InGenio Journal
Revista de Ciencias de la Ingeniería de la Universidad Técnica Estatal de Quevedo
https://revistas.uteq.edu.ec/index.php/ingenio
e-ISSN: 2697-3642 - CC BY-NC-SA 4.0

Marco de trabajo referencial basado en la norma ISO/IEC 27001:2022 para entornos de seguridad de las SDN

(Referential framework based on the ISO/IEC 27001:2022 standard for SDN security environments)

Narcisa Mariana Fernández Lectong, Bethsy Alexandra Molina Aquino
Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López
narcisa.fernandez@espam.edu.ec, bmolina@espam.edu.ec

Resumen: Las redes definidas por software (SDN) presentan muchas vulnerabilidades potenciales en la seguridad, debido a su innovadora estructura, interfaz de administración de sus componentes y la capacidad de crear entornos programables. En este contexto, el objetivo de la presente investigación fue diseñar un marco de trabajo referencial para la gestión de la seguridad en SDN, fundamentado en los controles de la norma ISO/IEC 27001:2022. Se adoptó un enfoque metodológico cualitativo, estructurado en cuatro etapas: revisión de literatura e identificación de vulnerabilidades, construcción del marco referencial, elaboración y validación del instrumento aplicando criterios de pertinencia y aplicabilidad; y finalmente, la validación del marco de trabajo propuesto mediante juicio de expertos. La propuesta fue validada mediante un instrumento estructurado de 25 preguntas, evaluado por cinco expertos en seguridad de la información y redes. Los resultados revelan que el 78 % de los expertos considera pertinente y aplicable el marco de trabajo, destacando su utilidad para mitigar riesgos en entornos SDN. En conclusión, el modelo propuesto representa una herramienta efectiva, replicable y alineada a estándares internacionales, aportando una solución contextualizada para fortalecer la seguridad en infraestructuras definidas por software.

Palabras clave: Redes definidas por software, seguridad, vulnerabilidades.

Abstract: Software-Defined Networks (SDN) present multiple potential security vulnerabilities due to their innovative architecture, component management interface, and ability to create programmable environments. In this context, the objective of the present study was to design a reference framework for security management in SDN, based on the controls defined in the ISO/IEC 27001:2022 standard. A qualitative methodological approach was adopted, structured into four stages: literature review and vulnerability identification, construction of the reference framework, development and validation of the evaluation instrument using criteria of relevance and applicability; and finally, expert-based validation of the proposed framework. The proposal was validated through a structured instrument consisting of 25 questions, reviewed by five subject matter experts in information security and networking. The results indicate that 78 % of the experts consider the framework both relevant and applicable, emphasizing its potential to mitigate risks within SDN environments. In conclusion, the proposed model constitutes an effective, replicable, and standards-aligned tool, offering a contextualized solution to strengthen the security posture of software-defined infrastructures.

Keywords: Software-defined networks, security, vulnerabilities.

Volumen 8 | Número 2 | Pp. 1–18 | Julio 2025
DOI: https://doi.org/10.18779/ingenio.v8i2.1010
Recibido (Received): 2025/01/09
Aceptado (Accepted): 2025/05/21

1. INTRODUCCIÓN

Una SDN es una arquitectura emergente que es dinámica, administrable, rentable, y adaptable; lo que la hace ideal para los entornos dinámicos de las aplicaciones de hoy en día. Estas redes son tecnologías versátiles que dan respuesta a la mejora en la calidad del servicio en redes, enmarcándola como una de las tecnologías que generará mayor impacto en las redes durante los próximos cinco años [1].

De acuerdo con el informe de investigación de mercado publicado por [2], en 2019 el tamaño del mercado a nivel mundial de SDN se valoró en 9.995 millones de dólares de los Estados Unidos y se prevé que al 2027 alcance los 72.630 millones de dólares, con un crecimiento de la tasa anual compuesta del 28,2 % de 2020 a 2027.

El inicio de esta tecnología se da desde el 2008 por investigaciones realizadas en las Universidades de Standford y Berkeley, las cuales fueron difundidas mediante publicaciones científicas de [3] y [4], sentando las bases para el origen del protocolo OpenFlow y el primer controlador para redes definidas por software. En el 2010 se convirtió en el protocolo para las SDN, posterior a la creación de la Open Networking Foundation, con aproximadamente 69 miembros, entre los que se encontraban Google y Yahoo; años más tarde se unieron Cisco, Juniper y HP.

Para el año 2014, CISCO presentaría un nuevo protocolo de enrutamiento de datos con el nombre de OpFlex; sin embargo, OpenFlow seguía liderando como el protocolo más usado. Y así fue hasta que, en el 2017, Google anunció su asociación con empresas de redes móviles, creando así una plataforma basada en SDN para que los operadores ejecuten sus servicios de red y con la visión de que con el pasar del tiempo se incrementará su uso en compañías de todo el mundo. Entre los casos de uso más exitosos y que hasta la actualidad utilizan SDN se encuentran empresas como Telefónica, VMware, Alcatel y HP [5].

Sin embargo, en comparación a las redes de datos tradiciones los cambios van desde el mecanismo de operación y control, topología de la red hasta la adaptación a políticas de seguridad superiores a las clásicas, por lo cual es necesario implementar medidas y controles de seguridad para garantizar la adaptabilidad, seguridad y solidez ante los cambios dinámicos de la red. Considerando que el 53 % de ataques en ciberseguridad generan pérdidas económicas superiores a $500.000 [6].

En los sistemas de información actuales, los datos y la información que albergan son considerados los activos más valiosos para las organizaciones, lo que hace imprescindible la implementación de mecanismos de protección para enfrentar las posibles vulnerabilidades en sus sistemas de seguridad [7]. Considerando la información como el activo más valioso, se convierte en un recurso esencial que puede determinar el éxito o el fracaso de una organización; por lo tanto, proteger los datos de una institución ha adquirido una relevancia crucial [8].

La seguridad informática se entiende como el proceso de diseñar y aplicar un conjunto de estrategias, políticas, técnicas, normativas, guías, prácticas y procedimientos destinados a prevenir, proteger y salvaguardar los recursos informáticos de una organización contra daños, alteraciones o robos, además de gestionar los riesgos asociados [9].

El uso de normas de calidad, como la ISO, asegura condiciones de calidad dentro de una empresa u organización. En cuanto a las mejores prácticas de seguridad de la información, se utiliza la norma técnica ISO/IEC 27001:2022 que al ser implementada permite a las empresas certificar su Sistema de Gestión de Seguridad de la Información generando confianza entre sus accionistas, clientes, autoridades, proveedore/s y otras partes interesadas. La atención adecuada a este aspecto crucial asegura la correcta asignación de recursos en las áreas de mayor impacto, lo que a su vez optimiza las inversiones y los costos de seguridad [10].

Con base en los antecedentes expuesto se tuvo como objetivo la creación de un marco de trabajo referencial para la seguridad de las SDN basado en la norma ISO/IEC 27001:2022.

2. METODOLOGÍA

La presente investigación se desarrolló bajo un enfoque cualitativo con alcance descriptivo, orientado a la construcción de un marco de trabajo referencial para la gestión de la seguridad en SDN, fundamentado en los controles establecidos por la norma ISO/IEC 27001:2022, con la finalidad de comprender e interpretar las vulnerabilidades inherentes a las SDN y vincularlas con los controles normativos vigentes, permitiendo así una propuesta estructurada y contextualizada.

