and prevention systems, and penetration testing. These approaches are critical for effectively countering cyber threats. The research concludes that an integrated security strategy, combining various measures such as advanced firewalls, data encryption, and regular penetration testing, is crucial in the infrastructure of ISPs.

Keywords: Threat Detection, Internet Services Providers, Network Security, Literature systematic review.

I. Introducción

La seguridad de las redes de Proveedores de Servicios de Internet (ISP, por sus siglas en inglés) es un aspecto fundamental en la actualidad [1]. Esto se debe a que la tecnología y la información transmitidas a través de estas redes son cada vez más esenciales para la vida cotidiana [2]. En este sentido, el trabajo de [3] y [4] mencionan que la creciente sofisticación de los ataques cibernéticos ha provocado que los ISP implementen medidas de seguridad efectivas que protejan la integridad,

Fecha de Recepción: 26/dic/2023. Fecha de Aceptación: 13/ene/2023 DOI: https://doi.org/10.47187/perspectivas.6.1.215

confidencialidad y disponibilidad de los datos y servicios que ofrecen a los usuarios. En este contexto, el análisis exhaustivo de la seguridad de las redes de los ISP es un área de investigación fundamental para identificar y cuantificar los riesgos a los que están expuestas estas redes [5], [6]. No obstante, la exploración integral de esta problemática presenta desafíos únicos debido a la complejidad y escala de dichas redes, así como las amenazas cibernéticas en constante evolución que enfrentan [7], [8]. Por otro lado, la Ingeniería de redes, la ciberseguridad y la Inteligencia Artificial son campos esenciales para la investigación que aborden una amplia gama de amenazas desde vulnerabilidad conocidas hasta técnicas nuevas por parte de los atacantes [9].

Esta revisión sistemática de literatura (RSL) tiene como objetivo proporcionar un análisis detallado de la seguridad en las redes de los ISP, proporciona una visión general de cómo han evolucionado las estrategias de seguridad a lo largo del tiempo, como han funcionado y cuáles son las tendencias que podrían afectar a la seguridad en el futuro. Entre las medidas de seguridad existentes, se puede destacar el escaneo de vulnerabilidades, análisis de configuraciones, las pruebas de penetración y la evaluación de riesgos [10], [11]. La pregunta central que guía esta revisión es: ¿Cómo han evolucionado los mecanismos de seguridad en las redes de los ISP y cuáles son las medidas más efectivas para mitigar los ataques cibernéticos en la actualidad? Dar respuesta a esta interrogante puede ayudar a los profesionales de la seguridad cibernética y a los ISP a comprender y aplicar de manera más efectiva las mejores prácticas en este campo. Además, se puede identificar oportunidades para desarrollar nuevas herramientas, enfoques o marcos de trabajo que aborden los desafíos específicos de seguridad en estas redes.

El artículo aborda la seguridad en redes de Proveedores de Servicios de Internet (ISPs), destacando su creciente importancia en un mundo cada vez más dependiente de la tecnología. La metodología emplea la revisión sistemática de literatura, siguiendo la guía de Kitchenham, para analizar 57 estudios relevantes. Se presentan resultados sobre diversas medidas de seguridad implementadas por ISPs, incluyendo firewalls y cifrado de datos, así como estrategias proactivas y colaborativas. La discusión y conclusiones resaltan la necesidad de un enfoque integral y adaptable en seguridad cibernética, subrayando la importancia de la innovación tecnológica y la colaboración intersectorial.

II. Metodología

La Revisión Sistemática de la Literatura (RSL) se establece como un procedimiento meticuloso orientado a identificar, evaluar y sintetizar la evidencia científica relacionada con un tema específico [12]. Este proceso se rige por una secuencia de pasos predefinidos, asegurando así que la revisión sea exhaustiva, imparcial y transparente. Barbara Kitchenham, reconocida por sus notables contribuciones en el desarrollo de metodologías, ofrece un enfoque estructurado y minucioso para la planificación, ejecución y presentación de una RSL [13]. Este garantiza no solo la rigurosidad en la recopilación de datos, sino también la claridad y la coherencia en la presentación de los resultados, aportando así a la credibilidad y solidez de la revisión [14]. Para este proceso se ha establecido las siguientes definiciones: las preguntas de investigación, el proceso de búsqueda, los criterios de inclusión y exclusión, la valoración de calidad, la recopilación de datos y el análisis de los datos [12], que se detallan en la Tabla I.

Tabla I.

Proceso de RSL propuesto por Kitchenham

Fase	Procedimientos
Planificar la revisión	Especificar las preguntas de investigación.
	Desarrollar el protocolo de revisión.
	Validar el protocolo de revisión.
Conducir la revisión	Identificar estudios relevantes.
	Seleccionar estudios primarios.
	Evaluar la calidad de los estudios,
	Extraer los datos requeridos.
	Sintetizar los datos.
Documentar la revisión	Escribir el informe de revisión.
	Validar el informe.

Fuente: *Traducido al español del original propuesto por Kitchenham [12].*

A. Preguntas de investigación

Las preguntas de investigación son fundamentales para cualquier estudio, debido a que definen su propósito y guían la recopilación y el análisis de datos [13]. Por lo tanto, se formularon tres preguntas de investigación, que se detallan en la Tabla II.

Tabla 2.

