Centro de Investigación en Métodos de Producción de Software

Informe Técnico / Technical Report

Una encuesta acerca de la Definición de Conceptos de Ciberseguridad

Lenin J. S.Gil, Beatriz F. Martins, José F. R. Román, José Ignacio Panach, and Óscar Pastor López

Ref. #:	**PROS-TR-2021-II**
Title:	**Una encuesta acerca de la Definición de Conceptos de Ciberseguridad**
Author (s):	**Lenin Javier Serrano Gil, Beatriz Franco Martins, José Fabián Reyes. Román, José Ignacio Panach, and Óscar Pastor**
Corresponding autor (s):	**lserrano@pros.upv.es, bmartins@pros.upv.es, jreyes@pros.upv.es, joigpana@uv.es, opastor@dsic.upv.es**
Document version number:	**1**
Final version:	**-**
Release date:	**-**
Keywords:	**Cybersecuridad, Ontología de Cybersecuridad, Definiciones de Cybersecuridad, ISO/IEC 27032:2012, ISO/IEC 27000:2018**

Una encuesta acerca de la Definición de Conceptos de Ciberseguridad

Lenin Javier Serrano Gil[1,2] [0000−0002−1631−7139],
Beatriz Franco Martins[1] [0000−0001−9190−1047],
José Fabian Reyes Román[1] [0000−0002−9598−1301],
José Ignacio Panach[3] [0000−0002−7043−6227], and
Oscar Pastor[1] [0000−0002−1320−8471]

[1] Valencian Research Institute for Artificial Intelligence (VRAIN),
Universitat Politècnica de València,
Camino de Vera s/n, 46022 Valencia, Spain,
{lserrano, bmartins, jreyes}@pros.upv.es,opastor@dsic.upv.es
[2] Ingeniería de Sistemas e Informática, Universidad Pontificia Bolivariana
Km 7 via Bucaramanga - Piedecuesta, Santander, Colombia
[3] Escola Tècnica Superior d'Enginyeria, Universitat de València,
Avinguda de l'Universitat, 46100 Burjassot, Valencia
joigpana@uv.es

Hoy en día brindar una gestión eficaz y eficiente de la "Ciberseguridad" es una actividad fundamental. En este contexto, la identificación de activos y la consideración de sus características de seguridad pueden reducir las amenazas del negocio. Por esta razón, las asociaciones de estándares como el *International Organization for Standardization and International Electrotechnical Commission* (ISO/IEC), la industria representada en el *Object Management Group* (OMG), entre otras, incluida la academia, desarrollan activamente enfoques/técnicas, herramientas y mecanismos para brindar soluciones eficientes. Así, es como se exploran los Grafos de Conocimiento (*Knowledge Graphs* – KG) apoyados en Inteligencia Artificial (AI) para realizar análisis de seguridad en modelos organizacionales. Sin embargo, el uso de estos artefactos añade nuevos desafíos, destacando la complejidad en la interpretación, el arbitraje, el intercambio de términos y definiciones en la especificación del modelo. Además, la gestión de grafos es una tarea de orden superior, ya que se generan a partir de diversas fuentes y de una gran cantidad de información. De acuerdo con lo anterior hemos iniciado un estudio piloto que descubre en primera instancia el estado del arte en "Ontologías de Ciberseguridad". Con el fin de proponer una base ontológica de referencia que contribuya en la generación y evite malas interpretaciones durante el desarrollo de grafos de conocimiento. En este documento, se presenta la segunda iteración del estudio con el objetivo específico de expandir nuestro enfoque en la terminología y definición de conceptos de Ciberseguridad a través de un experimento.

Keywords: Cybersecuridad, Ontología de Cybersecuridad, Definiciones de Cybersecuridad, ISO/IEC 27032:2012, ISO/IEC 27000:2018

1 Introducción

En la actualidad el uso de los grafos de conocimiento (Knowledge Graphs – KG) se ha extendido sobre varios dominios con el propósito de comprender, analizar y simu-

lar procesos de negocio [63]. Por ejemplo, tecnologías de la información, Deportes, Software, Ciberseguridad, entre otros [2]. Un KG es una instancia de grafo en la que se analiza entidades y relaciones entre los elementos de un sistema, utilizando diferentes técnicas de estudio basadas en la teoría de grafos [24]. Es importante señalar que el "conocimiento" (*Knowledge* - K) se asocia a los conceptos, la definición ontológica y la taxonomía aplicada a un dominio [15]. En el contexto de nuestro trabajo los grafos de conocimiento apoyan la creación de gemelos digitales basados en KG (Digital Twin Knowledge Graph - DTKG), los cuales son clones empleados en técnicas para análisis en profundidad de un dominio [1]. Por ejemplo, en el escenario de Ciberseguridad un DTKG puede abordar tres casos:

1. Se utiliza un DTKG para tareas de simulación y análisis, con el fin de anticipar ataques. Para ello, se hace uso de la "Teoría de Grafos" [62,49] para poder calcular la probabilidad de que un "riesgo" adopte la forma de un "ataque".
2. Se puede analizar un DTKG para determinar qué inversiones de seguridad realizar y cuáles son los controles de seguridad necesarios.
3. Los DTKG se utilizan para realizar análisis en el momento de los ataques, de tal manera que es posible obtener información sobre lo que está sucediendo para determinar el foco del ataque. Un ejemplo de esto, un DTKG puede relacionar la información de eventos capturados por los sistemas de detección de intrusos (Sistema de detección de intrusos - IDS) y revelar el vector de ataque, esto permite tomar acciones de mitigación.

