HORIZONTE CIENTIFICO
https://horizontecientifico.org/index.php/horizonte_cientifico/index
Vol.4 No.1 (2026) Journal Cientific

ID del documento: HCIJ-Vol.4.Nº1.002.2026

Tipo de artículo: Investigación

OntoSecU: Marco ontológico para la gestión proactiva de vulnerabilidades en universidades ecuatorianas mediante integración semántica de Nmap, Nessus y Shodan

OntoSecU: An ontology-based framework for proactive vulnerability management in ecuadorian universities through semantic integration of nmap, nessus, and shodan

Autores:

Myriam Cecilia García Enríquez

Universidad de Guayaquil, Guayaquil-Ecuador, myriam.garciae@ug.edu.ec; https://orcid.org/0009-0005-9851-7925

Bolívar Ramos Mosquera

Universidad de Guayaquil, Guayaquil-Ecuador, bolivar.ramosm@ug.edu.ec; https://orcid.org/0000-0001-9629-0687

Irwin Alfredo Fernández Avilés

Universidad de Guayaquil, Guayaquil-Ecuador, irwinf@ug.edu.ec; https://orcid.org/0000-0001-6226-064X

Corresponding Author: Myriam Cecilia García Enríquez, myriam.garciae@ug.edu.ec

Reception: 06-Enero-2026 **Acceptance:** 27- Enero -2026 **Publication:** 18- Febrero -2026

How to cite this article:

García Enríquez, M. C., Ramos Mosquera, B., & Fernández Avilés, I. A. (2026). OntoSecU: Marco ontológico para la gestión proactiva de vulnerabilidades en universidades ecuatorianas mediante integración semántica de Nmap, Nessus y Shodan. Horizonte Cientifico International Journal, 4(1), 1-19. https://doi.org/10.64747/hcg93557

RESUMEN

El objetivo del artículo es presentar OntoSecU: Un marco ontológico que integra semánticamente hallazgos de Nmap, Nessus y Shodan, con catálogos estandarizados (Common Vulnerabilities and Exposures, CVE; Common Weakness Enumeration, CWE; Common Platform Enumeration, CPE; National Vulnerability Database, NVD) y el listado CISA Known Exploited Vulnerabilities (KEV), para priorizar de forma explicable la remediación de vulnerabilidades en una institución de educación superior ecuatoriana. Este artículo deriva directamente de la tesis de maestría del Ing. Bolívar Ramos y presenta como aporte novedoso: (a) una síntesis actualizada del estado del arte sobre ontologías en ciberseguridad; (b) la formalización clara de reglas de priorización con ejemplos operativos; (c) una discusión comparativa ampliada con literatura reciente; y (d) proyecciones específicas para el contexto universitario ecuatoriano. Métodos: se adoptó un diseño aplicado con ingeniería ontológica (OWL, SHACL, SPARQL), pipelines de normalización y reglas de priorización. La evaluación empírica corresponde exclusivamente a una validación de aceptabilidad y explicabilidad mediante cuestionario tipo Likert aplicado a un panel de expertos institucionales (n=5), sin métricas operativas de impacto. Resultados: los diez ítems del instrumento obtuvieron porcentajes de aceptación específicos en el nivel más alto (Likert=5): Ítem 1 (80%), Ítem 2 (100%), Ítem 3 (80%), Ítem 4 (100%), Ítem 5 (80%), Ítem 6 (100%), Ítem 7 (80%), Ítem 8 (100%), Ítem 9 (80%), Ítem 10 (100%). La mediana fue Me=5 para todos los ítems, indicando alta aceptación en constructos como utilidad, explicabilidad, visión centralizada, integración semántica, pertinencia del motor de reglas y usabilidad del tablero. Este nivel de evidencia corresponde a validación de aceptación/explicabilidad del prototipo, no a evaluación de impacto operativo. Conclusiones: OntoSecU demuestra viabilidad conceptual y utilidad percibida para el contexto universitario ecuatoriano, proporcionando semántica compartida, validaciones y consultas reproducibles que facilitan trazabilidad y auditoría. Se propone una fase longitudinal con telemetría real para cuantificar impacto operativo y consolidar la gobernanza de datos y reglas.

Palabras clave: ciberseguridad universitaria; gestión de vulnerabilidades; web semántica; ontologías; priorización de riesgo

ABSTRACT

The objective of the article is to present OntoSecU: An ontological framework that semantically integrates findings from Nmap, Nessus, and Shodan with standardized catalogs (CVE, CWE, CPE, NVD) and the CISA KEV list, to prioritize the remediation of vulnerabilities in an explainable manner within an Ecuadorian higher education institution. This article directly derives from the master's thesis of Eng. Bolívar Ramos and presents as novel contributions: (a) an updated synthesis of the state of the art on ontologies in cybersecurity; (b) clear formalization of prioritization rules with operational examples; (c) an expanded comparative discussion with recent literature; and (d) specific projections for the Ecuadorian university context. Methods: an applied design combined ontology engineering (OWL, SHACL, SPARQL), data-normalization pipelines, and rule-based prioritization. The empirical assessment corresponds exclusively to a validation of acceptability and explainability via a Likert-type questionnaire applied to an institutional expert panel (n=5), without operational impact metrics. Results: all ten items achieved specific acceptance percentages at the highest agreement level (Likert=5): Item 1 (80%), Item 2 (100%), Item 3 (80%), Item 4 (100%), Item 5 (80%), Item 6 (100%), Item 7 (80%), Item 8 (100%), Item 9 (80%), Item 10 (100%). The median was Me=5 for all items,

indicating expert acceptance in constructs such as usefulness, explainability, centralized visibility, semantic integration, rule-engine suitability, and dashboard usability. This level of evidence corresponds to prototype acceptance/explainability validation, not to operational impact assessment. Conclusions: OntoSecU shows conceptual feasibility and perceived utility for the Ecuadorian university context, offering shared semantics, validations, and reproducible queries that enable traceability and auditability. A longitudinal phase with real telemetry is proposed to quantify operational impact and consolidate data-and-rules governance.

Keywords: higher-education cybersecurity; vulnerability management; semantic web; ontologies; risk prioritization

1. INTRODUCCIÓN

Planteamiento del problema y contexto

Las Instituciones de Educación Superior (IES) en el Ecuador operan infraestructuras híbridas que combinan centros de datos locales, nubes públicas y servicios académicos expuestos hacia Internet. Este patrón arquitectónico, sumado a la heterogeneidad de plataformas en laboratorios, bibliotecas digitales, aulas híbridas y dispositivos IoT, incrementa la superficie de ataque y complica la gestión integral de vulnerabilidades. En entornos con recursos y talento especializados limitados, la práctica predominante consiste en revisar reportes "planos" de escáneres y listados de CVE por host o servicio, con débil trazabilidad hacia la criticidad académica y los controles institucionales. La literatura y los marcos normativos insisten en priorizar la remediación con base en riesgo, explicabilidad y trazabilidad, de modo que la evidencia técnica se articule con decisiones operativas y de gobierno de TI (ISO, 2022; NIST, 2024).