PREGUNTAS DE INVESTIGACIÓN

N.	Fase	Procedimientos
P1	¿Cuáles son los mecanismos utilizados por los ISP para proteger la infraestructura de red?	Describir exhaustivamente los mecanismos empleados por los ISP para salvaguardar su infraestructura de red.
P2	¿Qué pruebas de penetración realizan los ISP para detectar amenazas y vulnerabilidades?	Examinar las pruebas de penetración llevadas a cabo por los ISP con el propósito de identificar amenazas y vulnerabilidades en su infraestructura de red.
P3	¿Cuáles son las medidas más efectivas en la actualidad para mitigar los ataques cibernéticos?	Determinar las medidas más efectivas en la actualidad para mitigar los ataques cibernéticos, teniendo en cuenta su efectividad y facilidad de implementación

B. Proceso de búsqueda

Se llevaron a cabo exhaustivas búsquedas en las renombradas bases de datos de SpringerLink, Web of Science y Scopus, abarcando estudios publicados en los últimos cinco años (2019-2023). Este proceso de búsqueda fue diseñado, teniendo en cuenta las funciones y características específicas de cada plataforma. Este enfoque asegura una búsqueda eficiente y adaptable a diversos contextos. Durante la fase de búsqueda, se identificaron las siguientes palabras clave para la identificación de estudios relevantes: "Internet Provider Networks", "Network Security", "Cybersecurity", "Evolution of security" y "Cyber threats". Además, para lograr una mayor concordancia y especificidad en los resultados, se realizaron combinaciones estratégicas de palabras clave, tales como "Evolution of ISP network security", "Measures to mitigate cyber-attacks", "Recent developments in ISP cybersecurity", "Emerging technologies in network security" "Strategies to protect against cyber threats at ISPs", "Penetration testing" y "ISP Vulnerability Assessment". En total, se recopilaron 312 documentos a través de esta búsqueda. En la tabla 3 se presenta la estrategia de búsqueda para cada base de datos utilizada.

Tabla 3.

ESTRATEGIA DE BÚSQUEDA

BD Científica	Cadena de búsqueda
SpringerLink	("Internet Provider Networks" OR "Network Security" OR "Cybersecurity" OR "Evolution of security" OR "Cyber threats") AND ("Penetration testing" OR "Vulnerability Assessment")
Web of Science	((((((TS=(Internet Provider Networks)) OR TS=(Network Security)) OR TS=(Cybersecurity)) OR TS=(Evolution of security)) OR TS=(Cyber threats)) AND TS=(Penetration testing)) AND TS=(Vulnerability Assessment)
Scopus	TITLE-ABS-KEY ("Internet Provider Networks" OR "Network Security" OR "Cybersecurity" OR "Evolution of security" OR "Cyber threats") AND TITLE-ABS-KEY ("Penetration testing" OR "Vulnerability Assessment") AND PUBYEAR > 2018 AND PUBYEAR < 2024 AND (LIMIT-TO (DOCTYPE , "ar"))

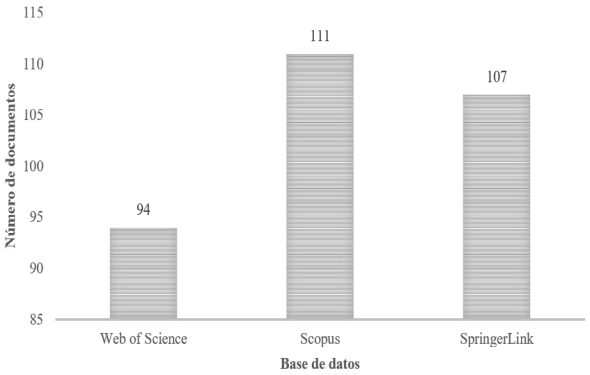

Fig. 1. *Número de documentos por base de datos.*

C. Criterios de inclusión y exclusión

La tabla IV presenta los criterios utilizados para determinar qué estudios se incluirían y excluirían de esta RSL. Estos fueron seleccionados con el propósito de facilitar la identificación y evaluación de estudios pertinentes, asegurando su consistencia metodológica y relevancia con respecto al tema de investigación. La muestra definitiva comprende un conjunto total de 57 trabajos que han sido la piedra angular para el desarrollo de este artículo.

Tabla 4.

CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterios	Inclusión	Exclusión	Doc. excluidos
Periodo de publicación	Estudios publicados desde 2019 hasta 2023.	Investigaciones más antiguas de 5 años.	200
Revisión por pares	Investigaciones revisadas por pares.	Estudios no revisados por pares.	51
Vigencia tecnológica	Estudios centrados en tecnologías vigentes.	Estudios centrados en tecnologías desactualizadas o en desuso.	23
Enfoque temático	Investigaciones centradas en proveedores de servicios de internet.	Estudios no relacionados con la infraestructura de red.	69

D. Recopilación de datos

La recopilación de datos tiene como objetivo reunir y organizar la información relevante de los estudios seleccionados, para responder a las preguntas de investigación. Este proceso se realizó con cuidado y atención, asegurando la coherencia y la integridad de los datos. Posteriormente, se realizó una revisión detallada de todas las fuentes bibliográficas para garantizar que se incluyera toda la información relevante para responder a las preguntas de investigación. Durante esta fase se recopilaron los siguientes atributos.

Tabla 5.

ATRIBUTOS DE LA RECOPILACIÓN DE DATOS

Criterio	Descripción
Tipo de documento	Artículo científico
Publicado en	Revistas científicas
Casa editora	Web of Science, Scopus y SpringerLink
Año de publicación	2019-2023
País	Países de todo el mundo
Enfoque de investigación	Descriptivo, explicativo y empírico
Método de investigación	Encuesta, estudio de caso y experimento
Área de investigación	Seguridad de la red de los ISP, mecanismos de seguridad y prácticas de medidas de seguridad

Con la finalidad de dar respuesta a las tres preguntas de investigación (P1, P2 y P3), fue necesario incluir dos tipos de artículos: a) original de investigación y b) de revisión. El primero presenta de forma detallada proyectos de investigación culminados; su estructura contiene: introducción, metodología, resultados y conclusiones. El segundo analiza, sistematiza e integra los resultados de investigaciones publicadas sobre un campo científico. Tiene como finalidad divulgar avances y tendencias en el campo en el que se desarrolle [14].

