Analysis of the alignment of Spanish Master's programs to US National Cybersecurity Workforce Framework

Ana I. González-Tablas
Computer Security (COSEC) Lab
University Carlos III of Madrid
Avda. de la Universidad 30, Leganés, 28911 (SPAIN)
aigonzal@inf.uc3m.es

***Abstract*—Building an adequate cybersecurity workforce is an strategic goal of main international stakeholders. Addressing this task passes through adapting graduate and undergraduate curricula so they are aligned to professional and research needs. In this work we present the preliminary results of analyzing the alignment of 25 Spanish cybersecurity Master's programs to the cyber roles specified in the US National Cybersecurity Workforce Framework. Our results suggest that there is no significant alignment between both data sets.**

***Index Terms*—Cybersecurity, education, skills, cyber roles, career development, workforce.**

Tipo de contribución: *Formación innovación*

I. Introduction

In the last years the problem of developing a skilled cybersecurity workforce has attracted an increasing attention from governments, industry and academic stakeholders. Particularly, governments are highlighting the need of analyzing cyber skills required by industry and administrations, and adapting the current graduate programs to be aligned to those required skills [1], [2].

In this work, we want to contribute to this challenge by developing a preliminary analysis of the alignment of main Spanish cybersecurity Master's programs to the US (United States) National Initiative for Cybersecurity Education (NICE) Workforce Framework (WF)[1]. We have chosen the US NICE WF to perform the analysis as there is no equivalent specification in the context of the European Union.

II. US National Cybersecurity Workforce Framework

The Workforce Framework has been developed by the US NICE and the US Department of Homeland Security to provide educators, students, employers, employees, training providers, and policy makers with a systematic and consistent way to address the developing of the US cybersecurity workforce. The US NICE WF defines 7 Categories and 31 Specialty Areas as a mean to organize similar types of work (see Fig. 1).

Each Specialty Area is linked to a set of Competencies (because of the very specific requirements of Categories *Collect and Operate* and *Analyze*, their Specialty Areas are not further analyzed within the Workforce Framework). Each Competency is in turn associated to a set of Knowledge, Skills and Abilities (KSAs).

Category	Specialty Area (SA)
Investigate	Digital Forensics
	Investigation
Operate and Maintain	Customer Service and Technical Support
	Data Administration
	Knowledge Management
	Network Services
	System Administration
	Systems Security Analysis
Oversight and Development	Education and Training
	Information Systems Security Operations (ISSO)
	Legal Advice and Advocacy
	Security Program Management (CISO)
	Strategic Planning and Policy Development
Protect and Defend	Computer Network Defense Analysis
	Computer Network Defense Infrast Support
	Incident Response
	Vulnerability Assessment and Management
Securely Provision	Information Assurance Compliance
	Software Assurance and Security Engineering
	Systems Development
	Systems Requirements Planning
	Systems Security Architecture
	Technology Research and Development
	Test and Evaluation
Collect and Operate	Collection Operations
	Cyber Operations
	Cyber Operations Planning
Analyze	All Source Intelligence
	Exploitation Analysis
	Targets
	Threat Analysis

Fig. 1: Categories and Specialty Areas defined in the US NICE WF.

III. Methodology

A. Approach

As the goal is to analyze the alignment of the Spanish cybersecurity Master's programs to the US NICE WF, an approach to perform the analysis has to be defined. In the light of the structure of the US NICE WF, we decided to perform the analysis at Competency level. This is also the approach taken to map the the Knowledge Units identified within the US

[1] https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework

TABLE I: Spanish cybersecurity Master's studies analyzed in this work.

ID	University	Title	Edition	Accredited by ANECA	Modality
M1	Universidad de Almería	Máster en Administración, Comunicaciones y Seguridad Informática [3]	VI (2014-2015)	No	Online
M2	Universidad de Sevilla	Master en seguridad de la Información y las Comunicaciones [4]	III (2015-2016)	No	Blended
M3	Universidad Católica Santa Teresa de Jesús de Ávila	Máster en Ciberseguridad UCAV-Deloitte [5]	—	No	Online
M4	Universidad de León	Máster Profesional en Tecnologías de la Seguridad [6]	VII (2015-2016)	No	On-site
M5	Universidad Oberta de Cataluña, Universidad Rovira i Virgili, Universidad Autónoma de Barcelona	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones [7]	V (2015-2016)	Yes	Online
M6	Universidad Politécnica de Cataluña	Cybersecurity Management [8]	III (2015-2016)	No	On-site
M7	Universidad Ramón Llull	Máster en Ciberseguridad [9]	II (2015-2016)	No	On-site
M8	Universidad Rovira i Virgili	Máster Universitario en Ingeniería Informática: Seguridad Informática y Sistemas Inteligentes [10]	I (2016-2017)	Yes	On-site
M9	Universidad a Distancia de Madrid	Máster Universitario en Seguridad, Defensa y Geoestrategia [11]	IV (2015-2016)	Yes	Online
M10	Universidad Alfonso X el Sabio	Máster Universitario en Ingeniería de Seguridad de la Información y las Comunicaciones [12]	VII (2015-2016)	Yes	Blended
M11	Universidad Autónoma de Madrid	Máster en Análisis de la Evidencia Digital y Lucha contra el cibercrimen [13]	I (2015-2016)	No	On-site
M12	Universidad Autónoma de Madrid	Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC [14]	VII (2015-2016)	No	On-site/Online
M13	Universidad Carlos III de Madrid	Máster Universitario en Ciberseguridad [15]	II (2015-2016)	Yes	On-site
M14	Universidad de Alcalá	Máster en Ciberdefensa [16]	I (2015-2016)	No	Blended
M15	Universidad Europea de Madrid	Máster Universitario en Seguridad de Tecnologías de la Información y Comunicaciones [17]	VIII (2015-2016)	Yes	On-site
M16	Universidad Internacional de La Rioja	Máster Universitario en Seguridad Informática [18]	III (2015-2016)	Yes	Online
M17	Universidad Internacional Menéndez Pelayo	Máster en Gestión de Seguridad Integral [19]	I (2016-2017)	No	On-site
M18	Universidad Nacional de Educación a Distancia	Máster en Sistemas de Gestión y Seguridad Informática [20]	To be extinguished (2016-2017)	No	Distance
M19	Universidad Politécnica de Madrid	Máster en Gobierno de la Ciberseguridad UPM-ISMS Forum [21]	IX (2015-2016)	No	On-site
M20	Universidad Politécnica de Madrid	Máster en Auditoría y Control de los Sistemas de Información [22]	—	No	On-site
M21	Universidad Politécnica de Madrid	Máster en Gestión del Aseguramiento, Protección y Defensa del Software, Operaciones y Sistemas [23]	II (2015-2016)	No	On-site
M22	IMF Business School - Universidad Camilo José Cela	Máster Online en Seguridad de la Información IMF [24]	II (2015-2016)	No	Online
M23	Universidad San Pablo-CEU	Máster Internacional Universitario en Protección de Datos, Transparencia y Acceso a la Información [25]	III (2015-2016)	Yes	Blended
M24	U-TAD	Máster INDRA en Ciberseguridad [26]	II (2015-2016)	No	On-site
M25	Universidad de Mondragón	Máster en Seguridad Informática (Online) [27]	II (2015-2016)	No	Online