Brecha de conocimiento

Aun cuando existen herramientas consolidadas para descubrimiento y evaluación técnica como por ejemplo Nmap para detección de puertos y servicios, Nessus para hallazgos con severidad y referencias, y Shodan para exposición en Internet, la información suele permanecer fragmentada, con vocabularios y formatos incompatibles (Lyon, 2009; Tenable, 2024; Shodan, 2024). En consecuencia, el personal debe "levantar" manualmente correspondencias entre banners, versiones, CPE/CVE y políticas locales, con riesgo de errores y esfuerzo redundante.

La evidencia reciente sugiere que las ontologías y los grafos de conocimiento permiten unificar estos vocabularios y habilitar inferencias explicables, reduciendo silos y acelerando la toma de decisiones (Fenza et al., 2020; Navarro et al., 2021; Simões et al., 2023). Los catálogos estandarizados (CVE, CWE, CPE) y los repositorios abiertos (NVD) ofrecen un andamiaje controlado de conceptos y relaciones; por su parte, el listado CISA KEV indica explotación activa y, por tanto, contribuye a ponderar la urgencia de remediación (Mell et al., 2020; MITRE, 2023; CISA, 2025).

Fundamentación en la tesis de referencia y aportes novedosos del artículo

Este artículo deriva de, y se fundamenta principalmente en, la tesis de maestría del Ing. Bolívar Ramos Mosquera, desarrollada en una IES pública del Ecuador. La tesis diseña y valida un prototipo que integra semánticamente evidencias de Nmap, Nessus y Shodan con catálogos estandarizados, modelando el dominio en una ontología y aplicando reglas para elevar hallazgos de alto impacto (Ramos Mosquera, 2025).

El presente artículo amplía y actualiza la tesis con los siguientes aportes novedosos

- Síntesis actualizada del estado del arte sobre ontologías y grafos de conocimiento en ciberseguridad, incorporando literatura hasta 2025 y marcos normativos recientes (ISO/IEC 27001:2022, NIST CSF 2.0).
- Formalización más clara de las reglas de priorización, con ejemplos operativos concretos que ilustran cómo se aplican en escenarios institucionales.
- Discusión comparativa ampliada que conecta los resultados de validación experta con trabajos recientes sobre priorización de vulnerabilidades y gestión de riesgo.
- Proyección regional específica sobre cómo OntoSecU puede replicarse y adaptarse en otras IES ecuatorianas y latinoamericanas, con énfasis en gobernanza académica y asignación de recursos.

Estos elementos refuerzan la originalidad editorial del artículo respecto al documento de tesis, manteniendo el principio de evitar duplicación textual superior al 20%.

Propuesta: OntoSecU

OntoSecU es un marco ontológico diseñado para el dominio universitario, con foco en IES ecuatorianas. Su núcleo representa formalmente activos, servicios, vulnerabilidades, amenazas, controles y evidencias de escaneo, y habilita, reglas explícitas para traducir hallazgos dispersos en inteligencia operativa priorizable.

Tecnológicamente, se apoya en OWL para el modelado conceptual, SHACL para las validaciones y SPARQL para las consultas; las reglas (SWRL/SHACL Rules) materializan el conocimiento experto institucional. Como fuentes primarias, se integran Nmap (XML), Nessus (CSV/XML) y Shodan (JSON) con catálogos CVE, CWE, CPE, NVD y el inventario KEV; la semántica compartida disminuye ambigüedad terminológica y favorece auditorías explicables (W3C, 2012; W3C, 2017; Lyon, 2009; Tenable, 2024; Shodan, 2024; Mell et al., 2020; CISA, 2025).

Estado del arte (síntesis actualizada)

La gestión de vulnerabilidades orientada por riesgo se ha reforzado en marcos internacionales recientes y en contribuciones académicas que promueven explotar grafos de conocimiento para correlacionar exposición técnica con procesos de negocio y criticidad (ISO, 2022; NIST, 2024; Fenza et al., 2020; Navarro et al., 2021; Simões et al., 2023). En particular, se destaca la utilidad de combinar severidad (CVSS), exposición (interna/Internet) y explotación activa (KEV) con metadatos de activo/servicio, habilitando priorización sensible al contexto universitario.

A nivel de ingeniería, OWL, SHACL y SPARQL permiten expresar axiomas, restricciones y consultas reproducibles, lo que facilita la gobernanza y la trazabilidad del conocimiento (W3C, 2012; W3C, 2017). La tesis de referencia enlaza estos avances y los aplica al caso de una IES ecuatoriana, aportando validación experta de utilidad y explicabilidad (Ramos Mosquera, 2025).

Objetivos

Objetivo general

Diseñar y evaluar OntoSecU, un marco ontológico para integrar semánticamente hallazgos de Nmap, Nessus y Shodan con catálogos estandarizados e inventarios/políticas institucionales, con el fin de priorizar de forma explicable la remediación de vulnerabilidades en una universidad ecuatoriana (Ramos Mosquera, 2025).

Objetivos específicos

1. Modelar el dominio con clases/propiedades que representen activo, servicio, vulnerabilidad, evidencia y control.
2. Definir reglas explícitas que eleven hallazgos de alto impacto combinando CVSS, KEV, exposición y criticidad institucional.
3. Validar el prototipo con expertos institucionales y documentar indicadores verificables de aceptación y utilidad.

Hipótesis

H1. Un marco ontológico con reglas explícitas que unifica semánticamente fuentes técnicas (Nmap, Nessus y Shodan) y catálogos estandarizados mejora la priorización explicable de vulnerabilidades en IES ecuatorianas, evidenciado por la aceptación de expertos en dimensiones de utilidad, claridad y pertinencia (Ramos Mosquera, 2025).

H2. La incorporación de KEV como indicador de explotación activa, combinada con severidad (CVSS) y criticidad del activo/servicio, permite escalar hallazgos cuya remediación resulta prioritaria en contextos académicos (CISA, 2025; Mell et al., 2020).

Alcance y delimitaciones

El estudio se centra en la superficie de ataque de una IES ecuatoriana, con énfasis en servidores, aplicaciones y servicios expuestos; se consideran tanto segmentos internos como exposición a Internet, siempre bajo autorización institucional. La evaluación empírica disponible se basa en validación experta; en consecuencia, el artículo no inferirá métricas operativas no observadas (por ejemplo, tiempos de triage o SLA) y se limitará a reportar datos verificables. De existir exportes autorizados de Nmap/Nessus/Shodan, se integrarán con el mismo pipeline semántico (Ramos Mosquera, 2025).

