QUID Nº27, pp. 13-21, julio-diciembre de 2016, ISSN: 1692-343X, Medellín-Colombia

MODELADO DE UNA ONTOLOGÍA PARA EL EXAMEN DE CERTIFICACIÓN COMPTIA SECURITY+

MODELING AN ONTOLOGY FOR COMPTIA SECURTY+ CERTIFICATION EXAM

(Recibido el 12-02-2016. Aprobado el 13-05-2016)

Esp. Juan Felipe Muñoz Fernández
Universidad Nacional de Colombia, sede Medellín
Grupo de Investigación SINTELWEB.
Carrera 80 No. 65-223. Medellín, Colombia
jfmunozf@unal.edu.co

PhD. Jaime Guzmán Luna
Universidad Nacional de Colombia, sede Medellín
Grupo de Investigación SINTELWEB.
Carrera 80 No. 65-223. Medellín, Colombia
jaguzman@unal.edu.co

Mg. Ingrid Durley Torres
Universidad Nacional de Colombia, sede Medellín
Grupo de Investigación SINTELWEB.
Carrera 80 No. 65-223. Medellín, Colombia
ingrid.torres@unal.edu.co

Resumen: En el dominio de las tecnologías de la información, los exámenes de certificación se han generalizado como un mecanismo de validación de conocimientos y experiencia en dominios de conocimiento específicos. CompTIA es una organización reconocida por la ANSI, creada para responder a la demanda de certificaciones de las tecnologías de la información. El examen de certificación CompTIA Security+ es reconocido internacionalmente en la validación de competencias relacionadas con la seguridad informática. La ausencia de ontologías para el marcado semántico de objetos de aprendizaje en el dominio de este examen de certificación, en el marco de la Web semántica, constituye la principal motivación para el desarrollo de esta propuesta. En este artículo se elabora una propuesta de ontología para el dominio de Network Security de este examen de certificación, alcanzando el modelado formal en Protégé del subdominio de los Firewalls.

Palabras clave: CompTIA, objetos de aprendizaje, ontologías, Security+, Web semántica.

Abstract: In the domain of information technologies, certification exams are widespread as a mechanism for validation of expertise in specific domains of knowledge. CompTIA is an organization recognized by the ANSI, created to respond to the demand for certification of information technology. The CompTIA Security + certification is internationally recognized validation of skills related to computer security. The absence of ontologies for semantic markup of learning objects in the domain of this certification exam in the context of the Semantic Web, is the main motivation for the development of this proposal. This article presents a proposal to the domain ontology of this Network Security certification exam is developed, reaching the formal modeling Protégé subdomain of Firewalls.

Keywords: CompTIA, learning objects, ontology, Security+, semantic Web**.**

1. INTRODUCCIÓN

Ha sido posible a través de la web semántica construir tecnologías que incluyan a los computadores, no sólo como recursos aprovechables por las personas para la interacción con los datos en la web, sino también para volverlos parte activa de esta interacción. En este contexto, un computador se convierte en un actor capaz de analizar los datos en la web (Yu, 2007). Esta capacidad de análisis de las máquinas viene de poder definir sin ambigüedad el contexto de los datos, y en este aspecto las ontologías han jugado un papel relevante en todo el desarrollo de lo que ha sido la web semántica (Boyce & Pahl, 2007).

Una definición ampliamente aceptada de ontología ha sido la de Grubber (Yun, Xu, Wei, & Xiong, 2009) que define las ontologías como "una especificación explícita y formal de una conceptualización compartida". Esta especificación explícita define términos con significados unívocos, es decir, sin ambigüedad. El hecho de que sea formal se refiere a que dicha especificación debe ser compresible por las máquinas (Gomez-Pérez, Fernández-López, & Corcho, 2006). Por conceptualización se refiere al modelo conceptual que las personas o un grupo de las mismas tengan sobre el mundo o dominio de conocimiento (Gomez-Pérez et al., 2006). Finalmente, una especificación compartida quiere decir que dicha especificación corresponde a un entendimiento común aceptado, consensuado entre la comunidad de dicho dominio (Gomez-Pérez et al., 2006).