Cabe destacar que la revisión de literatura se delimitó al periodo comprendido entre 2018 y 2022, en virtud de que la actualización de la norma ISO/IEC 27001 fue publicada oficialmente en el año 2022. Esta delimitación temporal asegura la inclusión de estudios contemporáneos y relevantes, tanto en términos de avances tecnológicos en SDN como de enfoques emergentes en seguridad de la información, garantizando la pertinencia de las fuentes seleccionadas con respecto al marco normativo actual.

2.1. Revisión de literatura e identificación de vulnerabilidades

La recopilación de información científica se efectuó conforme a la metodología de gestión del conocimiento propuesta por [11], que contempla tres fases: búsqueda, organización y análisis de la información.

Búsqueda de información. – Se emplearon ecuaciones booleanas adaptadas a los descriptores "software-defined networking", "vulnerabilities", "security", "ISO 27001", en la base de datos científica Scopus. Se priorizaron artículos arbitrados, publicaciones en proceedings de conferencias de alto impacto y revisiones sistemáticas publicadas entre 2018 al 2022. La expresión empleada se detalla a continuación:

(TITLE-ABS-KEY (software AND defined AND networking) AND TITLE-ABS-KEY (vulnerabilities) OR TITLE-ABS-KEY (security) AND TITLE-ABS-KEY (risk)) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018)) AND (LIMIT TO (DOCTYPE , "ar")) AND (LIMIT-TO (SUBJAREA , "COMP")).

La revisión de literatura se delimitó al periodo comprendido entre 2018 y 2022 con el propósito de asegurar la actualidad y pertinencia de los estudios seleccionados. Esta restricción temporal se fundamenta en dos consideraciones principales: la primera, por la necesidad de reflejar la evolución reciente de las tecnologías de SDN y de los enfoques de gestión de seguridad de la información; y la segunda consideración, debido a la publicación de la actualización de la norma ISO/IEC 27001:2022, que constituye el marco de referencia para el diseño del presente estudio.

No se consideraron artículos posteriores al año 2022 debido a que, al momento de realizar la investigación, los marcos regulatorios y tecnológicos posteriores aún no contaban con suficiente evidencia científica consolidada ni aplicaciones prácticas relacionadas directamente con la nueva versión de la norma. Asimismo, se reconoce como limitación el hecho de no incorporar estudios anteriores a 2018, los cuales, aunque relevantes históricamente, podrían no reflejar adecuadamente los requerimientos actuales de seguridad en infraestructuras SDN bajo los lineamientos de la ISO/IEC 27001:2022.

Organización de la información. - Los documentos obtenidos fueron clasificados por año y fuente, permitiendo un análisis cronológico de los riesgos y amenazas emergentes.

Análisis de información. - A partir de la lectura crítica de los documentos, se identificaron vulnerabilidades y posteriormente fueron agrupadas por similitud. Este análisis permitió

establecer las brechas de seguridad más recurrentes y relevantes en entornos de redes definidas por software, lo cual sirvió de insumo para la construcción del marco propuesto.

2.2. Construcción de marco de trabajo

Con base en la identificación de las vulnerabilidades, se diseñó un marco de trabajo referencial de seguridad, el cual propone una correspondencia entre dichas debilidades y los controles de seguridad especificados en la norma ISO/IEC 27001:2022. Para ello, se analizaron los atributos de control definidos en la norma. La finalidad de esta propuesta es mitigar los riesgos de seguridad en entornos SDN desde una perspectiva normativa, integrando criterios de aplicabilidad y pertinencia.

2.3. Elaboración y validación de instrumento de evaluación del marco de trabajo propuesto

Se elaboró un instrumento de evaluación estructurado en torno a preguntas objetivas dirigidas a valorar la correspondencia entre las vulnerabilidades y los controles propuestos, considerando su factibilidad en contextos reales. Este instrumento incluyó preguntas por cada vulnerabilidad identificada, evaluando las dimensiones de pertinencia y aplicabilidad de implementación.

La validación del instrumento se realizó mediante técnica de juicio de expertos, con el objetivo de asegurar su validez de contenido. Para ello, se aplicaron entrevistas a seis expertos en las áreas de seguridad informática, auditoría TI y redes de telecomunicaciones, con principios de equidad (tres hombres y 3 mujeres), con experiencia profesional entre 6 y 15 años, y formación de cuarto nivel en campos afines.

La evaluación de las respuestas se realizó utilizando una escala de Likert de tres niveles. La escala se definió de la siguiente manera: 1 = Ni de acuerdo ni en desacuerdo, 2 = De acuerdo y 3 = Totalmente de acuerdo. Esta escala permitió obtener una valoración cuantitativa precisa sobre la aceptación y viabilidad del marco propuesto en contextos reales.

2.4. Validación del marco de trabajo propuesto

La propuesta del marco de trabajo fue validada a través de entrevistas estructuradas, las cuales fueron dirigidas a otro grupo de expertos, conformado por cinco integrantes, seleccionados por su conocimiento y experiencia técnica-práctica. El grupo evaluador estuvo compuesto por tres hombres y dos mujeres, cuyas edades oscilan entre los 36 y 45 años, con relación laboral en los sectores de la educación y la justicia, desempeñándose como docentes-investigadores universitarios y responsables de departamentos de TI, lo que garantiza una perspectiva técnica y especializada.

Cada experto valoró la aplicabilidad de los controles mediante una escala de Likert de cinco niveles (1 = totalmente en desacuerdo, 5 = totalmente de acuerdo), permitiendo así un análisis cuantitativo de las medidas propuestas. Los resultados obtenidos permitieron identificar los controles con mayor tendencia de aceptación por parte de los expertos para atender las vulnerabilidades de las redes definidas por software, asegurando así la solidez y aplicabilidad en entornos SDN.

3. RESULTADOS Y DISCUSIÓN

3.1. Revisión de literatura e identificación de vulnerabilidades

3.1.1. Búsqueda y organización de información

Como resultado de la búsqueda, se identificaron 45 artículos científicos con un total acumulado de hasta 102 citas registradas en la base Scopus, lo que refleja una media de 12 citas por publicación. Estos estudios fueron desarrollados por 164 autores con filiación institucional en países como Australia, Alemania, India, Irak, Irlanda, Malasia, Arabia Saudita, España, Suiza y Estados Unidos. Esta diversidad geográfica y académica evidencia el carácter global y transversal de la investigación en seguridad para redes definidas por software.

Además, se observó un crecimiento progresivo en el volumen de publicaciones en los últimos cinco años (Figura 1), siendo el año 2022 el periodo con mayor producción científica sobre el tema, lo que coincide con la actualización de la norma ISO/IEC 27001, lo que sugiere una relación directa entre los avances normativos en seguridad de la información y el impulso académico en el estudio de entornos SDN. La evolución observada refuerza la necesidad de establecer marcos de seguridad alineados a estándares internacionales recientes.