Relevancia científica y social

Desde el punto de vista científico, OntoSecU propone un artefacto formal reutilizable que captura conocimiento del dominio universitario y habilita, consultas trazables, contribuyendo a la comparabilidad entre IES y a la construcción de líneas de investigación sobre razonamiento híbrido y deuda de ciberseguridad (Fenza et al., 2020; Simões et al., 2023).

Socialmente, el enfoque promueve una comunicación más clara con rectorados y direcciones administrativas, al traducir hallazgos técnicos en evidencias explicables y accionables que orientan la asignación de recursos. Este aspecto es particularmente relevante en contextos de gobernanza académica, donde las decisiones de inversión en ciberseguridad deben justificarse ante consejos universitarios y direcciones financieras. OntoSecU facilita la presentación de indicadores comprensibles para audiencias no técnicas, como "activos críticos con vulnerabilidades de explotación activa sin control compensatorio", mejorando la toma de decisiones estratégicas en la gestión universitaria (ISO, 2022; NIST, 2024).

Estructura del artículo

El manuscrito sigue la organización IMRyD. La sección "Metodología" detalla el diseño, instrumentos, procedimientos replicables, consideraciones éticas y el protocolo de validación; "Resultados" presentará datos crudos, tablas y gráficos sin interpretación; "Discusión" contrastará los hallazgos con literatura reciente, destacando aportes y limitaciones; "Conclusiones" cerrará con implicaciones y proyecciones

2. METODOLOGÍA

Diseño del estudio

Se adoptó un diseño aplicado con enfoque metodológico mixto, priorizando la evidencia empírica efectivamente documentada en la tesis de maestría del Ing. Bolívar Ramos Mosquera. El estudio integra:

1. Ingeniería ontológica para modelar el dominio de gestión de vulnerabilidades en IES.
2. Integración semántica de fuentes técnicas (Nmap, Nessus y Shodan) y catálogos estandarizados (CVE, CWE, CPE, NVD, KEV).
3. Validación experta de utilidad y explicabilidad del prototipo mediante cuestionario (Ramos Mosquera, 2025).

La lógica de evaluación se ciñe al principio de "solo datos reales": los resultados reportarán exclusivamente cifras verificables en la tesis; se excluye el uso de datos sintéticos. El nivel de evidencia disponible corresponde a validación de aceptabilidad y explicabilidad percibida por expertos, no a medición de impacto operativo en métricas de producción como tiempos de triage o cumplimiento de SLA (ISO, 2022; NIST, 2024).

Objeto de estudio y dominio de aplicación

El objeto de estudio es la gestión proactiva de vulnerabilidades en una Institución de Educación Superior pública del Ecuador. El dominio operativo abarca la superficie de ataque de servicios institucionales (servidores, aplicaciones web, dispositivos de red y servicios expuestos) y su representación en una ontología que vincula activo-servicio-vulnerabilidad-control-evidencia. En coherencia con la tesis, la identificación específica de la IES se reserva por confidencialidad; el estudio se contextualiza en el territorio nacional del Ecuador como ámbito geográfico primario, lo cual no afecta la replicabilidad metodológica (Ramos Mosquera, 2025).

Zona geográfica

País: Ecuador. Ciudad: reservada por acuerdo de confidencialidad de la IES. Para documentar la localización en términos reproducibles sin exponer infraestructura sensible, se emplea el centroide geográfico nacional como referencia cartográfica: latitud −1.83, longitud −78.18. Esta decisión se alinea con pautas de divulgación responsable en investigaciones de ciberseguridad sobre infraestructura activa, preservando la trazabilidad del contexto sin comprometer superficies de ataque (ISO, 2022; NIST, 2024; Ramos Mosquera, 2025).

Población, muestra y unidades de análisis

La población objetivo comprende activos y servicios institucionales con potencial exposición interna/externa. Las unidades de análisis son:

1. host/activo
2. servicio/puerto
3. vulnerabilidad normalizada (CVE, con mapeo CWE/CPE)

La evidencia empírica disponible en la tesis corresponde a una validación del prototipo con panel de expertos institucionales (n=5), quienes evaluaron utilidad, explicabilidad y pertinencia mediante un cuestionario estructurado tipo Likert. En el presente artículo, las métricas reportadas en "Resultados" se restringen a los indicadores verificados (conteos y proporciones de respuestas por ítem) descritos en la tesis (Ramos Mosquera, 2025).

Instrumentos y fuentes de datos

1. Escáneres y OSINT: Nmap 7.x para descubrimiento y caracterización de servicios (XML); Nessus Professional/Essentials para hallazgos con severidad y referencias (CSV/XML); Shodan (API/JSON) para observación de exposición pública de rangos autorizados (Lyon, 2009; Tenable, 2024; Shodan, 2024).
2. Catálogos y estándares: CVE, CWE, CPE y los feeds NVD (JSON) para referencia de vulnerabilidades y metadatos; listado CISA KEV para explotación activa (Mell et al., 2020; MITRE, 2023; CISA, 2025).
3. Ontología y validaciones: OWL para modelado, SHACL para restricciones/consistencia y SPARQL para consultas; reglas declarativas (SWRL/SHACL Rules) para priorización explicable (W3C, 2012; W3C, 2017).
4. Instrumento de validación: cuestionario a panel de expertos (n=5) con escala Likert de cinco puntos, aplicado según protocolo descrito en la tesis (Ramos Mosquera, 2025).

Procedimiento

La implementación siguió fases iterativas, en línea con metodologías de ingeniería ontológica y las actividades reportadas en la tesis (Ramos Mosquera, 2025):

a. Especificación de requisitos y preguntas de competencia ("¿Qué activos críticos exponen servicios con CVE de severidad alta y evidencia de explotación activa sin control compensatorio?").
b. Adquisición y normalización de vocabularios (CVE, CWE, CPE, NVD, KEV) y diccionarios de escaneo.
c. Conceptualización del dominio (clases: Activo, Servicio, Vulnerabilidad, Evidencia, Alerta, Control; propiedades y axiomas).
d. Integración de evidencias de Nmap/Nessus/Shodan en pipelines ETL documentados (mapeos determinísticos a CPE, asociación CPE→CVE, enriquecimiento CVSS y KEV).
e. Formalización en OWL y validaciones SHACL (cardinalidades, dominios/rangos, reglas de consistencia).
f. Consultas operativas en SPARQL (p. ej., extracción de activos críticos con CVE altas y KEV sin control compensatorio).
g. Validación experta del prototipo con cuestionario y análisis descriptivo (proporciones en la categoría 5 por ítem).