National Centers of Academic Excellence in Cyber Defense (CAE-CD)[2] to the US NICE WF. As Categories *Collect and Operate* and *Analyze* are not defined at the Competency level, they are not included in the study.

First, the Workforce Framework was analyzed for comparing the Competencies linked to each Specialty Area and to each Category (considering in this case the union of the Competencies linked to the Specialty Areas classified into the Category).

Next step was to identify main Spanish cybersecurity Master studies and retrieve their curricula. Only graduate studies with 60 ECTS (or more) are considered as target of the analysis. Afterward, each curricula was manually inspected with the goal of identifying the set of US NICE WF's Competencies covered.

Once both data sets were collected and elaborated, Competency-based frequency and similarity analysis between US NICE WF's Specialty Areas and Spanish cybersecurity Master's programs was performed.

B. Data collection and elaboration

First, the set of Competencies associated to each Specialty Area was retrieved from the interactive web page of the US NICE WF[3].

Second, main Spanish cybersecurity Master studies were identified. Sources used for this step are the web page of Criptored's MESI project[4] and the list of cybersecurity Master studies suggested by the Spanish National Cybersecurity Institute[5]. Web pages of each Master program were visited to check that the Masters were active (i.e., they were currently being offered or were about to in the following months). Table I lists the Masters included in the study.

Web pages of each Master program were used as source for retrieving the curricula of each study. In some cases, this information was not publicly available and had to be requested filling up a web form (more details were then sent by email). This information was carefully read and the courses programs were compared with the list of KSAs assigned to each Competency. A coarse-grained criteria was applied to decide whether a given Competency was covered by a Master's program, as both elements are described according different goals, detail level and with different vocabulary. When there was more than one track within a Master's program[6], the union of the Competencies identified in all tracks has been used to characterize the Master's program.

C. Analysis

In first place, we compared the relative frequency of each Competency within the whole set of the Specialty Areas respect its frequency within the whole set of Master's programs. This comparison provides with an overview of the relative importance of each Competency within both data sets. Absolute frequency is normalized, respectively, by the number of Specialty Areas (see Eq. 1, where Specialty Areas are denoted as SA) and the number of Master's programs (see Eq. 2, where Master's programs are denoted as MP).

$$f_1(c_i) = \frac{|Set\ of\ SA\ linked\ to\ c_i|}{|Set\ of\ SA|} \quad (1)$$

[2]https://niccs.us-cert.gov/education/national-centers-academic-excellence-cae

[3]https://niccs.us-cert.gov/training/tc/framework

[4]Proyecto MESI: Mapa de Enseñanza de la Seguridad de la Información (http://www.criptored.upm.es/mesi/proyectomesi.htm)

[5]https://www.incibe.es/excelencia/talento/becas

[6]Multiple tracks are usually implemented through the election of some courses from a given set while the main part of the curricula is common to all tracks.

$$f_2(c_i) = \frac{|Set\ of\ MP\ linked\ to\ c_i|}{|Set\ of\ MP|} \quad (2)$$

In second place, Competency-based similarity was computed between each Master's program and each Specialty Area. As elements to be compared are binary vectors, Jaccard similarity (also denoted as Tanimoto similarity) was considered an appropriate similarity metric [28].

In third place, we compared at a Competency level the distances between each pair of Master's programs within the analyzed set. Assuming that Jaccard similarity between programs M_i and M_j is denoted as $similarity(M_i, M_j)$, we computed distance as in Eq. 3.

$$distance(M_i, M_j) = 1 - similarity(M_i, M_j) \quad (3)$$

Computations and graphics have been performed and created with the R Programming Environment and Microsoft Office's Excel 2013.

IV. Results

Figure 2 compares the relative frequencies of Competencies in both data sets. Notice that both frequencies do not have the same interpretation. In the case of the Specialty Areas, the frequency conceptually represents how common is that competency in the spectrum of cyber jobs the workforce should cover. In the case of Master's programs, the frequency represents the emphasis that current Spanish graduate cybesecurity studies make on a specific Competency; that is, how common is its coverage by Master's programs considering the current set of Master studies.

Nonetheless, some issues can be identified from the comparison. If some alignment existed between both data sets, it would be expected that both relative frequency histograms presented a non-equal but similar shape or pattern. However, in Fig. 2 this alignment is not observed. Furthermore, it is highlighted the significant weight that *Legal, Government, and Jurisprudence* Competency, on one side, and, *Vulnerability Assessment* Competency, on the other side, are given within the analyzed Master's curricula, while they are not specially common within the US NICE WF. Additionally, it is noticeable the low emphasis made by Master's curricula on the 6 Competencies with higher frequencies in the US NICE WF.