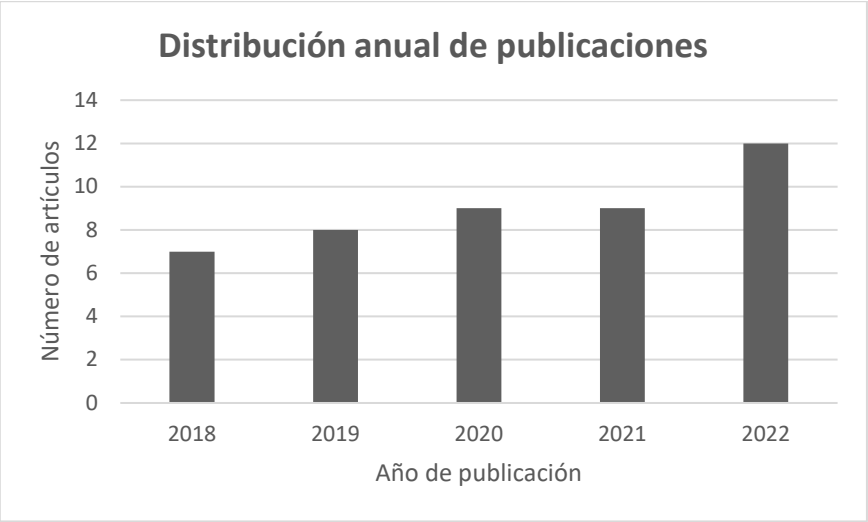

Figura 1. Distribución anual de publicaciones sobre SDN y seguridad de la información.

3.1.2. Análisis de información

Tras el análisis integral del contenido de los 45 artículos científicos seleccionados, se identificó que estos abordaban de forma explícita vulnerabilidades presentes en entornos de redes definidas por software (SDN). El proceso de revisión permitió clasificar las vulnerabilidades recurrentes en cinco categorías principales: Ataques de denegación de servicio DoS/DDoS, vulnerabilidades de hardware, vulnerabilidades de la ingeniería social, desafíos de la legislación y desconocimiento del usuario.

En la Figura 2 se representa la frecuencia con la que se reportan las cinco vulnerabilidades identificadas en la muestra de artículos científicos. Se observa que la vulnerabilidad denegación de servicio (V1) es la más frecuente, apareciendo en 30 publicaciones, lo que representa una tendencia significativa respecto al resto de vulnerabilidades. Las vulnerabilidades relacionadas con hardware (V2), ingeniería social (V3), desafíos normativos o legales (V4) y denegación de servicio (V5) presentan frecuencias notablemente menores, con 5, 4, 3 y 3 artículos respectivamente. Esta distribución sugiere que V1 constituye una preocupación prioritaria en la literatura académica del área SND, posiblemente debido a su impacto, recurrencia o criticidad en los entornos analizados.

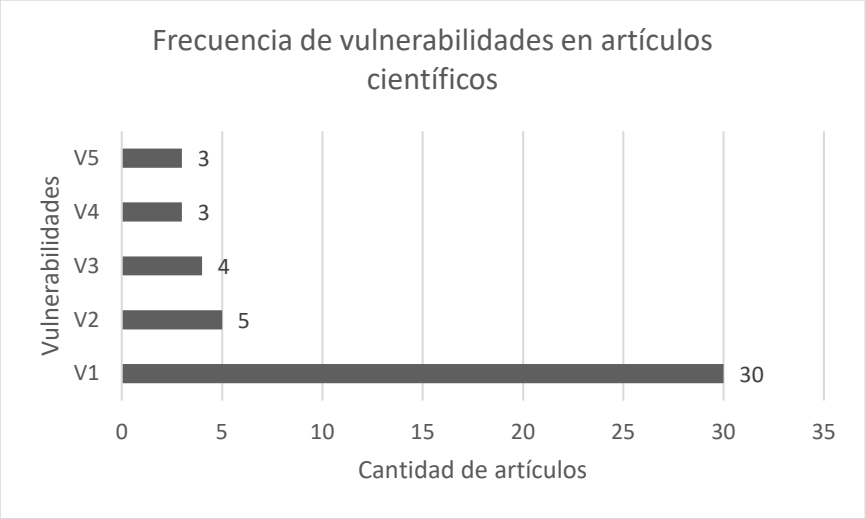

Figura 2. Identificación de vulnerabilidades.

Ataques de denegación de servicio DoS/DDoS (V1): Estos ataques fueron citados como la vulnerabilidad más frecuente entre los documentos analizados. Estos ataques se manifiestan especialmente en entornos con dispositivos inteligentes y sistemas IoT, como enrutadores y servidores Linux comprometidos, donde se explotan limitaciones de recursos como memoria, CPU, disco o ancho de banda.

Investigaciones como las de [12], [13], [14], [15] y [16] refieren que el objetivo principal de un atacante DoS en la red inteligente es interrumpir el servicio (ataque a la disponibilidad), por ejemplo, inundar un enlace de destino o atacar un servidor de automatización. El enfoque de los atacantes para la denegación de servicio es desactivar servicios, por lo que en caso de que ocurra alguna falla, no se podrán recuperar el servicio de manera inmediata. Además, al desactivar los sistemas de monitoreo en la red inteligente evita que las alarmas críticas propaguen información relevante a la atención de los operadores. Un ataque aislado tan simple puede desencadenar una cadena de fallas que conducen a que una gran cantidad de personas se queden sin servicio.

Vulnerabilidades de hardware (V2): Estas incluyen fallos en interfaces físicas y dispositivos expuestos, que pueden ser explotados de manera remota. La falta de mecanismos de protección en el hardware representa un riesgo significativo para la integridad del software y la seguridad de las operaciones críticas del sistema [17].

Vulnerabilidades de la ingeniería social (V3): Las interacciones humanas han generado un gran impacto en el uso de dispositivos y datos, lo que incrementa la generación de ataques. Uno de los ataques más frecuentes son los piratas informáticos, los cuales pueden tener el control de la red y dispositivos inteligentes [18].

Desafíos de la legislación (V4): La legislación no garantiza el uso seguro correcto de los datos; sin embargo, permite subsanar e indemnizar el daño causado por el uso indebido de los datos a través de controles de seguridad [19]. No obstante, los controles técnicos y organizacionales propuestos en normas como la ISO/IEC 27001 pueden contribuir a reducir estos riesgos.

Desconocimiento del usuario (V5): La falta de cultura de seguridad informática entre los usuarios finales los convierte en objetivos fáciles de ataques como spear phishing, fraudes o fuga de datos [20]. Esta vulnerabilidad se agudiza con el crecimiento en el uso de dispositivos móviles, donde las prácticas de seguridad suelen ser más laxas.

3.2. Construcción de marco de trabajo

La construcción del marco de trabajo se basó en la aplicación de controles de seguridad establecidos en la norma ISO/IEC 27001:2022, orientados a mitigar las cinco vulnerabilidades identificadas en entornos de SDN. Para cada vulnerabilidad se seleccionaron cinco controles específicos, considerando criterios de aplicabilidad y pertinencia al contexto de las amenazas observadas. Esta estructura permitió el desarrollo de una propuesta integral, diseñada para fortalecer la gestión de la seguridad de la información en SDN mediante mecanismos eficientes, replicables y alineados con estándares internacionales.

La integración de estos mecanismos se representa en la Tabla 1, se propone el uso de una combinación de controles centrados en la gestión de accesos, el uso de tecnologías de autenticación robusta y la implementación de políticas de respuesta a incidentes, para mitigar los ataques DoS/DDoS; estos controles apuntan a mejorar la disponibilidad y capacidad de recuperación de la red ante intentos de saturación maliciosa.

Mientras que, para la mitigación de las vulnerabilidades de hardware, los controles seleccionados se enfocan en la seguridad física y del entorno, incluyendo la protección de activos, restricciones al acceso físico no autorizado y mantenimiento de la integridad de los dispositivos; estas medidas buscan asegurar que el hardware no se convierta en un punto de entrada para ataques. Por otro lado, para la vulnerabilidad de ingeniería social, se incorporan controles dirigidos a la concientización y formación del personal, lo cual permite reducir la exposición ante manipulaciones psicológicas o engaños dirigidos a usuarios y operadores de red.