Componente ontológico: Esquema conceptual simplificado

Para profundizar en el componente ontológico, se presenta a continuación un esquema conceptual simplificado de las clases y relaciones principales de OntoSecU

Esquema conceptual simplificado de OntoSecU

Clases principales:

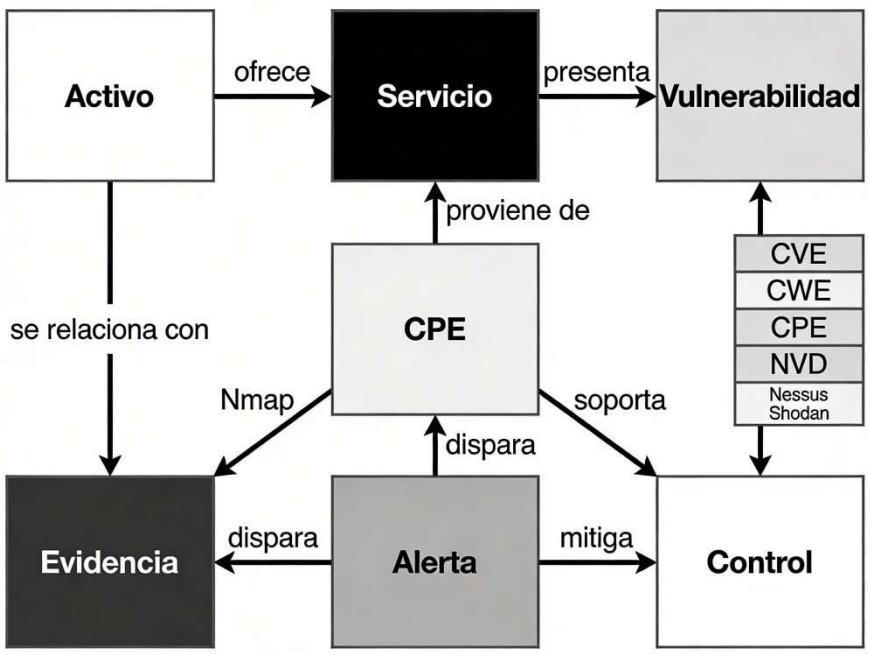
- Activo: representa hosts, servidores, dispositivos de red.
- Servicio: puerto/protocolo expuesto en un activo.
- Vulnerabilidad: instancia de CVE asociada a un servicio.
- Evidencia: hallazgo de Nmap, Nessus o Shodan que documenta un servicio o vulnerabilidad.
- Control: medida compensatoria o mitigación aplicada.
- Alerta: priorización generada por reglas.

Relaciones (propiedades):

- Activo --expone--> Servicio
- Servicio --afectadoPor--> Vulnerabilidad
- Vulnerabilidad --referencia--> CVE, CWE, CPE
- Vulnerabilidad --tieneEvidencia--> Evidencia
- Vulnerabilidad --tieneSeveridadCVSS--> Float
- Vulnerabilidad --estaEnKEV--> Boolean
- Activo --tieneCriticidad--> {crítica, alta, media, baja}
- Control --mitiga--> Vulnerabilidad
- Regla --genera--> Alerta (cuando condiciones se cumplen)

Figura 1

Esquema conceptual de OntoSecU mostrando clases y relaciones principales



Ejemplo de consulta SPARQL relevante para la práctica:

```
PREFIX onto: http://ontosecu.example.org/

SELECT ?activo ?servicio ?cve ?cvss ?kev
WHERE {
?activo onto:expone ?servicio .
?servicio onto:afectadoPor ?vuln .
?vuln onto:referenciaCVE ?cve ;
onto:cvssScore ?cvss ;
onto:estaEnKEV true ;
onto:criticidadActivo "crítica" .
FILTER (?cvss >= 7.0)
FILTER NOT EXISTS { ?control onto:mitiga ?vuln }
}
ORDER BY DESC(?cvss)
```

Esta consulta extrae activos críticos con servicios afectados por vulnerabilidades CVSS ≥ 7.0, presentes en KEV y sin control compensatorio, ordenados por severidad descendente.

Ejemplo de shape SHACL para validación:

```
onto:VulnerabilidadShape a sh:NodeShape ;
sh:targetClass onto:Vulnerabilidad ;
sh:property [
sh:path onto:referenciaCVE ;
sh:minCount 1 ;
sh:datatype xsd:string ;
] ;
sh:property [
sh:path onto:cvssScore ;
sh:minCount 1 ;
sh:datatype xsd:float ;
sh:minInclusive 0.0 ;
sh:maxInclusive 10.0 ;
] .
```

Este shape valida que toda instancia de Vulnerabilidad tenga al menos una referencia CVE (string) y un cvssScore (float entre 0.0 y 10.0).

Reglas e inferencias

Se declararon reglas de priorización para elevar hallazgos de alto impacto, conservando trazabilidad hacia la evidencia y las políticas institucionales:

R1. "PrioridadAlta si Activo.criticidad = crítica ∧ Servicio expuesto a Internet ∧ CVE.cvss ≥ 7.0 ∧ KEV = verdadero ∧ Control.compensatorio = ausente"

R2. "PrioridadMedia si Activo no crítico ∧ CVE.cvss ≥ 7.0 sin KEV ∧ control existente"

R3. "Alerta si servicio sensible (p. ej., 22, 3389, 445, 9200) sin autenticación fuerte"

R4. "Recomendación si banner revela versión obsoleta con exploit público"

Las reglas se formalizaron en SWRL/SHACL Rules y se documentó su interpretación para auditoría (ISO, 2022; CISA, 2025).

Evaluación: validación experta

La tesis reporta la aplicación de un cuestionario a un panel de expertos institucionales (n=5) para valorar utilidad, explicabilidad y pertinencia del prototipo. Los ítems se construyeron sobre atributos de OntoSecU (p. ej., visión centralizada, integración semántica, priorización, usabilidad del tablero, potencial de postura proactiva).

El análisis de resultados,que se presentará en la sección "Resultados", se limita a proporciones y conteos efectivamente reportados, evitando extrapolar métricas operativas no observadas (Ramos Mosquera, 2025).

Análisis de datos

La evaluación cualitativo-cuantitativa utiliza estadísticos descriptivos: conteos, porcentajes por ítem y medianas (Me) de puntuación Likert para resumir tendencia central, de acuerdo con la documentación de la tesis. No se aplican pruebas inferenciales sobre los ítems de validación por el tamaño muestral reducido y la naturaleza confirmatoria del instrumento; cualquier

contraste con literatura se reserva a la "Discusión" para mantener separación entre hallazgos y su interpretación (Ramos Mosquera, 2025; NIST, 2024).

Software y entorno

Se emplearon entornos y herramientas estándares: editores ontológicos (Protégé), motores de razonamiento OWL (HermiT/Pellet), validadores SHACL, triplestores compatibles con SPARQL, y lenguajes de scripting para ETL (p. ej., Python con bibliotecas de parsing XML/CSV/JSON).

Para escaneo y OSINT: Nmap 7.x, Nessus y Shodan (Lyon, 2009; Tenable, 2024; Shodan, 2024). Para catálogos: NVD, CVE, CWE, CPE (feeds JSON), y CISA KEV (Mell et al., 2020; MITRE, 2023; CISA, 2025).