E. Análisis de datos

El análisis de datos desempeña un papel crucial para la investigación científica. En este caso, permite comprender y responder las preguntas de investigación planteadas. Este apartado sirvió para examinar los datos recopilados durante la revisión sistemática de literatura sobre la seguridad en las redes de los ISP. Dichos estudios fueron tabulados y posteriormente se analizó todo su contenido con la finalidad de encontrar: Número de trabajos por año y por país, enfoques y métodos de investigación, áreas de investigación, mecanismos de seguridad en redes de proveedores de servicios de internet y medidas para mitigar ataques cibernéticos, enfoque y método de investigación.

III. Resultados

En el marco de esta RSL, se llevaron a cabo búsquedas exhaustivas en diversas bases de datos académicas con la finalidad de localizar estudios pertinentes que aborden las preguntas de investigación. Estas preguntas buscan obtener una comprensión detallada sobre cómo los proveedores de servicios de internet (ISP) definen y aplican los mecanismos de protección de su infraestructura de red. En la siguiente figura se presenta el dinamismo de las investigaciones por año.

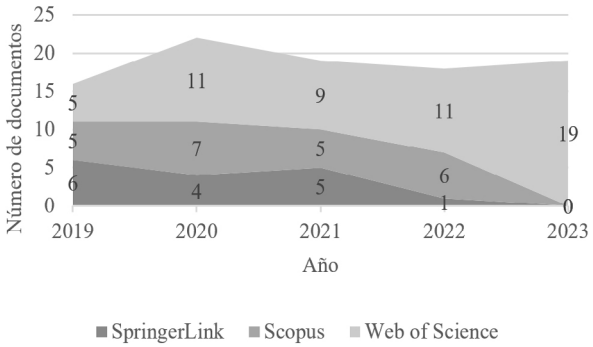

Fig. 2. *Número de documentos por año.*

La figura 2 muestra el número de publicaciones relacionadas con la seguridad en redes de los ISP en tres bases de datos académicas durante los últimos 5 años. La base de SpringerLink mantiene una producción constante de publicaciones, lo que indica que su contenido es estable. Por su parte, la base de Scopus crece moderadamente durante los primeros tres años, sin embargo, luego disminuye en los últimos dos. Por último, la base de Web of Science muestra un crecimiento constante y significativo, alcanzando su punto máximo en el último año.

Tabla 6.

Revistas científicas

Nombre de la revista	N. artículos
International Journal of Information Security	8
Computers & Security	5
The Journal of Supercomputing	4
Digital Investigation	3
Journal of Network and Systems Management	3
Sensors	3
Artificial Intelligence Review	2
Cogent Engineering	2
Computer Networks	2
Energy Reports	2
Human-centric Computing and Information Sciences	2
IEEE Communications Magazine	2
Journal of Big Data	2
Journal of Cloud Computing	2
Journal of Computer Virology and Hacking Techniques	2
Journal of Information Security and Applications	2
Personal and Ubiquitous Computing	2
SN Computer Science	2
Computer Supported Cooperative Work (CSCW)	1
Frontiers of Information Technology & Electronic Engineering	1
International Journal of Advanced Computer Science and Applications	1
Journal of Medical Systems	1
Mathematics	1
Security and Communication Networks	1
Systems Science & Control Engineering	1

La tabla VI muestra la cantidad de artículos publicados en revistas académicas sobre temas relacionados con la informática y la seguridad de la información. Esta información proporciona una visión general de las áreas de investigación que son más activas en este campo. Las revistas "International Journal of Information Security", "Computers & Security" y "The Journal of Supercomputing" se destacan por la cantidad de artículos publicados sobre temas relacionados con la seguridad y las tecnologías de la información. Otras revistas como "Journal of Network and Systems Management", "Digital Investigation", y "Sensors" también publicaron artículos relevantes sobre seguridad y tecnologías de la información.

P1: ¿Cuáles son los mecanismos utilizados por los ISP para proteger la infraestructura de red?

Los resultados muestran que los ISP utilizan una variedad de mecanismos para proteger su infraestructura de red. Los resultados de 24 estudios afirman que el uso de firewalls robustos es una de las estrategias de seguridad de red más comunes utilizadas por los ISP. Los firewalls actúan como una primera línea de defensa, filtrando el tráfico no autorizado y protegiendo la infraestructura de red contra intrusiones [15], [16]. Los ISP también utilizan sistemas de detección de intrusiones avanzados para complementar la protección proporcionada por los firewalls [17].

La integración de tecnologías emergentes, como la inteligencia artificial y el aprendizaje automático, está dando lugar a una evolución significativa [18]. De acuerdo con 8 estudios, estas tecnologías se han convertido en aliados importantes para el desarrollo de nuevas soluciones y aplicaciones. La inteligencia artificial y el aprendizaje automático permiten detectar amenazas de manera anticipada y adaptable. Este enfoque innovador ayuda a los ISP a responder de manera eficazmente a las amenazas cibernéticas en un entorno en constante cambio [19].

Los ISP también utilizan el cifrado de datos en tránsito, una medida de seguridad esencial que protege la confidencialidad de los datos mientras

viaja por la red. Esta medida ayuda a proteger los datos de ser manipulados o alterados, y a mantener la privacidad de los usuarios [20]. Con relación a esto, 12 estudios afirman que, además de las medidas técnicas, como el cifrado de datos en tránsito, es importante establecer políticas de seguridad sólidas que aborden tanto los aspectos técnicos como organizativos.

Por otra parte, la colaboración activa con expertos en ciberseguridad es una práctica importante para los ISP [21]. Esta colaboración les permite mantenerse actualizados sobre las últimas amenazas y adoptar medidas proactivas para prevenir y mitigar incidentes de seguridad [22]. Según 4 estudios, esta acción ayuda a prevenir incidentes de seguridad y a responder a amenazas emergentes, lo que crea un entorno digital más seguro y resistente. En conjunto, estas medidas forman una sólida red de defensa que demuestra la importancia que los ISP otorgan a la seguridad en sus operaciones (ver Tabla VII).