Figure 4 depicts the computed similarity between the elicited Competencies of each Master's program and the set of Competencies of each Specialty Area. Similarities are shown twofold: graphically (the longer the white bar in each cell is, the more similar both compared elements are) and numerically (similarity is written at the right inside each cell).

The first issue that can be noticed is that, in general, similarities are rather low. This result might have been influenced by the fact that analyzed graduate studies assume that some KSAs have already been acquired in undergraduate studies previously undertaken by students. Therefore, they are not specifically included in their curricula and might have been missed in the analysis.

A second issue is that, generally, Master's programs adopt a broad approach and do not aim matching a specific Specialty Area except a few ones. Besides, Masters M9 and M11 stand

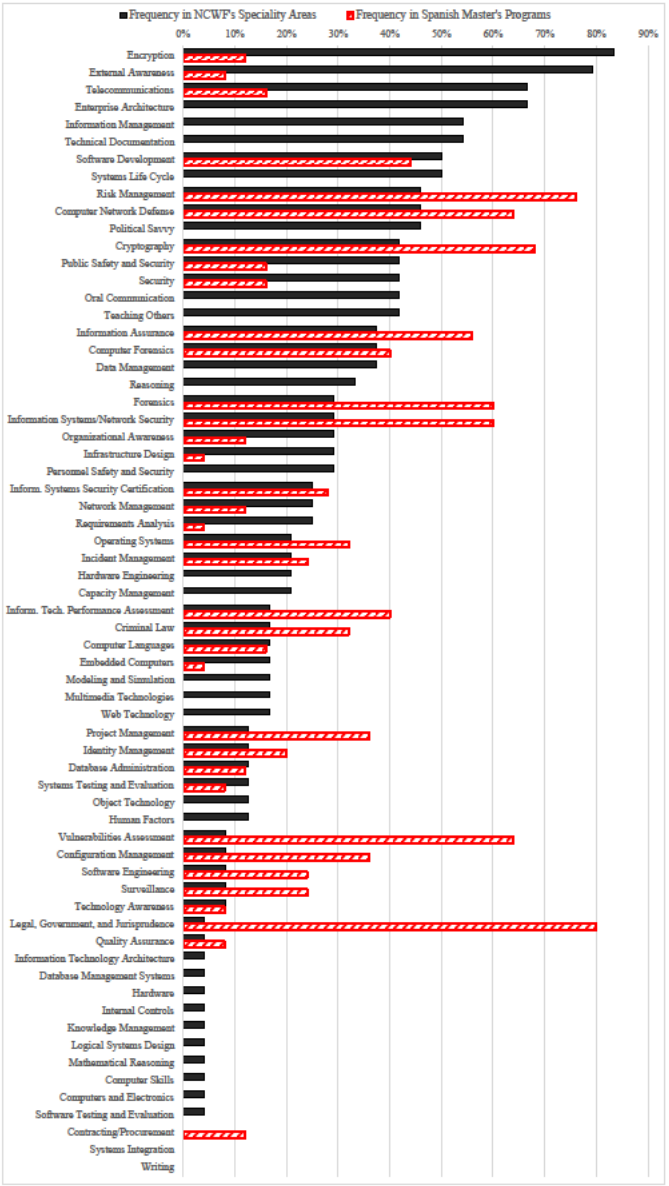

Fig. 2: Relative frequency of US NICE WF's Competencies in US NICE WF's Specialty Areas (black bars) and Spanish Master's Programs (red stripped bars).

out from the rest because of their significant differences in their Competencies profile with respect the other Masters. Although with a modest similarity ranks, more frequent Specialty Areas are *Digital Forensics* and *Computer Network and Defense Analysis*.

Finally, we took advantage of the Competency-based characterization elicited for each Master to compare the curricula of the 25 Masters analyzed in this work. Fig. 3 shows a heat map of the Competency-based distances between each pair of Master's programs. Notice that distances, not similarities, are depicted, and that a hierarchical clustering algorithm has been applied before depiction. Therefore, given a pair of Master's, the darker the cell in the heatmap is, the more similar at Competency-level they are.

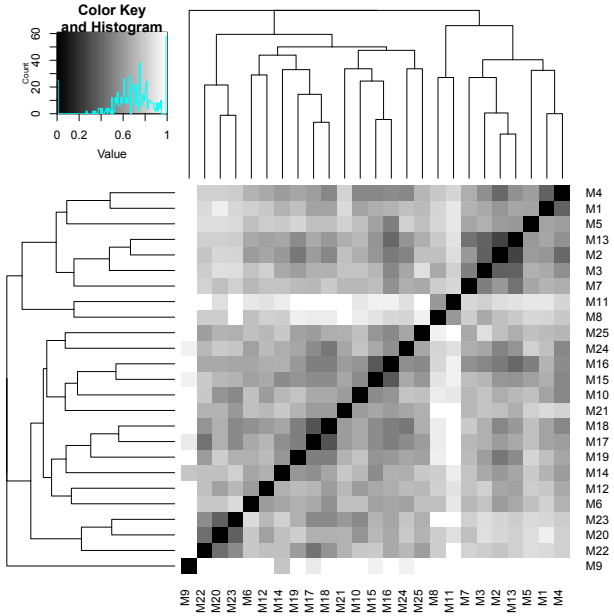

Fig. 3: Competency-based *distances* between Spanish cybersecurity Master's programs listed in Table I .

V. Threats to validity

Several threats to the validity of the preliminary analysis of the alignment of main Spanish cybersecurity Master's programs to the US NICE WF have been identified. First threat is that the detail of definition of the Master's programs is varied. In some cases, the detail might be insufficient to perform a grounded assessment.

A second threat is that only authors of this work have decided which competencies were covered by a Master's program. A larger number of educators, professionals and researchers should collaborate in the analysis, and moreover, it would be highly advisable that the teachers staff of each Master were involved in the assessment.

A third threat is that it is necessary to apply a coarse-grained criteria to decide whether a Specialty Area is covered by a Master's program, given the different contexts both data sets emerge from. It would be better to count with more granular and adjustable criteria.

