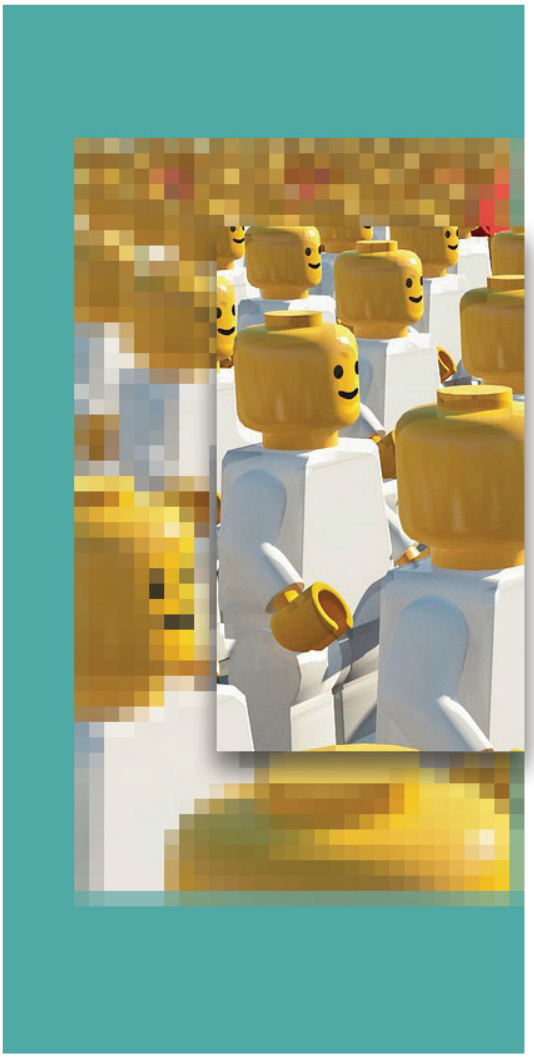
PIXEL BIT

Nº 63 ENERO 2022
CUATRIMESTRAL
e-ISSN:2171-7966
ISSN:1133-8482

Revista de Medios y Educación



PIXEL-BIT

REVISTA DE MEDIOS Y EDUCACIÓN

Nº 63 - ENERO - 2022

https://revistapixelbit.com

Pixel-Bit. Revista de Medios y Educación. 2022 - ISSN: 1133-8482. e-ISSN: 2171-7966.

EDITORIAL
UNIVERSIDAD DE SEVILLA

PIXEL-BIT
REVISTA DE MEDIOS Y EDUCACIÓN
ENERO 2022

Nº 63

Pixel-Bit. Revista de Medios y Educación. 2022 - ISSN: 1133-8482. e-ISSN: 2171-7966.

Pixel-Bit. Revista de Medios y Educación. 2022 - ISSN: 1133-8482. e-ISSN: 2171-7966.

FACTOR DE IMPACTO (IMPACT FACTOR)

SCOPUS (CiteScore Tracker 2021: 3.0) - Journal Citation Indicator (JCI). Posición 400 de 722 revistas Puntuación: 44.67 (Q3) - FECYT: Ciencias de la Educación. Cuartil 2. Posición 16. Puntuación: 39,80- DIALNET MÉTRICAS (Factor impacto 2019: 1,355. Q1 Educación. Posición 11 de 2228) - REDIB Calificación Glogal: 29,102 (71/1.119) Percentil del Factor de Impacto Normalizado: 95,455- ERIH PLUS - Clasificación CIRC: B- Categoría ANEP: B - CARHUS (+2018): B - MIAR (ICDS 2020): 9,9 - Google Scholar (global): h5: 42; Mediana: 42 - Journal Scholar Metric Q2 Educación. Actualización 2016 Posición: 405ª de 1,115- Criterios ANECA: 20 de 21 - INDEX COPERNICUS Puntuación ICV 2019: 95.10

Píxel-Bit, Revista de Medios y Educación está indexada entre otras bases en: SCOPUS, Fecyt, DOAJ, Iresie, ISOC (CSIC/CINDOC), DICE, MIAR, IN-RECS, RESH, Ulrich's Periodicals, Catálogo Latindex, Biné-EDUSOL, Dialnet, Redinet, OEI, DOCE, Scribd, Redalyc, Red Iberoamericana de Revistas de Comunicación y Cultura, Gage Cengage Learning, Centro de Documentación del Observatorio de la Infancia en Andalucía. Además de estar presente en portales especializados, Buscadores Científicos y Catálogos de Bibliotecas de reconocido prestigio, y pendiente de evaluación en otras bases de datos.

EDITA (PUBLISHED BY)

Grupo de Investigación Didáctica (HUM-390). Universidad de Sevilla (España). Facultad de Ciencias de la Educación. Departamento de Didáctica y Organización Educativa. C/ Pirotecnia s/n, 41013 Sevilla.
Dirección de correo electrónico: revistapixelbit@us.es . URL: https://revistapixelbit.com/
ISSN: 1133-8482; e-ISSN: 2171-7966; Depósito Legal: SE-1725-02
Formato de la revista: 16,5 x 23,0 cm

PIXEL-BIT
REVISTA DE MEDIOS Y EDUCACIÓN

índice

Nº 63
ENERO 2022

Pixel-Bit. Revista de Medios y Educación. 2022 - ISSN: 1133-8482. e-ISSN: 2171-7966.

PIXEL-BIT
e-ISSN: 2171-7966
REVISTA DE MEDIOS Y EDUCACIÓN
MEDIA & EDUCATION JOURNAL

Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura

Competency-based cybersecurity training and awareness: a systematic literature review

D. Josu Mendivil Caldentey
Titulado Superior. Universidad de Deusto. España

Dr. Borja Sanz Urquijo
Profesor Asociado. Universidad de Deusto. España

Dra. Miren Gutierrez Almazor
Profesora Contratad Doctora. Universidad de Deusto. España

Recibido: 2021/09/14; **Revisado:** 2021/10/16; **Aceptado:** 2021/12/10; **Preprint:** 2021/12/21; **Publicado:** 2022/01/07

RESUMEN

La capacidad de una organización para hacer frente a las amenazas y vulnerabilidades depende en gran medida de los niveles de formación y concienciación en ciberseguridad de su personal, y en consecuencia, de la existencia de un marco de competencias que identifique los contenidos y niveles de formación y concienciación necesarios para cada puesto de trabajo.
Este artículo lleva a cabo una revisión sistemática de la literatura con el objetivo de explorar el uso de modelos de competencias en la elaboración de programas de formación y concienciación en ciberseguridad dirigidos al personal no técnico de las organizaciones.
El examen de la literatura muestra que, aunque existe un elevado número de estudios que abordan la formación y concienciación en ciberseguridad, las investigaciones relacionadas con modelos de competencias para el personal no especializado son significativamente escasas, las metodologías no han evolucionado de manera relevante, y los escasos modelos competenciales propuestos incorporan de forma limitada perfiles laborales.
Como resultado, y con el objetivo de avanzar en el conocimiento en este campo, este artículo propone la elaboración de un modelo basado en competencias para el personal no TIC que permita la configuración de planes de formación y concienciación por perfiles laborales, incorporando de este modo las necesarias competencias en ciberseguridad.

ABSTRACT

The ability of an organization to face threats and to overcome vulnerabilities in cybersecurity depends to a large extent on the level of training and awareness of its personnel and consequently on the existence of a competency framework that identifies the indicators in training awareness required for each job.
This article makes a systematic review of the literature to explore the use of competency models when developing training and awareness programs in cybersecurity aimed at non-technical personnel in organizations.
An examination of the literature shows that, although there is a high number of studies that address cybersecurity training and awareness, research related to competency models for non-specialized personnel is significantly scarce, methodologies have not evolved significantly, and the few skills models available incorporate job profiles in a limited way.
As a result, and with the aim to advance the knowledge in this particular field, this article presents a model based on competencies for non-ICT personnel which includes the configuration of training and awareness plans according to job profiles, thus incorporating the necessary cybersecurity competencies.

PALABRAS CLAVES · KEYWORDS

Medida de seguridad; Formación; Investigación pedagógica; Competencia profesional; Normalización
Safety; Professional training; Educational research; Skills development; Standardization

1. Introducción

Las economías, las organizaciones, las empresas, el mundo físico e incluso las relaciones personales son cada vez más digitales. Gran parte de las actividades, tanto humanas como no humanas, se transforman en datos para su posterior análisis, en un proceso que Viktor Mayer-Schoenberger y Kenneth Cukier han denominado datificación (Mayer-Schönberger & Cukier, 2013). Las actuales tecnologías de la información y comunicación (TIC), se han introducido en todos los ámbitos de nuestras sociedades occidentales, modificando nuestra forma de producir, trabajar, estudiar, consumir o socializar.

En el ámbito empresarial, la aparición de plataformas como Google, Amazon o Facebook, de alcance global y basadas en las TIC, facilitan la conversión de procesos y la creación de modelos de negocio disruptivos, provocando una profunda transformación en las organizaciones. La industria, a través de la digitalización y la interconexión de los procesos productivos, la gestión online de la producción y la aplicación de inteligencia no sólo a los procesos, sino también a los productos, está inmersa desde comienzos de este siglo en lo que se conoce como la cuarta revolución industrial (Schwab, 2016).