Tabla 7.

Mecanismos de seguridad de infraestructura de red

Mecanismo de seguridad	Nivel de aceptación	Beneficios	Consideraciones y limitaciones	Fuente
Cortafuegos/Firewalls	Altamente aceptado	- Filtrado de tráfico no autorizado. - Prevención de accesos no deseados. - Protección ataques de denegación de servicio (DDoS).	- Una configuración incorrecta puede afectar la conectividad legítima. - Limitaciones en la detección de amenazas avanzadas.	[9], [21], [23], [24]
Sistemas de detección de intrusiones	Moderadamente aceptado	- Detección temprana de actividades maliciosas. - Monitoreo continuo para identificar patrones sospechosos. - Respuesta automática para mitigar amenazas.	- Requiere ajustes continuos para mantener la eficacia. - Puede generar carga adicional en los recursos de red.	[25], [28]
Cifrado de datos	Altamente aceptado	- Protección de confidencialidad de la información. - Seguridad en la transmisión de datos. - Prevención de acceso no autorizado mediante la encriptación.	- Requiere gestión de claves efectiva. - Impacto potencial en el rendimiento en algunas operaciones.	[29], [32]
Colaboración con expertos en ciberseguridad	Altamente aceptado	- Acceso a conocimientos especializados en amenazas emergentes. - Desarrollo de estrategias efectivas de seguridad. - Respuestas rápidas y efectivas ante incidentes de seguridad.	- Dependencia de la disponibilidad de expertos. - Posibles costos asociados a servicios de consultoría. - Importancia de establecer acuerdos de colaboración claros.	[32], [36]

Nota. El nivel de aceptación se refiere a la correspondencia entre los artículos seleccionados y el tema abordado.

P2: ¿Qué pruebas de penetración realizan los ISP para detectar amenazas y vulnerabilidades?

En cuanto a las pruebas de penetración, se identificó que los ISPs emplean un enfoque integral para evaluar la seguridad de sus redes mediante estrategias de seguridad [37]. Simulan ataques cibernéticos para evaluar la solidez de la infraestructura ante diversas amenazas [26]. De acuerdo con los resultados de 29 estudios, estas pruebas incluyen la evaluación de vulnerabilidades en sistemas, la revisión de configuraciones de seguridad y la simulación de ataques para evaluar la capacidad de respuesta ante amenazas reales. La evaluación de vulnerabilidades busca identificar puntos débiles en la infraestructura, desde configuraciones que pueden ser explotadas por atacantes hasta posibles brechas de seguridad que podrían permitir el acceso no autorizado. Este proceso examina políticas de acceso, actualizaciones de software y configuraciones de firewall. [27]. Según 14 estudios, la revisión detallada de configuraciones de seguridad verifica que los ajustes de se establezcan y mantengan correctamente. Esta fase tiene como objetivo mejorar la seguridad,

corrigiendo vulnerabilidades y preparando los sistemas para resistir ataques [38]. Además, se está utilizando cada vez más herramientas de escaneo de vulnerabilidades avanzadas, que brindan una evaluación más automatizada y completa de las posibles debilidades de la infraestructura [31]. Los resultados de 7 estudios señalan que este enfoque incluye el uso de técnicas de ingeniería social para simular ataques que evalúan la resistencia de la organización a amenazas internas y externas. Esto considera los factores humanos que podrían representar riesgos de seguridad [36]. Estas y otras pruebas de penetración se detallan en la tabla VIII.

P3: ¿Cuáles son las medidas más efectivas en la actualidad para mitigar los ataques cibernéticos?

En cuanto a las medidas más efectivas para mitigar ataques cibernéticos, los resultados destacan la importancia de enfoques integrales que van más allá de la tecnología pura [30]. En base a esto, 36 estudios afirman que las medidas más efectivas para erradicar estos ataques son las que combinan la tecnología con otras estrategias, como la educación, la concienciación y la colaboración. La seguridad debe abordarse desde una perspectiva que tenga en cuenta tanto los factores humanos como los organizativos [35]. Las políticas de seguridad robustas también son esenciales para proteger las redes de los ISP. Según 8 estudios, dichas políticas no solo definen lo que se debe hacer, sino que también ayudan a crear una cultura en la que la seguridad es importante. Las organizaciones deben trabajar en estrecha colaboración con entidades especializadas en ciberseguridad para protegerse de las amenazas emergentes [34]. Dicha colaboración permite adoptar las mejores prácticas y compartir información importante sobre amenazas emergentes. Además, se destaca la importancia de utilizar técnicas avanzadas de cifrado y autenticación para proteger las redes y los sistemas informáticos [32], [33]. Estas medidas protegen los datos de alteraciones y garantizan que las comunicaciones sean auténticas. De acuerdo con 13 estudios, esto ayuda a prevenir el acceso no autorizado y los ataques de suplantación de identidad. La combinación de estas estrategias crea una defensa sólida que protege las redes de los ISP de amenazas cibernéticas más complejas. En la tabla IX se mencionan estas y otras medidas de mitigación de ciberataques en redes de proveedores de servicios de internet que es esencial para mantener una seguridad efectiva.