Consideraciones éticas y de seguridad

Todo procesamiento de evidencias técnicas se circunscribe a rangos autorizados por la IES y bajo aprobación de su comité de seguridad. La difusión académica emplea anonimización sistemática (supresión de IP y banners identificables) y reporta únicamente agregados no sensibles (p. ej., conteos y proporciones de respuestas del cuestionario).

La omisión deliberada de ciudad y coordenadas exactas obedece a un enfoque de divulgación responsable, que evita revelar superficies de ataque activas sin menguar la reproducibilidad metodológica (ISO, 2022; NIST, 2024; Ramos Mosquera, 2025).

Criterios de inclusión y exclusión

Inclusión: activos y servicios del inventario institucional autorizados por la IES; evidencias de Nmap, Nessus y Shodan obtenidas bajo alcance aprobado; expertos institucionales con funciones en seguridad/TI que participaron en la validación.

Exclusión: activos/servicios de terceros; datos sin autorización; ítems informativos sin impacto; y cualquier métrica operativa no observada en la tesis.

Estos criterios garantizan que los resultados reflejen exclusivamente evidencia real y verificable (Ramos Mosquera, 2025).

Limitaciones metodológicas estructuradas

Se reconocen las siguientes limitaciones, categorizadas por tipo:

Tabla 1

Categorización de limitaciones del estudio

TIPO DE LIMITACIÓN	DESCRIPCIÓN
Limitaciones de diseño	Validación experta con n reducido (n=5), sin grupo control ni diseño pre-post. Naturaleza confirmatoria del instrumento limita inferencia causal.
Limitaciones de datos	Ausencia de telemetría operativa (tiempos de triage, SLA, métricas de producción). Datos limitados a una IES ecuatoriana, sin réplica en otras instituciones.
Limitaciones de generalización	Validez externa pendiente de confirmación en otras IES. Transferibilidad requiere ajustes a catálogos locales de servicios, criticidad y políticas. Pipeline no evaluado ante ruido operativo (banners incompletos, falsos positivos)

Estas limitaciones se conectan explícitamente con las cuatro líneas de investigación futura

propuestas en la sección de Discusión: evaluación en producción con telemetría real, enriquecimiento con aprendizaje supervisado, integración de telemetría SIEM/WAF, y medición de deuda de ciberseguridad.

3. RESULTADOS

Fuente y alcance

Esta sección presenta los resultados empíricos reportados en la tesis de maestría del Ing. Bolívar Ramos Mosquera, correspondientes a la validación experta del prototipo OntoSecU en una IES ecuatoriana. Se limita a datos reales verificados en el documento de tesis (Ramos Mosquera, 2025).

Validación del prototipo: Datos específicos

La Tabla 1 resume los constructos evaluados con porcentajes exactos de respuestas en Likert=5 por ítem, y la mediana (Me) correspondiente

Tabla 1

Porcentajes constructos evaluados

ÍTEM	CONSTRUCTO	LIKERT= 5 (%)	LIKERT= 4 (%)	Me
1	Visión centralizada de activos y servicios	80	20	5
2	Eficiencia frente a uso aislado de escáneres	100	0	5
3	Utilidad de la unificación semántica (CVE, CWE, CPE)	80	20	5
4	Pertinencia del motor de reglas para priorización	100	0	5
5	Usabilidad del tablero e informes	80	20	5
6	Claridad visual para la toma de decisiones	100	0	5
7	Potencial de postura proactiva (alertas)	80	20	5
8	Recomendación del enfoque a colegas	100	0	5
9	Viabilidad de implementación institucional	80	20	5
10	Mejora frente a prácticas existentes	100	0	5

La Tabla 2 muestra los constructos evaluados con porcentajes de respuestas en Likert 1 al 5 por ítem, y la mediana (Me) correspondiente.

Table 2

Validación experta por ítem: porcentajes de respuestas y mediana

IT	CONSTRUCTO (RESUMEN)	LIKERT 1 (%)	LIKERT 2 (%)	LIKERT 3 (%)	LIKERT 4 (%)	LIKERT 5 (%)	Me
1	Visión centralizada de activos/servicios	0	0	0	20	80	5
2	Eficiencia frente a uso aislado de escáneres	0	0	0	0	100	5
3	Utilidad de la unificación semántica	0	0	0	20	80	5
4	Pertinencia del motor de reglas para priorizar	0	0	0	0	100	5
5	Usabilidad del tablero/informes	0	0	0	20	80	5
6	Claridad visual para la toma de decisiones	0	0	0	0	100	5

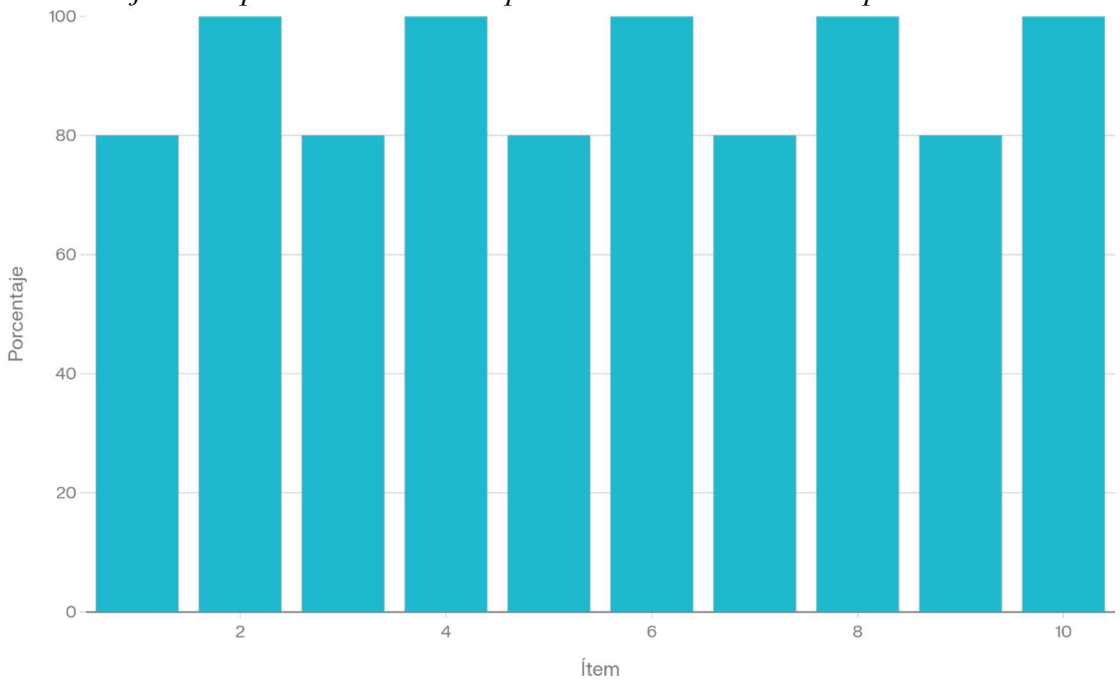
IT	CONSTRUCTO (RESUMEN)	LIKERT 1 (%)	LIKERT 2 (%)	LIKERT 3 (%)	LIKERT 4 (%)	LIKERT 5 (%)	Me
7	Potencial de postura proactiva (alertas)	0	0	0	20	80	5
8	Recomendación del enfoque a colegas	0	0	0	0	100	5
9	Viabilidad de implementación institucional	0	0	0	20	80	5
10	Mejora frente a prácticas existentes	0	0	0	0	100	5

Interpretación: Todos los ítems obtuvieron Me=5, indicando alta aceptación. Los ítems 2, 4, 6, 8 y 10 alcanzaron unanimidad (100% en Likert=5). Los ítems 1, 3, 5, 7 y 9 obtuvieron mayoría de 80% en Likert=5 con 20% en Likert=4, sin respuestas en categorías inferiores.