Desde su inicio a finales de los años ochenta del siglo pasado, el crecimiento de la industria TIC es constante, con expectativas de que este crecimiento continúe (IDC, 2019). En el caso de España, la cifra de negocio de las empresas del sector TIC español no ha dejado de aumentar desde el año 2014, situándose en el año 2019 en los 95.473 millones de euros, presentando un crecimiento respecto al año 2018 de un 3,9% (ONTSI, 2020).

Este auge presenta sin embargo puntos débiles. El avance tecnológico no ha venido acompañado de un progreso similar en el ámbito de la ciberseguridad. En una sociedad que proclama que su recurso más valioso ya no es el petróleo sino los datos (The Economist, 2017), estos se encuentren expuestos a cada vez mayores riesgos (Haqaf & Koyuncu, 2018).

El primer ciberataque considerado global ocurrió en mayo de 2017. Más de 230.000 ordenadores en todo el mundo sufrieron el ataque de un ransomware conocido como WannaCry. Apenas un mes más tarde se produjo un nuevo ataque, en esta ocasión con una variante denominada Petya, más sofisticada y dañina (Lozano, 2017).

Desde entonces, los ataques contra empresas e instituciones, tanto en España como en el resto del mundo se han sucedido de manera regular y sin interrupción. Todos los medios de comunicación generalistas han informado de manera exhaustiva sobre los ataques sufridos por la Cadena SER, otras emisoras de Prisa Radio o la consultora Everis en el año 2019, la aseguradora Mapfre o el Administrador de Infraestructuras Ferroviarias, Adif, en el año 2020, o el Servicio Público Estatal de Empleo y el Instituto Nacional de Estadística en el año 2021, por señalar algunos de ellos. Fuera de España, aún perdura el recuerdo del ciberataque al oleoducto de la empresa Colonial en Estados Unidos. El hecho de que algunas de las víctimas de estos ataques sean medios informativos, organismos públicos o infraestructuras críticas no ha hecho sino incrementar su notoriedad (e.g., Sanchez-Vallejo, 2021; Muñoz, 2021).

En España, el CCN-CERT recoge, en su informe Ciberamenazas y Tendencias 2020, el constante incremento de los incidentes de seguridad. Tan sólo en el año 2019, este organismo gestionó 42.997 ciberincidentes, lo que representa un 11 % de incremento con respecto al año anterior (CCNCERT, 2020).

A las amenazas externas se deben añadir las amenazas internas, consideradas como uno de los mayores problemas no resueltos de seguridad de la información (Bailey et al., 2018). En el citado informe del CCN-CERT, se señala que en el año 2019 se produjo un incremento de aproximadamente un 28% de incidentes relacionados con actividades llevadas a cabo por empleados. La mayor parte de estos incidentes están ligados no a una intención dañina por parte de las personas que trabajan en una organización, sino a errores y a la falta de formación y concienciación adecuadas.

A este respecto, el IBM X-Force Research, uno de los equipos de investigación en seguridad de la información más prestigiosos del mundo, señala que los incidentes de seguridad debidos a errores no intencionados representaron más del 20 por ciento de los incidentes de seguridad reportados públicamente. Y lo que resulta más grave, el mismo informe indica que más de un tercio de la actividad involuntaria llevada a cabo por los clientes monitorizados por este equipo fue debida a ataques cuyo objetivo era engañar a los usuarios y usuarias para que accedieran a un enlace o abrieran un archivo adjunto (IBM, 2018). La compañía aseguradora Hiscox, en su "Informe Siniestros 2020" presenta datos más preocupantes. De acuerdo con este informe, El 55% de las reclamaciones de ciberseguridad cursadas por esta compañía en el año 2020 se debieron a accidentes o errores humanos, mientras que el 39% de los siniestros gestionados fueron debidos a ataques basados en ingeniería social (Hiscox, 2020).

El coste económico real de todas estas amenazas, tanto por su repercusión directa como por el esfuerzo de protección al que obligan, y los costes ocultos asociados a la pérdida de oportunidades o de confianza, es imposible de calcular. Existen algunas estimaciones que calculan el coste acumulado global desde el año 2018 hasta la actualidad, derivado de los delitos cibernéticos, en unos 800,000,000,000 de euros (Malekos & Lostri, 2020).

Más allá de estimaciones, el "Internet Crime Complaint Center" (IC3, 2020), en el año 2020 gestionó más de 700,000 incidencias sólo en Estados Unidos, con unas pérdidas reales de más de 3,500,000,000 de euros.

Esta realidad explica que la ciberseguridad se haya convertido en los últimos años en uno de los campos de estudio e investigación más relevantes en el ámbito de las TIC. El Foro Económico Mundial en su informe anual "The Global Risks Report 2021" sitúa, un año más, a los ciberataques entre los principales riesgos globales percibidos (WEF, 2021). Esta preocupación puede constatarse, tal y como muestra la Figura 1, en el constante incremento en los últimos diez años del número de búsquedas en todo el mundo del término "cybersecurity" en el buscador de Google.

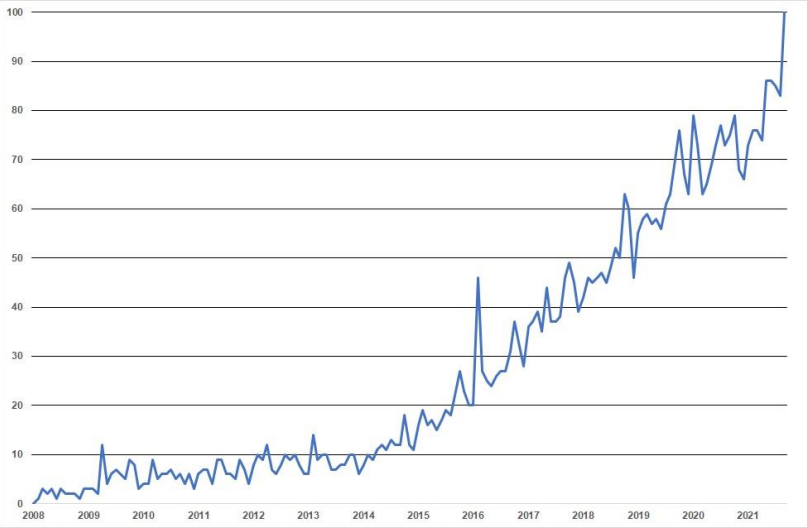
Pero esta preocupación e interés no se limita al ámbito tecnológico. La seguridad está conformada por la tecnología, pero también por las políticas y procedimientos de una organización y por las personas que trabajan o se relacionan con ellas (Calder, 2016; Eloff & Eloff, 2005). Estos tres componentes, tecnología, políticas y personas, mantienen una estrecha relación e influencia entre sí, siendo por tanto necesaria su participación coordinada para una asegurar una adecuada gestión de la seguridad de la información en general y de la ciberseguridad en particular.

En uno de los documentos considerados fundacionales sobre seguridad TIC, "The Protection of Information in Computer Systems", Jerome Saltzer y Michael Schroeder ya incluían entre los principios de diseño que deben aplicarse para establecer mecanismos de

protección que estos debían ser “psicológicamente aceptables” para el usuario, de manera que puedan ser aplicados de forma rutinaria y automática, y por ello correcta. Afirmaban que “en la medida en que la imagen mental que tiene el usuario sobre las medidas de protección coincida con los mecanismos que debe utilizar, se minimizarán los errores” (Saltzer & Schroeder, 1975).

Figura 1

Evolución del número de búsquedas del término "cybersecurity"



En el año 2001, Maconachy et al. (Maconachy et al., 2001) ya definían a las personas como “el corazón y el alma de los sistemas seguros”, afirmando que las personas “requieren concienciación, alfabetización, capacitación y educación en prácticas sólidas de seguridad para que los sistemas estén protegidos”.

Este enfoque centrado en las personas está recibiendo en los últimos años un creciente reconocimiento. Las medidas técnicas por sí solas no van a resolver los actuales problemas de seguridad, siendo necesario que operen de manera coordinada con los usuarios de las empresas y organizaciones (ENISA, 2018; Aldawood & Skinner, 2018; Zhang-Kennedy & Chiasson, 2021). Abundando en esta idea, el CCN-CERT en su informe “Ciberamenazas y Tendencias 2019” alerta sobre la necesidad de esta formación, afirmando que “los seres humanos siguen siendo el eslabón débil en todos los sistemas de seguridad, por lo que, a medida que aumente la eficacia de las protecciones contra código dañino, los agentes de las amenazas modificarán su objetivo, atacando a las personas”.

Por ello, las empresas y organizaciones necesitan nuevas y eficientes iniciativas en el ámbito de la formación y concienciación en ciberseguridad, especialmente del personal no TIC, que se sumen al continuo desarrollo de tecnologías y procesos. A diferencia de los profesionales dedicados a las TIC en las empresas, los usuarios finales son uno de los eslabones más débiles de la cadena de seguridad, debido a sus limitados conocimientos y escasa concienciación (Carlton et al., 2019).

La capacidad de una organización para hacer frente a las amenazas y vulnerabilidades depende en gran medida de la actitud y la aptitud en ciberseguridad de su personal no TIC, y en consecuencia, de la existencia de un marco adecuado de competencias que identifique los ítems y niveles de formación y concienciación necesarios para cada puesto de trabajo (Mendívil et al., 2021). Sin embargo, aunque existen numerosos estudios que en efecto señalan la importancia y necesidad de emplear la evaluación por competencias para garantizar la calidad de la formación y concienciación en ciberseguridad, (e.g., Brilingaite et al., 2020; Jacob et al., 2018; Mäses, 2020), la realidad parece señalar que no se llevan a cabo de manera generalizada políticas de formación y capacitación formalizadas basadas en un enfoque por competencias en ciberseguridad (Nielsen, 2017; PWC, 2020). Una realidad probablemente más acusada en el caso del personal no TIC de las organizaciones.