Asimismo, para los desafíos de la legislación, se incluye la implementación de políticas para el tratamiento de la información, cumplimiento de requisitos legales, gestión de contratos con partes externas y auditorías internas; estos controles fortalecen el marco legal y documental de la seguridad en SDN. Finalmente, en la vulnerabilidad de desconocimiento del usuario, se priorizan mecanismos de capacitación continua, protección contra malware, restricciones al uso de medios removibles y monitoreo del comportamiento del usuario; estas acciones son clave para elevar la conciencia del riesgo entre usuarios finales y mitigar errores humanos.

Tabla 1. Marco de trabajo aplicando controles de seguridad de la norma ISO / IEC 27001: 2022

Vulnerabilidades	**ISO / IEC 27001: 2022**		
	Control	**Atributos del control**	**Descripción**
Ataques de denegación de servicio DoS/DDoS (V1)	**A.8.32** Control del código fuente	Tipo: Técnico Propósito: Prevenir Aplicabilidad: Desarrollo	El código fuente debe estar protegido contra accesos no autorizados, modificaciones o divulgación, especialmente ante amenazas como ataques DoS que pueden explotar debilidades en versiones no controladas.
	A.8.25 Seguridad de las transacciones	Tipo: Técnico Propósito: Prevenir Aplicabilidad: Producción	Se deben proteger las transacciones en servicios y aplicaciones, asegurando integridad, confidencialidad y autenticidad frente a ataques DoS que puedan explotar el tráfico o carga.
	A.8.10 Resiliencia de servicios	Tipo: Operacional Propósito: Mitigar Aplicabilidad: General	Se deben tomar medidas para garantizar la continuidad del suministro eléctrico y de otros servicios críticos ante ataques que saturen o apaguen la infraestructura.

	A.8.20 Seguridad de la red	Tipo: Técnico Propósito: Prevenir Aplicabilidad: Comunicaciones	Las redes deben estar protegidas y segmentadas para mitigar ataques como DDoS, incluyendo monitoreo, filtrado y redundancia.
	A.8.3 Gestión de acceso	Tipo: Técnico Propósito: Prevenir Aplicabilidad: General	El acceso a redes y servicios debe estar controlado y limitado según las autorizaciones, reduciendo vectores de ataque y el impacto de DoS.
Vulnerabilidades de hardware (V2)	**7.4.** Controles de acceso físico	Tipo: Físico Propósito: Prevenir Aplicabilidad: Instalaciones	Se deben establecer controles para evitar el acceso físico no autorizado a las instalaciones que albergan información sensible.
	7.4. Controles de acceso físico	Tipo: Físico Propósito: Prevenir Aplicabilidad: Instalaciones	Medidas físicas deben proteger las oficinas e instalaciones frente a amenazas ambientales o acceso no autorizado.
	7.10. Ubicación y protección de equipos	Tipo: Físico Propósito: Prevenir Aplicabilidad: Infraestructura	Los equipos deben ubicarse estratégicamente para protegerlos contra amenazas ambientales y accesos no autorizados.
	8.3. Gestión de acceso	Tipo: Técnico Propósito: Prevenir Aplicabilidad: General	Separar entornos de desarrollo, prueba y producción ayuda a controlar los accesos y mitigar errores o modificaciones no autorizadas.
	7.9. Seguridad del cableado	Tipo: Físico Propósito: Prevenir Aplicabilidad: Infraestructura	El cableado debe protegerse frente a daños físicos, sabotajes o interferencias.
Vulnerabilidades de la ingeniería social (V3)	**8.2.** Gestión de la información de autenticación	Tipo: Técnico Propósito: Prevenir Aplicabilidad: Usuarios	Los usuarios deben seguir las políticas sobre la gestión segura de contraseñas u otros medios de autenticación.
	8.3. Gestión de acceso	Tipo: Técnico Propósito: Prevenir Aplicabilidad: General	El acceso a la información debe restringirse de acuerdo con los requisitos del negocio y la política de seguridad.
	5.2. Responsabilidades de seguridad de la información	Tipo: Organizacional Propósito: Prevenir Aplicabilidad: General	Es fundamental asignar responsabilidades claras para la seguridad de la información.
	8.11. Uso de programas utilitarios	Tipo: Técnico Propósito: Prevenir Aplicabilidad: Sistemas	El uso de herramientas que puedan afectar sistemas o datos debe estar controlado.
	8.32. Protección del código fuente	Tipo: Técnico Propósito: Prevenir Aplicabilidad: Desarrollo	El acceso al código fuente debe estar restringido y controlado.

Desafíos de la legislación (V4)	**5.1.** Políticas de seguridad de la información	Tipo: Organizacional Propósito: Gobernar Aplicabilidad: General	Debe existir una política general de seguridad de la información, aprobada y comunicada.
	5.1. Políticas de seguridad de la información	Tipo: Organizacional Propósito: Gobernar Aplicabilidad: General	Las políticas deben revisarse de forma periódica o ante cambios relevantes.
	5.17. Acuerdos de confidencialidad	Tipo: Legal Propósito: Proteger Aplicabilidad: General	Debe documentarse y revisarse el uso de acuerdos de confidencialidad con empleados y terceros.
	8.24. Uso de criptografía	Tipo: Técnico Propósito: Proteger Aplicabilidad: Comunicaciones	Las organizaciones deben definir políticas claras sobre el uso de mecanismos criptográficos.
	8.1. Política de control de acceso	Tipo: Técnico Propósito: Prevenir Aplicabilidad: General	Debe establecerse una política formal sobre el acceso a sistemas e información.
Desconocimiento del usuario (V5)	**8.7.** Protección contra malware	Tipo: Técnico Propósito: Prevenir Aplicabilidad: General	Se deben implementar controles contra malware y promover la sensibilización del usuario.
	8.1. Política de control de acceso	Tipo: Técnico Propósito: Prevenir Aplicabilidad: General	El control de acceso debe estar documentado y basado en requisitos del negocio.
	8.2. Gestión de la información de autenticación	Tipo: Técnico Propósito: Prevenir Aplicabilidad: Usuarios	Debe existir un proceso formal para asignar o revocar acceso.
	8.2. Gestión de la información de autenticación	Tipo: Técnico Propósito: Prevenir Aplicabilidad: Usuarios	Los accesos privilegiados deben estar especialmente protegidos y gestionados.
	8.2. Gestión de la información de autenticación	Tipo: Técnico Propósito: Prevenir Aplicabilidad: Usuarios	La información de autenticación debe gestionarse bajo procesos formales.

3.3. Elaboración y validación de instrumento de la propuesta del marco de trabajo

Se diseñó un instrumento de evaluación compuesto por 25 preguntas estructuradas, orientadas a valorar la aplicabilidad y pertinencia de los controles propuestos como mecanismo de mitigación frente a las vulnerabilidades identificadas en SDN. Las preguntas se formularon en correspondencia con los cinco grupos de vulnerabilidades abordadas, integrando controles de la norma ISO/IEC 27001:2022 como posibles soluciones técnicas y organizacionales (Tabla 2).

Tabla 2. Lista de preguntas para validar la propuesta del marco de trabajo.