En este escenario, donde los conjuntos de relaciones entre objetos son más importantes que los propios objetos, los KG son más apropiados que los bancos de datos tradicionales, y para que sea posible ejecutar las tareas de *Análisis de Datos* ("Analytics") en KG, estos no pueden ser creados de manera *ad-hoc*. Para la creación de un KG se necesita un soporte holístico que permita que los objetos y sus relaciones sean tratadas como conceptos bien definidos. Por ello, las mejores prácticas de "Modelado Conceptual" se presentan como solución a esta cuestión, especialmente cuando se habla de ontologías [20].

Las ontologías tienen un gran número de aplicaciones y el soporte conceptual de KG es uno de los más importantes, ya que los KG son instancias conceptuales de ontologías operacionales ("Operational Ontologies"). Una ontología operacional es una versión procesable de una ontología de referencia ("Reference Ontologies"), que utiliza el lenguaje más apropiado con el objetivo de garantizar propiedades computacionales deseables sin comprometer el compromiso ontológico previamente definido. Mientras, la ontología de referencia debe ser construida con el objetivo de hacer la mejor descripción posible del dominio en realidad con respecto a un cierto nivel de granularidad y punto de vista [22]. Por lo tanto, no existe ontología operacional sin la existencia de datos y sus relaciones como instancias de conceptos previamente bien definidos. Cuando los KG no están bien respaldados, los conceptos que se representan como datos, es decir, como objetos y relaciones de KG, pueden producir malas interpretaciones tanto con respecto a los análisis como para los humanos que los utilizan. En ambos casos los costos y daños son altos, existe la necesidad de utilizar las mejores prácticas en Modelado Conceptual y Análisis Ontológico. En consecuencia, conocer y analizar la terminología del dominio es esencial.

Para resolver esta cuestión, proponemos la encuesta que presentamos en este documento. Hemos organizado el resto de este documento de la siguiente manera: La sección 2 presenta la caracterización conceptual de las ontologías de Ciberseguridad. La sección 3 presenta la encuesta para el estudio piloto que sustenta este trabajo, y finalmente la sección 4 expone las conclusiones y direcciones futuras del trabajo de investigación.

2 Caracterización Conceptual de las Ontologías de Ciberseguridad

Nuestra investigación tiene un enfoque fuerte y pragmático, este trabajo está enmarcado dentro de un proyecto para desarrollar KGs (TKG y DTKG) a través de una solución integral con el apoyo financiero de Accenture LTD. Es parte de los requisitos de esta investigación que el enfoque sea adecuado para dominios complejos dentro del alcance de "Big Data" [71]. Entonces, elegir un dominio complejo como la ciberseguridad para el estudio de caso es fundamental.

Determinar cuáles son la terminología y sus definiciones en la base de conocimiento del dominio por intermedio de sus principales estándares es esencial, así como la fundamentación ontológica de esos conceptos, sus propiedades y relaciones en un modelo conceptual es el elemento clave para atender a los requisitos impuestos en el desarrollo de KGs. Por lo tanto, dentro del dominio de Ciberseguridad se detectó la necesidad de discernir un vocabulario común y consensuado para el desarrollo de KG, el cual permita facilitar el desempeño de tareas de integración, comunicación y representación dentro del dominio. La construcción de un modelo para el dominio de Ciberseguridad puede ser susceptible a diferentes problemas de interpretaciones (ambigüedad) al ser un entorno en permanente evolución (adopta nuevas tecnologías y genera un sin número de sinónimos en las organizaciones). Por ello, se desarrolló un estudio piloto [52].

El estudio piloto tenía como objetivo identificar las propuestas en el campo transversal de Ciberseguridad y Ontologías, así como también evaluar el nivel de aplicabilidad de las Ontologías de Ciberseguridad existentes para identificar posibles fuentes de datos de información de Ciberseguridad. Por lo tanto, la investigación se apoyó desde una perspectiva de Ciberseguridad utilizando los estándares ISO/IEC 27032:2012 [29] e ISO/IEC 27000:2018 [31]. Estos estándares definen un vocabulario con los términos de Ciberseguridad más utilizados. Como conclusión de este estudio, detectamos problemas relacionados con el proceso de Modelado Conceptual, especialmente en Ingeniería Ontológica. Estos problemas solo se destacaron porque tomamos nuestra investigación desde dos perspectivas diferentes: i) una sobre el dominio en sí, y ii) otra centrada en las ontologías involucradas. También como resultado del estudio piloto, verificamos que las ontologías involucradas generalmente presentan conceptos (o entidades) respaldados principalmente por todos los estándares de Ciberseguridad consagrados (más allá de ISO/IEC). La Tabla 1 muestra el número total de ocurrencias –43 términos de los 156 definidos en las normas ISO/IEC adoptadas– de terminología de Ciberseguridad. Estos resultados son los términos utilizados en este documento. Sin embargo, estaba fuera del alcance del estudio piloto garantizar y verificar si todos los términos significan la misma "Cosa" (*"Thing"* – en términos de base ontológica). En verdad, el análisis ontológico es el paso adelante que permite identificar los significados de cada "Cosa" (*"Thing"*).

Con respecto a la comunidad de Modelado Conceptual, un "análisis ontológico se puede definir como el proceso de obtener y descubrir distinciones y relaciones relevantes vinculadas a la propia naturaleza de las entidades involucradas en un determinado dominio, con el propósito práctico de términos que eliminan la ambigüedad que tienen diferentes interpretaciones en diferentes contextos" [21]. Este trabajo trata exactamente de la búsqueda de las definiciones necesarias para efectuar un análisis ontológico bien fundado dentro del dominio de Ciberseguridad.

Table 1. Total de citas de acuerdo con la terminología ISO/IEC 27000 e ISO/IEC 27032 del estudio piloto [50,52].