En este entorno de la web semántica, las plataformas de e-learning son una aproximación para facilitar la enseñanza y el aprendizaje con base en Internet y el uso de tecnologías (El-Ghalayini, 2011). En este sentido, las ontologías son consideradas como un medio altamente confiable para el soporte de sistemas educacionales basados en tecnología (Boyce & Pahl, 2007). Así, las ontologías, como modelo formal en la web semántica, buscan facilitar la automatización de tareas que actualmente son desempeñadas por humanos, a través de la estructuración de recursos en la web (I. D. Torres, Luna, & Builes, 2013), de tal manera que agentes de software obtengan la información con un significado completo para que esta pueda emparejarse con las necesidades específicas del usuario (Boyce & Pahl, 2007).

Algunos de estos recursos estructurados que pueden ser comprendidos por las máquinas y recuperados automáticamente en los entornos de e-learning, según las necesidades y capacidades de aprendizaje, lo constituyen los objetos de aprendizaje (OA).

Este artículo presenta una propuesta de ontología para representar el conocimiento del dominio del examen de certificación CompTIA Security+. Este examen de certificación valida las competencias de los profesionales en el dominio de la seguridad informática y es aceptado como un primer paso en certificaciones de seguridad informática de más alto nivel (Gibson, 2014).

Es claro que las ontologías no son el único mecanismo de representación del conocimiento de un dominio particular. Sin embargo, la ausencia de ontologías para representar este dominio de conocimiento en el contexto de la web semántica y los OA constituyen las principales motivaciones para esta propuesta. Existen ontologías que se aproximan a varios de los conceptos que el dominio de este examen requiere. Sin embargo, tienen alcances que están por fuera de representar conocimiento para los OA. Al final se propone una ontología formal modelada en Protégé que representa el conocimiento del subdominio de los Firewalls en el dominio de Network Security del examen de certificación CompTIA Security+.

El resto de este artículo está organizado de la siguiente manera: la segunda sección explora los conceptos y las relaciones entre los OA, la web semántica y las ontologías; la tercera sección sintetiza los trabajos relacionados en el modelado de ontologías en el dominio de la seguridad informática y los alcances pretendidos por estos; la cuarta sección presenta un detalle más amplio del examen de certificación CompTIA Security+; la quinta sección describe cómo fue construida la propuesta de ontología en este dominio de conocimiento; la última parte de este artículo describe las conclusiones y trabajo futuro.

2. LOS OBJETOS DE APRENDIZAJE LA WEB SEMÁNTICA Y LAS ONTOLOGÍAS

Es difícil definir precisamente lo que es un objeto de aprendizaje (OA). Los autores dedicados a la investigación en este dominio hacen aproximaciones convergentes en cuanto a la definición de un OA en algunos aspectos, pero divergentes en otros. I. Torres & Guzman-Luna, 2007 señalan esta dificultad en cuanto a una definición concertada de los OA. De este

(Committee & others, 2002; Del Moral & Cernea, 2010; I. Torres & Guzman-Luna, 2007; I.-D. Torres & Guzmán-Luna, 2015) se han tomado elementos para definir un OA como aquel recurso digital de información que tiene un objetivo educativo, de aprendizaje o de entrenamiento.

Autodescrito a través de metadatos que permiten estructurarlo y catalogarlo en repositorios particulares de OA. A través de estos últimos, los OA pueden recuperarse a través de las consultas en la web. El intercambiarlo y la reutilización de los OA son dos características deseables en los entornos de e-learning, en tanto los OA deben adecuarse a los estándares de la web semántica para permitir su accesibilidad e interoperabilidad entre diferentes plataformas de e-learning (Del Moral & Cernea, 2010). Estas plataformas de e-learning precisan de ontologías que representen adecuadamente el dominio de conocimiento, el modelo del usuario o aprendiz, el modelo del instructor y el modelo de enseñanza (Del Moral & Cernea, 2010; El-Ghalayini, 2011; Yun et al., 2009).