Lastly, it is necessary to consider that analyzed Master's programs generally assume that certain KSAs and Competencies have already been acquired by students in previous undergraduate studies. These KSAs and Competencies are broadly stated in the Master's programs but have not been considered in the presented work. Including them may change at least the similarities between the Master's programs and the Specialty Areas, although it is probable that the general patterns remain unmodified.

VI. Conclusions and future work

In this work we have analyzed, using a Competency-based approach, the alignment of 25 Spanish Master's programs to the Specialty Areas defined in the US NICE WF. Our results suggest that there is no significant alignment between both data sets. Particularly, it appears to be uncommon that a Master's program clearly matches specific Specialty Areas. This approach might be insufficient for preparing students to reliably join in the cybersecurity workforce under a specific role.

On the other side, this is a preliminary analysis and several threats to its validity have been identified. Future works should address mentioned issues.

Acknowledgments

This work was supported by the MINECO grant TIN2013-46469-R (SPINY: Security and Privacy in the Internet of You) and by the CAM grant S2013/ICE-3095 (CIBERDINE: Cybersecurity: data, information and risk).

Appendix: Main subjects in each Master Program

M1 *Máster en Administración, Comunicaciones y Seguridad Informática* • Administración de sistemas windows, Administración de sistemas GNU/Linux, Administración Avanzada de Sistemas Informáticos • Networking, Introducción a la Telefonía IP mediante Software Libre, Redes Inalámbricas • Aspectos básicos y legales de la seguridad informática, Seguridad Informática en sistemas Windows y GNU/Linux, Analista de Seguridad Informática • Diseño y Creación de Portales Web • Desarrollo de la Competencia de Trabajo en Equipo • Trabajo Final de Máster

M2 *Máster en seguridad de la Información y las Comunicaciones* • Introducción a la seguridad e indentificación digital • Seguridad en Redes de Datos • Seguridad en Servicios y Sistemas de Información • Hacking ético y auditorías de seguridad • Gestión de la seguridad en organizaciones • Sistemas IDS/IPS. Seguridad en el acceso remote. • Seguridad en el desarrollo de software y apps móviles • Seguridad en Cloud Computing • Informática Forense • Trabajo Final de Máster

M3 *Máster en Ciberseguridad UCAV-Deloitte* • Hacking ético • Laboratorio de Ciber Inteligencia • Análisis Forense • Desarrollo seguro • Tecnologías SIEM • Deontología Profesional • Criminalidad Informática, Aspectos legales • Criptografía • Conexiones Seguras • Trabajo Fin de Máster • Prácticas en el CyberSOC

M4 *Máster Profesional en Tecnologías de la Seguridad* • Sistemas operativos y la seguridad • Redes de sistemas TIC y la seguridad • Desarrollo y programación seguras • Criptografía • Sistemas para la gestión de la seguridad de la información (SGSI) (online) • Legislación y regulación: aspectos jurídicos de la seguridad (online) • Bastionado de sistemas operativos • Configuración para servicios seguros • Seguridad en redes • Sistemas complejos robustos • Auditoría de seguridad en sistemas y servicios • Análisis forense • Análisis de malware y reversing

M5 *Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones* • Legislación y regulación • Vulnerabilidades de seguridad • Identidad digital • Prácticas profesionales • Trabajo fin de master • (Esp. Prof. 1) Seguridad en redes • (Esp. Prof. 1) Seguridad en sistemas operativos • (Esp. Prof. 1) Seguridad en bases de datos • (Esp. Prof. 2) Comercio electrónico • (Esp. Prof. 2) Programación de código seguro • (Esp. Prof. 2) Biometría • (Esp. Prof. 3) Sistemas de gestión de la seguridad • (Esp. Prof. 3) Auditoría técnica • (Esp. Prof. 3) Análisis forense • (Esp. Inv. 4) Criptografía avanzada • (Esp. Inv. 4) Metodologías de investigación • (Esp. Inv. 4) Técnicas de investigación • (Opt.) Técnicas de marcado de la información • (Opt.) Dirección estratégica de sistemas y tecnologías de la informació

M6 *Cybersecurity Management* • Auditoría de sitemas: Hacking ético • Monitorización de acontecimientos de seguridad • Data Driven Security • Entornos ubicuos: SCADA y móviles • Respuesta a incidents • Análisis de malware • Amenazas y análisis de riesgos • Gobierno de la seguridad • Diseño,

desarrollo e implantación • Cumplimiento • Criptografía y autenticación • Proyecto final de master

M7 *Máster en Ciberseguridad* • Hacking ético • Análisis de seguridad • Ingeniería inversa • Análisis forense • Ciberinteligencia • Seguridad Web • Seguridad en entornos móviles • Prácticas • Trabajo Final de Máster

M8 *Máster Universitario en Ingeniería Informática: Seguridad Informática y Sistemas Inteligentes* • Computer Forensics • Cryptology and Information Security • Biometric Identification • Privacy Protection • Multi-agent Systems • Artificial Vision & Pattern Recognition • Neuronal & Evolutionary Computation • Multi-criteria Decision Support Systems • (Opt.) Secure Distributed Systems • (Opt.) Multimedia Security • (Opt.) Ubiquitous Computing • (Opt.) Planning & Approximate Reasoning • (Opt.) Knowledge Representation • (Opt.) Complex Networks • (Opt.) Research & Entrepreneurship • (Opt.) Visualisation & Interaction Systems • Final Master's Project

M9 *Máster Universitario en Seguridad, Defensa y Geoestrategia* • Los conceptos clave: seguridad, geoestrategia y defensa de las naciones • Tipología de los conflictos y evolución de las amenazas bélicas globales • Actores nacionales e internacionales de la seguridad y la defensa • Amenaza y reacción contra el terrorismo global y el crimen organizado • Fundamentos de la inteligencia y la contrainteligencia • Fuerzas armadas • Impacto de la industria military en el desarrollo de la economía y la tecnología • Hitos y estrategia military en la historia contemporánea • Metodología de la investigación aplicada a la seguridad y la defensa • Trabajo Fin de Máster