	Preguntas
1.	¿La aplicación de controles de acceso a código fuente de programas permite mitigar la vulnerabilidad de ataques de denegación de servicio DoS/DDoS?
2.	¿La aplicación de controles de seguridad de transacciones de los servicios permite mitigar la vulnerabilidad de ataques de denegación de servicio DoS/DDoS?
3.	¿La implementación de controles de resiliencia del servicio permite mitigar la vulnerabilidad de ataques de denegación de servicio DoS/DDoS?
4.	¿La implementando políticas de controles de la seguridad de las redes permite mitigar la vulnerabilidad de ataques de denegación de servicio DoS/DDoS?
5.	¿Con la implementación de controles de gestión de acceso a redes y a servicios en la red se podría mitigar la vulnerabilidad de ataques de denegación de servicio DoS/DDoS?
6.	¿Con la aplicación de políticas de controles de acceso físico para el personal se contribuye con la mitigación de las vulnerabilidades de hardware?
7.	¿Con la implementación de controles para evitar el acceso a las oficinas al personal no autorizado contribuye con la mitigación de las vulnerabilidades de hardware?
8.	¿La implementación de controles de ubicación y protección de los equipos permite mitigar las vulnerabilidades de hardware?
9.	¿La implementación de controles de separación de entornos de desarrollo, pruebas y operación permite mitigar las vulnerabilidades de hardware?
10.	¿La implementación de controles de seguridad del cableado permite mitigar las vulnerabilidades de hardware?
11.	¿La implementación de controles de gestión de la información de autenticación permite mitigar las vulnerabilidades de la ingeniería social?
12.	¿La implementación de controles para el acceso restringido de la información permite mitigar las vulnerabilidades de la ingeniería social?
13.	¿La implementación de controles para la gestión de responsabilidades para la seguridad de la información permite mitigar las vulnerabilidades de la ingeniería social?
14.	¿La implementación de políticas de uso de programas utilitarios privilegiados permite mitigar las vulnerabilidades de la ingeniería social?
15.	¿La implementación de controles para la protección código fuente de programas permite mitigar las vulnerabilidades de la ingeniería social?
16.	¿La implementación de políticas para la seguridad de la información permite mitigar la vulnerabilidad de desafíos de la legislación?
17.	¿La implementación de controles para la revisión de las políticas de seguridad de la información permite mitigar la vulnerabilidad de desafíos de la legislación?
18.	¿La implementación de controles para la firma de acuerdos de confidencialidad con empleados y terceros permite mitigar la vulnerabilidad de desafíos de la legislación?
19.	¿La implementación de controladores criptográficos permite mitigar la vulnerabilidad de desafíos de la legislación?
20.	¿La implementación de controles de acceso deben emplearse para mitigar la vulnerabilidad de desafíos de la legislación?
21.	¿La implementación de controles contra códigos maliciosos y malware permite mitigar la vulnerabilidad de desconocimiento del usuario?
22.	¿La implementación de controles de acceso debe estar documentado para que permita mitigar la vulnerabilidad de desconocimiento del usuario?
23.	¿En la implementación de controles de acceso se debería exigir el proceso formal para asignar o revocar acceso, con la finalidad de mitigar la vulnerabilidad de desconocimiento del usuario?

24.	¿La implementación de controles de acceso como los privilegiados deben estar protegidos y gestionados para mitigar la vulnerabilidad de desconocimiento del usuario?
25.	¿La implementación de controles para gestionar el acceso debe autenticarse bajo procesos formales para mitigar la vulnerabilidad de desconocimiento del usuario?

La validación del instrumento se llevó a cabo mediante entrevistas a seis expertos en redes, telecomunicaciones y seguridad de la información. Tres de los entrevistados consideraron que las preguntas eran totalmente pertinentes para validar el marco de trabajo, ya que responden de manera adecuada con los requisitos relacionados con las vulnerabilidades de las SDN. Por su parte, dos expertos coincidieron en la pertinencia general del instrumento, aunque identificaron oportunidades de mejora en la redacción de ciertas preguntas, sugiriendo un mayor nivel de especificidad en la aplicación de los controles normativos. Adicionalmente, un experto expresó una postura crítica, indicando que el instrumento, si bien útil como referencia inicial, no sería suficiente para estandarizar de manera efectiva la gestión de la seguridad de la información. Según su criterio, la implementación de controles y políticas debe asumir un enfoque dinámico, que se ajuste continuamente a los contextos tecnológicos y operativos específicos de cada organización.

En conjunto, los resultados evidencian una aceptación mayoritaria del instrumento propuesto, al tiempo que resaltan la necesidad de considerar marcos de gestión más flexibles y adaptativos, especialmente en entornos altamente cambiantes como SDN (Figura 3).

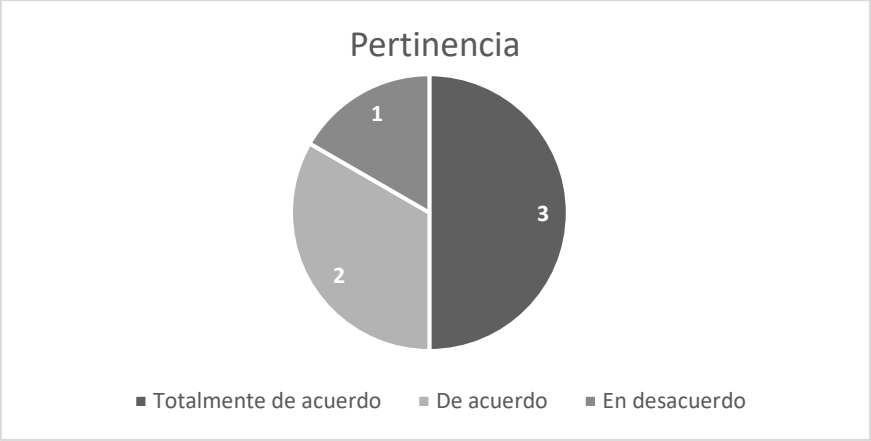

Figura 3. Evaluación de la pertinencia del instrumento.

El análisis de la aplicabilidad del instrumento, evaluado por seis expertos, muestra que el 50% (tres expertos) están totalmente de acuerdo en que las preguntas son pertinentes y están alineadas con la naturaleza de las vulnerabilidades, ofreciendo diversas opciones para mitigarlas. Además, el 33% (dos expertos) están de acuerdo en que el instrumento es eficiente y contempla mecanismos adecuados para la mitigación de vulnerabilidades.

Sin embargo, el 17% (un experto) manifestó una postura neutral (ni de acuerdo ni en desacuerdo), argumentando que las preguntas podrían no incluir suficiente flexibilidad en la validación del marco de trabajo. Este experto señaló que limitar a cinco los controles propuestos para cada vulnerabilidad podría no adaptarse a las necesidades específicas de las organizaciones, lo que sugiere que los controles deberían ser más dinámicos y ajustables según el contexto.

Estos resultados reflejan un alto nivel de aceptación del instrumento, lo cual respalda su utilización para evaluar el marco propuesto. La opinión crítica registrada no afectó significativamente la valoración global, dado que la limitación en el número de controles responde a una estrategia de estandarización y facilidad de implementación en entornos técnicos diversos. El marco puede ser evaluado mediante auditorías internas o validaciones cruzadas entre equipos técnicos. Su implementación, por otra parte, puede llevarse a cabo de forma progresiva, iniciando

con la identificación de las vulnerabilidades críticas en la infraestructura SDN, la aplicación de los controles establecidos por el marco, y su posterior ajuste conforme a las necesidades organizacionales, promoviendo así una gestión proactiva y dinámica de la seguridad de la información (Figura 4).