Tabla 8.
Pruebas de penetración

Prueba de Penetración	Nivel de Aceptación	Beneficios	Consideraciones y Limitaciones	Resultados Esperados	Frecuencia Recomendada	Fuente
Escaneo de vulnerabilidades	Ampliamente aceptado	Identificar vulnerabilidades Identificación de puertos abiertos, permitiendo su corrección proactiva.	Puede generar falsos positivos o negativos. No detecta vulnerabilidades nuevas.	Lista detallada de vulnerabilidades y sus ubicaciones.	Trimestralmente o después de cambios significativos.	[17], [39], [40]
Pruebas de intrusión	Ampliamente aceptado	Simula ataques controlados para evaluar la resistencia de la red.	Puede interrumpir servicios si no se realiza correctamente.	Evaluación de la capacidad de defensa y detección de intrusiones.	Anualmente o tras cambios importantes.	[15], [16], [41]
Análisis de configuración	Ampliamente aceptado	Revisión de configuraciones incorrectas que podrían ser explotadas.	Requiere acceso a la configuración del sistema.	Configuraciones seguras y alineadas con las políticas de seguridad.	Trimestralmente o tras actualizaciones.	[18], [20], [22]
Evaluación de políticas de seguridad	Ampliamente aceptado	Revisión y evaluación de las políticas de seguridad y aplicar las mejores practicas	Depende de la precisión y actualización de las políticas.	Identificación de desviaciones y áreas de mejora en las políticas.	Anualmente o tras cambios en políticas.	[33], [35], [36]
Análisis de tráfico	Moderadamente aceptado	Monitoreo y análisis de trafico de red para identificar patrones de tráfico para detectar anomalías.	Puede generar falsas alarmas en situaciones normales.	Identificación de patrones de tráfico inusuales o sospechosos.	Mensualmente o según la criticidad del entorno.	[15], [26], [41]
Pruebas de social engineering	Moderadamente aceptado	Evalúa la resistencia de los usuarios ante engaños.	Puede afectar la moral y la confianza del personal.	Identificación de empleados susceptibles a ataques de ingeniería social	Anualmente y en sesiones de entrenamiento.	[9], [21], [25], [29]

Nota. El nivel de aceptación se refiere a la correspondencia entre los artículos seleccionados y el tema abordado.

Tabla 9.
Medidas de mitigación

Medida de Mitigación	Características de Efectividad	Caso de Estudio	Fuente
Firewalls y filtros de red	Establecen barreras de protección, controlan el tráfico y bloquean accesos no autorizados.	En caso de ataque cibernético, un firewall bloquea con éxito intentos de intrusiones externas, protegiendo la red de un proveedor de servicios de internet (ISP).	[19], [23], [25], [29]
Monitoreo de red continuo	Permite la detección temprana de comportamientos anómalos y actividades sospechosas.	Mediante un sistema de monitoreo continuo, es posible identificar actividades inusuales, lo que permite una respuesta rápida para mitigar una amenaza potencial.	[20], [22], [24]
Protección contra DDoS	Mitiga ataques de denegación de servicio distribuido, preservando la disponibilidad de servicios.	Durante un ataque DDoS, la implementación de medidas de protección permite mantener la operatividad de los servicios críticos, evitando interrupciones significativas.	[16], [17], [40]
Actualizaciones y parches	Mantiene el software actualizado para cerrar vulnerabilidades conocidas.	La aplicación regular de parches y actualizaciones evita la explotación de vulnerabilidades, asegurando un entorno más resistente a amenazas.	[19], [37], [38]
Autenticación y control de acceso	Requiere verificación de identidad y limita el acceso a recursos sensibles.	La implementación de autenticación multifactor y controles de acceso rigurosos reduce los riesgos de accesos no autorizados.	[30], [32], [33]
Cifrado de tráfico	Asegura la confidencialidad de la información durante la transmisión.	El cifrado de datos protege la comunicación entre servidores y usuarios, garantizando la privacidad de la información transmitida.	[9], [15], [42]
Segmentación de red	Divide la red en segmentos para limitar el impacto de posibles compromisos.	En un incidente, la segmentación de red impide la propagación lateral del ataque, confinándolo a un segmento específico.	[18], [39], [43]
Gestión de vulnerabilidades	Identifica, evalúa y aborda las vulnerabilidades de manera proactiva.	Una gestión eficiente de vulnerabilidades permite corregir debilidades antes de que fueran explotadas, fortaleciendo la postura de seguridad.	[38], [44], [45]
Educación en ciberseguridad	Sensibiliza a los usuarios y el personal sobre prácticas seguras.	A través de programas de educación, los usuarios son capaces de reconocer amenazas y actuar de manera segura, reduciendo la probabilidad de caer en ataques de ingeniería social.	[36], [40], [41]
Políticas de seguridad robustas	Establece directrices claras y medidas de seguridad a seguir.	La implementación de políticas sólidas define claramente las responsabilidades y protocolos de seguridad, mejorando la adherencia a las mejores prácticas.	[22], [23], [25], [37]
Respaldo y recuperación de datos	Garantiza la disponibilidad y la capacidad de recuperación en caso de pérdida de datos.	Tras un incidente, la capacidad de recuperación mejorada por estrategias de respaldo permite restaurar rápidamente los servicios afectados.	[35], [46], [47]
Colaboración con la comunidad de ciberseguridad	Comparte información y mejores prácticas con otros actores de ciberseguridad.	Participar en comunidades de ciberseguridad facilita el intercambio de inteligencia, fortaleciendo las defensas contra amenazas compartidas.	[15], [27], [29]

IV. Discusión

La RSL proporciona una visión detallada y completa de las prácticas de seguridad que utilizan los ISPs. Estos resultados se alinean con los hallazgos de estudios anteriores y brindan una valiosa perspectiva sobre el tema. Los ISP utilizan una variedad de mecanismos de seguridad para proteger sus redes, siendo los cortafuegos los más comunes (45%), los sistemas de detección de intrusiones (30%) y el cifrado de datos (20%), pero la colaboración con expertos en ciberseguridad tiene un valor bajo del 5%, por lo que es esencial para abordar las amenazas emergentes.