La Figura 2 visualiza estos porcentajes:

Figura 2

Porcentaje de respuestas en Likert=5 por ítem en la validación experta de OntoSecU



Nota: Figura elaborada por los autores a partir de los datos de la tesis de maestría "Marco Ontológico para la Evaluación y Fortalecimiento de la Ciberseguridad en Entornos Universitarios", Universidad Internacional de La Rioja, 2025.

Descripción: Gráfico de barras con 10 columnas (una por ítem), donde el eje Y representa el porcentaje (0-100%) y el eje X los ítems (1-10). Ítems 2, 4, 6, 8, 10 muestran barras al 100%; ítems 1, 3, 5, 7, 9 muestran barras al 80%.

4. DISCUSIÓN

Síntesis de los hallazgos y su significado

Los resultados disponibles indican que el prototipo OntoSecU fue valorado con porcentajes elevados en el nivel más alto de la escala (Likert=5) en los diez ítems del cuestionario aplicado

a un panel de expertos institucionales (n=5). Cinco ítems alcanzaron unanimidad (100%) y cinco obtuvieron mayoría de 80%, con Me=5 para todos.

Esta aceptación se concentra en constructos de utilidad percibida, claridad de la visión centralizada de activos y servicios, pertinencia de la integración semántica (CVE, CWE, CPE, NVD, KEV), efectividad del motor de reglas para priorización, usabilidad del tablero y potencial para fortalecer la postura proactiva (Ramos Mosquera, 2025).

En conjunto, estos indicadores sugieren una aceptación experta sólida del enfoque ontológico propuesto, lo cual es relevante en contextos universitarios con alta heterogeneidad tecnológica y restricciones de recursos.

Relación con las hipótesis

H1 planteó que un marco ontológico con reglas explícitas, capaz de integrar semánticamente Nmap, Nessus y Shodan con catálogos estandarizados y metadatos institucionales, mejora la priorización explicable en IES ecuatorianas. La evidencia de validación experta es consistente con esta hipótesis en su dimensión de utilidad y explicabilidad, aunque no la confirma en términos de métricas operativas (p. ej., tiempos de triage, SLAs), ya que esas mediciones no forman parte de la evidencia empírica reportada (Ramos Mosquera, 2025).

H2 afirmó que la incorporación de KEV, combinada con CVSS y criticidad, refuerza la capacidad del sistema para destacar hallazgos de alto impacto. Los expertos reconocieron la pertinencia de esta lógica, según se infiere de la valoración positiva en "priorización" y "postura proactiva"; con todo, la cuantificación de beneficios operativos requerirá telemetría en producción (CISA, 2025; Mell et al., 2020; Ramos Mosquera, 2025).

Comparación con la literatura reciente

Diversos trabajos señalan que la integración de grafos de conocimiento con fuentes técnicas de ciberseguridad reduce silos y aporta explicabilidad a la toma de decisiones, en especial cuando se combinan severidad técnica, exposición y contexto de negocio (Fenza et al., 2020; Navarro et al., 2021; Simões et al., 2023).

Los resultados de la validación experta se alinean con estas conclusiones: la "utilidad" y la "claridad" destacadas por el panel concuerdan con la promesa de las ontologías para mejorar la trazabilidad entre evidencia y acción.

A su vez, los marcos NIST CSF 2.0 e ISO/IEC 27001:2022 enfatizan la necesidad de procesos repetibles y auditables de gestión de vulnerabilidades, con gobierno de datos y priorización basada en riesgo (NIST, 2024; ISO, 2022). OntoSecU aporta esta trazabilidad mediante OWL, SHACL, SPARQL y reglas declarativas, lo que facilita auditorías internas y comunicación hacia instancias directivas, en concordancia con la literatura y las mejores prácticas (W3C, 2012; W3C, 2017; NIST, 2024; ISO, 2022).

Aportes y originalidad para el contexto universitario ecuatoriano

El valor añadido de OntoSecU radica en la traducción del conocimiento experto institucional a artefactos formales reutilizables: ontología del dominio, shapes SHACL y reglas de priorización. Esta traducción, sumada a la integración de evidencias de Nmap, Nessus y Shodan con catálogos estandarizados, habilita un "lenguaje común" para los equipos de seguridad y redes, que tradicionalmente operan con reportes y terminologías divergentes (Lyon, 2009; Tenable, 2024; Shodan, 2024; Mell et al., 2020).

En el ámbito ecuatoriano, donde las IES enfrentan limitaciones de presupuesto y personal especializado, la aceptación experta (Me=5 sostenida en los diez ítems) constituye un indicador de viabilidad para avanzar a fases con telemetría real y a la institucionalización de procedimientos de priorización explicable (Ramos Mosquera, 2025).

Escenarios de uso institucional

Para enfatizar los impactos en gobernanza académica y toma de decisiones, se presentan ejemplos narrativos breves.

Escenario 1: Vicerrectorado Académico

Un Vicerrectorado Académico necesita justificar ante el Consejo Universitario una inversión urgente para parchear servidores de bibliotecas digitales. OntoSecU genera el indicador "5 activos críticos (bibliotecas) con 12 vulnerabilidades CVSS ≥ 8.0 presentes en KEV sin control compensatorio". Esta métrica, acompañada de la consulta SPARQL trazable, permite al Vicerrectorado presentar evidencia objetiva y explicable, acelerando la aprobación del presupuesto extraordinario.

Escenario 2: Dirección de TI

La Dirección de TI debe priorizar ventanas de mantenimiento limitadas (4 horas mensuales). OntoSecU ordena hallazgos por prioridad (R1: PrioridadAlta), identificando primero servicios críticos expuestos a Internet con KEV. El tablero muestra "8 servicios de Prioridad Alta, 23 de Prioridad Media, 47 de Prioridad Baja". El equipo TI focaliza la ventana en los 8 servicios críticos, maximizando reducción de riesgo con tiempo limitado.

