Modelos de Madurez en Ciberseguridad: una revisión sistemática

Maturity Models in Cybersecurity: a systematic review

[1]A.M. Rea-Guaman, [2]I.D. Sánchez-García
[1] Universidad Politécnica de Madrid
ETS Ingenieros Informáticos
Madrid, España
marcelo.rea.guaman@alumnos.upm.es,
{joseantonio.calvomanzano, tomas.sanfeliu}@upm.es

[1]T. San Feliu, [1]J.A. Calvo-Manzano
[2] Instituto Politécnico Nacional
Escuela Superior de Ingeniería Mecánica y Eléctrica
Ciudad de México, México
issanchez@ipn.mx

Resumen **— La ciberseguridad es un proceso que implica prevención, detección y reacción o respuesta, y que debe incluir un elemento de aprendizaje para la mejora continua del propio proceso. Este artículo busca determinar cuáles son los modelos de madurez en ciberseguridad más utilizados. Para ello, se realizó una revisión sistemática de estudios publicados desde el 2012 hasta el 2017. Se han encontrado 201 artículos que mencionan a los diferentes modelos de madurez en ciberseguridad, de los cuales se seleccionaron 12 artículos primarios, identificando los principales modelos utilizados en ciberseguridad. Finalmente, se ha observado que no existen muchos modelos de madurez enfocados en ciberseguridad.**

Palabras clave: ***Ciberseguridad; modelo de madurez; revisión sistemática.***

Abstract — Cybersecurity is a process that involves prevention, detection and reaction or response, and must include a learning element for the continuous improvement of the process itself. This study aims to determine the most used models of cybersecurity maturity. For this, a systematic review of studies published from 2012 to 2017 was carried out. Finding 201 articles that mention the different maturity models from which 12 primary articles were selected, identifying the most used models. Finally, it was observed that there are not many maturity models focused on cybersecurity.

Keywords – Cybersecurity; maturity model; systematic review.

I. INTRODUCCIÓN

El interés en la ciberseguridad está en aumento [1]. A medida que nuestro mundo se vuelve cada vez más interconectado y cada vez más en línea, el daño que las amenazas cibernéticas pueden causar a nuestro mundo cibernético está aumentando dramáticamente, día a día. Para muchos de nosotros en edad adulta, es difícil recordar la vida antes de las computadoras personales, por no hablar de Internet por supuesto; es asombroso considerar cómo toda esta conectividad ha transformado nuestra vida cotidiana. Sin embargo, como el mundo en línea se ha desarrollado en menos de una generación, la capacidad de proteger el mundo en línea ha tenido aún menos tiempo para desarrollarse y todavía está madurando.

Cada semana o a diario se escucha y se anuncia sobre la violación de la seguridad cibernética o algún incidente parecido. Los más comunes son los siguientes [1]:

- Información personal comprometida.
- Tarjetas de crédito robadas.
- Empresas hackeadas (vulneradas).

La manera en que las organizaciones abordan la capacidad de seguridad cibernética es esencial para contar con una seguridad cibernética eficaz, eficiente y sostenible. Para que las organizaciones puedan mejorar la seguridad cibernética, la industria y la comunidad técnica han desarrollado modelos de madurez en ciberseguridad que miden las capacidades de seguridad cibernética y las posicionan en diferentes niveles para la mejora continua. Por ello, es necesario identificar cuáles son los principales modelos de madurez en ciberseguridad que existen en el mercado.

En base a los anterior, para poder identificar cuáles son los principales modelos de madurez en ciberseguridad se realizado una revisión sistemática. Así, el presente artículo se organiza de la siguiente manera: la sección II presenta el concepto de modelo de madurez; la sección III presenta los detalles del proceso de revisión sistemática; en la sección IV se analiza e interpreta los resultados de la revisión sistemática; en la sección V se informa de los resultados de la revisión sistemática en base a los modelos de madurez en ciberseguridad más utilizados y, finalmente, la sección VI presenta las conclusiones.