La creciente adopción de tecnologías emergentes, como la Inteligencia Artificial y el Aprendizaje Automático, pone de manifiesto la necesidad de innovar en la detección proactiva de amenazas. Según Steinberger et al. en su estudio sobre Denegación de servicio distribuido (DDoS), la capacidad de los ISP para aprender y adaptarse constantemente a las amenazas cibernéticas les permite anticiparse y responder a estas amenazas de manera más eficaz [26]. Una amplia gama de medidas de seguridad, desde cortafuegos avanzados hasta el cifrado de datos en tránsito, demuestra un enfoque integral para proteger la seguridad de las redes [27], [28].

La combinación de tecnologías tradicionales con enfoques innovadores demuestra que los ISPs entienden la importancia de proteger sus redes desde todos los frentes [30], [31]. Esto refuerza sus defensas contra las amenazas cibernéticas en constante evolución. Este enfoque integrado demuestra un compromiso activo con la protección de la infraestructura de red en todos sus aspectos [32], [33]. Las pruebas de penetración, junto con el uso cada vez mayor de herramientas avanzadas y estrategias de ingeniería social, ponen de manifiesto la importancia de realizar evaluaciones continuas y adaptables de amenazas y vulnerabilidades. Los autores Ugochukwu et al. afirman que este enfoque demuestra que los ISP están tomando medidas proactivas para hacer frente a un entorno de amenazas cibernéticas en constante evolución [34]. Esta práctica no solo destaca la importancia de estar preparados y ser flexibles para identificar posibles amenazas, sino que también demuestra el compromiso continuo de los ISP con la seguridad de sus redes [35], [36].

La eficacia de las estrategias organizativas, como la concienciación y formación del personal, demuestra que la seguridad cibernética no solo se trata de implementar tecnologías, sino también de educar y empoderar a las personas. La colaboración con expertos en ciberseguridad, junto con la implementación de medidas avanzadas de seguridad, como el cifrado y la autenticación, fortalece significativamente la capacidad de las redes de los ISP para resistir a amenazas cada vez más complejas [38]. Un enfoque integral de seguridad cibernética para ISP debe centrarse en la capacitación continua del personal y las tecnologías avanzadas [37].

Aunque se han logrado avances significativos en seguridad cibernética, es importante reconocer que aún existen desafíos persistentes [22]. El panorama cibernético cambia constantemente, por lo que es importante que las organizaciones sean flexibles y estén dispuestas a cambiar sus estrategias de seguridad [20]. La seguridad no es un estado estático, sino un proceso continuo de revisión y mejora. Por lo tanto, la cooperación entre los ISP, la comunidad de seguridad y los gobiernos podría ser fundamental para mejorar la capacidad de respuesta a las amenazas cibernéticas a gran escala [19].

Limitaciones del estudio

Las limitaciones del estudio señalan áreas donde los resultados pueden no ser precisos o generalizables. La revisión se ha centrado en estudios de regiones específicas, por lo que los resultados pueden no ser aplicables a otros lugares. Además, las condiciones de seguridad pueden variar según la zona. Por otra parte, aunque se realizó una búsqueda exhaustiva, la calidad y disponibilidad de los estudios identificados puede afectar la confiabilidad de los resultados.

V. Conclusiones

La integración de diversas medidas de seguridad en los ISPs va desde avanzados firewalls hasta el cifrado de datos, junto con la realización periódica de pruebas de penetración, resalta la importancia crítica de adoptar una estrategia integral de seguridad. Además, la eficacia de las estrategias organizativas, como la concientización de los empleados, subraya la relevancia fundamental de los aspectos humanos en el ámbito de la ciberseguridad. Por ende, la colaboración entre los ISPs, la comunidad de seguridad y las autoridades gubernamentales se revela como una pieza clave para abordar los desafíos emergentes en el panorama cibernético en constante cambio. La revisión sistemática de literatura sobre la seguridad en las redes de los ISP destaca tendencias y prácticas cruciales en ciberseguridad. La integración de tecnologías emergentes, como la Inteligencia Artificial, pone de manifiesto la necesidad de soluciones más sofisticadas para la detección de amenazas, para anticipar amenazas subraya la importancia de contar con soluciones avanzadas para salvaguardar las redes. Sin embargo, se reconoce la necesidad constante de mejora para adaptarse a las amenazas. Además, la colaboración emerge como una estrategia efectiva para compartir conocimientos y recursos, fortaleciendo así la capacidad de detectar y responder a las vulnerabilidades existentes, asegurando la robustez a largo plazo de las infraestructuras tecnológicas de dichos proveedores.

Las futuras investigaciones deben centrarse en ampliar el alcance geográfico para obtener una visión integral y global de las prácticas de seguridad. Es esencial explorar la integración y eficacia de tecnologías emergentes, como la Inteligencia Artificial y el Aprendizaje Automático, en la detección proactiva de amenazas cibernéticas, así como evaluar el impacto de las estrategias organizativas en la concienciación y formación del personal en ciberseguridad. Además, se debe profundizar en el estudio del rol de la colaboración entre diversos actores, incluyendo expertos en ciberseguridad y entidades gubernamentales, para mejorar la capacidad de respuesta frente a amenazas cibernéticas.

VI. Referencias

[1] C. Hesselman et al., "A Responsible Internet to Increase Trust in the Digital World," Journal of Network and Systems Management, vol. 28, no. 4, 2020, doi: 10.1007/s10922-020-09564-7.

[2] M. Alanazi and A. Aljuhani, "Anomaly Detection for Internet of Things Cyberattacks," Computers, Materials and Continua, vol. 72, no. 1, 2022, doi: 10.32604/cmc.2022.024496.

[3] F. E. Catota, M. Granger Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the Ecuadorian financial sector," J Cybersecur, vol. 4, no. 1, 2018, doi: 10.1093/cybsec/tyy002.