M10 *Máster Universitario en Ingeniería de Seguridad de la Información y las Comunicaciones* • Seguridad en los Sistemas de Información • Tecnologías para la seguridad • Implantación de sistemas seguros • Seguridad en sistemas inalámbricos y celulares • Dirección de la seguridad y gestión de riesgos • Seguridad en comercio electrónico • Auditoría y prestación de servicios • Aspectos jurídicos de la seguridad • Prácticas en empresa • Trabajo Fin de Máster

M11 *Máster en Análisis de la Evidencia Digital y Lucha contra el cibercrimen* • Fundamentos en ciberseguridad • Fundamentos en cibercrimen y ciber-terrorismo • Fundamentos en informática forense • Análisis de evidencias forenses y sistemas biométricos • Linux para investigadores • Scripting forense • Investigación forense de datos volátiles • Técnicas computacionales avanzadas para el análisis de datos • Redes de comunicaciones • Investigación forense de móviles • (Esp. A) Fuentes Abiertas • (Esp. A) Investigación de VOIP y redes inalámbricas • (Esp. A) Hacking y malware • (Esp. A) Crímenes contra menores • (Esp. A) Delitos financieros en Internet y lavado de dinero • (Esp. B) Forensics readiness • (Esp. B) Análisis y prevención de ciber-riesgos • (Esp. B) Análisis de malware • (Esp. B) Auditorías de seguridad informática • (Esp. B) Amanazas persistentes avanzadas y ciber-espionaje • Trabajo Final de Máster

M12 *Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC* • Fundamentos tecnológicos de los sistemas de información • Control Interno • Seguridad Informática I • Auditoría de los sistemas de información I • Derechos y garantías en sistemas de información • Seguridad Informática II • Gobierno de los sistemas de Información I • Protección Jurídica de los Bienes Inmateriales • Auditoría de los sistemas de información II • Gobierno de los sistemas de información II • Auditoría de los sistemas de información III • Gestión Económico financier • Seguridad Informática III • Firma electronica y certificación digital • Informática forense • Gobierno de los sistemas de información III • Estándares • Capital Humano en la gestión del Capital Intelectual • Proyecto Fin de Máster

M13 *Máster Universitario en Ciberseguridad* • Secure Communications • Software Systems Exploitation • Data Protection • Cyber Defense Systems • Cyber Attack Techniques • Identification and Authentication • Cyber Security Management and Administration • Seminar I • Seminar II • (Esp. 1) Systems Security Engineering • (Esp. 1) Secure Architecture • (Esp. 1) Mobile Security • (Esp. 2) Malware analysis and engineering • (Esp. 2) Persistent Threat and Information Leakage • (Esp. 2) computer Forensics • (Opt.) Cyber crime, Cyber terrorism, and Cyber war • (Opt.) Risk Analysis and Systems Certification

M14 *Máster en Ciberdefensa* • Bases de ciberseguridad • Introducción a la ciberdefensa • Aspectos legales, politicos y éticos del ciberespacio • Aspectos doctrinales. Planeamiento de Operaciones • Ciberamenazas a las infraestructuras críticas • Experimentación en ciberdefensa(CD&E) • Análisis de riesgo estático y dinámico • Detección y defensa frente a amenazas cibernéticas • Respuesta a incidents y análisis forense • Análisis de malware • Recuperación y fusión y análisis de datos • Concienciación de situación y compartición información • Ciberinteligencia y fuentes abiertas • Amenzas avanzadas persistentes (APT's) • Ataques de denegación de servicio • Hacking ético • Ingeniería social • Trabajo Fin de Máster

M15 *Máster Universitario en Seguridad de Tecnologías de la Información y Comunicaciones* • Sistemas de gestión de seguridad • Análisis de riesgos • Criptografía aplicada y control de accesos • La seguridad en el software de base y en las aplicaciones • La seguridad física y del entorno • La seguridad en las comunicaciones • La seguridad en las operaciones • Auditoría y cumplimiento del marco jurídico • (Esp. 1) Formación de investigación • (Esp. 2) Formación práctica/professional • Proyecto de Fin de Máster

M16 *Máster Universitario en Seguridad Informática* • Aspectos legales y regulatorios • Gestión de la seguridad • Seguridad en redes • Seguridad en sistemas operativos • Análisis forense • Criptografía y mecanismos de seguridad • Análisis de vulnerabilidades • Análisis de riesgos legales • Auditoría de la seguridad • Seguridad en aplicaciones online y bases de datos • Seguridad en el software • Delitos informáticos • Prácticas en empresa • Trabajo fin de máster

M17 *Máster en Gestión de Seguridad Integral* • Gestión y organización de la seguridad integral • Gestión de situaciones de crisis y riesgos • Legislación, criminología y delincuencia • Protección física y electronica • Protección civil, contra incendios y prevención de riesgos laborales • Segruidad patrimonial, de entidades y protección de personas • Protección de la información y criptología • Seguridad en redes y control de acceso • Seguridad en arquitecturas, desarrollos y operaciones de sistemas • Trabajo de fin de máster

M18 *Máster en Sistemas de Gestión y Seguridad Informática* • Sistemas de seguridad de la información • Hacking ético • Criptografía • Diseño y gestión de redes seguras y gestión de riesgos • Implantación de un SGSI según las normas ISO 27000 • La propiedad industrial e intellectual en el ámbito tecnológico • La contratación y el sector TIC • Protección de datos, privacidad e intimidad • La facturación y la firma electronica • Principales delitos vinculados a los sistemas de información y a las redes telemáticas • Trabajo Fin de Máster