Término	Total de citaciones
Access Control	30
Application	208
Asset	348
Attack	942
Authentication	14
Bot	121
Availability	61
Competence	2
Confidentiality	37
Consequence	61
Control	154
Countermeasure	75
Event	333
Indicator	9

Término	Total de citaciones
Information Need	5
Information Security	40
Information System	8
Integrity	45
Internet	96
Likelihood	14
Malicious Software	3
Malware	218
Measure	117
Measurement	6
Monitoring	82
Objective	29
Organization	271
Performance	33
Phishing	3

Término	Total de citaciones
Policy	117
Process	401
Provider	75
Reliability	11
Requirement	93
Review	42
Risk	259
Risk Assessment	10
Risk Management	7
Stakeholder	50
Threat	348
Trojan	12
Trojan Horse	2
Vulnerability	775

3 Buscando definiciones de Ciberseguridad

Este estudio fue complementario de [50] y se centró en la detección del problema principal de diferentes estándares y buenas prácticas que utilizan los mismos términos con diferentes significados, enfoques o contextos.

La investigación estuvo enmarcada en el desarrollo del curso de ciclo profesional en "Seguridad Informática", que se imparte como asignatura en la línea de "Seguridad Informática y Redes de Datos" en la Facultad de Ingeniería de Sistemas e Informática de la Universidad Pontificia Bolivariana Seccional Bucaramanga (UPB) [4].

3.1 Objetivos

El objetivo de este trabajo consiste en estudiar y delimitar el uso de términos en el contexto de la Ciberseguridad con la finalidad de delinear el uso de términos en los contextos de este dominio con el fin de describir si existiera una relación, consolidación o discrepancia entre ellos, para sustentar un análisis ontológico posterior. Además, se tomó una muestra de cincuenta y dos (52) publicaciones de documentos especializados en Ciberseguridad mediante un análisis sistemático de la literatura, con respecto a los estándares presentados en la Tabla 2.

Es importante resaltar que se trabajó en productos perfeccionados por las organizaciones y autores más relevantes en el campo, como son:

[4] https://www.upb.edu.co/es/home

Table 2. Perspectiva de Ciberseguridad: Estándares ISO/IEC 27032:2012 [29] e ISO/IEC 27000:2018 [31], entre otros.

Institution	Standard
ISO and IEC	ISO/IEC 154081:2009 [28], ISO/IEC 154082:2008 [27], ISO/IEC 154083:2008 [26], ISO/IEC ISO/IEC 27002:2013 [30]
ITU-T	ITU-T-RecX805 [39], ITU-T-RecX810 [34], ITU-T-RecX811 [36] ITU-T-RecX812 [37], ITU-T-RecX813 [38], ITU-T-RecX814 [33], ITU-T-RecX815 [32], ITU-T-RecX816 [35], RecITU-T-X1205 [40], RecITU-T-X1209 [41], RecITU-T-X1212 [43], RecITU-T-X1500 [42]
CCITT & ITU-T	Data Communication Networks: Open Systems Interconnection (OSI) [8]
CCMB	CCDB-2017-05-xxx [7], CCMB-2017-04-001 [9], CCMB-2017-04-002 [10], CCMB-2017-04-003 [11], CCMB-2017-04-004 [12]
NIST	Framework for Improving Critical Infrastructure Cybersecurity (NIST-CSWP-04162018) [56], Framework for Improving Critical Infrastructure Cybersecurity (NIST-CSWP-04162014) [55], Security Self-Assessment Guide for Information Technology Systems [54], Digital Identity Guidelines [3], Digital Identity Guidelines: Enrollment and Identity Proofing [17], Digital Identity Guidelines: Authentication and Lifecycle Management [18], An Introduction to Information Security An Introduction to Information Security [60], Guide to ICS Security NIST Special Publication 800-82 [67], Risk Management Framework for Information Systems and Organizations [44], Generally accepted principles and practices for securing information technology systems [61], Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations [45], National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [59], Federation and Assertions [65]
MAEC 50	MAEC™ Specification - Core Concepts [47], MAEC™ Specification - Vocabularies [48]
OASIS Committee Specification	STIX™ Version 2.1 [6], TAXII™ Version 2.1 [70]
MITRE Corporation	CVE-1999-0001 [5], MITRE ATT & CK: Design and Philosophy [68], Ten Strategies of a World-Class Cybersecurity Operations Center [72], Science of Cyber-Security [53], Standardizing Cyber Threat Intelligence Information with the STIX™ [4] The trusted automated exchange of indicator information (TAXII™) [16]
NERC	Glossary of Terms Used in NERC Reliability Standards [58] CIPC Control Systems Security Working Group (NERC-CIPv3-v5) [57]
CCRA	Common Criteria Portal (CCv31-Release 5) [13]
Spain Government	Security Guide (CCN-STIC-401) [19]
Spanish National Cybersecurity Institute	Cybersecurity Terms Glossary [25]
Common Criteria	Standard 1300 - Cyber Security [66]

1. Organización Internacional de Normalización y Comisión Electrotécnica Internacional (ISO/IEC)
2. Unión Internacional de Telecomunicaciones (ITU-T)
3. Comité Consultivo Internacional Telegráfico y Telefónico (CCIT)
4. Instituto Nacional de Estándares y Tecnología (NIST)
5. Centro Criptológico Nacional. Gobierno de España (CCN-CERT)
6. Criterios comunes para la evaluación de la seguridad de la tecnología de la información (Common Criteria), entre otros (Tabla 2)

3.2 Instrumento

Para la realización de la encuesta se presentó un cuestionario que incluía cuatro (4) preguntas de investigación (PI) expuestas en la Figura 1[5].