[4] C. W. Lee and S. Madnick, "Cybersafety approach to cybersecurity analysis and mitigation for mobility-as-a-service and internet of vehicles," Electronics (Switzerland), vol. 10, no. 10, 2021, doi: 10.3390/electronics10101220.

[5] Z. Wenhua et al., "Data security in smart devices: Advancement, constraints and future recommendations," IET Networks. 2023. doi: 10.1049/ntw2.12091.

[6] O. S. Althobaiti and M. Dohler, "Cybersecurity challenges associated with the internet of things in a post-quantum world," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3019345.

[7] R. Tapiero, A. Gonzalez, and N. Novoa, "Seguridad en redes SDN y sus aplicaciones," Revista colombiana de tecnologias de avanzada (RCTA), vol. 1, no. 37, 2023, doi: 10.24054/rcta.v1i37.1262.

[8] P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei, and A. K. M. N. Islam, "Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity," Solar Energy, vol. 263, 2023, doi: 10.1016/j.solener.2023.111921.

[9] M. Á. Álvarez Roldán and H. F. Montoya Vargas, "Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos," Ingeniería y Desarrollo, vol. 38, no. 2, pp. 279–297, 2020, doi: https://doi.org/10.14482/inde.38.2.006.31.

[10] G. Carrión-Barco, M.-J. Sánchez-Chero, C. I. Del Castillo Castro, F. W. Campos Flores, and M. Timaná Alvarez, "Modelo de seguridad informática para un medio de conexión pública," Revista de la Universidad del Zulia, vol. 12, no. 32, 2021, doi: 10.46925//rdluz.32.21.

[11] J. J. Cano M., "Seguridad y ciberseguridad 2009-2019. Lecciones aprendidas y retos pendientes," Revista SISTEMAS, no. 155, 2020, doi: 10.29236/sistemas.n155a6.

[12] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," Inf Softw Technol, vol. 51, no. 1, pp. 7–15, 2009, doi: https://doi.org/10.1016/j.infsof.2008.09.009.

[13] E. Henríquez Fierro and M. I. Zepeda Gonzales, "Elaboración de un artículo científico de investigación," Ciencia y enfermería, vol. 10, pp. 17–21, 2004, doi: https://dx.doi.org/10.4067/S0717-95532004000100003.

[14] E. Serna M. and D. Morales V., "La investigación en verificación formal- un estado del arte," Revista Cubana de Ciencias Informáticas, vol. 7, no. 3, pp. 114–126, 2013, [Online]. Available: https://www.redalyc.org/articulo.oa?id=378334198010

[15] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021, doi: https://doi.org/10.1016/j.egyr.2021.08.126.

[16] P. R. Kshirsagar, H. Manoharan, H. A. Alterazi, N. Alhebaishi, O. B. J. Rabie, and S. Shitharth, "Construal Attacks on Wireless Data Storage Applications and Unraveling Using Machine Learning Algorithm," J Sens, vol. 2022, p. 9386989, 2022, doi: 10.1155/2022/9386989.

[17] M. Husák, N. Neshenko, M. S. Pour, E. Bou-Harb, and P. eleda, "Assessing Internet-wide Cyber Situational Awareness of Critical Sectors," Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018, [Online]. Available: https://api.semanticscholar.org/CorpusID:51981620

[18] L. Megouache, A. Zitouni, and M. Djoudi, "Ensuring user authentication and data integrity in multi-cloud environment," Human-centric Computing and Information Sciences, vol. 10, no. 1, p. 15, 2020, doi: 10.1186/s13673-020-00224-y.

[19] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," Human-centric Computing and Information Sciences, vol. 10, no. 1, p. 9, 2020, doi: 10.1186/s13673-020-0214-5.

[20] Swati, S. Roy, J. Singh, and J. Mathew, "Design and analysis of DDoS mitigating network architecture," Int J Inf Secur, vol. 22, no. 2, pp. 333–345, 2023, doi: 10.1007/s10207-022-00635-1.

[21] S. O. Tumbo, K. M. Villalba, Siler, and A. Donado, "An adaptable Intelligence Algorithm to a Cybersecurity Framework for IIOT Un algoritmo de inteligencia adaptable a un marco de ciberseguridad para IIOT," 2022. doi: DOI: 10.25100/iyc.v24i2.11762.

[22] S. Creese, W. H. Dutton, and P. Esteve-González, "The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions," Pers Ubiquitous Comput, vol. 25, no. 5, pp. 941–955, 2021, doi: 10.1007/s00779-021-01569-6.

[23] J. Singh, "Mitigating Cyber-Attacks in Cloud Environments: Hardware-Supported Multi-Point Conceptual Framework," International Journal of Cyber Warfare and Terrorism (IJCWT), vol. 11, no. 4, pp. 43–57, 2021, doi: 10.4018/IJCWT.2021100103.

[24] D. S. Pacheco, "Seguridad en redes de comunicaciones: Perspectivas y desafíos," Ingeniare. Revista chilena de ingeniería, vol. 30, pp. 215–217, 2022, doi: https://dx.doi.org/10.4067/S0718-33052022000200215.

[25] S. K. Kodali and C. H. Muntean, "An Investigation into Deep Learning Based Network Intrusion Detection System for IoT Systems," in 2021 IEEE International Conference on Data Science and Computer Application (ICDSCA), 2021, pp. 374–377. doi: 10.1109/ICDSCA53499.2021.9650111.

[26] J. Steinberger, A. Sperotto, H. Baier, and A. Pras, "Distributed DDoS Defense: A collaborative Approach at Internet Scale," in NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, 2020, pp. 1–6. doi: 10.1109/NOMS47738.2020.9110300.

[27] P. Benlloch-Caballero, Q. Wang, and J. M. Alcaraz Calero, "Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks," Computer Networks, vol. 222, p. 109526, 2023, doi: https://doi.org/10.1016/j.comnet.2022.109526.