La web semántica es el escenario de interacción adecuado entre los OA, las ontologías y las plataformas de e-Learning, en tanto permite que los recursos digitales disponibles como OA puedan adaptarse a peculiaridades específicas del aprendiz (Del Moral & Cernea, 2010). Esta necesidad particular del aprendiz, hace que i) sea necesaria la separación explícita del conocimiento y el contenido (Boyce & Pahl, 2007) y ii) se usen agentes de software en la recuperación automática de contenidos, adaptados de acuerdo al nivel de conocimiento del aprendiz (Boyce & Pahl, 2007; Del Moral & Cernea, 2010). Aquí las ontologías juegan un papel fundamental ya que a través de ellas i) se representa formalmente y de manera consensuada el conocimiento de un dominio de interés particular (El-Ghalayini, 2011; I. D. Torres et al., 2013; Yun et al., 2009) y ii) estas representaciones son compartidas y reutilizadas (Yun et al., 2009). Este aspecto colaborativo involucra no sólo a las personas, sino también a las máquinas, de tal manera que los documentos en la web puedan ser procesados, transformados y ensamblados por estas (Yu, 2007). Una aproximación al vínculo entre máquinas e información, en la recuperación de contenidos específicos en los entornos de e-learning, lo constituyen los servicios web. Estos pueden verse como agentes de software pedagógicos que buscan, localizan, seleccionan e integran diferentes materiales educativos, almacenados en diferentes servidores (Del Moral & Cernea, 2010). Para que estas actividades puedan llevarse a cabo de manera precisa, se requiere del marcado semántico de los OA. Así, estos agentes pedagógicos usan dicho marcado semántico para rastrear los recursos digitales asociados y devolver al usuario los contenidos relevantes (Del Moral & Cernea, 2010). El éxito de estas operaciones en entornos de e-learning dependerá entonces de i) el soporte ontológico para el marcado semántico usado como API (Application Program Interface) para la ejecución automática de los servicios Web (Del Moral & Cernea, 2010)y ii) el desarrollo de ontologías en dominios específicos de conocimiento (El-Ghalayini, 2011).

3. TRABAJOS RELACIONADOS

La siguiente tabla resume los trabajos que incluyen el modelado de ontologías en el dominio de la seguridad informática. Aunque estos trabajos no están específicamente relacionados con los OA y los entornos de e-Learning, nos parece importante destacarlos debido a que algunos elementos de estas propuestas ontológicas podrían servir de referencia para el modelado de dominios como los de esta propuesta.

Tabla 1. Trabajos relacionados con el modelado de ontologías en el dominio de la seguridad informática

Autores	Descripción de la propuesta ontológica
(Li & Tian, 2010)	Un Sistema Multi-Agente en donde los agentes de software se encargan de procesar la información de diferentes sensores encargados de recolectar información relativa al estado de seguridad de un sistema y la información relativa a un ataque de seguridad informática. Los agentes procesan dicha información para convertirla en una ontología y así establecer un sistema de alerta basado en técnicas de correlación para mejorar los Sistemas de Detección de Intrusos.
(Geneiatakis & Lambrinoudakis, 2007)	Una ontología para formalizar y describir ampliamente las vulnerabilidades conocidas en el protocolo SIP, usado en los servicios de telefonía IP, con propósitos de pruebas en entornos reales o para detección de intrusos.

(Razzaq, Anwar, Ahmad, & Latif, 2014)	Proponen una ontología para un prototipo de un sistema de detección de ataques y de estimación de impacto de dichos ataques en aplicaciones Web, específicamente relacionados con el protocolo HTTP. Los autores hacen una revisión de ontologías relacionadas en el dominio de la detección de intrusos y de ataques a sistemas informáticos, comparando las características más importantes de dichas propuestas.
(Blanco, Lasheras, Fernández-Medina, Valencia-García, & Toval, 2011)	Realizan una revisión sistemática de las ontologías propuestas en el dominio de la seguridad informática. Seleccionan las ontologías más maduras en el dominio para hacer una síntesis de las características y aportes de cada una en este dominio. Sin embargo, en esta revisión no se encuentran ontologías propuestas en el dominio de este examen de certificación.
(Feledi, Fenz, & Lechner, 2013)	Es una propuesta general de ontología para compartir e intercambiar conocimientos relacionados al dominio de la seguridad de la información. El enfoque principal es la construcción compartida usando una versión modificada de Web Protégé, de una ontología en los dominios de: amenazas, vulnerabilidades e ISO 27001.
(Yao et al., 2014)	Proponen un método para la construcción de una arquitectura que permita construir ontologías en el dominio de la seguridad de la información, resaltando la complejidad de dicha información y la necesidad de representar esta creciente información en este dominio para los análisis de seguridad y la evaluación de riesgos.