1. RQ1: ¿Se emplea un mismo término con diferentes significados? ¿Cuáles?
2. RQ2: ¿Existen diferentes términos con el mismo significado? ¿Cuáles?
3. RQ3: ¿Hay conceptos y términos superpuestos? ¿Cuáles?
4. RQ4: De los términos analizados, por favor concluya en un axioma de acuerdo con su experiencia y criterio.

[5] Nota: se ha reducido las filas en la imagen para efectos de presentación

		Definición	SI	NO
1	1			
1	2			
...				
11	1			
11	2			
11	3			
11	4			
11	5			
		Preguntas	SI	NO
		¿Se utiliza el mismo término con diferentes significados?		
		¿Cuáles?		
		¿Existen diferentes términos con el mismo significado?		
		¿Cuáles?		
		¿Hay conceptos y términos superpuestos?		
		¿Cuáles?		
		De los términos citados, por favor concluya en un axioma de acuerdo con su experiencia y criterio:		
		Escriba aquí		

Fig. 1. Instrumento para la encuesta.

Fue así como los entrevistados fueron guiados en la lectura de los documentos. Los términos estuvieron fundados en ISO/IEC 27000 como se describen [50] y fueron obtenidos mediante la extracción automática de palabras clave de documentos individuales utilizando la implementación en Python de "RAKE short for Rapid Automatic Keyword Extraction algorithm" [64].

3.3 Participantes

Para la realización de la encuesta contamos con la participación de diez y ocho (18) estudiantes de Grado, que buscaron para cada término una o más definiciones en todos los estándares seleccionados para la encuesta. Seleccionamos específicamente para componer este grupo, los estudiantes asignados en "Seguridad Informática y Redes de Datos" para proporcionar a ellos la oportunidad de conocer los principales estándares involucrados en Ciberseguridad mientras recopilamos los datos necesarios para nuestra investigación.

Para la realización de esta actividad/tarea se estableció este grupo de candidatos (18 alumnos), porque es deseable que las búsquedas y análisis no estén influenciados por una gran experiencia en el contexto de la Ciberseguridad, donde los términos elegidos vengan con una definición preconcebida –con respecto al proceso cognitivo de cada uno. El propósito es que formulen sus opiniones más de acuerdo con las definiciones dadas por los documentos adoptados, sin sesgos tomados de muchos años de experiencia en el área.

El proceso cognitivo elegido en nuestra búsqueda está basado en la noción de que hay una relación entre una "cosa" (real o imaginaria) [6], su conceptualización (modelo

[6] Aquí tomamos la noción de cosa adoptada en el contexto filosófico.

mental) y su representación simbólica [23]. Figura 2 ilustra esa noción por intermedio del triángulo de Ullmann [69].

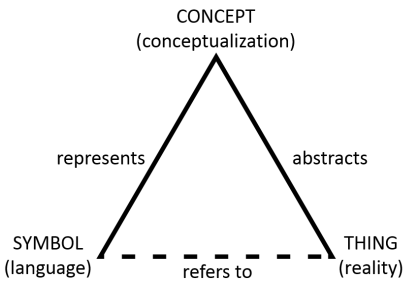

Fig. 2. Triángulo de Ullmann: las relaciones entre una cosa en la realidad, su conceptualización y una representación simbólica de esta conceptualización.

Con efecto al contexto cognitivo adoptado en la investigación, es posible impartir la encuesta a profesionales de la seguridad en lugar de los estudiantes, sin embargo eso requiere un conjunto adicional de cuestiones (RQs) además de las cuatro (4) definidas. Estas RQs adicionales deben clarificar la experiencia de cada profesional, su sesgo, y una preparación previa más detallada. O sea, es necesario contextualizar la separación entre lo que sean las definiciones adoptadas en las normas de los sesgos que cada profesional haya adoptado en su carrera profesional. Dada esta limitación, preferimos no aplicar la encuesta a profesionales. Además, creemos ser suficiente para esta investigación las informaciones obtenidas por intermedio de la encuesta apenas con estudiantes.

3.4 Ejecución de la Encuesta

Para la realización de la encuesta los participantes buscaron para cada término una o más definiciones en todos los estándares seleccionados para la encuesta. Para ello, se generó un cuestionario con una plantilla de hoja de cálculo en la que los estudiantes introdujeron sus impresiones sobre i) el significado, ii) contexto y iii) uso de cada definición dependiendo de qué fuente sea.

Es importante mencionar que los términos fueron repartidos entre los estudiantes, por lo que cada estudiante trabajó con dos términos diferentes, cubriendo un total de 36 términos individuales. Sin embargo, los estudiantes pudieron agregar terminología adicional que compone un conjunto de expresiones regulares con estos términos, que ellos han considerado importantes. Como, por ejemplo, cuando los estudiantes buscaban definiciones asociadas al término “Risk”, también consideraban las definiciones de expresiones regulares con este término, o sea, términos como “Risk Acessement” y “Risk Management”. Por lo tanto, cubrimos 43 de los términos encontrados en la búsqueda del estudio piloto del artículo. La Tabla 3 presenta los términos adicionales (expresiones regulares) añadidos por los estudiantes con soporte en los términos originales.

Table 3. Términos adicionales a los 36 términos iniciales - ISO/IEC 27000 e ISO/IEC 27032.