Ante este escenario, el presente estudio tiene como objetivo investigar en la literatura especializada el uso de modelos de competencias en la elaboración de programas de formación y concienciación en ciberseguridad dirigidos al personal no TIC de empresas y organizaciones. Con ello se pretende conocer el grado de madurez y las principales características de la formación y concienciación en ciberseguridad basada en competencias.

2. Metodología

Existen múltiples estudios secundarios que abordan diferentes aspectos relacionados con la ciberseguridad, (e.g., Ulven & Wangen, 2021; Ali et al., 2021; Rahim et al., 2015), pero no se han encontrado estudios recientes que analicen las actividades de formación y concienciación en ciberseguridad para empleados no TIC desde la perspectiva de las competencias.

Este artículo llena este hueco mediante el análisis de la producción científica a través de la revisión sistemática de la literatura (RSL), propuesta por (Kitchenham, 2004).

De acuerdo con esta metodología, los pasos que se van a llevar cabo son los siguientes:

a) Definir las preguntas de investigación.
b) Determinar las fuentes de datos.
c) Definir la estrategia de búsqueda.
d) Establecer los criterios de inclusión y exclusión.
e) Realizar el proceso de selección.
f) Presentar los resultados.

2.1. Preguntas de investigación

La RSL realizada tiene como objetivo el dar respuesta a las siguientes preguntas de investigación:

- PI1. ¿Cuál es la evolución en el número de publicaciones relacionadas con el uso de competencias en la formación y concienciación en materia de ciberseguridad para personal no TIC desde el año 2016 hasta la actualidad?
- PI2 ¿Cuáles son las metodologías que se utilizan para identificar las competencias en ciberseguridad?
- PI3. ¿Se identifican diferentes roles de acuerdo a las distintas necesidades en el ámbito de la ciberseguridad de los puestos de trabajo y responsabilidades de una organización?
- PI4: ¿Cuáles son los objetivos que se persiguen?

2.2. Selección de las bases de datos

El análisis de las bases de datos se llevó a cabo entre los meses de julio y agosto del año 2021. Después de un examen de las bases de datos existentes, se seleccionaron como fuentes de búsqueda de datos primarios IEEE Xplore, ACM Digital Library y SCOPUS.

IEEE Xplore es una base de datos de investigación académica que cuenta con una amplia literatura en el ámbito de las TIC. ACM Digital Library es la mayor base de datos existente especializada en informática y tecnologías de la información, y SCOPUS es una de las bases de datos con mayor número de resúmenes y citas de artículos de revistas científicas revisadas por pares. La selección de estas bases de datos, de gran prestigio y uso, ayudan a garantizar la calidad y fiabilidad de los estudios y artículos seleccionados.

2.3. Estrategia de búsqueda

Para las búsquedas se han utilizado los términos “formación“, “concienciación“, “ciberseguridad“ y “competencias“, algunos términos equivalentes, así como los conectores lógicos “Y“ y “O“, tanto en español como en inglés. La cadena de búsqueda inicial diseñada fue, para fuentes primarias en ingés:

(„cybersecurity“ OR „cyber security“ OR „computer security“ OR „IT Security“) AND „awareness“ AND „training“ AND („skills“ OR „competences“ OR „competencies“).

2.4. Criterios de inclusión y exclusión

Acotadas las bases de datos y definida la cadena general de búsqueda, se seleccionan los estudios primarios de acuerdo con los siguientes criterios.

Criterios de inclusión:

a) Estudios primarios que reporten iniciativas de investigación en el ámbito de formación y concienciación en ciberseguridad en empresas y organizaciones que utilicen marcos de competencias.

b) Las búsquedas se realizan en todo el texto del artículo, incluyendo el título, palabras clave y resumen.

c) Estudios primarios reportados tanto en idioma inglés como en español.

d) Estudios primarios reportados entre enero de 2016 y agosto de 2021.

e) Artículos de revistas o conferencias.

Criterios de exclusión:

a) Artículos duplicados.

b) Artículos cuyo contenido completo no sea accesible.

c) Artículos que hagan referencia a formación en ciberseguridad, pero no relacionada con el uso de competencias.

d) Artículos sobre formación y concienciación en ciberseguridad pero que no están orientados al personal no TIC de empresas y organizaciones.

2.5. Proceso de selección

En esta fase se ejecuta la cadena de búsqueda en las bases de datos seleccionadas, ajustando la cadena a la sintaxis de cada base de datos, considerando los criterios de inclusión.

A continuación se señalan las cadenas utilizadas para las búsquedas en inglés:

IEEE: (((„Full Text Only“:“cybersecurity“ OR „cyber security“ OR „computer security“ OR „IT Security“) AND „Full Text Only“:“awareness“ AND „Full Text Only“:“training“ AND („Full Text Only“:“skills“ OR „Full Text Only“:“competences“ OR „competencies“)))

Filters Applied: Conferences. Journals. 2016 – 2021.

ACM: [[All: „cybersecurity“] OR [All: „cyber security“] OR [All: „computer security“] OR [All: „it security“]] AND [All: awareness] AND [All: training] AND [All: skills OR competences OR competencies] AND [Publication Date: (01/01/2016 TO 08/31/2021)]

SCOPUS: TITLE-ABS-KEY („cybersecurity“ OR „cyber security“ OR „computer security“ OR „IT Security“) AND „awareness“ AND „training“ AND („skills“ OR „competencies“ OR „competences“) AND (LIMIT-TO (DOCTYPE,“cp“) OR LIMIT-TO (DOCTYPE,“ar“)) AND (LIMIT-TO (PUBYEAR,2021) OR LIMIT-TO (PUBYEAR,2020) OR LIMIT-TO (PUBYEAR,2019) OR LIMIT-TO (PUBYEAR,2018) OR LIMIT-TO (PUBYEAR,2017) OR LIMIT-TO (PUBYEAR,2016)) AND (LIMIT-TO (LANGUAGE, „English“) OR LIMIT-TO (LANGUAGE,“Spanish“))

Las búsquedas llevadas a cabo dieron como resultado 1,300 artículos. A continuación se llevó a cabo una primera selección, revisando los títulos, abstracts y, en caso necesario leyendo los artículos completos, con el objetivo tanto de comprobar si la información estaba relacionada con el objeto de estudio como de evaluar si se cumplían los criterios de exclusión. En este primer proceso de selección se recopilaron 49 artículos.

Los artículos seleccionados fueron sometidos a un segundo examen más detallado. Fueron leídos, analizados y evaluados, cumpliendo todos los criterios de selección únicamente 10 de ellos. En esta fase se utilizaron como criterios de selección:

a) La formación y concienciación en ciberseguridad debe tener un alcance global, y no estar limitada a un área específica, como por ejemplo el ransomware, el phising, la telefonía móvil o la gamificación.

b) Debe estar diseñada para los trabajadores y trabajadoras no TIC de las empresas y organizaciones.

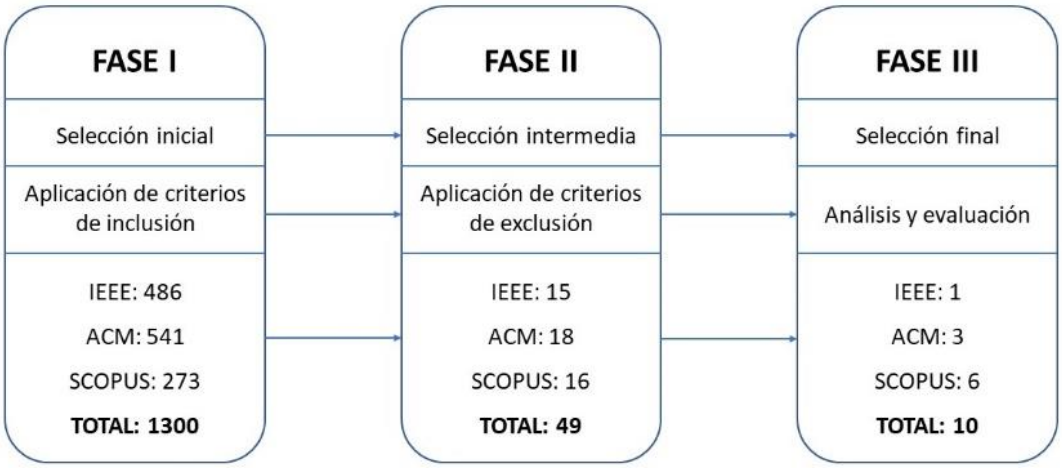
c) La identificación de las competencias tiene que ser un elemento central en la definición de las actividades de formación y concienciacion.

d) La investigación debe centrarse en la selección y diseño de los contenidos, y no en las metodologías de impartición, modelos de medición o aspectos pedagógicos.

La Figura 2 muestra de forma gráfica el proceso de selección llevado a cabo y los resultados obtenidos.

Figura 2

Proceso de selección de estudios primarios



Tal y como puede apreciarse en la Figura 2, la selección final está compuesta por un artículo de IEEE Explore, tres artículos de ACM Digital Library y seis artículos de SCOPUS, que ayudan a responder a las preguntas de investigación. La Tabla 1 recoge el detalle de los estudios concretos seleccionados.