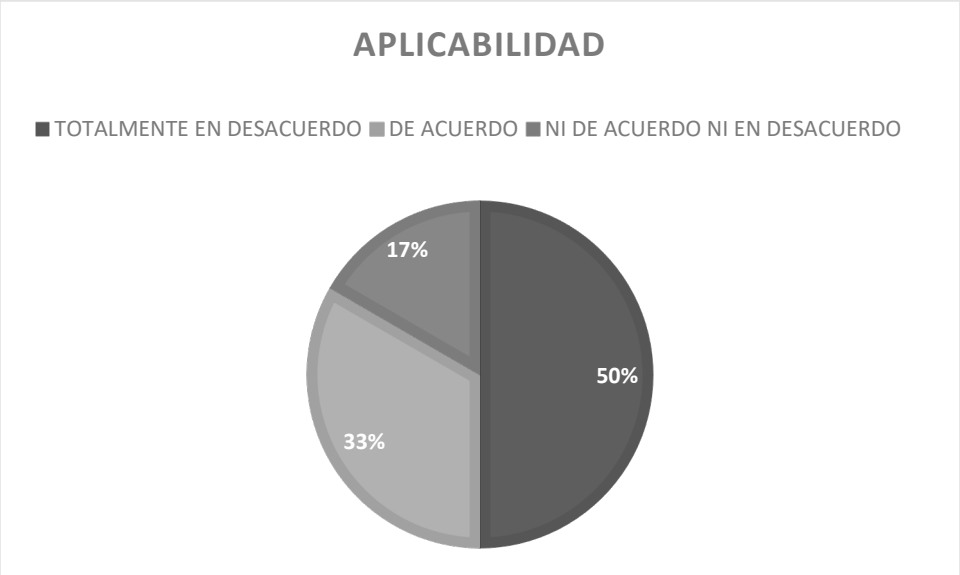

Figura 4. Evaluación de la aplicabilidad del instrumento.

3.4. Validación de la propuesta del marco de trabajo

Para la validación de la propuesta del marco de trabajo se consideraron las respuestas de los cinco expertos seleccionados, a los cuales se les asignaron los siguientes nombres: Exp.1, Exp.2, Exp.3, Exp.4 y Exp.5. Los resultados del análisis de la vulnerabilidad referida al ataque de denegación de servicio representada en la Figura 5, los expertos sostienen que mantener controles en seguridad de las redes informáticas, permite el acceso solamente a los usuarios y a los servicios de la red autorizados, da mayor seguridad para evitar el ataque de denegación de servicio. Mediante el sistema de control de redes, se garantiza la limitada gestión a las aplicaciones y servicios exclusivos asignados al usuario. Otro de los controles que los expertos consideraron oportuno, se basa en la gestión de acceso a redes, limitando exclusivamente el acceso al personal autorizado. Generalmente, entre los mecanismos utilizados para permitir accesos a usuarios a redes es el uso de contraseñas complejas para acceder a la red inalámbrica, filtrado de direcciones MAC de los clientes que acceden a la red, cambiar la configuración introducida por los fabricantes de equipos y restringir el acceso a ordenadores específicamente, ya sea por dirección IP o MAC [21].

Aunque se recopilaron respuestas de cinco expertos, en la Figura 5 solo se distinguen tres líneas. Esto ocurre porque algunos expertos coincidieron plenamente en sus respuestas: el experto 1 respondió de forma idéntica al experto 5, y lo mismo sucedió entre el experto 2 y el experto 3. Esta coincidencia hizo que sus líneas se superpusieran en la visualización, generando menos trayectorias visibles de las que realmente participaron. Esto no significa que falten datos, sino que algunos expertos expresaron su criterio de manera muy similar.

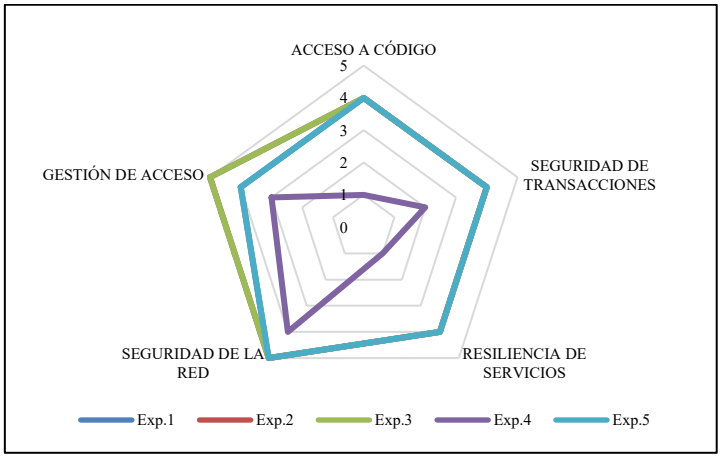

Figura 5. Validación de controles en V1.

Dentro de los factores que determinan la vulnerabilidad de hardware, fueron analizados los criterios de controles de acceso físico, ubicación y protección de los equipos, gestión de acceso en entornos de desarrollo, y la seguridad del cableado (Figura 6). La mayor cantidad de los criterios emitidos por los expertos coinciden que limitar el acceso físico al hardware y dispositivos informáticos, generan mayor seguridad y protección, lo cual no solo garantiza la protección de los equipos ante eventos ambientales, sino que también evita el acceso físico al personal no autorizado. Entre los sistemas de control de acceso a oficinas empleados, se consideran, el uso presentación de credencial o tarjeta inteligente, introducción de contraseñas o lector biométrico y reconocimiento de huella dactilar [22]. Además, los evaluadores consideran de mucha importancia mantener seguridad en las oficinas, tener buena ubicación y protección de los equipos.

El uso de dispositivos y datos ha generado incremento de ataques informáticos, logrando el control de la red y dispositivos inteligentes. Se han presentado varias alternativas para evadir la vulnerabilidad de la ingeniería social en las redes definidas por software (Figura 7). Se ha reconocido tres alternativas de mayor interés entre los expertos, el cual engloba la gestión de la información de autentificación, la gestión de acceso, y la asignación de roles y responsabilidades para la seguridad de la información.

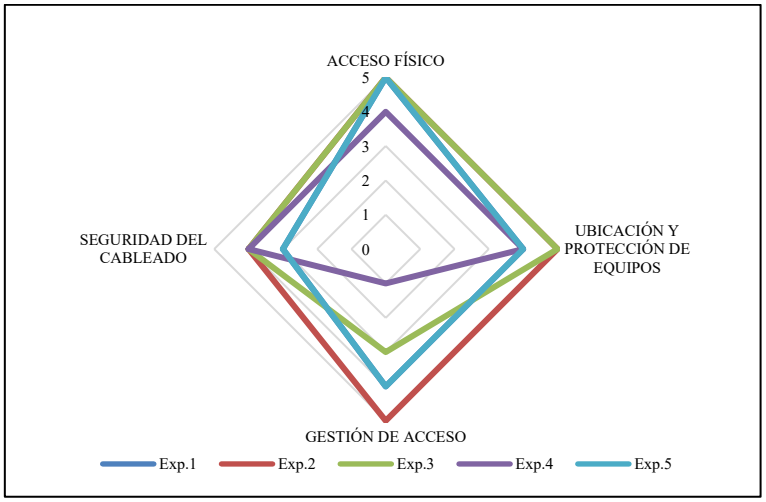

Figura 6. Validación de controles en V2.

El implementar más de un control dentro de los sistemas informáticos, podría garantizar una eficiencia en la vulnerabilidad social de las redes. Asociaciones de mecanismos como la

autenticación, en el que se implementan prácticas de no divulgar las contraseñas, evitar el registro de las contraseñas en archivos físicos y electrónicos, educar al personal con el cambio permanente de contraseñas [23]; además, de la gestión de acceso a la información, mediante el uso de menú de acceso, ocultar funciones de administración a usuarios regulares y regularizar la accesibilidad de datos en función de cada usuario de acuerdo a los roles y responsabilidades asignadas [24].