Término	Expressión Regular
Control	Access Control
Information	Information Need
Security	Information Security
System	Information System
Risk	Risk Assessment
Risk	Risk Management
Trojan	Trojan Horse

De acuerdo con lo anterior el procedimiento se realizó en dos sesiones de dos horas cada una. Las cuales se desarrollaron de la siguiente manera:

1. En la primera sesión se presentó mediante seminario la importancia de la ciberseguridad en el contexto del análisis de riesgos y la protección de activos en las organizaciones. De manera que se instituyeron los temas previstos del curso para la realización de la observación. Además, se dio entrega de los documentos indexados y las explicaciones necesarias para el diligenciamiento del instrumento.
2. La siguiente sesión ocurrió una semana después y se concentró en socializar y generar discusión sobre los temas que estudiaban los entrevistados, así como la respuesta a preguntas del procedimiento.
3. Dos semanas después de las sesiones se analizan los resultados de la encuesta.
4. A partir de los resultados obtenidos en la encuesta, los datos compilados fueran grabados en nuestra base de información usando la REST-API que desarrollamos en [51]. Ese proceso tomó el tiempo de un investigador por un mes.

3.5 Resultados de la Encuesta

Como resultado de la ejecución se recolectaron diez y ocho (18) formularios. La encuesta fue ordenada y procesada para mantener la coherencia y la integridad [46]. Algunos formularios no estaban completos, pero no fueron retirados porque el instrumento requería sintetizar las ideas de cada uno de los artículos antes de responder las preguntas de investigación. De esta forma se obtuvo suficiente información para deducir la relación entre el término y su cita bibliográfica. Los participantes asistieron a dos sesiones donde se contextualizó el tema, se asignaron documentos, se dio orientación sobre el instrumento y se realizó seguimiento y control.

En la consulta para RQ1, RQ2 y RQ3, se obtiene la Tabla 4 en la que se relacionan los términos derivados de la primera parte del estudio, junto con la cita bibliográfica y la frecuencia en la que se ubica cada uno. A partir de los datos hemos descubierto que la mayor variabilidad de los términos se da en RQ1 con una incidencia del 56%, seguida de un 23% para RQ2 y un 21% para RQ3. Así, el uso de un mismo término con diferentes significados presenta la mayor frecuencia en el dominio de la Ciberseguridad. Además, los términos *"Control, Reliability, Policy, Confidentiality, Event, Process, Vulnerability, Countermeasure y Risk"*. En el orden mostrado, están sobre de la media aritmética ocupando este aspecto. Del mismo modo *"Access control, Requirement y Malware"* encabezan términos que toleran diferentes términos con el mismo significado y *"Authentication, Objective, y Non-repudiation"* son términos de uso impreciso en la literatura.

Table 4. Resultados de la encuesta, definiciones de los términos, preguntas y literatura.

Term	RQ1: ¿Se usa el mismo término con diferentes significados?	RQ2: ¿Existen diferentes términos con el mismo significado?	RQ3: ¿Hay conceptos y términos superpuestos?
Access control	[19] [45]	[37] [10] [27] [37] [19] [37] [31] [8] [38] [33] [35] [60] [44] [55] [67] [57] [40] [61]	[19] [45] [67] [61] [37]
Application	[19]		[19] [44] [29]
Asset	[19] [29]		
Attack	[60] [6]	[10] [27] [7] [41] [45] [44] [3]	[25] [41] [47]
Authentication	[31] [19] [8] [36] [38] [67] [61] [25]		[9] [10] [11] [7] [14] [27] [30] [39] [34] [32] [35] [40] [43] [48] [44] [3] [18] [65] [6] [70] [66]
Availability	[19] [27] [55] [25]		
Bot	[9]		[25]
Competence	[12] [7] [31]		
Confidentiality	[10] [12] [7] [19] [31] [30] [8] [33] [32] [35] [72] [60] [44] [67] [61] [54]	[60] [44] [44] [45] [39] [34]	
Consequence	[19]		[60] [61] [54]
Control	[9] [11] [12] [7] [19] [14] [26] [27] [28] [29] [30] [8] [39] [36] [37] [38] [32] [35] [40] [41] [43] [42] [47] [72] [68] [55] [56] [60] [44] [45] [18] [65] [67] [59] [61] [53] [66] [25]	[10] [5] [31] [34] [33]	[48] [3] [17] [54] [6] [70] [57] [58]
Countermeasure	[9] [7] [28] [29] [8] [42] [72] [68] [60] [44] [45] [67]		
Event	[10] [7] [14] [27] [31] [35] [48] [72] [55] [56] [60] [44] [67] [61] [57] [58]	[19]	[31] [8] [30] [33]
Indicator	[19] [31] [43] [48] [72] [6]		
Information	[19] [31] [44] [45]		
Integrity	[60] [3] [8] [36] [37]	[19] [31]	[32]
Internet			
Likelihood	[19] [31] [60]		
Malware	[19] [29] [30] [48] [60] [44] [67]	[19] [14] [29] [68] [67] [6] [25] [72] [60] [44] [45] [48] [25]	[19] [29] [48] [72] [60] [67] [6] [25]
Measure	[11] [12] [7] [19] [31]		
Measurement	[8]		
Monitoring	[57] [61] [40] [27] [14]	[12] [7] [19] [14] [29] [31] [48]	[61] [55] [19]
Objective	[11] [12] [31] [30] [41] [72] [68]		[7] [9] [7] [19] [14] [26] [27] [28] [29] [60] [44] [45] [67] [6] [25]
Organization	[30] [55] [44] [6] [70]		
Performance	[19] [31] [58]		
Policy	[7] [19] [28] [31] [35] [72] [10] [27] [30] [37] [11] [26] [33] [32] [68] [45] [70] [57] [66]	[19] [8] [34] [45]	[26] [40] [30] [28]
Process	[12] [7] [19] [14] [31] [30] [37] [47] [48] [68] [55] [56] [3] [6]	[31] [55] [56]	
Provider	[19] [35] [60] [3] [17]		
Reliability	[11] [12] [7] [19] [14] [26] [31] [29] [30] [39] [40] [41] [42] [72] [55] [56] [60] [44] [45] [65] [67] [59] [61] [70] [57]		
Requirement		[7] [9] [11] [12] [7] [19] [5] [14] [26] [28] [31] [37] [35] [72] [68] [60] [44] [45]	
Review	[11] [31] [66]	[28] [14]	[11] [27]
Risk	[19] [14] [31] [29] [55] [56] [60] [45] [67] [59]	[19] [55] [60] [45] [59]	[19] [55] [56] [60]
Stakeholder			
Threat	[27] [9] [19] [67]	[67] [19]	[60]
Vulnerability	[9] [11] [12] [19] [26] [28] [31] [29] [42] [47] [48] [72] [60]		
Non-repudiation			[10] [7] [19] [27] [31] [30] [8] [39] [34] [36] [38] [35] [45] [54]