4. EL EXAMEN COMPTIA SECURITY+

CompTIA (http://www.comptia.org/) se define como una entidad sin ánimo de lucro, reconocida como entidad certificadora de tecnologías de la información (TI) por la ANSI (American National Standars Institute por sus siglas en inglés). Define diferentes dominios de certificación en la industria de las TI, independiente de los fabricantes; es decir, los exámenes de certificación están orientados al conocimiento en general sobre los conceptos de un dominio de conocimiento específico en lugar de enfatizar sobre las implementaciones particulares de dichos dominios del conocimiento que un fabricante específico haya decidido evidenciar a través de sus productos.

El examen CompTIA Security+ salió por primera vez en 2002 y los objetivos del examen se han modificado en 2008, 2012 y en abril de 2014. El examen CompTIA Security+ tiene las siguientes características (CompTIA, 2013):

- Número de preguntas: 90
- Tiempo disponible: 90 minutos, alrededor de 1 minuto por pregunta.
- Puntaje mínimo para pasar el examen: 750 puntos en una escala de 100 a 900. CompTIA no especifica si las preguntas se ponderan con diferentes pesos o no.
- Tipo de preguntas: Selección múltiple (única respuesta o múltiples respuestas), preguntas basadas en desempeño, es decir, preguntas que miden la capacidad del aspirante para resolver problemas en entornos simulados.
- Prerrequisitos: Ninguno, pero se recomienda certificación CompTIA Network+.
- El examen debe presentarse en un sitio Pearson Vue autorizado (http://www.pearsonvue.com).

Este examen de certificación está estructurado en diferentes dominios de conocimiento. A saber, los dominios de conocimiento y sus respectivos porcentajes de importancia dentro de la prueba son los siguientes (CompTIA, 2013):

1) Network Security (20%)
2) Compliance and Operational Security (18%)
3) Threats and vulnerabilities (20%)
4) Applicattion, data and host security (15%)
5) Access control and Identify management (15%)
6) Cryptography (12%)

Nuestra propuesta de ontología en el dominio de este examen de certificación, está asumiendo el lenguaje inglés para la representación del conocimiento. Es importante destacar que este examen de certificación es tomado como un paso inicial en certificaciones de seguridad informática de más alto nivel (Gibson, 2014).

5. MOTIVACIÓN

La sección anterior indicó como algunos de los trabajos relacionados están orientados al modelado de ontologías en el dominio de la seguridad de la información, la seguridad de sistemas de información, la detección y el análisis de ataques a sistemas informáticos, aplicaciones web, entre otros. Sin embargo, estas revisiones y las que estos mismos trabajos indican, dan cuenta de la falta de ontologías en el dominio del examen de certificación CompTIA Security+.

La Tabla 2 indica las expresiones de búsqueda usadas y los resultados obtenidos.

Tabla 2. Expresiones de búsqueda usadas en cada herramienta bibliográfica y el número de resultados obtenidos

Expresión de búsqueda	Herramienta Bibliográfica	Resultados
TITLE-ABS-KEY(("Ontology") AND ("for Network Security" OR " for Information Security" OR "for CompTIA")) AND PUBYEAR > 2000	Scopus	31
Tema: ("Ontology for Network Security") OR Tema: ("Ontology for Information Security") OR Tema: ("Ontology for CompTIA") Período de tiempo: 2000-2015. Idioma de búsqueda=Auto	Web Of Science	1
TITLE-ABS-KEY(("Ontology Comptia")	Scopus	0
Tema: ("Ontology Comptia")	Web Of Science	0

Es importante resaltar además que la sola necesidad de ontologías en los entornos de e-learning basados en OA, como facilitadores del aprendizaje, orientados a realzar el rol del aprendiz como artífice de la construcción de su propio conocimiento (Del Moral & Cernea, 2010), constituye una motivación en el desarrollo de esta propuesta.