II. CONTEXTO

Un modelo de madurez es un conjunto de características, atributos, indicadores o patrones que representan la capacidad y la progresión en una disciplina en particular. El contenido del modelo típicamente ejemplifica las mejores prácticas y puede incorporar normas u otros códigos de práctica de la disciplina.

978-989-98434-7-9/17/$31.00

Los modelos de madurez en ciberseguridad consideran la seguridad cibernética a través de diferentes áreas/dimensiones, entendiendo que cada dimensión no es necesariamente independiente de las otras.

Cada dimensión ofrece una serie de factores e indicadores de capacidad cibernética para que una organización comprenda la etapa de madurez en la que se encuentra. Se han identificado etapas de madurez y éstas varían desde una etapa inicial, donde una organización puede que apenas haya comenzado a considerar la seguridad cibernética, hasta un escenario dinámico, donde una organización es capaz de adaptarse rápidamente a los cambios en el panorama de la seguridad cibernética en lo relativo a las amenazas, las vulnerabilidades, los riesgos, la estrategia económica o el cambio de las necesidades organizacionales.

Un modelo de madurez, por lo tanto, proporciona un punto de referencia con el que una organización puede evaluar el nivel actual de capacidad de sus prácticas, procesos y métodos, y establecer objetivos y prioridades para la mejora. Además, cuando un modelo es ampliamente utilizado en una industria en particular (y los resultados de la evaluación son compartidos), las organizaciones pueden comparar su desempeño con otras organizaciones.

Para medir la progresión, los modelos de madurez en ciberseguridad típicamente tienen "niveles" a lo largo de una escala (algunos utilizan una escala de niveles de indicadores de madurez). Cada nivel de madurez está definido por un conjunto de atributos. Si una organización alcanza estos atributos, ha logrado tanto ese nivel como las capacidades que representa el nivel. Los niveles permiten a una organización utilizar la escala para [2]:

- Definir su estado actual.
- Determinar su futuro, estado más maduro.
- Identificar las capacidades que debe alcanzar para alcanzar ese estado futuro.

Y la información que se va a cuestionar con un modelo de madurez será:

- ¿Qué estamos haciendo? De un conjunto de elementos, cuales cumplimos, cuáles no.
- ¿Cómo lo estamos haciendo? De los elementos que cumplimos, ¿cómo los cumplimos? Mejor, pero …; Manual, automático …; En papel, o en digital …; En diferido o en tiempo real …

Existen una serie de modelos de referencia que se ofrecen dentro de la industria para la evaluación de los niveles de madurez. En este artículo, se pretende a través de una revisión sistemática de la literatura responder a la siguiente pregunta:

¿Cuáles son los principales modelos de madurez en ciberseguridad que existen en el mercado?

Para ello, se ha utilizado la técnica de revisión sistemática propuesta por Kitchenham [3], [4]. La revisión sistemática es un proceso formal y verificable que el investigador realiza para documentar el estado de conocimiento sobre un tema en particular.

Según Kitchenham [3], una revisión sistemática es una manera de evaluar e interpretar toda la investigación disponible, que sea relevante respecto de una interrogante de investigación particular, en el área temática o fenómeno de interés. La revisión sistemática [4] permite: (1) revisar los trabajos relevantes que han sido realizados en el área de estudio, (2) examinar los resultados, evaluarlos y contrastarlos, e (3) identificar lagunas en investigaciones actuales con el fin de hacer una propuesta adecuada de una actividad nueva de investigación.

III. Revisión Sistemática

La revisión sistemática incluye las siguientes actividades: (A) identificar las necesidades para realizar la revisión sistemática, (B) proponer un protocolo de revisión, (C) llevar a cabo la revisión (identificar los estudios primarios, evaluar los estudios y sintetizar la información), (D) analizar e interpretar los resultados de la revisión sistemática, y (E) informar de los resultados de la revisión sistemática.

A continuación, se detalla el proceso de la revisión sistemática de los modelos de madurez en ciberseguridad que existen en la industria. En la sección IV y V del artículo se presentan, las actividades D y E de la revisión sistemática.