M19 *Máster en Gobierno de la Ciberseguridad UPM-ISMS Forum* • Introducción a la ciberseguridad • Análisis y gestión de riesgos de ciberseguridad • Aplicación de tecnologías criptográficas • Seguridad en las arquitecturas de red y comunicaciones • Seguridad en la plataforma • Seguridad en el diseño y desarrollo de sistemas • Gestión y monitorización de la ciberseguridad. Servicios preventivos, detectivos y reactivos. Modelos organizativos para SOCs y CERTs. • Gestión del cumplimiento y protección de la información corporative • Estrategias corporativas de ciberseguridad • Modelos de gestión para el gobierno de la ciberseguridad • Estrategias públicas de ciberseguridad • Habilidades para la dirección y el liderazgo • Fundamentos y conceptos empresariales

M20 *Máster en Auditoría y Control de los Sistemas de Información* • Introducción a la seguridad y a la auditoria de los S.I. • El Sistema de gestión de la seguridad de la información (SGSI). Normas ISO 27000. • Organización Corporativa de la seguridad de la información. Gestión de activos. Análisis y evaluación de riesgos. • La aplicación de la norma ISO 27002. • Cumplimiento con el marco jurídico. • El plan de

continuidad de la organización. • Gestión de la seguridad: Métricas, indicadores y cuadro integral de mando. • Informática Forense. Introducción a los centros de respuesta a incidents de seguridad (CERT y CSIRT) • Las nuevas funciones del auditor de SI y competencias necesarias. El proceso de auditoria. • Técnicas y marcos de la auditoria. Práctica de la auditoria. • Herramientas del auditor. Evolución de la auditoria de Sistema de información. • Conferencias. • Trabajo Fin de Máster

M21 *Máster en Gestión del Aseguramiento, Protección y Defensa del Software, Operaciones y Sistemas* • Assurance Assessment • System Operational Assurance • Assured Software Development 1 • System Security Assurance • Assured Software Development 2 • Assured Software Analytics • Assured Software Development 3 • Assurance Management • Trabajo Fin de Máster (Software Assurance Capstone Experience)

M22 *Máster en Ciberseguridad* • Ciberinteligencia • Hacking Ético • Desarrollo Seguro • Análisis Forense • Ingeniería inversa • Tecnologías SIEM • Seguridad en Smartphones • Trabajo Fin de Máster

M23 *Máster Internacional Universitario en Protección de Datos, Transparencia y Acceso a la Información* • Protección de datos de carácter personal • Transparencia y acceso a la información • Auditoría y seguridad • Prácticas externas • Trabajo de Fin de Máster

M24 *Máster INDRA en Ciberseguridad* • Certificación y acreditación de productos y sistemas • Comunicaciones seguras • Diseño y construcción de redes y sistemas seguros • Introducción a la ciberseguridad • Criptografía • Ingeniería de software seguro • Técnicas avanzadas de explotación del software • Análisis y gestión de riesgos tecnológicos • Análisis forense de redes y sistemas informáticos • Diseño y construcción de ciberarmas • Seguridad en Sistemas de Control Industrial • Sesiones de entrenamiento práctico • Técnicas avanzadas de ataque a sistemas de control industrial • Trabajo Fin de Máster

M25 *Máster en Seguridad Informática (Online)* • Fundamentos de redes • Fundamentos de programación C y Python • Fundamentos de Arquitectura y de sistemas operativos • Criptografía • Seguridad en Nodos y Redes • Autenticación y Gestión de Identidades • Seguridad Perimetral • Seguridad del Software • Auditoría de Seguridad Informática • Seguridad en la Nube • Monitorización de redes y servicios • Incidentes de seguridad • Seguridad física • Normativas, estándares y aspectos legales de la seguridad • Gestión de proyectos de seguridad • Proyecto Fin de Máster

REFERENCES

[1] European Union Agency For Network And Information Security (ENISA): "Status of privacy and NIS course curricula in Member States", October 2015.

[2] Spanish National Cybersecurity Institute (INCIBE): "Estudio de viabilidad, oportunidad y diseño de una red de centros de excelencia en I+D+I en ciberseguridad", Mayo 2015.

[3] http://masteracsi.ual.es/

[4] http://trajano.us.es/~rafa/seguridad/index.html

[5] http://online.ucavila.es/master-ciberseguridad-deloittehttp://www.ucavirtual.es/moodle/course/index.php?categoryid=71

[6] http://masterseguridad.unileon.es/

[7] http://estudios.uoc.edu/es/masters-universitarios/seguridad-tecnologias-informacion-comunicaciones/

[8] http://www.talent.upc.edu/esp/professionals/presentacio/codi/221100/cybersecurity-management/

[9] http://www.beslasalle.net/portal/masters/masters-electronica-mcs-barcelona-presentation

[10] http://www.urv.cat/masters_oficials/enginyeria_arquitectura/Enginyeriaseguretat/master_seguretat_informatica.html http://deim.urv.cat/~mesiia/index.php

[11] http://www.udima.es/es/master-seguridad-defensa-geoestrategia.html

[12] http://www.openuax.com/master-universitario-en-ingenieria-de-seguridad-de-la-informacion-y-las-comunicaciones.html

[13] http://www.uam.es/ss/Satellite/es/1242654675830/1242683206845/estudiopropio/estudioPropio/Master_en_Analisis_de_Evidencias_Digitales_y_Lucha_contra_el_Cibercrimen.htm https://www.cnec.university/formacion/master-evidencias/

[14] http://www.uam.es/ss/Satellite/EscuelaPolitecnica/es/estudios/ensenanzas-propias-de-la-uam/programa-de-titulos-propios/Page/subhome/master-en-auditoria,-seguridad,--gobierno-y-derecho-de-las-tic.htm

[15] http://www.uc3m.es/ss/Satellite/Postgrado/es/Detalle/Estudio_C/1371209197821/1371208956904/Master_Universitario_en_Ciberseguridad

[16] http://masterciberdefensa.in-nova.org/index.php/master

[17] http://universidadeuropea.es/estudios-universitarios/master-universitario-en-seguridad-de-tecnologias-de-la-informacion-y-de-las-comunicaciones