Otra motivación para nuestra propuesta es precisamente la orientación por dominios de conocimiento de este examen de certificación, lo cual lo hace idóneo para sistemas de e-learning que componen automáticamente rutas de aprendizaje a partir de OA (I.-D. Torres & Guzmán-Luna, 2015). Así, modelar cada dominio de esta prueba podría servir en el marcado semántico de OA que tengan que ver con intenciones educativas en alguno de dichos dominios para componer una ruta de aprendizaje completa del examen CompTIA Security+.

6. CONSTRUCCIÓN DE LA ONTOLOGÍA

Es claro que existen diferentes propuestas metodológicas que se han dado a través del tiempo para la composición de ontologías. Hüsemann & Vossen, 2005; Siricharoen, 2015, por ejemplo, se hacen propuestas metodológicas para la construcción de ontologías. Cada propuesta hace sus mejores aproximaciones, unas con más formalismos que otras, algunas con más etapas que otras, Yao et al., 2014; elaboran una propuesta que está orientada a la construcción de ontologías en un dominio particular de conocimiento. Lo que aparece claro en el escenario de metodologías para la construcción de ontologías es que no hay una sola y correcta metodología para construir ontologías (Noy & McGuinness, 2001).

Esta propuesta consideró la propuesta metodológica que hacen a manera de guía las autoras de Ontology Development 101 (Noy & McGuinness, 2001), debido a que esta propuesta está enfocada en la etapa de construcción de la ontología como tal y no hace énfasis en etapas que quedan por fuera del modelado de la ontología. Sin embargo, en la práctica hemos tomado elementos de la experiencia práctica descrita en la metodología On-To-Knowledge (Sure, Staab, & Studer, 2004).

6.1 Software utilizado

Esta propuesta hizo uso de los siguientes elementos de software para la construcción de la ontología.

CmapTools (http://cmap.ihmc.us/): Software utilizado para modelar la ontología semi-informal.

Protégé 3.4.8 (http://protege.stanford.edu/): Software utilizado en la implementación de la ontología formal, usando Pellet como razonador y Jess como motor de inferencia de la reglas SWRL.

6.2 Metodología

Noy & McGuinness, 2001, elaboran una guía para la construcción de ontologías. Hemos seguido el siguiente listado de pasos para la propuesta ontológica de este artículo.

1) **Determinar el dominio y el alcance de la ontología.**

Nuestra propuesta tiene por dominio el examen de certificación CompTIA Security+ y el alcance está delimitado al subdominio de Firewalls dentro del dominio de Network Security de dicho examen. Noy & McGuinness, 2001, sugieren definir en este paso aspectos como: i) ¿para qué será usada la ontología?, ii) ¿qué tipo de preguntas de competencia deberá responder la ontología? y iii) ¿quién hará mantenimiento a la ontología? Hemos señalado en secciones anteriores la respuesta a la primera pregunta, las preguntas restantes se exponen más adelante en esta misma sección.

2) **Considerar reutilizar ontologías existentes.**

En la sección 3 de este artículo se expuso la revisión de la literatura asociada a ontologías en dominios similares y sus alcances.

3) **Enumerar términos importantes en la ontología.**

Para este paso hemos tomado como referencia el libro CompTIA Security get certified get ahead SYO-401 study guide (Gibson, 2014), el cual es una guía para estudiar y pasar este examen de certificación. Tomamos el concepto de Firewall al interior del capítulo 3, para enumerar manualmente, los términos más importantes asociados a este concepto. En este sentido, hemos seguido una aproximación Top-Down en el diseño de la ontología, partiendo de los conceptos más generales hasta los conceptos específicos.