Para RQ4, la síntesis elaborada por los participantes sobre la definición de los términos está sujeta en gran medida al contexto, la experiencia y el uso del lenguaje. Este hallazgo corresponde al desequilibrio en la definición de términos en el campo de la Ciberseguridad que se presenta en la Figura 3. Como puede verse, los términos están distorsionados según RQ1 o RQ2 o RQ3 en una escala porcentual de cero a cien. Donde el color azul representa la inestabilidad del término que se asocia con diferentes significados. Además, el color naranja muestra cómo diversos términos se asocian con uno mismo y en el caso del gris, el término se superpone con otros términos. Para esta observación el noventa y cuatro por ciento (94%) de los términos carecen de una única interpretación estable y el seis por ciento (6%) de los términos (*"Internet y Stakeholder"*) por el contrario son precisos en diferentes contextos, su manejo y uso.

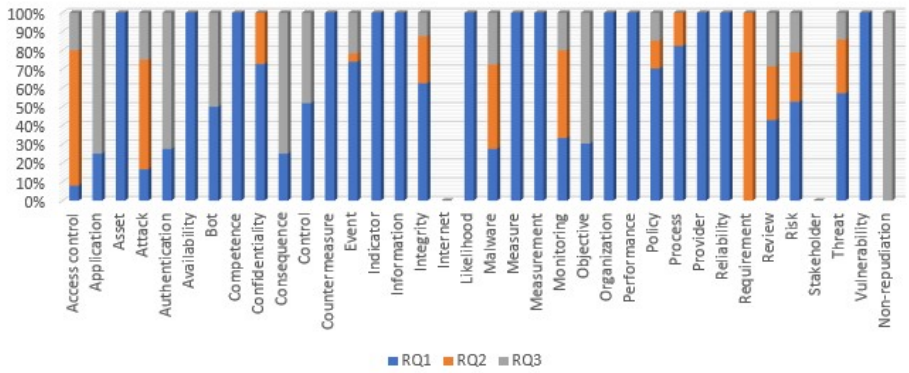

Fig. 3. Desequilibrio en la definición de términos en el ámbito de la Ciberseguridad.

4 Conclusiones

En este trabajo se han presentado los resultados de una encuesta en el marco de la investigación del uso de términos en el contexto de la Ciberseguridad, cuyo objetivo fue describir si existía relación, consolidación o discrepancia entre ellos.

El análisis revela que diferentes consorcios o grupos cognitivos generan diferentes interpretaciones, incluida la variabilidad entre la definición de términos en un mismo estándar. Este problema afecta la interpretación y análisis de la seguridad en los sistemas de las organizaciones y en nuestro caso afecta la creación y generación de KG. Por tanto, el estudio ha servido de validación para demostrar la necesidad de realizar un análisis ontológico posterior que contribuya a la consolidación de los términos en una visión unificada y aceptada en el dominio. Asimismo, el estudio afirma que un compromiso ontológico logrado por la aceptación global permite que las definiciones de los términos sean integrales. Como lo es para las definiciones de *"Internet y Stakeholders"*, cuya difusión en diferentes contextos, se ha generalizado y no permite definiciones variadas, confusas o mal utilizadas.

Acknowledgments. Este trabajo ha sido desarrollado bajo el marco de los proyectos "Digital Knowledge Graph – Adaptable Analytics API" y "PROMETEO/2018/176" con el apoyo financiero de Accenture LTD y la Generalitat Valenciana co-financiada con ERDF.

References

1. Generating Digital Twin models using Knowledge Graphs for Industrial Production Lines. Workshop on Industrial Knowledge Graphs, co-located with the 9th International ACM Web Science Conference 2017 pp. 1–5 (2017), http://ebiquity.umbc.edu/paper/html/id/779/Generating-Digital-Twin-models-using-Knowledge-Graphs-for-Industrial-Production-Lines%0Ahttp://ebiquity.umbc.edu/get/a/publication/850.pdf