Tabla 1

Estudios seleccionados

Código	Referencia	Título	Base de datos
C01	(Bada & Nurse, 2019)	Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs).	SCOPUS
C02	(Ani et al., 2019)	Human factor security: evaluating the cybersecurity capacity of the industrial workforce.	SCOPUS
C03	(Carlton et al., 2019)	Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills.	SCOPUS
C04	(Hatzivasilis et al., 2020)	Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees.	SCOPUS
C05	(Sithole et al., 2020)	A framework for a foundational cyber counter-intelligence awareness and skills training programme.	SCOPUS
C06	(Trim & Lee, 2021)	The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement.	SCOPUS
C07	(Wang, 2018)	Framework of Raising Cyber Security Awareness.	IEEE
C08	(Khan, 2019)	viCyber: An Intelligent Curriculum Design Tool for Cybersecurity Education.	ACM
C09	(Remmele & Peichl, 2021)	Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro- and Small Enterprises.	ACM
C10	(Vicente, 2021)	GEIGER: Solution for small businesses to protect themselves against cyber-threats	ACM

3. Análisis y resultados

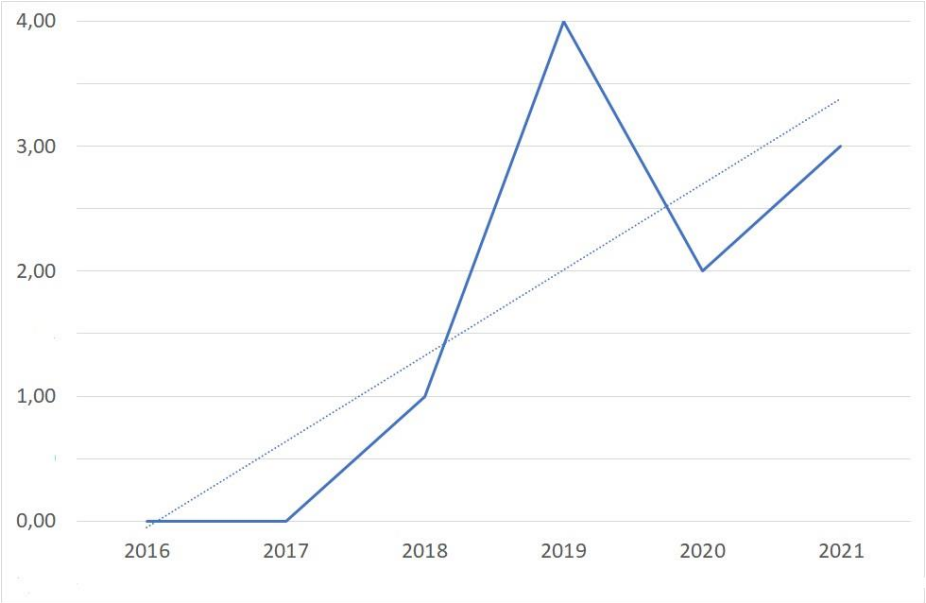
Con la información recogida en estos artículos pueden darse respuesta a las preguntas de investigación planteadas.

- **PI1. ¿Cuál es la evolución en el número de publicaciones relacionadas con el uso de competencias en la formación y concienciación en materia de ciberseguridad para personal no TIC desde el año 2016 hasta la actualidad?**

Una vez señalada la importancia y necesidad de trabajar la formación y concienciación dirigida al personal no TIC en el ámbito de la ciberseguridad utilizando modelos basados en competencias, el aspecto tal vez más destacado, y una aportación relevante de esta investigación, es la constatación del escaso número de artículos que contemplan el uso de marcos de competencia a la hora de abordar la formación y concienciación del personal no TIC de empresas y organizaciones. Pese a este limitado número de publicaciones y estudios que cumplen los criterios de selección, la evolución en su número muestra una clara línea ascendente, tal y como refleja la Figura 3, lo que permite apuntar un interés creciente.

Figura 3

Número de publicaciones por año y tendencia



Fuente: Elaboración propia

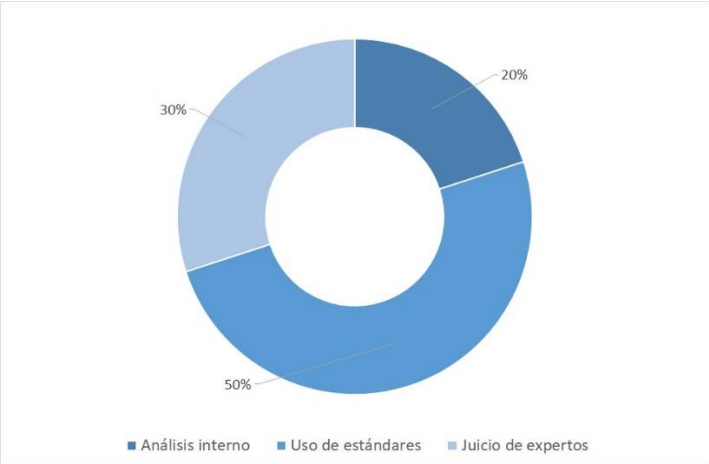
- **PI2 ¿Cuáles son las metodologías que se utilizan para identificar las competencias en ciberseguridad?**

Los artículos analizados se han agrupado en tres grandes grupos, de acuerdo con las metodologías empleadas en la identificación de las competencias o conocimientos que deben alcanzar los trabajadores no TIC. En primer lugar se han agrupado las investigaciones que emplean estándares internacionales de seguridad de la información como referencia. En segundo lugar, los estudios que proponen marcos de formación y concienciación basados en la realización de análisis internos *ad hoc* en las empresas y organizaciones, y finalmente, aquellos que emplean como metodología de trabajo el juicio de expertos, tanto mediante la realización de entrevistas como empleando el método Delphi.

Como se puede apreciar en la Figura 4, el uso de estándares de seguridad para la identificación de competencias en ciberseguridad para empleados no TIC es la metodología más empleada. La Tabla 2 muestra los estándares tomados como referencia. Se utilizaron el Programa sobre formación y concienciación en ciberseguridad de la London Digital Security Centre (LDSC), la serie de publicaciones NIST 800 sobre seguridad y privacidad para organizaciones y sistemas de información del Instituto Nacional de Estándares y Tecnología (NIST) del gobierno de los Estados Unidos, el Marco de trabajo para la Educación en Ciberseguridad (NICE), recogido en la publicación NIST 800-181, y finalmente el programa GEIGER de Aprendizaje estándar en ciberseguridad, desarrollado por un consorcio de empresas y organizaciones del ámbito de la ciberseguridad con fondos del programa Horizonte 2020 de la Unión Europea.

Figura 4

Distribución de las metodologías empleadas



Fuente: Elaboración propia

La segunda metodología empleada ha sido el análisis de las necesidades de formación y concienciación en materia de ciberseguridad de una empresa u organización específica, y la posterior configuración de un programa de formación y concienciación a medida.

Tabla 2

Estándares empleados y frecuencia

Estándar	Organismo	Estudio Primario
Programa sobre formación y concienciación en ciberseguridad.	LDSC	[C01]
NIST 800	NIST	[C07]
NIST 800 -181 – NICE	NIST	[C08]
GEIGER	Consorcio / ENISA	[C09], [C10]

La tercera metodología empleada es el uso del juicio de expertos para, a partir del mismo, definir y establecer un modelo de formación y concienciación en ciberseguridad.

- **PI3. ¿Se identifican diferentes roles de acuerdo a las distintas necesidades en el ámbito de la ciberseguridad de los puestos de trabajo y responsabilidades de una organización?**

Tan sólo en uno de los estudios analizados plantea la necesidad de establecer diferentes contenidos y niveles de formación y concienciación de acuerdo con el sector industrial, el perfil laboral y el puesto de trabajo específico del personal. En otros dos artículos se utiliza el concepto de “nivel“ para establecer diferentes grados de formación

para el personal no TIC, aunque estos niveles no se encuentran relacionados directamente a perfiles laborales. En el resto de publicaciones no se hacen referencia a estos perfiles, considerando por ello que las necesidades de formación y concienciación en ciberseguridad son iguales para todo el personal usuario de las TIC en una organización.

- **PI4: ¿Cuáles son los objetivos que se persiguen?**

Todos los estudios analizados tienen como objetivo principal el proponer un programa de formación y concienciación en materia de ciberseguridad dirigido a personal laboral no TIC. Aunque en todos ellos se consideran las competencias, los enfoques varían. En la Tabla 3 se presentan los diferentes enfoques de los estudios analizados. La mitad de las investigaciones se orientan a los aspectos educativos, pedagógicos o de diseño de los modelos propuestos, tres artículos hacen énfasis en la medición de las capacidades y conocimientos de los empleados sobre aspectos de ciberseguridad, y finalmente otros estudios se enfocan en la contrainteligencia o en el incremento de la resiliencia.

Tabla 3

Objetivos

Objetivos	Estudio Primario
Aspectos educativos, pedagógicos o de diseño del marco propuesto	[C01], [C04], [C08], [C09], [C10]
Medición de capacidades y conocimientos	[C02], [C03], [C07],
Enfoque de contrainteligencia	[C05]
Incremento de la resiliencia	[C06]

4. Discusión

La ciberseguridad se ha convertido en una de las áreas de las TIC que mayor atención y esfuerzo ha recibido en los últimos años, debido tanto a la necesidad de dar respuesta al constante crecimiento y sofisticación de los ataques y riesgos a los que se enfrenta la sociedad, como al desarrollo incesante de la propia tecnología. En este entorno, en el que el factor humano es un aspecto crucial, las actividades de formación y concienciación en ciberseguridad son elementos críticos, en los que se debe profundizar, actualizar y mejorar de manera constante.