Ante la deficiencia de normas y políticas que sancionen el uso indebido de los datos, se presenta como vulnerabilidad constante los desafíos de la legislación. Sin embargo, las empresas pueden definir políticas internas de seguridad que dan a conocer al personal laboral de la empresa, lo cual, a través de ellas permite subsanar los daños causados en el uso indebido de los datos. De acuerdo al criterio de evaluadores expertos en la información de las redes (Figura 8), la revisión de las políticas de seguridad constante y planificados para asegurar su eficacia; y acuerdos de confidencialidad entre los empleados y la empresa que permita proteger la información, por esta razón es necesario que los conceptos de seguridad y confidencialidad sean implementados en normativas y contactos que fomente la confianza entre los participantes del mismo [25].

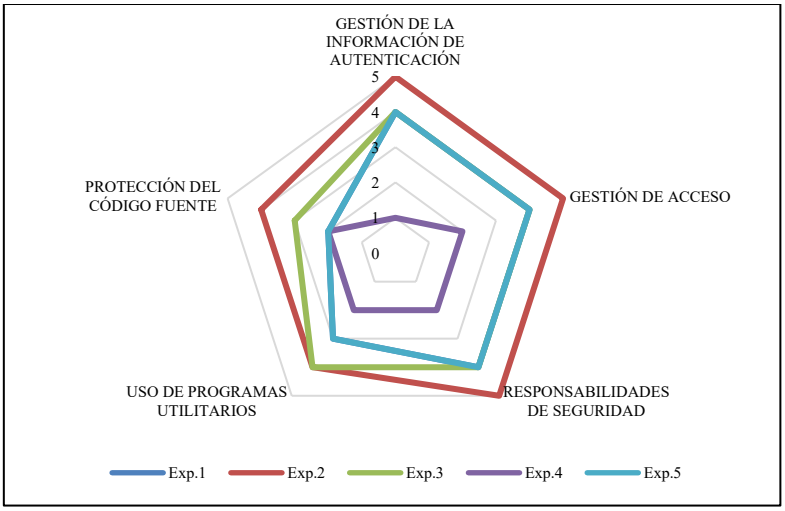

Figura 7. Validación de controles en V3.

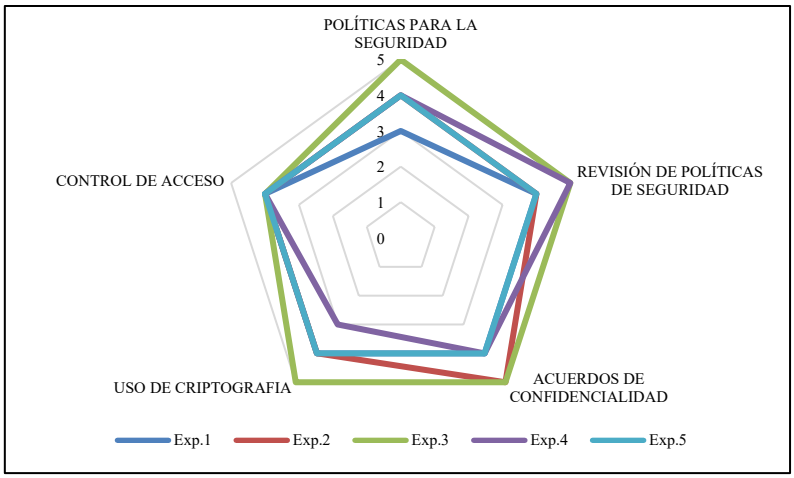

Figura 8. Validación de controles en V4.

La falta de conocimiento en temas de seguridad vuelve a los usuarios vulnerables ante ataques cibernéticos. Según aspectos relacionados a la vulnerabilidad de desconocimiento del usuario, los resultados mostrados en la Figura 9, indica que las estrategias de mayor control se basan en la

gestión de autenticación de usuarios, en el que se asignan permisos a los usuarios de acuerdo al cargo que desempeñan. Además, de implementar controles para la protección de malware, mediante la concientización de los usuarios sobre el acceso a redes detectadas como fraudulentas, ya que son los más expuestos para ser víctimas de fraudes a través de la red, entre las acciones a las pueden enfrentarse constan la suplantación de correo electrónico o uso de sus direcciones electrónicas y uso de su identidad para fines maliciosos.

La propuesta de un marco referencial basado en la norma ISO/IEC 27001:2022 para la seguridad en entornos SDN responde a la necesidad de afrontar vulnerabilidades críticas como los ataques DoS/DDoS, el desconocimiento del usuario y las fallas de hardware se alinea con investigaciones recientes que destacan la importancia de vincular directamente las amenazas con controles normativos específicos [26], [27].

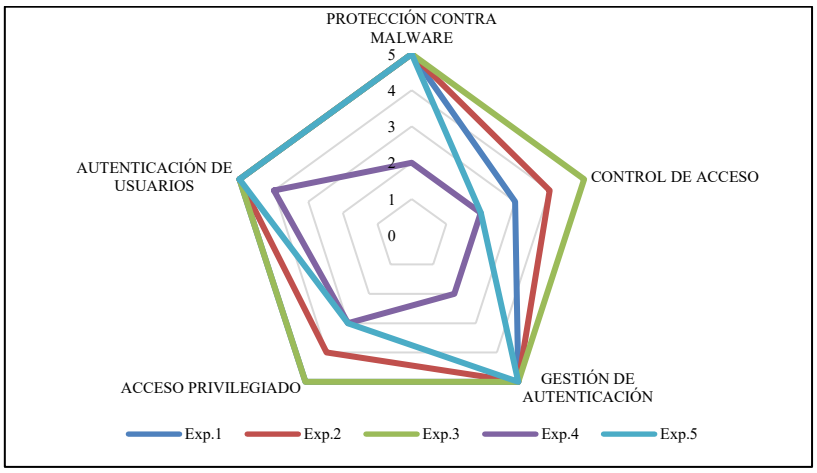

Figura 9. Validación de controles en V5.

La validez de la propuesta fue respaldada por expertos, quienes valoraron su pertinencia y aplicabilidad; sin embargo, también se señaló la importancia de mantener un enfoque flexible y dinámico ante escenarios tecnológicos cambiantes [28].

Además, el enfoque integral del modelo al incluir dimensiones técnicas, físicas, organizacionales y legales lo convierte en una herramienta replicable para instituciones que buscan fortalecer su infraestructura de seguridad, especialmente en contextos donde la ciberseguridad se ha vuelto una prioridad estratégica [25].

4. CONCLUSIONES

La metodología articuló de manera secuencial la revisión documental, la identificación y clasificación de vulnerabilidades, la construcción del marco referencial y su validación mediante juicio de expertos, esta revisión de 45 artículos científicos (2018–2022) confirmó que los ataques DoS/DDoS son la principal amenaza en entornos SDN.

El marco se distingue por vincular cada vulnerabilidad con cinco controles específicos de la norma ISO/IEC 27001:2022, seleccionados por su pertinencia y aplicabilidad, lo que otorga al modelo un carácter integral, normativo y adaptable a distintos contextos institucionales.

La validación del instrumento evidenció un alto nivel de aceptación por parte de los expertos, quienes destacaron su utilidad para valorar la efectividad de los controles propuestos, ellos también señalaron la conveniencia de incorporar enfoques más dinámicos, los resultados respaldan la viabilidad del instrumento como herramienta inicial de evaluación.