4) Definir las clases y la jerarquía de clases.
5) Definir las propiedades de las clases.
6) Definir las restricciones de las clases y propiedades, el dominio y el rango de las propiedades.
7) Crear instancias.

Los pasos 4 y 5 se han desarrollado conjuntamente en la construcción de la ontología semi-informal. Con la ontología semi-informal completamente modelada, se procedió a su implementación en Protégé. En esta etapa del proceso se definieron las restricciones de las clases y se crearon las instancias (pasos 6 y 7). Es importante resaltar en este punto, que a pesar de que la ontología semi-informal sirve como punto de partida, al momento de su implementación formal, esta sufrió correcciones en algunos aspectos como algunas relaciones de jerarquía entre sus clases, los nombres de las clases y propiedades que dieran cuenta de la semántica en el dominio de interés.

6. 3 Preguntas de competencia

Las siguientes preguntas de competencia se han elaborado para que sean respondidas por la ontología.

1. ¿Cómo se compone una regla genérica de un Firewall?
2. ¿Cómo está compuesta la regla por defecto de un Firewall?
3. ¿Qué tipo de firewalls existen?
4. ¿Qué capacidades tiene un firewall?

6.4 Consultas SPARQL y resultados

Se definieron las siguientes consultas SPARQL (SPARQL Protocol and RDF Query Language) para responder a las preguntas de competencia.

La Tabla 3 describe la consulta SPARQL usada para responder a la pregunta de competencia No. 1. Por su parte, la Fig. 1, ilustra los resultados de esta consulta.

Tabla 3. Consulta SPARQL para responder la pregunta de competencia No. 1.

```
SELECT ?property
WHERE {?fr a ont:FilterRule .
      ?fr ?property ?value
FILTER (!regex(str(?property),'(rdf)','I') )}
```

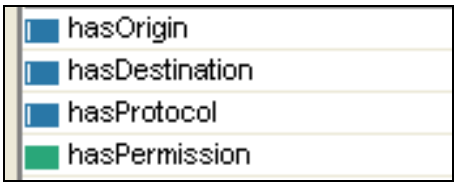

Fig. 1. Resultados obtenidos con la consulta SPARQL No. 1.

Estos resultados están indicando que una regla de un Firewall tiene una dirección IP fuente (hasOrigin), una dirección IP destino (hasDestination) un protocolo (hasProtocol) y un permiso (hasPermission,) que indica si se aceptar o se deniega el tráfico de red (Gibson, 2014).

La Tabla 4 describe la consulta SPARQL usada para responder esta pregunta de competencia No. 2.

Tabla 4.Consulta SPARQL para responder la pregunta de competencia No 2.

```
SELECT ?rule ?origin ?destination ?protocol ?permission
WHERE { ?rule rdf:type ont:FilterRule .
      ?rule ont:hasOrigin ?origin .
      ?rule ont:hasDestination ?destination .
      ?rule ont:hasProtocol ?protocol .
      ?rule ont:hasPermission ?permission
FILTER  ( regex(str(?origin),'(Any)','i')
        && regex(str(?destination),'(Any)','i')
        && regex(str(?protocol),'(Any)','i')
        && regex(str(?permission),'(Drop)','i'))}
```

La Fig. 2 ilustra los resultados obtenidos de esta consulta.

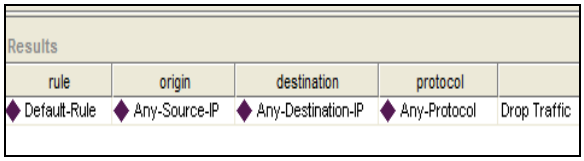

Fig. 2. Resultados obtenidos con la consulta SPARQL No. 2.

La regla por defecto de un Firewall indica que el tráfico de red de cualquier protocolo (Any-Protocol, Fig. 4), de cualquier origen (Any-Source-IP, Fig. 4) a cualquier destino (Any-Destination-IP, Fig. 4), es denegado (Drop Traffic, Fig. 4) (Gibson, 2014).