A. *Identificación de las Necesidades para Realizar la Revisión Sistemática*

Se requirió realizar la revisión sistemática que permita: (1) identificar los diferentes modelos de madurez en ciberseguridad que existen en el mercado, (2) identificar los modelos más nombrados por los estudios realizados.

B. *Protocolo de Revisión*

En este punto se definió lo siguiente: las preguntas a realizar, los criterios para seleccionar las fuentes de bases de datos, las fuentes de bases de datos que deben usarse para realizar la búsqueda, elaborar las cadenas de búsqueda según los criterios definidos y la búsqueda en las fuentes, para localizar y seleccionar los estudios.

1) Formulación de la pregunta

Se planteó la problemática y las preguntas que están relacionadas con las necesidades y objetivos de la revisión.

- *Problema*: existe la necesidad de implementar modelos de madurez en ciberseguridad en las organizaciones, pero no se saben cuáles son los más utilizados en los estudios de investigación. Ello además permitiría determinar una tendencia de implementación de los mismos. Es necesario determinar cuáles son los más conocidos para ser considerados en las estrategias de su implementación en las organizaciones.
- *Preguntas*: las preguntas a responder son: ¿cuáles son los modelos de madurez en ciberseguridad que existen en el mercado?, ¿Cuáles son los principales que se utilizan en los estudios de investigación?
- *Población*: las publicaciones relacionadas con los modelos de madurez en ciberseguridad, gestión de seguridad en sistemas de información, y aplicaciones en las organizaciones.

- *Intervención*: diferentes modelos de madurez en ciberseguridad y los principales utilizados en los estudios de investigación.
- *Efecto*: modelos de madurez en ciberseguridad y los principales utilizados en los estudios de investigación.
- *Medida del resultado*: frecuencia de nombrado de los modelos de madurez en ciberseguridad en publicaciones por año de publicación.
- *Aplicación*: conocer las investigaciones que hacen mención a los diferentes modelos de madurez en ciberseguridad y qué modelos son los más utilizados en los estudios de investigación, así como identificar las tendencias actuales de uso de dichos modelos.

2) Criterios para la selección de fuentes

Se establecieron los criterios para la identificación y selección de las fuentes bibliográficas, y las bases de datos especializadas en las que se llevó a cabo la búsqueda de los estudios.

Los criterios para la selección de las fuentes fueron:

- Bases de datos que incluyan revistas y artículos enfocados en modelos de madurez en ciberseguridad, sistemas de gestión de seguridad de la información, y la aplicación de los modelos de madurez en ciberseguridad en las organizaciones.
- Bases de datos que cuenten con mecanismos de búsqueda avanzada, haciendo uso de los términos y sinónimos usados en las preguntas de búsqueda.
- Disponibilidad del texto completo de los artículos.
- Artículos disponibles en la Web de forma gratuita.
- Revistas especializadas disponibles en la biblioteca de la Escuela Técnica Superior de Ingenieros Informáticos de la Universidad Politécnica de Madrid.
- Artículos en inglés o español.

3) Identificación de las fuentes

Las bases de datos fueron seleccionadas tomando en consideración los siguientes términos que identifican las áreas de investigación: "maturity model", "cybersecurity", "cybersecurity capability", e "information security management system".

Entre las fuentes seleccionadas están las bases de datos especializadas como IEEE Computer, Science Direct, SpringerLink, Institute for Scientific Information (ISI) web of knowledge.

4) Cadena de búsqueda

Los términos usados en la revisión sistemática fueron construidos usando los siguientes criterios: (1) "capability maturity model for cybersecurity", deduciendo los principales términos o palabras claves de las preguntas para identificar la población, intervención y resultados esperados, (2) "capability maturity model for information security management system" identificando las palabras alternativas y sinónimos de los términos principales y también (3) "capability maturity model for cybersecurity applied in organizations". Estas palabras claves combinadas con los operadores lógicos AND (para enlazar términos de población, intervención y efecto) y OR (para incorporar palabras alternativas y sinónimos), así como el operador NOT para refinar la búsqueda, se utilizaron en los motores de búsquedas de las bases de datos especializadas.

Las palabras usadas en la cadena de búsqueda incluyen: "maturity model", "cibersecurity", "capability", "information security management system", "organizations".