[18] http://www.unir.net/ingenieria/master-seguridad-informatica/549200001557/

[19] http://www.uimp.es/postgrado/estudios/fichaestudio.php?plan=P03G&any=2015-16&verasi=N&lan=es

[20] http://www2.uned.es/gestion-seguridad-informacion/index.html

[21] http://www.master.etsit.upm.es/masterGOCS/ https://www.ismsforum.es/curso/27/master-en-gobierno-de-la-ciberseguridad/

[22] http://www.fi.upm.es/acsi/

[23] http://www.fi.upm.es/mastergapds/

[24] http://www.imf-formacion.com/masters-profesionales/master-seguridad-informatica

[25] http://www.postgrado.uspceu.es/pages/proteccion_datos/presentacion.php?ID_M=84#mc

[26] https://www.u-tad.com/estudios/master-indra-en-ciberseguridad/

[27] http://www.mondragon.edu/cursos/es/tematicas/informatica-telecomunicaciones-sistemas-empotrados/master-en-seguridad-informatica-online/?set_language=es

[28] Michel Marie Deza, Elena Deza: "Encyclopedia of Distances", Springer, 2009.

Category	Specialty Area (SA)	M1	M2	M3	M4	M5	M6	M7	M8	M9	Maximum similarity per SA	Mean similarity per SA
Investigate	Digital Forensics	0.29	0.44	0.38	0.36	0.22	0.33	0.41	0.21	0.00	0.44	0.25
	Investigation	0.13	0.21	0.27	0.18	0.20	0.20	0.24	0.30	0.10	0.30	0.14
Operate and Maintain	Customer Service and Technical Support	0.18	0.08	0.05	0.15	0.05	0.05	0.04	0.07	0.00	0.24	0.09
	Data Administration	0.12	0.14	0.05	0.10	0.25	0.00	0.05	0.15	0.00	0.25	0.07
	Knowledge Management	0.13	0.09	0.05	0.11	0.06	0.06	0.05	0.08	0.09	0.22	0.09
	Network Services	0.25	0.19	0.08	0.22	0.08	0.08	0.16	0.05	0.00	0.25	0.15
	System Administration	0.23	0.18	0.16	0.25	0.17	0.04	0.19	0.10	0.00	0.32	0.14
	Systems Security Analysis	0.21	0.21	0.19	0.27	0.24	0.20	0.18	0.11	0.00	0.34	0.18
Oversight and Development	Education and Training	0.25	0.18	0.10	0.21	0.17	0.05	0.09	0.07	0.08	0.25	0.11
	Information Systems Security Operations (ISSO)	0.13	0.19	0.08	0.16	0.13	0.23	0.11	0.10	0.00	0.35	0.17
	Legal Advice and Advocacy	0.21	0.21	0.27	0.18	0.20	0.20	0.17	0.18	0.10	0.27	0.17
	Security Program Management (CISO)	0.35	0.27	0.21	0.30	0.22	0.27	0.19	0.15	0.00	0.35	0.21
	Strategic Planning and Policy Development	0.22	0.22	0.14	0.19	0.28	0.28	0.30	0.06	0.14	0.33	0.22
Protect and Defend	Computer Network Defense Analysis	0.35	0.38	0.26	0.36	0.27	0.27	0.29	0.15	0.00	0.44	0.24
	Computer Network Defense Infrast. Support	0.29	0.22	0.14	0.19	0.21	0.21	0.24	0.13	0.00	0.29	0.18
	Incident Response	0.33	0.22	0.20	0.27	0.21	0.31	0.25	0.09	0.00	0.33	0.21
	Vulnerability Assessment and Management	0.24	0.23	0.21	0.26	0.29	0.22	0.32	0.13	0.00	0.33	0.19
Securely Provision	Information Assurance Compliance	0.09	0.20	0.08	0.13	0.14	0.25	0.17	0.11	0.06	0.35	0.19
	Software Assurance and Security Engineering	0.11	0.19	0.18	0.21	0.19	0.19	0.17	0.04	0.00	0.32	0.17
	Systems Development	0.18	0.18	0.14	0.24	0.14	0.18	0.16	0.06	0.00	0.27	0.16
	Systems Requirements Planning	0.17	0.14	0.09	0.16	0.13	0.17	0.12	0.07	0.00	0.33	0.15
	Systems Security Architecture	0.17	0.14	0.12	0.23	0.13	0.13	0.11	0.07	0.00	0.28	0.14
	Technology Research and Development	0.27	0.31	0.25	0.29	0.21	0.16	0.23	0.14	0.05	0.31	0.19
	Test and Evaluation	0.12	0.14	0.05	0.22	0.11	0.11	0.10	0.07	0.00	0.25	0.15
	Maximum similarity per Master	0.35	0.44	0.38	0.36	0.29	0.33	0.41	0.30	0.14		
	Mean similarity per Master	0.21	0.21	0.16	0.22	0.18	0.17	0.18	0.11	0.03		