Del análisis de fuentes primarias realizado en este estudio y de los resultados obtenidos pueden extraerse como características relevantes para el propósito de este trabajo:

Primero: existe un elevado número de artículos y estudios que abordan de maneras muy diversas la formación y concienciación en ciberseguridad desde un punto de vista competencial, lo que demuestra el interés que suscita la materia. Sin embargo, los estudios relacionados de manera específica con la identificación y creación de modelos de competencias para trabajadores no TIC es significativamente bajo. Esta escasez de estudios evidencia una carencia que debiera ser corregida, y al mismo tiempo constata lo

señalado con anterioridad; aunque se reconoce la importancia y necesidad de trabajar la formación y concienciación en el ámbito de la ciberseguridad mediante un enfoque basado en competencias, la realidad es que su grado de desarrollo es testimonial. Se necesitan nuevos estudios que amplien y mejoren el actual estado del arte en la materia con propuestas metodológicas que faciliten la creación de marcos de competencias ajustados a las necesidades de las organizaciones y que permitan identificar los contenidos y niveles de formación y concienciación necesarios para cada perfil laboral y puesto de trabajo.

Segundo: el número de estudios analizados que contemplan de manera explícita el uso de perfiles laborales a la hora de definir los contenidos de los planes de formación y concienciación es prácticamente nulo. Sin embargo, los distintos roles profesionales que existen en las empresas y organizaciones requieren actividades de formación y concienciación específicas y adecuadas a sus diversos desempeños y niveles de responsabilidad. No atender estas diferencias impide a las organizaciones alcanzar el nivel adecuado de formación y concienciación en ciberseguridad de su personal, lo que conlleva un problema de seguridad.

Tercero: la investigación llevada a cabo demuestra que las metodologías que se emplean en la confección de programas de formación y concienciación se siguen basando en los tres enfoques clásicos: estándares de seguridad, análisis internos *ad hoc* y juicios de expertos. Estos enfoques sin duda han demostrado su validez, pero también presentan limitaciones. En efecto, la aplicación de estándares sin una adaptación y adecuación a las distintas necesidades de cada perfil laboral puede dar como resultado un modelo de carácter excesivamente generalista, y que en consecuencia no satisfaga las exigencias reales en el ámbito de la ciberseguridad de muchos puestos de trabajo. El uso de programas de formación y concienciación basados en la definición de contenidos determinados por juicios de expertos adolece de la misma limitación. Por otro lado, los análisis y desarrollos internos, construidos a medida y desde cero, se ajustan sin duda a las necesidades de la empresa u organización analizada, pero llevan aparejados un nivel de esfuerzo y coste en tiempo, recursos humanos y económicos, que son soluciones tan sólo al alcance de un limitado número de organizaciones. Y sus resultados no pueden extrapolarse o ser utilizados por otras organizaciones, al ser desarrollados para dar respuesta específica al alcance y entorno definidos. Sin embargo, y pese a estas limitaciones, tal y como se comprueba en este estudio, no existen propuestas alternativas que planteen nuevos enfoques o mejoras a estos modelos.

5. Conclusiones

El estudio llevado a cabo en este trabajo permite concluir que el nivel de madurez en las actividades de formación y concienciación en ciberseguridad basada en competencias para el personal no TIC es, pese a su relevancia, muy escaso. Siendo en líneas generales un importante campo de investigación en el ámbito del personal TIC, el uso de marcos de competencias asociados a roles laborales para personal no TIC sin embargo no presenta el mismo grado de desarrollo.

También puede constatarse que los escasos estudios que abordan la materia se siguen basando en metodologías que no parecen haber sido revisadas ni actualizadas.

Existe por ello un importante ámbito de mejora orientado a la elaboración de nuevas propuestas que investiguen modelos de referencia estándar basados en competencias para

el personal no TIC. Estos modelos deberán facilitar la configuración o validación de planes de formación y concienciación definidos y ajustados a roles y perfiles laborales, permitiendo de este modo la incorporación al mapa general de competencias laborales de las empresas y organizaciones las competencias en ciberseguridad, otorgándoles de este modo su necesaria visibilidad y consideración.

Competency-based cybersecurity training and awareness: a systematic literature review

1. Introduction

Economies, organizations, companies, the physical world, and even personal relationships are becoming increasingly digital. Many activities, both human and non-human, are transformed into data for later analysis, in a process that Viktor Mayer-Schoenberger and Kenneth Cukier have called datafication (Mayer-Schönberger & Cukier, 2013). The current information and communication technologies (ICT) have been introduced in all areas of our western societies, modifying our way of producing, working, studying, consuming and socializing.

In the business field, the emergence of platforms such as Google, Amazon or Facebook, characterized by global reach and ICT-based facilitate the conversion processes and the creation of disruptive business models, causing a profound transformation in organizations. The industry, through digitization and interconnection of production operations, online management of production, and application of intelligence not only to processes but also to products, has been immersed since the beginning of this century in what is known as the fourth industrial revolution (Schwab, 2016).

Since its inception at the end of the 1980s, the growth of the ICT industry has been steady, with expectations that this growth will continue in the future (IDC, 2019). In the case of Spain, the turnover of companies in the Spanish ICT sector has been constantly rising since 2014, standing in 2019 at 95,473 million euros and registering a 3, 9% growth compared to 2018 (ONTSI, 2020).

However, this boom has its weaknesses. Technological advance has not been accompanied by similar progress in cybersecurity. In a society that proclaims that its most valuable resource is no longer oil but data (The Economist, 2017), data are exposed to increasing risks (Haqaf & Koyuncu, 2018).

The first cyber attack regarded as global took place in May 2017. More than 230,000 computers around the world were attacked by a ransomware known as WannaCry. Just a month later, a new attack occurred, this time with a variant called Petya, more sophisticated and harmful than the previous one (Lozano, 2017).

Since then, attacks against companies and institutions, both in Spain and in the rest of the world have occurred regularly and without interruption. Generalist media have exhaustively reported about the attacks on Radio Cadena SER, other Prisa Radio stations and the consulting firm Everis in 2019; insurer company Mapfre and Railway Infrastructure Administrator Adif in 2020; the Public State Employment Service and the National Institute of Statistics in the year 2021, to mention just a few. Outside of Spain, the memory of the cyberattack on the Colonial company's oil pipeline in the United States still persists. The fact that some of the victims of these attacks are the media, public organizations or critical infrastructures has only increased their notoriety (e.g., Sanchez-Vallejo, 2021; Muñoz, 2021).

In Spain, the CCN-CERT collects in its *Ciberamenazas y Tendencias 2020* (Cyber Threats and Trends) report the constant increase in security incidents. In the course of 2019

alone, this agency handled 42,997 cyber incidents, which represents an 11% increase over the previous year (CCNCERT, 2020).

To external threats internal threats must be added, regarded as one of the largest unsolved information security problems (Bailey et al., 2018). In the aforementioned CCN-CERT report, it is noted that in 2019 there was an increase of approximately 28% in incidents related to activities carried out by employees. Most of these incidents are not linked to harmful intent on the part of the people who work in an organization, but to mistakes and lack of adequate training and awareness.

In this regard, IBM X-Force Research, one of the world's most prestigious information security research teams, notes that security incidents due to unintentional errors account for more than 20 percent of publicly reported security incidents. And what is more serious, the same report indicates that more than a third of the involuntary activity carried out by the clients monitored by this team was due to attacks whose objective was to trick users into accessing a link or open an attachment (IBM, 2018). The insurance company Hiscox, in its *Claims Report 2020* presents even more worrying data.

According to this report, 55% of the cybersecurity claims filed by this company in 2020 were due to accidents or human errors, while 39% of the claims managed were due to attacks based on social engineering (Hiscox, 2020).

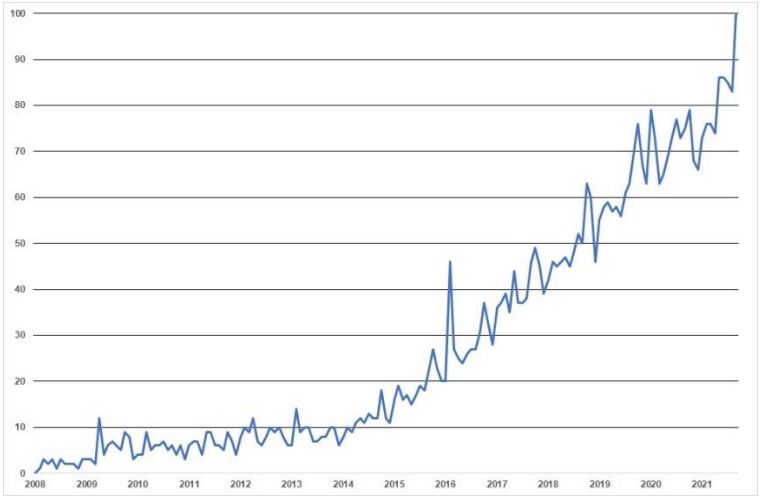
The real economic cost of all these threats, due to both their direct impact and the protection effort required, and to the hidden costs associated with the loss of opportunities and lack of trust, is impossible to calculate. There are some estimates that calculate the global accumulated cost from 2018 to the present derived from cyber crimes at about 800,000,000,000 euros (Malekos & Lostri, 2020).