La Tabla 5 describe la consulta SPARQL usada para responder la pregunta de competencia No. 3.

Tabla 5. Consulta SPARQL para responder la pregunta de competencia No 3.

```
SELECT ?entity
WHERE { ?entity rdf:type ?type .
      ?entity rdfs:subClassOf ont:Firewall}
```

La Fig. 3 ilustra los resultados obtenidos de esta consulta.

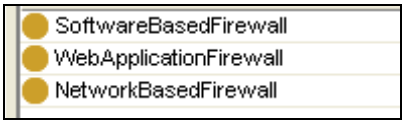

Fig.. 3. Resultados obtenidos con la consulta SPARQL No. 3.

La Fig. 3 indica que hay tres tipos de Firewalls: Firewalls de Software (SoftwareBasedFirewall), Firewalls de redes de datos (NetworkBasedFirewall) y Firewalls de aplicaciones Web (WebApplicationFirewall) (Gibson, 2014).

La Tabla 6 describe la consulta SPARQL usada para responder la pregunta de competencia No. 4.

Tabla 6. Consulta SPARQL para responder la pregunta de competencia No 4.

```
SELECT ?entity
WHERE { ?entity rdf:type ?type .
      ?entity rdfs:subClassOf ont:FirewallCapabilities}
```

La Figura 5 ilustra los resultados obtenidos de esta consulta.

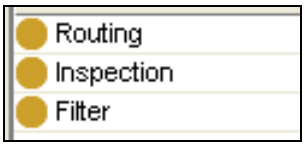

Fig. 4. Resultados obtenidos con la consulta SPARQL No. 4.

La figura 5 está indicando que los Firewalls tienen tres capacidades básicas: Enrutamiento de paquetes (Routing, Fig.7) IP, inspección de paquetes IP (Inspection, Fig. 7) y filtrado de paquetes IP (Filter, Fig. 7) (Gibson, 2014).

En las consultas realizadas a la ontología propuesta, decidimos trabajar con el lenguaje de consultas SPARQL en lugar de elaborar reglas SWRL (Semantic Web Rule Language), debido que estas últimas trabajan sobre individuos (instancias) de las clases. Para responder las preguntas de competencia 1, 3 y 4 era necesario recuperar nombres de clases y propiedades, en lugar de nombres de individuos. La pregunta 2 podría responderse con lógica de primer orden usando reglas SWRL, sin embargo, por facilidad en la lectura de los resultados, preferimos usar SPARQL.

7. CONCLUSIONES

Este trabajo demostró la ausencia de ontologías en el dominio del examen de certificación CompTIA Security+ como mecanismo para de representación del conocimiento para el marcado semántico de OA.

Se construyó una ontología formal implementada en Protégé usando una metodología que se enfoca en el modelado de la ontología más que en otros aspectos que pueden encontrarse en otras metodologías. La ontología construida cumple con las restricciones semánticas del domino y responde a las preguntas de competencia formuladas.

8. TRABAJO FUTURO

Se propone como trabajo futuro: i) expandir la ontología a todo el dominio completo de Network Security en el contexto del examen de certificación CompTIA Security+ y a los demás dominios de esta prueba, ii) validar la ontología, de ser posible con un experto en seguridad informática que se haya obtenido esta certificación CompTIA Security+ ó bien que pertenezca a CompTIA, y iii) usar la ontología en algún prototipo de sistema e-Learning para el marcado semántico de OA para la verificación de la recuperación de rutas de aprendizaje basadas en los dominios de este examen

9. REFERENCIAS

Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R., & Toval, A. (2011). Basis for an integrated security ontology according to a systematic review of existing proposals. Computer Standards & Interfaces, 33(4), 372–388. doi:10.1016/j.csi.2010.12.002

Boyce, S., & Pahl, C. (2007). Developing Domain Ontologies for Course Content The Development of Ontologies. Educational Technology & Society, 10(3), 275–288. Retrieved from www.ifets.info/journals/10_3/19.pdf

Committee, L. T. S., & others. (2002). IEEE Standard for learning object metadata. IEEE Standard, 1484(1), 2004–2007.