2. Al-Moslmi, T., Gallofre Ocana, M., Opdahl, A.L., Veres, C.: Named Entity Extraction for Knowledge Graphs: A Literature Overview. IEEE Access **8**, 32862–32881 (2020). https://doi.org/10.1109/ACCESS.2020.2973928
3. And, P.A.G., And, M.E.G., Fenton, J.L.: Digital Identity Guidelines. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-63-3
4. Barnum, S.: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX ™). Mitre Corporation **11**(Version 1.1, Revision 1), 1–22 (2014)
5. Board, C.E.: Common Vulnerabilities and Exposures - CVE downloads data last generated: 2020-06-23. https://cve.mitre.org/data/downloads/index.html (2006), [Online; accessed 23-Jun-2020]
6. Bret Jordan, Rich Piazza, and Trey Darley (ed.): OASIS - STIX™ Version 2.1. OASIS Committee Specification 01 (2020)
7. CCDB (ed.): CC and CEM addenda Exact Conformance , Selection-Based SFRs , Optional SFRs, vol. V0.5. CCDB, Geneva - Switzerland (May 2017)
8. CCITT & ITU-T (ed.): DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATION - SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS. CCITT & ITU-T, Geneva - Switzerland (1991)
9. CCMB (ed.): Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model, vol. Version3.1. CCDB, revision 5 edn. (2017)
10. CCMB (ed.): Common Criteria for Information Technology Security Evaluation Part 2 : Security functional components, vol. Version3.1. CCDB, revision 5 edn. (2017)
11. CCMB (ed.): Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components, vol. Version3.1. CCDB, revision 5 edn. (2017)
12. CCMB (ed.): Common Methodology for Information Technology Security Evaluation Evaluation methodology, vol. Version3.1. CCDB, revision 5 edn. (2017)
13. CCRA: Common Criteria Portal. https://www.commoncriteriaportal.org/cc/ (2017), [Online; accessed 23-Jun-2020]
14. Chaplin, M., Creasey, J., Frost, N., Lopez-portillo, M., Thorne, S., Liu, L.: The 2011 Standard of Good Practice Principal authors Review and quality assurance (June) (2011)
15. Chen, X., Jia, S., Xiang, Y.: A review: Knowledge reasoning over knowledge graph. Expert Systems with Applications **141** (2020). https://doi.org/10.1016/j.eswa.2019.112948, https://www.scopus.com/inward/record.uri?eid=2-s2.0-85072272885&doi=10.1016%2Fj.eswa.2019.112948&partnerID=40&md5=0ff55c46a9bc1a4179f6cc776cc6eb82
16. Connolly, J., Davidson, M., Schmidt, C.: The trusted automated exchange of indicator information (taxii). The MITRE Corporation pp. 1–20 (2014)
17. Fenton, J.L., Lefkovitz, N.B., Danker, J.M., Greene, K.K., Theofanos, M.F.: Digital Identity Guidelines: Enrollment and Identity Proofing. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-63a
18. Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E., Richer, J.P., Lefkovitz, N.B., Danker, J.M., Greene, K.K., Theofanos, M.F., Newton, E.M., Burr, W.E.: Digital Identity Guidelines: Authentication and Lifecycle Management. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-63b
19. GUÍA DE SEGURIDAD (CCN-STIC-401) GLOSARIO Y ABREVIATURAS (2015)
20. Guarino, N.: The ontological level. Philosophy and the Cognitive Sciences (1994)
21. Guarino, N., Welty, C.: Ontological analysis of taxonomic relationships. In: Laender, A.H.F., Liddle, S.W., Storey, V.C. (eds.) Conceptual Modeling — ER 2000. pp. 210–224. Springer Berlin Heidelberg (2000)
22. Guizzardi, G.: On ontology, ontologies, conceptualizations, modeling languages, and (meta) models. Frontiers in artificial intelligence and applications **155**, 18 (2007)

23. Guizzardi, G.: On ontology, ontologies, conceptualizations, modeling languages, and (meta) models. Frontiers in artificial intelligence and applications **155** (2007)
24. Iannacone, M., Bohn, S., Nakamura, G., Gerth, J., Huffer, K., Bridges, R., Ferragut, E., Goodall, J.: Developing an ontology for cyber security knowledge graphs. In: Proceedings of the 10th Annual Cyber and Information Security Research Conference. pp. 12:1–12:4. CISR '15, ACM, New York, NY, USA (2015)
25. Instituto Nacional de Ciberseguridad - Spanish National Cybersecurity Institute (ed.): Glosario de términos de ciberseguridad - Una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad - Spanish National Cybersecurity Institute (2017)
26. ISO Central Secretary: Information technology Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components. Standard ISO/IEC 154083:2008, International Organization for Standardization, Geneva (2008)
27. ISO Central Secretary: Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components. Standard ISO/IEC 154082:2008, International Organization for Standardization, Geneva (2008)
28. ISO Central Secretary: Irmation technology — Security techniques — Evaluation criteria for IT — Part 1: Introduction and general model Technologies. Standard ISO/IEC 154081:2009, International Organization for Standardization, Geneva (2009)
29. ISO Central Secretary: Information technology — security techniques — guidelines for cybersecurity. Standard ISO/IEC 27032:2012, International Organization for Standardization, Geneva (2012)
30. ISO Central Secretary: Information technology — Security techniques — Code of practice for information security controls. Standard ISO/IEC 27002:2013, International Organization for Standardization, Geneva (2013)
31. ISO Central Secretary: Information technology — security techniques — information security management systems — overview and vocabulary. Standard ISO/IEC 27000:2018-02, International Organization for Standardization, Geneva (2018)
32. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATION SECURITY - INFORMATION TECHNOLOGY - OPEN SSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS: INTEGRITY FRAMEWORKS, vol. 11/95. ITU-T, Geneva - Switzerland (1995)
33. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS - SECURITY - INFORMATION TECHONOLOGY - OPEN SYSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS: CONFIDENTIALITY FRAMEWORK, vol. 11/95. ITU-T, Geneva - Switzerland (1995)
34. ITU-T (ed.): Data Networks and Open System Communications - Security - Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Overview, vol. 11/95. ITU-T (1996)
35. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS - SECURITY - INFORMATION TECHNOLOGY - OPEN SYSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS: SECURITY AUDIT AND ALLARMS FRAMEWORK, vol. 11/95. ITU-T, Geneva - Switzerland (1996)
36. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS - SECURITY - INFORMATION TECHONOLOGY - OPEN SYSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS: AUTHENTICATION FRAMEWORK, vol. 04/95. ITU-T, Geneva - Switzerland (1996)
37. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS SECURITY - INFORMATION TECHNOLOGY - OPEN SYSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS : ACCESS CONTROL, vol. 11/95. ITU-T, Geneva - Switzerland (1996)