Beyond estimates, the "Internet Crime Complaint Center" (IC3, 2020) managed more than 700,000 incidents in the United States alone in 2020, with real losses over 3,500,000,000 euros.

This situation explains why cybersecurity has become in recent years one of the most relevant fields of study and research in the field of ICT. The World Economic Forum in its annual report *The Global Risks Report 2021* places, once again, cyberattacks among the main perceived global risks (WEF, 2021). This concern can be seen, as shown in Figure 1, in the constant increase in the last ten years in the number of searches around the world for the term "cybersecurity" in the Google search engine.

Figure 1

Evolution of the number of searches for the term "cybersecurity"



Source: Elaboration by the authors

But such concern and interest are not limited to the technological field. Security is shaped by technology but also by the policies and procedures of an organization and by the people who work or interact with them (Calder, 2016; Eloff & Eloff, 2005). These three components, technology, policies and people, maintain a close relationship and influence each other; therefore their coordinated participation is necessary to ensure adequate management of information security in general and cybersecurity in particular.

In one of the documents deemed foundational on ICT security, *The Protection of Information in Computer Systems*, Jerome Saltzer and Michael Schroeder already included among the design principles that should be applied to establish protection mechanisms the fact that these should be "psychologically acceptable" for the user, so that they can be applied routinely and automatically, and therefore correctly. They affirmed that "to the extent that the mental image that the user has of the protection measures coincides with the mechanisms that he must use, errors will be minimized" (Saltzer & Schroeder, 1975).

In 2001, Maconachy et al. (Maconachy et al., 2001) already defined people as “the heart and soul of secure systems”, stating that people “require awareness, literacy, training and education in sound security practices for systems to be protected ".

This people-centered approach is receiving increasing recognition in recent years. Technical measures alone will not solve current security problems; it is necessary that they operate in a coordinated manner with users of companies and organizations (ENISA, 2018; Aldawood & Skinner, 2018; Zhang-Kennedy & Chiasson, 2021) . Expanding on this idea, the CCN-CERT in its report *Cyber threats and Trends 2019* warns about the need for this training, stating that "human beings continue to be the weak link in all security systems; therefore, as the effectiveness of the protections against malicious code increases, the agents of the threats will modify their target, attacking people.“ Thus, companies and organizations need new and efficient initiatives in the field of cybersecurity training and awareness, especially for non-ICT personnel, initiatives that can adapt to the continuous development of technologies and processes. Unlike professionals dedicated to ICT in

companies, end users are one of the weakest links in the security chain, due to both their limited knowledge and low awareness (Carlton et al., 2019).

The ability of an organization to face threats and vulnerabilities depends to a large extent on the cybersecurity attitude and aptitude of its non-ICT personnel, and consequently, on the existence of an adequate framework of competencies that identifies the items and levels of training and awareness necessary for each job (Mendívil et al., 2021). However, although there are numerous studies that point out the importance and need of using competency assessment to guarantee the quality of training and awareness in cybersecurity, (eg, Brilingaite et al., 2020; Jacob et al., 2018; Mäses, 2020), reality seems to indicate that formalized education and training policies based on a competency-based approach to cybersecurity are not widely implemented (Nielsen, 2017; PWC, 2020). A reality that is probably more prominent in the case of non-ICT staff in organizations.

Faced with this scenario, the present study aims to investigate in the specialized literature the use of competency models in the development of training and awareness programs in cybersecurity aimed at non-ICT personnel of companies and organizations. The objective is to explore the degree of maturity and the main characteristics of training and awareness in cybersecurity based on competencies.

2. Methodology

There are many sources that address different aspects related to cybersecurity, (eg, Ulven & Wangen, 2021; Ali et al., 2021; Rahim et al., 2015), but no recent studies have been found that analyze training activities and cybersecurity awareness for non-ICT employees from a competency perspective. This article fills that gap by analyzing scientific production through the systematic review of the literature (RSL) proposed by (Kitchenham, 2004).

According to this methodology, the steps to be carried out are the following:

a) Define the research questions.

b) Determine the data sources.

c) Define the search strategy.

d) Establish the inclusion and exclusion criteria.

e) Carry out the selection process.

f) Present the results.

2.1. Research questions

The objective of the RSL carried out is to answer the following research questions:

- RQ1. What is the evolution in the number of publications related to the use of competencies in cybersecurity training and awareness for non-ICT personnel from 2016 to the present?
- RQ2 What are the methodologies used to identify cybersecurity competencies?
- RQ3. Are different roles identified according to the different needs in the field of cybersecurity of the jobs and responsibilities of an organization?
- RQ4: What are the objectives pursued?

2.2. Database selection

The analysis of the databases was carried out between the months of July and August of the year 2021. After an examination of the existing databases, IEEE Xplore, ACM Digital Library and SCOPUS were selected as primary data search sources.

IEEE Xplore is an academic research database with extensive literature in the field of ICT. ACM Digital Library is the largest existing database specialized in computing and information technology, and SCOPUS is one of the databases with the highest number of abstracts and citations of articles in peer-reviewed scientific journals. The choice of these databases, of high prestige and use, guarantees the quality and reliability of the selected publications.

2.3. Search strategy

For the searches, the terms "training", "awareness", "cybersecurity" and "competencies" and some equivalent terms, as well as the logical connectors "AND" and "OR", both in Spanish and English, have been used. The initial search string designed was, for primary English sources:

(“cybersecurity” OR “cyber security” OR “computer security” OR “IT Security”) AND “awareness” AND “training” AND (“skills” OR “competencies” OR “competencies”)

2.4. Inclusion and exclusion criteria

Once the databases were limited and the general search chain defined, the primary studies were selected according to the following criteria:

Inclusion criteria:

a) Primary studies that report research initiatives in the field of cybersecurity training and awareness in companies and organizations that use competency frameworks.

b) Searches are carried out on the entire text of the article, including the title, keywords and abstract.

c) Primary studies reported in both English and Spanish.

d) Primary studies reported between January 2016 and August 2021.

e) Articles from magazines or conferences.

Exclusion criteria:

a) Duplicate articles.

b) Articles whose full content is not accessible.

c) Articles that refer to cybersecurity training, but not related to the use of skills.

d) Articles on training and awareness in cybersecurity which are not aimed at non-ICT personnel of companies and organizations.

2.5. Selection process

In this phase, the search string is executed in the selected databases, adjusting the string to the syntax of each database, considering the inclusion criteria.

The following are the strings used for English searches:

IEEE: (((“Full Text Only”:“cybersecurity” OR “cyber security” OR “computer security” OR “IT Security”) AND “Full Text Only”:“awareness” AND “Full Text Only”:“training” AND (“Full Text Only”:“skills” OR “Full Text Only”:“competencies” OR “competencies”)))

Filters Applied: Conferences. Journals. 2016 – 2021.

ACM: [[All: “cybersecurity”] OR [All: “cyber security”] OR [All: “computer security”] OR [All: “it security”]] AND [All: awareness] AND [All: training] AND [All: skills OR competencies OR competencies] AND [Publication Date: (01/01/2016 TO 08/31/2021)]

SCOPUS: TITLE-ABS-KEY (“cybersecurity” OR “cyber security” OR “computer security” OR “IT Security”) AND “awareness” AND “training” AND (“skills” OR “competencies” OR “competencies”) AND (LIMIT-TO (DOCTYPE,“cp”) OR LIMIT-TO (DOCTYPE,“ar”)) AND (LIMIT-TO (PUBYEAR,2021) OR LIMIT-TO (PUBYEAR,2020) OR LIMIT-TO (PUBYEAR,2019) OR LIMIT-TO (PUBYEAR,2018) OR LIMIT-TO (PUBYEAR,2017) OR LIMIT-TO (PUBYEAR,2016)) AND (LIMIT-TO (LANGUAGE, “English”) OR LIMIT-TO (LANGUAGE,“Spanish”))

The searches carried out resulted in 1,300 articles. This was followed by a first selection, in which titles and abstracts were reviewd and, if necessary, full articles were read, with the aim of both checking whether the information was related to the object of study and assessing whether the criteria for exclusion were fulfilled. In this first selection process, 49 articles were collected.

The selected articles were subjected to a second, more detailed examination. They were read, analyzed and evaluated, with the result that only 10 of them met all the selection criteria. In this stage, the following were used as selection criteria:

a) Cybersecurity training and awareness must have a global scope, and not be limited to a specific area, such as ransomware, phishing, mobile telephony or gamification.

b) They must be designed for non-ICT workers in companies and organizations.

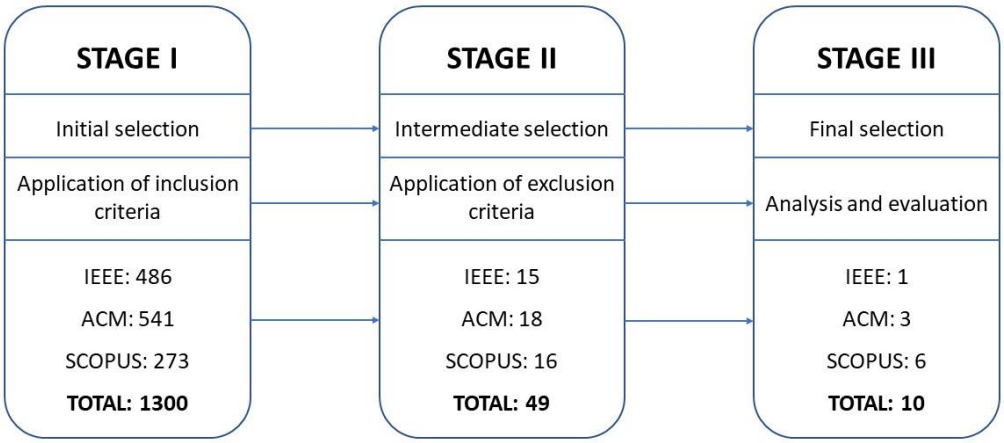
c) The identification of competencies must be a central element in the definition of training and awareness activities.

d) Research should focus on the selection and design of content, and not on teaching methodologies, measurement models or pedagogical aspects.