Category	Specialty Area (SA)	M10	M11	M12	M13	M14	M15	M16	M17	M18	Maximum similarity per SA	Mean similarity per SA
Investigate	Digital Forensics	0.22	0.11	0.13	0.33	0.29	0.31	0.35	0.27	0.22	0.44	0.25
	Investigation	0.20	0.25	0.14	0.18	0.17	0.09	0.14	0.06	0.06	0.30	0.14
Operate and Maintain	Customer Service and Technical Support	0.24	0.00	0.06	0.07	0.14	0.17	0.12	0.05	0.05	0.24	0.09
	Data Administration	0.05	0.09	0.00	0.12	0.05	0.13	0.13	0.00	0.00	0.25	0.07
	Knowledge Management	0.06	0.00	0.06	0.08	0.22	0.09	0.08	0.12	0.12	0.22	0.09
	Network Services	0.24	0.00	0.09	0.21	0.12	0.23	0.22	0.13	0.18	0.25	0.15
	System Administration	0.17	0.05	0.04	0.29	0.11	0.21	0.21	0.04	0.08	0.32	0.14
	Systems Security Analysis	0.24	0.00	0.10	0.26	0.15	0.27	0.34	0.16	0.20	0.34	0. 8
Oversight and Development	Education and Training	0.11	0.08	0.06	0.12	0.14	0.13	0.12	0.11	0.11	0.25	0.11
	Information Systems Security Operations (ISSO)	0.35	0.00	0.19	0.17	0.15	0.22	0.21	0.13	0.17	0.35	0.17
	Legal Advice and Advocacy	0.20	0.00	0.23	0.18	0.24	0.14	0.19	0.20	0.20	0.27	0.17
	Security Program Management (CISO)	0.27	0.05	0.13	0.20	0.19	0.26	0.30	0.27	0.27	0.35	0.21
	Strategic Planning and Policy Development	0.28	0.00	0.24	0.24	0.30	0.21	0.25	0.28	0.28	0.33	0.22
Protect and Defend	Computer Network Defense Analysis	0.17	0.05	0.08	0.39	0.19	0.36	0.35	0.22	0.27	0.44	0.24
	Computer Network Defense Infrast. Support	0.15	0.07	0.05	0.29	0.24	0.26	0.20	0.21	0.21	0.29	0. 8
	Incident Response	0.21	0.13	0.07	0.19	0.25	0.28	0.20	0.31	0.31	0.33	0.21
	Vulnerability Assessment and Management	0.22	0.08	0.11	0.25	0.14	0.22	0.26	0.22	0.22	0.33	0.19
Securely Provision	Information Assurance Compliance	0.25	0.00	0.28	0.22	0.22	0.19	0.23	0.19	0.25	0.35	0.19
	Software Assurance and Security Engineering	0.19	0.00	0.03	0.21	0.17	0.31	0.30	0.19	0.19	0.32	0.17
	Systems Development	0.21	0.00	0.12	0.26	0.13	0.24	0.27	0.14	0.21	0.27	0. 6
	Systems Requirements Planning	0.25	0.00	0.14	0.19	0.12	0.24	0.24	0.13	0.13	0.33	0.15
	Systems Security Architecture	0.16	0.00	0.06	0.19	0.11	0.20	0.23	0.13	0.16	0.28	0.14
	Technology Research and Development	0.16	0.05	0.08	0.28	0.19	0.21	0.24	0.26	0.16	0.31	0.19
	Test and Evaluation	0.25	0.00	0.06	0.08	0.15	0.18	0.17	0.18	0.18	0.25	0.15
	Maximum similarity per Master	0.35	0.25	0.28	0.39	0.30	0.36	0.35	0.31	0.31		
	Mean similarity per Master	0.20	0.04	0.11	0.21	0.17	0.21	0.22	0.17	0.18		

Category	Specialty Area (SA)	M19	M20	M21	M22	M23	M24	M25	Maximum similarity per SA	Mean similarity per SA
Investigate	Digital Forensics	0.32	0.09	0.18	0.14	0.09	0.36	0.32	0.44	0.25
	Investigation	0.00	0.07	0.10	0.00	0.00	0.14	0.00	0.30	0.14
Operate and Maintain	Customer Service and Technical Support	0.10	0.13	0.13	0.06	0.13	0.04	0.13	0.24	0.09
	Data Administration	0.05	0.06	0.00	0.06	0.00	0.04	0.09	0.25	0.07
	Knowledge Management	0.11	0.07	0.04	0.07	0.07	0.19	0.09	0.22	0.09
	Network Services	0.23	0.15	0.11	0.10	0.16	0.14	0.24	0.25	0.15
	System Administration	0.16	0.09	0.14	0.04	0.09	0.17	0.32	0.32	0.14
	Systems Security Analysis	0.16	0.10	0.21	0.14	0.10	0.24	0.24	0.34	0. 8
Oversight and Development	Education and Training	0.10	0.00	0.04	0.00	0.06	0.23	0.18	0.25	0.11
	Information Systems Security Operations (ISSO)	0.17	0.20	0.33	0.14	0.21	0.18	0.28	0.35	0.17
	Legal Advice and Advocacy	0.12	0.07	0.15	0.15	0.08	0.20	0.15	0.27	0.17
	Security Program Management (CISO)	0.21	0.09	0.22	0.14	0.14	0.31	0.32	0.35	0.21
	Strategic Planning and Policy Development	0.20	0.18	0.22	0.18	0.19	0.26	0.33	0.33	0.22
Protect and Defend	Computer Network Defense Analysis	0.32	0.04	0.14	0.09	0.09	0.36	0.44	0.44	0.24
	Computer Network Defense Infrast. Support	0.26	0.11	0.17	0.11	0.12	0.21	0.27	0.29	0. 8
	Incident Response	0.29	0.08	0.22	0.08	0.18	0.28	0.22	0.33	0.21
	Vulnerability Assessment and Management	0.15	0.06	0.23	0.06	0.13	0.33	0.23	0.33	0.19
Securely Provision	Information Assurance Compliance	0.18	0.22	0.30	0.16	0.24	0.35	0.25	0.35	0.19
	Software Assurance and Security Engineering	0.22	0.12	0.32	0.16	0.12	0.27	0.28	0.32	0.17
	Systems Development	0.14	0.12	0.25	0.12	0.13	0.24	0.25	0.27	0. 6
	Systems Requirements Planning	0.16	0.10	0.25	0.10	0.15	0.17	0.33	0.33	0.15
	Systems Security Architecture	0.16	0.10	0.14	0.14	0.10	0.24	0.28	0.28	0.14
	Technology Research and Development	0.15	0.04	0.17	0.13	0.09	0.30	0.31	0.31	0.19
	Test and Evaluation	0.17	0.21	0.19	0.21	0.23	0.24	0.25	0.25	0.15
	Maximum similarity per Master	0.32	0.22	0.33	0.21	0.24	0.36	0.44		
	Mean similarity per Master	0.17	0.10	0.18	0.11	0.12	0.23	0.24		

Fig. 4: Similarities between Spanish cybersecurity Master's programs listed in Table I and US NICE WF's Specialty Areas.