CompTIA. (2013). Certification Exam Objectives: SY0-401. Retrieved from http://www.comptia.jp/pdf/comptia-security-sy0-401.pdf

Del Moral, M., & Cernea, A. (2010). Diseñando Objetos de Aprendizaje como facilitadores de la construcción del conocimiento. Proceeding of II Simposio Pluridisciplinar Sobre Diseño, Evaluación Y Descripción de Contenidos Educativos Reutilizables (SPDECE05)., 12.

El-Ghalayini, H. (2011). E-Course Ontology for Developing E-Learning Courses. 2011 Developments in E-Systems Engineering, 245–249. doi:10.1109/DeSE.2011.29

Feledi, D., Fenz, S., & Lechner, L. (2013). Toward web-based information security knowledge sharing. Information Security Technical Report, 17(4), 199–209. doi:10.1016/j.istr.2013.03.004

Geneiatakis, D., & Lambrinoudakis, C. (2007). An ontology description for SIP security flaws. Computer Communications, 30(6), 1367–1374. doi:10.1016/j.comcom.2006.12.023

Gibson, D. (2014). Understanding Basic Network Security. In L. YCDA (Ed.), CompTIA Security get certified get ahead SYO-401 study guide (3rd ed.).

Gomez-Pérez, A., Fernández-López, M., & Corcho, Ó. (2006). Theoretical Foundations of Ontologies. In Springer (Ed.), Ontological engineering with examples from the areas of knowledge management, e-commerce and the Semantic Web.

Hüsemann, B., & Vossen, G. (2005). Ontology engineering from a database perspective. Advances in Computer Science – ASIAN 2005, Lecture Notes in Computer Science, Vol. 3818, 49–63. Retrieved from http://dx.doi.org/10.1007/11596370_6

Li, W., & Tian, S. (2010). An ontology-based intrusion alerts correlation system. Expert Systems with Applications, 37(10), 7138–7146. doi:10.1016/j.eswa.2010.03.068

Noy, N., & McGuinness, D. (2001). Ontology development 101: A guide to creating your first ontology. Development, 32, 1–25. doi:10.1016/j.artmed.2004.01.014

Razzaq, A., Anwar, Z., Ahmad, H. F., & Latif, K. (2014). Ontology for attack detection : An intelligent approach to web application security. Computers & Security, 45, 124–146. doi:10.1016/j.cose.2014.05.005

Siricharoen, W. V. (2015). Social Networking Ontology Engineering Walkthrough: Practical Approach for Non-Expert User Learning. Mobile Networks and Applications. doi:10.1007/s11036-014-0559-y

Sure, Y., Staab, S., & Studer, R. (2004). On-to-knowledge methodology (OTKM). In Handbook on ontologies (pp. 117–132). Springer.

Torres, I. D., Luna, J. A. G., & Builes, J. A. J. (2013). Lyrebird: A Learning Object Repository Based on a Domain Taxonomy Model. In Innovations and Advances in Computer, Information, Systems Sciences, and Engineering (pp. 949–960). Springer.

Torres, I., & Guzman-Luna, J. (2007). Estándares Semánticos para Representar Objetos de Aprendizaje.

Revista De Investigación Del Instituto Tecnológico De Orizaba, 1, 720–727.

Torres, I.-D., & Guzmán-Luna, J. (2015). Reactive Planning to Compose Learning Routes in Uncertain Environments. In New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering (pp. 101–108). Springer.

Yao, Y., Ma, X., Liu, H., Yi, J., Zhao, X., & Liu, L. (2014). A Semantic Knowledge Base Construction Method for Information Security. 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 803–808. doi:10.1109/TrustCom.2014.106

Yu, L. (2007). From Traditional Web to Semantic Web. In C. Press (Ed.), Introduction to the semantic web and semantic web services (pp. 3–15).

Yun, H., Xu, J., Wei, M., & Xiong, J. (2009).

Development of domain ontology for e-learning course. IT in Medicine & Education, 2009. ITIME '09. IEEE International Symposium on, 1, 501–506. doi:10.1109/ITIME.2009.5236370