Figure 2 graphically shows the selection process carried out and the results obtained.

Figure 2

Selection process for primary studies



Source: Elaboration by the authors

As can be seen in Figure 2, the final selection consists of an IEEE Explore article, three ACM Digital Library articles, and six SCOPUS articles, which help answer the research questions. Table 1 shows the details of the specific studies selected.

Tabla 1

Selected studies

Código	Referencia	Título	Base de datos
C01	(Bada & Nurse, 2019)	Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs).	SCOPUS
C02	(Ani et al., 2019)	Human factor security: evaluating the cybersecurity capacity of the industrial workforce.	SCOPUS
C03	(Carlton et al., 2019)	Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills.	SCOPUS
C04	(Hatzivasilis et al., 2020)	Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees.	SCOPUS
C05	(Sithole et al., 2020)	A framework for a foundational cyber counter-intelligence awareness and skills training programme.	SCOPUS
C06	(Trim & Lee, 2021)	The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement.	SCOPUS

C07	(Wang, 2018)	Framework of Raising Cyber Security Awareness.	IEEE
C08	(Khan, 2019)	viCyber: An Intelligent Curriculum Design Tool for Cybersecurity Education.	ACM
C09	(Remmele & Peichl, 2021)	Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro- and Small Enterprises.	ACM
C10	(Vicente, 2021)	GEIGER: Solution for small businesses to protect themselves against cyber-threats	ACM

3. Analysis and results

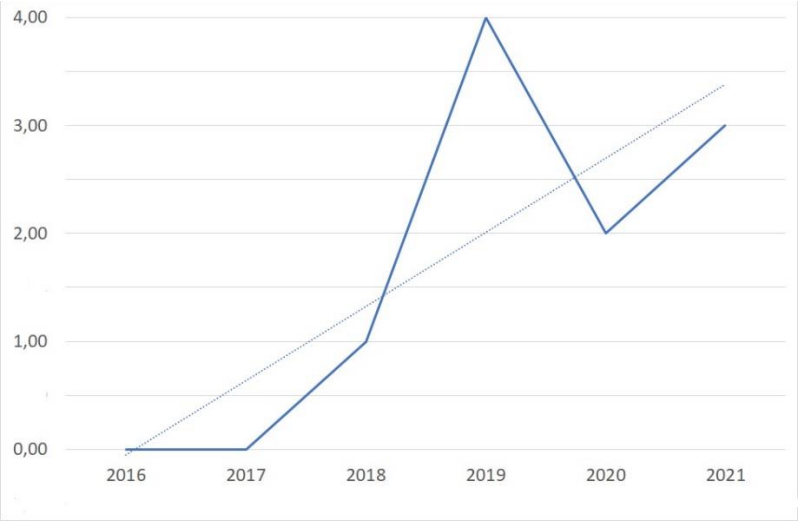
The information collected in these articles provides answers to the research questions posed.

- **RQ1. What is the evolution in the number of publications related to the use of competencies in cybersecurity training and awareness for non-ICT personnel from 2016 to the present?**

Once the importance and need to work on training and awareness aimed at non-ICT personnel in the field of cybersecurity using models based on competencies has been pointed out, the most prominent aspect and a relevant contribution of this research is the verification of the small number of articles that contemplate the use of competence frameworks when addressing the training and awareness of non-ICT personnel of companies and organizations. Despite this limited number of publications and studies that meet the selection criteria, the evolution in their number shows a clear ascending line, as shown in Figure 3, which clearly indicates a growing interest in this area of study.

Figure 3

Number of publications per year and trend



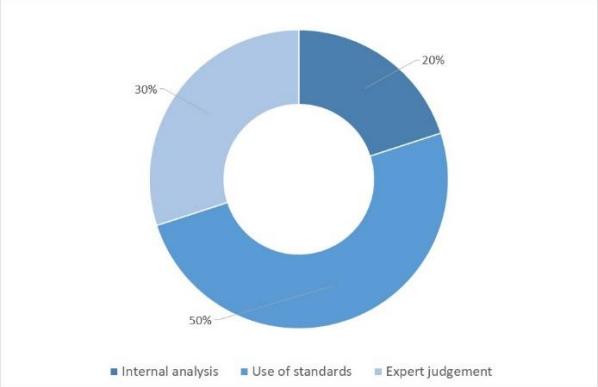
Source: Elaboration by the authors

- **RQ2. What are the methodologies used to identify cybersecurity competencies?**

The articles analyzed were classified into three large groups, according to the methodologies used to identify the skills or knowledge that non-ICT workers should achieve. In the first group, the investigations that use international information security standards as a reference were included. In the second group, the studies that propose training and awareness frameworks based on conducting ad hoc internal analyzes in companies and organizations were placed, and finally, those that use expert judgment as a work methodology, both through interviews and use of the Delphi method were located in the third group.

Figure 4

Distribution of the methodologies used



Source: Elaboration by the authors

As can be seen in Figure 4, the use of security standards to identify cybersecurity competencies for non-ICT employees is the most widely used methodology. Table 2 shows the standards taken as a reference. The standards use were the London Digital Security Center (LDSC) Cybersecurity Training and Awareness Program, the NIST 800 series of publications on security and privacy for organizations and information systems of the United States government's National Institute of Standards and Technology (NIST), the National Initiative for Cybersecurity Eductaion (NICE), included in the publication NIST 800-181, and finally, the GEIGER Cybersecurity Counter, a program developed by a consortium of companies and organizations in the field of cybersecurity with funds from the Horizon 2020 program of the European Union.

Table 2

Standards used and frequency

Standard	Agency	Primary study
Cybersecurity Training and Awareness Program	LDSC	[C01]
NIST 800	NIST	[C07]
NIST 800 -181 – NICE	NIST	[C08]
GEIGER	Consortium / ENISA	[C09], [C10]

The second methodology used has been the analysis of the training and awareness needs in cybersecurity of a specific company or organization, and the subsequent configuration of a customized training and awareness program.

The third methodology used is the use of expert judgment to define and establish a cybersecurity training and awareness model based on it.

- **RQ3. Are different roles identified according to the different needs in the field of cybersecurity of the jobs and responsibilities of an organization?**

Only one of the studies analyzed raises the need to establish different contents and levels of training and awareness according to the industrial sector, the job profile, and the specific job position of the staff. In two other articles the concept of "level" is used to establish different degrees of training for non-ICT personnel, although these levels are not directly related to job profiles. In the rest of the publications, no reference is made to these profiles, considering that training and awareness needs in cybersecurity are the same for all the personnel who use ICT in an organization.

- **RQ4: What are the objectives pursued?**

The main objective of all studies analyzed is to propose a training and awareness program on cybersecurity aimed at non-ICT workforce. Although competencies are considered in all of them, the approaches vary. Table 3 presents the different approaches of the analyzed studies. Half of the investigations are oriented to the educational, pedagogical or design aspects of the proposed models; three articles emphasize the measurement of the skills and knowledge of employees on cybersecurity aspects; and, finally, other studies focus on counterintelligence or in increasing resilience.

Table 3

Objectives

Objectives	Primary study
Educational, pedagogical or design aspects of the proposed framework	[C01], [C04], [C08], [C09], [C10]
Measurement of skills and knowledge	[C02], [C03], [C07],
Counterintelligence approach	[C05]
Increased resilience	[C06]

4. Discussion

Cybersecurity has become one of the ICT areas to receive the most attention and effort in recent years, due to the need to respond to the constant growth and sophistication of the attacks and risks that society faces and to the incessant development of technology itself. In this environment, in which the human factor is a crucial aspect, cybersecurity training and awareness activities are critical elements, which must be constantly examined, updated, and improved.

From the analysis of primary sources carried out in this study and the results obtained the following points are drwan as relevant characteristics for the purpose of this work:

First: there is a large number of articles and studies that address training and awareness in cybersecurity from a competency point of view in very different ways, which shows the interest that the subject arouses. However, the number of studies related specifically to the identification and creation of competency models for non-ICT workers is significantly low. This scarcity of studies shows a deficiency that should be corrected, while confirming the aforementioned finding. Although the importance and need to work on training and awareness in the field of cybersecurity is recognized through a competency-based approach, the reality is that its degree of development is testimonial. New studies are needed to expand and improve the current state of the art in the field with methodological proposals that facilitate the creation of frameworks of competencies adjusted to the needs of organizations which allow identifying the contents and levels of training and awareness necessary for each career profile and job position.

Second: the number of studies analyzed that explicitly contemplate the use of job profiles when defining the contents of training and awareness plans is practically nil. However, the different professional roles that exist in companies and organizations require specific training and awareness activities appropriate to their various roles and levels of responsibility. Failure to address these differences prevents organizations from reaching the appropriate level of training and awareness in cybersecurity of their personnel, which entails a security problem.