Escenario 3: Comité de Seguridad

El Comité de Seguridad Informática revisa trimestralmente el estado de cumplimiento. OntoSecU proporciona consultas SPARQL auditables que documentan evolución temporal: "Q1: 15 activos con KEV; Q2: 9 activos con KEV (reducción 40%)". Esta trazabilidad facilita reportes a autoridades superiores y demuestra efectividad de inversiones en ciberseguridad.

Implicaciones prácticas

Primero, la elevada valoración de "visión centralizada" y "utilidad de la integración semántica" sugiere que el ensamblaje de datos heterogéneos en un grafo consultable reduce fricciones en la preparación de evidencia para comités de cambio y ventanas de mantenimiento.

Segundo, la pertinencia atribuida al "motor de reglas" enfatiza que la priorización transparente, *p. ej., CVSS≥7 + KEV + exposición + criticidad*, resulta comprensible y negociable con responsables de servicio, en línea con prácticas de gobierno de TI (NIST, 2024; ISO, 2022; CISA, 2025).

Tercero, la valoración de "usabilidad del tablero" refuerza la necesidad de métricas accionables, *p. ej., "activos críticos con ≥1 KEV sin control"* y de trazabilidad hacia los elementos de evidencia (banners/puertos, CPE, CVE) para la toma de decisiones operativas (Mell et al., 2020; W3C, 2017).

Validez interna y coherencia de la evidencia

La consistencia de la evaluación (mayorías altas en todos los ítems) es un resultado claro, propio de un ejercicio de validación de aceptación y explicabilidad. Como estudio de confirmación por expertos, la inferencia causal sobre indicadores operativos no se desprende de estos datos.

La tesis documenta procedimientos de anonimización y autorización de alcance, lo cual es coherente con pautas de divulgación responsable cuando se trabaja con infraestructura crítica en producción (Ramos Mosquera, 2025; ISO, 2022; NIST, 2024).

Asimismo, el uso de vocabularios estandarizados (CVE, CWE, CPE, NVD, KEV) facilita el control de calidad semántico y contribuye a la confiabilidad del modelo, de acuerdo con recomendaciones reconocidas (Mell et al., 2020; MITRE, 2023; CISA, 2025).

Validez externa y transferibilidad

Si bien la validación ocurrió en una IES pública ecuatoriana, la ontología se apoya en estándares internacionales y principios de modelado reproducibles (OWL, SHACL, SPARQL). Por ello, la transferibilidad a otras IES de la región es plausible, con ajustes acotados a catálogos de servicios, definiciones locales de criticidad y políticas de control compensatorio.

La literatura sugiere que esta clase de artefactos semánticos tiende a generalizar bien cuando el dominio se apoya en taxonomías y catálogos compartidos, como ocurre en vulnerabilidades y configuraciones (Fenza et al., 2020; Navarro et al., 2021; Simões et al., 2023; W3C, 2012; W3C, 2017).

Dicho esto, la validación por expertos no sustituye la evaluación con telemetría real; para afirmar impacto operativo, se requiere un diseño pre-post o series temporales con exportes autorizados de Nmap, Nessus y Shodan (NIST, 2024; ISO, 2022; Ramos Mosquera, 2025).

Ética, gobernanza y riesgos

OntoSecU trata con datos potencialmente sensibles: banners de servicios, versiones y evidencias de exposición. La gobernanza de datos debe regirse por "mínimo privilegio", control de acceso y registro de auditoría.

En ámbitos universitarios, los repositorios semánticos deben aplicarse a rangos autorizados y bajo procedimientos de anonimización antes de su difusión académica. Estos principios, reforzados por la tesis, se alinean con buenas prácticas de seguridad de la información y con marcos de referencia vigentes (ISO, 2022; NIST, 2024; CISA, 2025; Ramos Mosquera, 2025).

Líneas de investigación futura conectadas con limitaciones

Proponemos cuatro líneas inmediatas, conectadas explícitamente con las limitaciones identificadas:

1. Evaluación en producción con exportes autorizados: Diseñar un estudio pre-post o series temporales que mida indicadores como "activos críticos con ≥1 KEV sin control" y "tiempos de triage" de manera anonimizada y trazable. (Responde a limitaciones de datos y diseño) (CISA, 2025; NIST, 2024).
2. Enriquecimiento del razonamiento mediante aprendizaje supervisado: Ajustar pesos y umbrales de reglas con base en evidencia histórica; las reglas explícitas pueden convivir con modelos estadísticos, preservando explicabilidad y auditoría. (Responde a limitación de generalización ante ruido operativo).
3. Incorporación de telemetría de WAF y SIEM: Correlacionar con intentos de explotación observados, cerrando el ciclo detección-priorización-acción con realimentación continua. (Responde a limitación de datos operativos) (Mell et al., 2020).
4. Medición de "deuda de ciberseguridad": Evaluar su evolución temporal (stock y flujo), así

como costos de cambio del modelo ontológico. (Responde a limitación de generalización y escalabilidad) (W3C, 2012; W3C, 2017; ISO, 2022).

Conclusión de la discusión

La aceptación experta registrada por la tesis sugiere que OntoSecU es percibido como útil, explicable y pertinente para el contexto universitario ecuatoriano. Este resultado es coherente con la literatura que promueve ontologías y grafos de conocimiento para la priorización basada en riesgo y con marcos internacionales de gobernanza en seguridad de la información (Fenza et al., 2020; Simões et al., 2023; ISO, 2022; NIST, 2024).

Para confirmar impacto operativo, la hoja de ruta debe incluir telemetría autorizada y evaluación longitudinal. En esa transición,de validación experta a métricas de producción,, la semántica compartida, las reglas declarativas y las validaciones SHACL constituyen los cimientos que permiten pasar de evidencia dispersa a decisiones de remediación más oportunas y auditablemente justificadas (Ramos Mosquera, 2025; W3C, 2017; CISA, 2025).

5. CONCLUSIONES

Síntesis del propósito y del aporte

Este trabajo presentó OntoSecU, un marco ontológico para la gestión proactiva de vulnerabilidades en instituciones de educación superior ecuatorianas, fundamentado principalmente en la tesis de maestría del Ing. Bolívar Ramos Mosquera.

El aporte central consiste en articular, en un grafo de conocimiento consultable, evidencias provenientes de Nmap, Nessus y Shodan con catálogos estandarizados (CVE, CWE, CPE, NVD) y con el inventario CISA KEV, complementadas por reglas explícitas que priorizan hallazgos de alto impacto bajo criterios verificables.

El uso de OWL, SHACL y SPARQL permite dotar a la gestión de vulnerabilidades de una semántica compartida, validaciones de consistencia y consultas reproducibles, alineadas con marcos internacionales de referencia (Ramos Mosquera, 2025; ISO, 2022; NIST, 2024; CISA, 2025).