[28] I. Ko, D. Chambers, and E. Barrett, "Feature dynamic deep learning approach for DDoS mitigation within the ISP domain," Int J Inf Secur, vol. 19, no. 1, pp. 53–70, 2020, doi: 10.1007/s10207-019-00453-y.

[29] M. S. Alkatheiri, M. A. Alqarni, and S. H. Chauhdary, "Cyber security framework for smart home energy management systems," Sustainable Energy Technologies and Assessments, vol. 46, p. 101232, 2021, doi: https://doi.org/10.1016/j.seta.2021.101232.

[30] B. Ayodele and V. Buttigieg, "SDN as a defence mechanism: a comprehensive survey," Int J Inf Secur, 2023, doi: 10.1007/s10207-023-00764-1.

[31] S. Kaur, A. K. Sandhu, and A. Bhandari, "Investigation of application layer DDoS attacks in legacy and software-defined networks: A comprehensive review," Int J Inf Secur, vol. 22, no. 6, pp. 1949–1988, 2023, doi: 10.1007/s10207-023-00728-5.

[32] I. Ko, D. Chambers, and E. Barrett, "Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain," ETRI Journal, vol. 41, no. 5, pp. 574–584, Oct. 2019, doi: https://doi.org/10.4218/etrij.2019-0109.

[33] F. S. de Lima Filho, F. A. F. Silveira, A. de Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," Security and Communication Networks, vol. 2019, p. 1574749, 2019, doi: 10.1155/2019/1574749.

[34] N. A. Ugochukwu, S. B. Goyal, A. S. Rajawat, S. M. N. Islam, J. He, and M. Aslam, "An Innovative Blockchain-Based Secured Logistics Management Architecture: Utilizing an RSA Asymmetric Encryption Method," Mathematics, vol. 10, no. 24, 2022, doi: 10.3390/math10244670.

[35] I. Ko, D. Chambers, and E. Barrett, "Adaptable feature-selecting and threshold-moving complete autoencoder for DDoS flood attack mitigation," Journal of Information Security and Applications, vol. 55, p. 102647, 2020, doi: https://doi.org/10.1016/j.jisa.2020.102647.

[36] T. Gangavarapu, C. D. Jaidhar, and B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," Artif Intell Rev, vol. 53, no. 7, pp. 5019–5081, 2020, doi: 10.1007/s10462-020-09814-9.

[37] A. Papanikolaou, A. Alevizopoulos, C. Ilioudis, K. Demertzis, and K. Rantos, "An autoML network traffic analyzer for cyber threat detection," Int J Inf Secur, vol. 22, no. 5, pp. 1511–1530, 2023, doi: 10.1007/s10207-023-00703-0.

[38] M. Repetto, D. Striccoli, G. Piro, A. Carrega, G. Boggia, and R. Bolla, "An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains," Journal of Network and Systems Management, vol. 29, no. 4, p. 37, 2021, doi: 10.1007/s10922-021-09607-7.

[39] Y. Palmo, S. Tanimoto, H. Sato, and A. Kanai, "IoT Reliability Improvement Method for Secure Supply Chain Management," in 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE), 2021, pp. 364–365. doi: 10.1109/GCCE53005.2021.9622088.

[40] N. Yakin, M. Zhitkov, A. Chernikov, and P. Pepelyaev, "Security Threats and Service Degradation Detection in LoRaWAN Networks," in 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2021, pp. 455–458. doi: 10.1109/USBEREIT51232.2021.9455123.

[41] D. Mendez Mena and B. Yang, "Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things," IoT, vol. 2, no. 1, pp. 1–16, 2021, doi: 10.3390/iot2010001.

[42] B. Rodrigues, E. Scheid, C. Killer, M. Franco, and B. Stiller, "Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks," Journal of Network and Systems Management, vol. 28, no. 4, pp. 953–989, 2020, doi: 10.1007/s10922-020-09559-4.

[43] P. M. Santos et al., "Towards a Distributed Learning Architecture for Securing ISP Home Customers," in Artificial Intelligence Applications and Innovations. AIAI 2021 IFIP WG 12.5 International Workshops, I. Maglogiannis, J. Macintyre, and L. Iliadis, Eds., Cham: Springer International Publishing, 2021, pp. 311–322.

[44] D. Mustefa and S. Punnekkat, "Cybersecurity Analysis for a Remote Drug Dosing and Adherence Monitoring System," in IoT Technologies for HealthCare, R. Goleva, N. R. da C. Garcia, and I. M. Pires, Eds., Cham: Springer International Publishing, 2021, pp. 162–178. Accessed: Dec. 18, 2023. [Online]. Available: https://doi.org/10.1007/978-3-030-69963-5_12

[45] A. U. Sudugala, W. H. Chanuka, A. M. N. Eshan, U. C. S. Bandara, and K. Y. Abeywardena, "WANHEDA: A Machine Learning Based DDoS Detection System," in 2020 2nd International Conference on Advancements in Computing (ICAC), 2020, pp. 380–385. doi: 10.1109/ICAC51239.2020.9357130.

[46] F. M. Isiaka, S. A. Audu, and M. A. Umar, "Developing a fail-safe culture in a cyber environment using MySQL replication

technique," International Journal of Crowd Science, vol. 4, no. 2, pp. 149–170, Jan. 2020, doi: 10.1108/IJCS-04-2018-0008.

[47] D. Suvarna and S. Pathak, "Threat Modeling for Breaking of CAPTCHA System," in Intelligent Computing, Information and Control Systems, A. P. Pandian, K. Ntalianis, and R. Palanisamy, Eds., Cham: Springer International Publishing, 2020, pp. 94–104. Accessed: Dec. 18, 2023. [Online]. Available: https://bv.unir.net:2133/10.1007/978-3-030-30465-2_12