Este estudio aporta al campo de la seguridad de la información al proponer un modelo estructurado, replicable y alineado a estándares internacionales, con potencial de aplicación en organizaciones que busquen fortalecer sus capacidades de protección en entornos SDN.

Como proyección futura, se sugiere aplicar el marco en escenarios reales mediante pruebas piloto y explorar la integración de técnicas de inteligencia artificial para la detección proactiva de vulnerabilidades, así como su adaptación a arquitecturas híbridas y entornos cloud.

REFERENCIAS

[1] C. Astudillo y A. Cabrera, "Políticas de gestión de seguridad de la información, fundamentadas en la norma ISO/IEC 27001, centro de datos diseñado con el estándar ANSI/TIA 942", *Revista Dominios de la Ciencia*, vol. 5, no. 3, jul. 2019. [En línea]. Disponible en: https://doi.org/10.23857/dc.v5i3.929

[2] Valuates Reports, "Mercado de SDN por componentes, servicios, industria vertical TI y región – Global Forecast to 2027", 8 de Octubre de 2020.

[3] N. McKeown et al., "OpenFlow: enabling innovation in campus networks", *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, mar. 2008. [Online]. Available: https://doi.org/10.1145/1355734.1355746

[4] N. Gude et al., "NOX: Towards an operating system", *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 3, pp. 105–110, jul. 2008. [Online]. Available: https://doi.org/10.1145/1384609.1384625

[5] D. A. Priano, "Análisis de protocolos de enrutamiento en Redes definidas por software (Software Defined Networks)", Tesis de maestría, Universidad Nacional de La Plata, Buenos Aires, Argentina, 2021. [En línea]. Disponible en: https://sedici.unlp.edu.ar/handle/10915/122842

[6] CISCO, "Informe de ciberseguridad anual de Cisco 2018," 2018.

[7] F. Solarte Solarte, E. Enriquez Rosero y M. Benavides, "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001", *Revista Tecnológica - ESPOL*, vol. 28, no. 5, pp. 492-507, dic. 2015. [En línea]. Disponible en: https://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

[8] CISCO, "Tendencias globales en redes 2020", 2019.

[9] J. Voutssas, "Preservación documental digital y seguridad informática", *IB*, vol. 24, no. 50, 127–155, nov. 2010. [En línea]. Disponible en: https://doi.org/10.22201/iibi.0187358xp.2010.50.21416

[10] ICONTEC, NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 9001 Requisitos NTC-ISO-IEC 9001, 2020.

[11] E. Gómez-Luna, D. Fernando-Navas, G. Aponte-Mayor y L. A. Betancourt-Buitrago, "Metodología para la revisión bibliográfica y la gestión de información en temas científicos, a través de su estructuración y sistematización", Dyna, vol. 81, no. 184, pp. 158-163, abr. 2014. [En línea]. Disponible en: https://www.redalyc.org/articulo.oa?id=49630405022

[12] I. Makhdoom, M. Abolhasan, J. Lipman y R. Liu, "Anatomía de las amenazas al Internet de las cosas", *IEEE Communications Surveys & Tutorials,* vol. 21, no. 2, pp. 1636–1675, oct. 2018. [Online]. Available: https://doi.org/10.1109/COMST.2018.2874978

[13] H. Maziku, S. Shetty, y D. Nicol, "Security risk assessment for SDN-enabled smart grids", *Computer Communications*, vol. 133, jan. 2019. [Online]. Available: https://doi.org/10.1016/j.comcom.2018.10.007

[14] W. Chen, S. Xiao, L. Liu, and X. Jian, "A DDoS attacks traceback scheme for SDN-based smart city", *Computers and Electrical Engineering*, vol. 81, jan. 2020. [Online]. Available: https://doi.org/10.1016/j.compeleceng.2019.106503

[15] T. Wang, H. Chen, G. Cheng, and Y. Lu, "SDN Manager: A Safeguard Architecture for SDN DoS Attacks Based on Bandwidth Prediction", *Security and Communication Networks*, jan. 2018. [Online]. Available: https://doi.org/10.1155/2018/7545079

[16] Y. Guo, F. Miao, L. Zhang, and Y. Wang, "CATH: An effective method for detecting denial-of-service attacks in software defined networks", *Science China Information Sciences,* vol. 62, no. 3, 2019. [Online]. Available: https://doi.org/10.1007/s11432-017-9439-7

[17] S. Zonouz, J. Rrushi y S. McLaughlin, "Detección de malware de control industrial mediante análisis de código de PLC automatizado", *IEEE Security & Privacy,* vol. 12, no. 6, pp. 40–47, dic. 2014. [Online]. Available: https://doi.org/10.1109/MSP.2014.113

[18] J. Deogirikar, and A. Vidhate, "Security attacks in IoT: A survey", en 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 32–37. [Online]. Available: https://doi.org/10.1109/I-SMAC.2017.8058363

[19] P. Voigt y A. Von dem Bussche, *El reglamento general de protección de datos de la UE (GDPR), "Una guía práctica",* Cham: Springer International Publishing, 2017. [En línea]. Disponible en: https://doi.org/10.1007/978-3-319-57959-7

[20] AT&T, "The CEO's Guide to Data Security," 2016. [Online]. Available: https://www.business.att.com/cybersecurity/docs/vol5-datasec

[21] P. Zanu Sotenga, K. Djouan, and A. Matthew, "A virtual network model for gateway media access control virtualisation in Large Scale", *Internet of Things,* vol. 21, apr. 2023. [Online]. Available: https://doi.org/10.1016/j.iot.2022.100668

[22] I. Singh, and B. Singh, "Access management of IoT devices using access control mechanism and decentralized authentication: A review", *Measurement: Sensors*, vol. 25, 2023. [Online]. Available: https://doi.org/10.1016/j.measen.2022.100591

[23] H. Cui, Z. Wan, H. Qi, B. Qin, and X. Yi, "Password-authenticated proofs of retrievability for multiple devices checking cloud data", *Journal of Information Security and Applications*, vol. 75, june. 2023. [Online]. Available: https://doi.org/10.1016/j.jisa.2023.103480

[24] Y. Luo et al., "Platform perspective verse user perspective: The role of expression perspective in privacy disclosure", *Journal of Retailing and Consumer Services*, vol. 73, jul. 2023. [Online]. Available: https://doi.org/10.1016/j.jretconser.2023.103372

[25] R. Fillmore, D. McKinley, and E. F. Tallman, "Chapter 6 - Managing privacy, confidentiality, and risk: towards trust", in Health Information Exchange (Second Edition), pp. 131-147, 2023. [Online]. Available: https://doi.org/10.1016/B978-0-323-90802-3.00030-7

[26] D. Ganji, C. Kalloniatis, H. Mouratidis, and S. M. Gheytassi, "Approaches to Develop and Implement ISO/IEC 27001 Standard: A Systematic Literature Review,", *International Journal On Advances in Software*, vol. 12, no. 3, pp. 228–238, dec. 2019. [Online]. Available: https://personales.upv.es/thinkmind/dl/journals/soft/soft_v12_n34_2019/soft_v12_n34_2019_4.pdf

[27] International Organization for Standardization, ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements, ISO, Geneva, Switzerland, 2022.

[28] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", *The TQM Journal*, vol. 33, no. 7, pp. 76–105, dic. 2021. [Online]. Available: https://doi.org/10.1108/TQM-09-2020-0202