38. ITU-T (ed.): SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATION - Security - Information techology - Open Systems Interconnection - Security Frameworks in open systems: Non-repudiation framework, vol. 10/96. ITU-T (1997)
39. ITU-T (ed.): SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS Security - Security architecture for systems providing end-to-end communications, vol. 10/2003. ITU-T (2003)
40. ITU-T (ed.): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security - Overview of cybersecurity, vol. 04/2008. ITU-T (2008)
41. ITU-T (ed.): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Cyberspace security – Cybersecurity - Capabilities and their context scenarios for cybersecurity information sharing and exchange, vol. 12/2010. ITU-T, 1.0 edn. (2010)
42. ITU-T (ed.): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY- Cybersecurity information exchange – Overview of cybersecurity - Overview of cybersecurity information exchange, vol. 04/2011. ITU-T, 1.0 edn. (2012)
43. ITU-T (ed.): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Cyberspace security – Cybersecurity - Design considerations for improved end-user perception of trustworthiness indicators, vol. 03/2017. ITU-T, 1.0 edn. (2017)
44. JOINT TASK FORCE: Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy. Tech. rep., NIST (2018). https://doi.org/https://doi.org/10.6028/NIST.SP.800-37r2
45. JOINT TASK FORCE TRANSFORMATION INITIATIVE: Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations. Tech. rep., NIST (2013). https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-53r4
46. Kitchenham, B., Pfleeger, S.L.: Principles of survey research part 6: Data analysis. SIGSOFT Softw. Eng. Notes **28**(2), 24–27 (Mar 2003). https://doi.org/10.1145/638750.638758, https://doi.org/10.1145/638750.638758
47. MAEC™ Specification - Core Concepts (2017)
48. MAEC™ Specification - Vocabularies (2017)
49. Martínez Zarzuelo, A.: Selección, organización y secuenciación del conocimiento matemático mediante teoría de grafos (2018)
50. Martins, B.F., Serrano, L., Reyes, J.F., Panach, J.I., Pastor, O.: Towards the Consolidation of Cybersecurity Standardized Definitions. Tech. Rep. Version 2, Universidad Politecnica de Valencia (2021)
51. Martins, B.F., Serrano, L., Reyes, J.F., Panach, J.I., Pastor, O.: Towards the consolidation of cybersecurity standardized definitions: a tool for ontological analysis. In: Proceedings of the XXIV Iberoamerican Conference on Software Engineering, CIbSE 2021, San José, Costa Rica, 2021. pp. 1–14 (2021)
52. Martins, B.F., Serrano, L., Reyes, J.F., Panach, J.I., Pastor, O., Rochwerger, B.: Conceptual characterization of cybersecurity ontologies. In: 13th IFIP WG 8.1 working conference on the Practice of Enterprise Modelling (PoEM 2020). pp. 323–338. Springer (2020)
53. Mitre Corporation: Science of Cyber-Security. Tech. rep., The MITRE Corporation, McLean, Virginia (2010)
54. National Institute of Standards and Technology: Security Self-Assessment Guide for Information Technology Systems. Tech. rep., National Institute of Standards and Technology, Gaithersburg, MD (2001)
55. National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity. Tech. rep., National Institute of Standards and Technology (2014)

56. National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity. Tech. rep., National Institute of Standards and Technology (2018). https://doi.org/https://doi.org/10.6028/NIST.CSWP.04162018
57. NERC: CIPC Control Systems Security Working Group. Tech. rep., NERC (2014)
58. NERC: Glossary of Terms Used in NERC Reliability Standards. Tech. rep., NERC (2020)
59. Newhouse, W., Newhouse, W., Scribner, B., Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-181
60. Nieles, M., Dempsey, K., Pillitteri, V.Y.: An Introduction to Information Security An Introduction to Information Security. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-12r1
61. NIST (ed.): Generally accepted principles and practices for securing information technology systems. NIST (2018)
62. PAJARES CAMACHO, Á.: Teoría de grafos: Origen, evolución y aplicaciones (2020)
63. Paulheim, H.: Knowledge Graph Refinement: A Survey of Approaches and Evaluation Methods. Semantic Web **8**(3), 489–508 (2017). https://doi.org/10.3233/SW-160218, http://www.semantic-web-journal.net/content/knowledge-graph-refinement-survey-approaches-and-evaluation-methodshttps://doi.org/10.3233/SW-160218
64. Rose, S., Engel, D., Cramer, N., Cowley, W.: Automatic keyword extraction from individual documents. In: Berry, M.W., Kogan, J. (eds.) Text Mining. Applications and Theory, pp. 1–20. John Wiley and Sons, Ltd (2010)
65. Squire, S.K., Fenton, J.L., Nadeau, E.M., Danker, J.M., Greene, K.K., Theofanos, M.F.: Federation and Assertions. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-63c
66. Standard 1300 — Cyber Security (2004)
67. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A.: Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control Syst. Tech. rep., NIST (2015). https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-82r2
68. Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B.: MITRE ATT&CK(trademark): Design and Philosophy. Tech. rep., The MITRE Corporation, McLean, VA (2018 (revised 2020))
69. Ullmann, S.: Semantics: An Introduction to the Science of Meaning. Barnes & Noble (1979)
70. Varner, B.J., Drew (eds.): OASIS - TAXII™ Version 2.1. OASIS Committee Specification 01 (2020)
71. Wang, L., Jones, R.: Big data analytics in cyber security: network traffic and attacks. Journal of Computer Information Systems pp. 1–8 (2020)
72. Zimmerman, C.: Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation, Bedford, MA (2014)