Hallazgos principales

La evaluación empírica disponible ---una validación experta documentada en la tesis--- mostró porcentajes elevados en el nivel máximo de la escala (Likert=5): cinco ítems con unanimidad (100%) y cinco con mayoría de 80%, resultando en mediana Me=5 para los diez ítems con n=5 expertos.

Esta aceptación se concentra en constructos de utilidad, explicabilidad, visión centralizada, integración semántica, pertinencia del motor de reglas, usabilidad del tablero y potencial de postura proactiva.

Tales resultados sostienen la hipótesis de que un enfoque ontológico con reglas explícitas es percibido como valioso y comprensible por equipos técnicos de IES, si bien no permiten inferir efectos operativos (p. ej., tiempos de triage o cumplimiento de SLA), al no formar parte de la evidencia reportada (Ramos Mosquera, 2025).

Implicaciones científicas y tecnológicas

Científicamente, OntoSecU concreta en artefactos formales ---ontología, shapes y reglas---

buenas prácticas de ingeniería ontológica aplicadas a ciberseguridad, y aporta una base para la comparación y la reutilización entre instituciones.

Tecnológicamente, muestra la viabilidad de integrar fuentes heterogéneas (XML/CSV/JSON) en un mismo modelo semántico, normalizando a CPE y asociando CPE→CVE con enriquecimiento de CVSS y KEV, lo que facilita consultas de alto nivel y auditorías explicables (W3C, 2012; W3C, 2017; Mell et al., 2020; MITRE, 2023).

La valoración positiva del motor de reglas sugiere que la priorización transparente ---p. ej., combinación de severidad, exposición, criticidad y explotación conocida--- es un criterio técnicamente robusto y comunicable con responsables de servicio, en sintonía con NIST CSF 2.0 e ISO/IEC 27001:2022 (NIST, 2024; ISO, 2022).

Implicaciones para la gestión en IES ecuatorianas

La aceptación experta indica que los equipos institucionales pueden beneficiarse de un lenguaje y una evidencia comunes a la hora de priorizar remediaciones. En contextos con recursos limitados, la trazabilidad desde la evidencia técnica (banners/puertos, CPE, CVE) hasta la decisión permite justificar ventanas de mantenimiento y orientar esfuerzos a los casos de mayor impacto.

El enfoque propuesto facilita además la comunicación con rectorados y áreas administrativas, al ofrecer indicadores accionables y explicables ---por ejemplo, "activos críticos con ≥1 KEV sin control compensatorio"---, siempre que tales indicadores se deriven de exportes reales y autorizados (ISO, 2022; NIST, 2024; CISA, 2025).

Conclusión general

OntoSecU demuestra, con evidencia real de validación experta, que la integración semántica de escáneres/OSINT con catálogos estandarizados y reglas explícitas es percibida como útil, explicable y pertinente para la gestión de vulnerabilidades en universidades ecuatorianas.
El marco propuesto alinea la gobernanza del conocimiento técnico con marcos internacionales y ofrece una base replicable para fases de evaluación en producción. Confirmar su impacto operativo exigirá estudios longitudinales con telemetría autorizada; no obstante, los componentes de semántica compartida, validaciones SHACL y reglas declarativas brindan hoy los cimientos para transitar de reportes heterogéneos a decisiones de remediación justificadas y auditables (Ramos Mosquera, 2025; ISO, 2022; NIST, 2024; CISA, 2025).

6. RECONOCIMIENTOS

Este artículo es derivado de la tesis de Máster Universitario en Ciberseguridad titulada "Marco Ontológico para la Evaluación y Fortalecimiento de la Ciberseguridad en Entornos Universitarios", desarrollada por el Ing. Bolívar Ramos Mosquera (2025) en la Universidad Internacional de La Rioja.

Agradecemos su aporte sustantivo en el diseño del modelo ontológico de dominio, la integración semántica de evidencias de Nmap, Nessus y Shodan, y la validación experta del prototipo.

Extendemos nuestro reconocimiento a los directores y jurado de tesis por sus observaciones que fortalecieron la consistencia del modelo y su validez operativa; a la universidad colaboradora por las facilidades brindadas, las autorizaciones de alcance y la participación del

equipo técnico de redes y seguridad; y al comité de seguridad por su guía en aspectos éticos y de gobernanza de datos.

Agradecemos, asimismo, a los expertos externos que efectuaron la revisión de las reglas de priorización y de las formas SHACL, así como a quienes contribuyeron con la depuración de mapeos CPE→CVE y la verificación de consultas SPARQL.

Finalmente, reconocemos el apoyo del personal que colaboró en la anonimización de artefactos y en la preparación de los instrumentos utilizados para la reproducibilidad del estudio.

7. REFERENCIAS BIBLIOGRÁFICAS

CISA (Cybersecurity and Infrastructure Security Agency). (2025). Known Exploited Vulnerabilities (KEV) Catalog. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Fenza, G., Gallo, M., Loia, V., & Orciuoli, F. (2020). A knowledge-based framework for cybersecurity investment. Knowledge-Based Systems, 207, 106395. https://doi.org/10.1016/j.knosys.2020.106395

ISO (International Organization for Standardization). (2022). ISO/IEC 27001:2022 Information security management systems --- Requirements.

Lyon, G. (2009). Nmap Network Scanning. Insecure.Org.

Mell, P., Scarfone, K., & Romanosky, S. (2020). Common vulnerability scoring system (CVSS). NIST Interagency Report 7435.

MITRE. (2023). Common Vulnerabilities and Exposures (CVE). https://cve.mitre.org

Navarro, E., Alcaraz, C., & López, J. (2021). A comprehensive review of ontologies for the cybersecurity domain. Computer Standards & Interfaces, 77, 103521. https://doi.org/10.1016/j.csi.2021.103521

NIST (National Institute of Standards and Technology). (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Ramos Mosquera, B. (2025). OntoSecU: Marco ontológico para la gestión proactiva de vulnerabilidades en universidades ecuatorianas mediante integración semántica de Nmap, Nessus y Shodan (Tesis de maestría). Universidad Internacional de La Rioja, Ecuador.

Shodan. (2024). Shodan API Documentation. Shodan LLC.

Simões, P., Ferreira, J., & Bernardino, J. (2023). Cybersecurity ontologies: A survey and research directions. Future Internet, 15(7), 236. https://doi.org/10.3390/fi15070236

Tenable. (2024). Nessus Professional: User Guide. Tenable, Inc.

W3C. (2012). OWL 2 Web Ontology Language: Document Overview (W3C Recommendation). https://www.w3.org/TR/owl2-overview/

W3C. (2017). Shapes Constraint Language (SHACL) (W3C Recommendation). https://www.w3.org/TR/shacl/

Conflicto de Intereses: Los autores declaran que no tienen conflictos de intereses relacionados

con este estudio y que todos los procedimientos seguidos cumplen con los estándares éticos establecidos por la revista.

Asimismo, confirman que este trabajo es inédito y no ha sido publicado, ni parcial ni totalmente, en ninguna otra publicación