Third: the research carried out shows that the methodologies used in the creation of training and awareness programs are still based on the three classic approaches: security standards, ad hoc internal analysis and expert judgments. These approaches have undoubtedly proven their validity but they also have limitations. Indeed, the application of standards without adaptation to the different needs of each job profile can result in a model that is excessively general in nature, and consequently does not meet the real demands in the field of cybersecurity for many jobs. The use of training and awareness programs based on the definition of content determined by expert judgments suffers from the same limitation. Additionally, internal anayses and developments built to measure from scratch are undoubtedly adjusted to the needs of the company or organization analyzed, but are accompanied by a considerable level of effort and cost in time, human and financial resources; thus, these are solutions only available to a limited number of organizations. Furthermore, results cannot be extrapolated or used by other organizations, as they are developed to give a specific response to the defined scope and environment. However, despite such limitations, as this study shows, there are no alternative proposals that formulate new approaches or improvements to these models.

5. Conclusions

The literature review carried out in this article allows us to conclude that the level of academic development in cybersecurity training and awareness activities based on competencies for non-ICT personnel is, despite its relevance, very low. While considered as an important field of research in the field of ICT personnel, the use of competency frameworks associated with work roles for non-ICT personnel, however, does not present the same degree of development.

It can also be concluded that the few studies that address the matter are still based on methodologies that do not appear to have been reviewed or updated.

For this reason, there is an important area of improvement aimed at the development of new proposals that investigate standard reference models based on competencies for non-ICT personnel. These models facilitate the configuration or validation of training and awareness plans defined and adjusted to roles and job profiles, thus allowing the incorporation of cybersecurity competencies into the general map of labor competencies of companies and organizations, therefore granting them their necessary visibility and consideration.

References

Aldawood, H. & Skinner, G. (2018). A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications. *26th International Conference on Systems Engineering (ICSEng)* https://doi.org/10.1109/ICSENG.2018.8638166

Ali, R., Dominic, P., Ali, S., Rehman, M. & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences*, *11*(8), 3383. https://doi.org/10.3390/app11083383

Ani, U. D., He, H. & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2-35. https://www.doi.org/10.1108/JSIT-02-2018-0028

Bada, M. & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393-410. https://www.doi.org/10.1108/ICS-07-2018-0080

Bailey, T., Kolo, B., Rajagopalan & K., Ware, D. Insider threat: The human element of cyberrisk. (2018). *Technical Report.* McKinsey. https://mck.co/2Yzb7YB

Brilingaitė, A., Bukauskas, L. & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, (88). https://doi.org/10.1016/j.cose.2019.101607

Calder, A., (2016). Nueve pasos para el éxito: Una visión de conjunto para la aplicación de la ISO 27001:2013. *IT Governance Publishing.*

Carlton, M., Levy, Y. & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & Computer Security*, *27*(1), 101-121. https://doi.org/ 10.1108/ICS-11-2016-0088

CCN-CERT (2019). Ciberamenazas y Tendencias. Edición 2019. https://bit.ly/31WMmr8

CCN-CERT (2020). Ciberamenazas y Tendencias. Edición 2020. https://bit.ly/3BQnvlh

Eloff, J. & Eloff, M. (2005). Information security architecture. *Computer Fraud & Security*, (11), 10-16. https://doi.org/10.1016/S1361-3723(05)70275-X

ENISA (2018). Cybersecurity CultureGuidelines: Behavioural Aspects of Cybersecurity. *European Union Agency for Cybersecurity*. https://bit.ly/3GLbVub

Haqaf, H. & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, 43, 165-172. https://doi.org/10.1016/j.ijinfomgt.2018.07.013

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G. & Koshutanski, H. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences*, *10*(16), 5702. https://doi.org/10.3390/app10165702

Hiscox (2020). Hiscox cyberclaims report 2020. https://bit.ly/3oRm5Dw

IBM (2018). IBM X-Force Threat Intelligence Index 2018. *IBM Security*. https://ibm.co/3m3brYN

IC3. (2020). Internet Crime Report 2020. *Technical Report.* FBI. https://bit.ly/3tv3RbF

IDC. (2020). Global ICT Spending. Forecast 2020 - 2023. https://bit.ly/3tlrio0

Jacob, J., Wei, W., Sha, K., Davari, S. & Yang, A. (2018). Is the NICE cybersecurity workforce framework (NCWF) effective for a workforce comprised of interdisciplinary majors? *Proceedings of the International Conference on Scientific Computing (CSC); Athens.*

Khan, S., Wang, S. & Hodhod, R. (2019). viCyber: An Intelligent Curriculum Design Tool for Cybersecurity Education. *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. https://doi.org/ 10.1145/3287324.3293788

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. *Technical Report.* Keele University.

Lozano, M. (2017). 2017, el año en que las empresas se concienciaron en ciberseguridad. INCIBE. https://bit.ly/2VjkGK0

Maconachy, W., Schou, C., Ragsdale, D. & Welch, D. (2001). A Model for Information Assurance: An Integrated Approach. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.* https://bit.ly/3GLexbQ

Malekos, Z. & Lostri, E. (2020). The Hidden Costs of Cybercrime. *Technical Report.* McAfee. https://bit.ly/3zYkcZ1

Mäses, S. (2020). Evaluating Cybersecurity-Related Competences through Simulation Exercises. *Phd Thesis*. Tallinn University of Technology.

Mayer-Schönberger, V. & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. John Murray Press.

Mendívil, J., Gutiérrez, M., & Sanz, B. (2021). Mapa Funcional de competencias en seguridad para el personal no TI de las universidades españolas. *Investigación en Ciberseguridad. Jornadas Nacionales de Investigación en Ciberseguridad* (34), 319-326. https://doi.org/10.18239/jornadas_2021.34.64

Muñoz, S., (2021) Everis revela que el ciberataque de finales de 2019 le costó 15 millones de euros. El País. https://bit.ly/2YCuShV.

Nilsen, R. (2017). Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges. *Phd Thesis.* https://bit.ly/3yjtG0I

ONTSI. Informe Anual del sector de las TIC, los medios y los servicios audiovisuales 2020. *Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información.* https://bit.ly/3uZBX8k

Rahim, N., Hamid, S., Kiah, M., Shamshirband, S. & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness, *44*(4), 606-622. https://doi.org/10.1108/K-12-2014-0283

Remmele, B. & Peichl, J. (2021). Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro- and Small Enterprises. *The 16th International Conference on Availability, Reliability and Security,* 159, 1-7. https://doi.org/10.1145/3465481.3469198

Saltzer, J. H. & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. *Fourth ACM Symposium on Operating System Principles*, *63*(9), 1278-1308. https://doi.org/10.1109/PROC.1975.9939

Sanchez-Vallejo, M.A. (2021). Uno de los mayores oleoductos de Estados Unidos suspende sus operaciones tras sufrir un ciberataque. El País. https://bit.ly/3Dxz29Y

Sithole, T., du Toit, J., Jaquire, V. & von Solms, S. (2020). A framework for a foundational cyber counterintelligence awareness and skills training programme. *Proceedings of the 19th European Conference on Cyber Warfare*. 510-517. https://doi.org/10.34190/EWS.20.036

Schwab, K., (2016). *La cuarta revolución industrial*. Editorial Debate.

Trim, P., & Lee, Y. (2021). The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement. *Big Data and Cognitive Computing*, *5*(3), 32. https://doi.org/10.3390/bdcc5030032

Ulven, J., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39. https://doi.org/10.3390/fi13020039

Vicente de, J.J., Mallouli, W., Ruiz, J.F. & van Haastrecht, M. (2021). GEIGER: Solution for small businesses to protect themselves against cyber-threats. *The 16th International Conference on Availability, Reliability and Security*, 157, 1-4.

Wang, Y., Qi, B., Zou, H. & Li, J. (2018). Framework of Raising Cyber Security Awareness. *18th International Conference on Communication Technology (ICCT).* 865-869. https://doi.org/10.1109/ICCT.2018.8599967

WEF. (2021). The Global Risks Report 2021. World Economic Forum. *Technical Report.* https://bit.ly/3tuGe3c

Zhang-Kennedy, L. & Chiasson, S. (2021) A Systematic Review of Multimedia Tools for CybersecurityAwareness and Education. *Association for Computing Machinery*, *54*(1). https://doi.org/10.1145/3427920

Cómo citar:

Mendivil-Caldentey, J., Sanz-Urquijo, B., & Gutiérrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura [Competency-based cybersecurity training and awareness: a systematic literature review]. *Pixel-Bit. Revista de Medios y Educación*, 63, 197-225. https://doi.org/10.12795/pixelbit.91640

CALL FOR PAPERS

EL PAPEL DE LA TECNOLOGÍA
en el diseño y la implementación del modelo
FLIPPED LEARNING

The role of technology in the design and implementation of the Flipped Learning model

PIXEL-BIT
REVISTA DE MEDIOS Y EDUCACIÓN
MEDIA & EDUCATION JOURNAL
eISSN: 2171-7966
SEPTIEMBRE 2022. Nº 65

Call for Papers

Flipped Learning

Jon Bergmann
Houston Christian High School
EE.UU.
jon@jonbergmann.com
@jonbergmann

Dr. Raúl Santiago
Universidad de La Rioja
España
raul.santiago@unirioja.es
@santiagoraul

Dra. Carmen Llorente
Universidad de Sevilla
España
karen@us.es
@karenllorente

FECHAS CLAVE

Inicio de envíos	Límite de envíos	Publicación
01-07-2021	20-02-2022	01-09-2022