5) Búsqueda en las fuentes

Se realizó la búsqueda en las fuentes usando los criterios definidos para su selección. Se incluyeron todas las fuentes de bases de datos identificadas. Se aplicaron las cadenas de búsqueda en las bases de datos electrónicas y en las otras fuentes (revistas y conferencias). Se contó con la participación de dos expertos en modelos de madurez en ciberseguridad para evaluar la lista de fuentes obtenidas.

C. Revisión

En este punto se muestra la búsqueda realizada de los artículos en las bases de datos seleccionadas con las cadenas de búsquedas predefinidas. Al resultado de las búsquedas se les aplicaron los criterios de inclusión y exclusión establecidos a continuación.

1) Criterios de selección de estudios y procedimientos para inclusión y exclusión dentro de los estudios primarios

En la Tabla I se presentan los criterios de inclusión y exclusión que se aplicaron a los resultados de la búsqueda inicial. La selección de estudios se centró en aquellos relacionados con los modelos de madurez en ciberseguridad y los más utilizados en los estudios de investigación.

En una primera fase de la revisión sistemática, haciendo uso de los motores de búsqueda de las bases de datos identificadas y poniendo la cadena de búsqueda elaborada en el protocolo de revisión paso 4, se encontraron un total de 12.952 estudios.

TABLA I. CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Inclusión (I)	***Exclusión (E)***
I1. Estudios empíricos de modelos de madurez en ciberseguridad y gestión de sistemas de seguridad de la información. Artículos que tratan sobre los factores que condicionan los modelos de madurez en ciberseguridad en las organizaciones. I2. Artículos que hablan sobre los modelos de madurez en ciberseguridad y gestión de sistemas de seguridad de la información. I3. Artículos que utilizan las palabras claves. I4. Artículos cuyo título, resumen o contenido está relacionado con el tema.	E1. Artículos que están basados sólo en una opinión particular que no aborde la ciberseguridad. E2. Artículos cortos. E3. Estudios que no son relevantes para las preguntas de investigación o no están relacionados con el estudio en particular. E4. Estudios que no son claros o presentan ambigüedad. E5. Publicaciones duplicadas. E6 Estudios anteriores a 2012 debido a la constante actualización en el área.

En una segunda fase, se revisaron cada uno de los estudios tomando en consideración los criterios de inclusión y exclusión anteriores, obteniendo un total de 201 estudios relevantes. Para seleccionar los estudios relevantes, se siguieron los siguientes pasos:

Paso 1. Leer el título. Si éste proporciona suficiente información, el estudio es seleccionado y guardado. Si no proporciona suficiente información, se realiza el paso 2.

Paso 2. Leer el resumen del artículo. Si éste proporciona suficiente información, el estudio es seleccionado y guardado. Si no proporciona información o existe la evidencia de que no pueda estar relacionado con el tema, se realiza el paso 3.

Paso 3. Leer las conclusiones. Si éstas proporcionan suficiente información, el estudio es seleccionado y guardado. En caso contrario se elimina.

En una tercera fase, se obtuvieron 12 estudios primarios que respondían a las preguntas formuladas inicialmente. La Tabla II muestra en primera instancia las fuentes, el número total de artículos y el número de artículos primarios seleccionados por fuente.

TABLA II. DISTRIBUCIÓN DE LOS ESTUDIOS POR FUENTE

Fuente	*Total*	*Primarios*
IEEE Explore	37	3
Science Direct	106	2
SpringerLink	49	5
ISI WoK	9	2
Total	**201**	**12**

2) Evaluación de la calidad del estudio

Para evaluar la calidad de los estudios, se realizaron las siguientes preguntas:

- ¿Es el estudio primario relevante para la investigación que se está realizando?
- ¿Los estudios primarios proveen la suficiente información como para que los resultados se beneficien de la revisión sistemática?
- ¿Los estudios revisados dan un valor agregado a la investigación que se está realizando?

De las preguntas anteriores se pudo comprobar que los 12 estudios primarios seleccionados son relevantes, proveen suficiente información y dan un valor agregado a la revisión sistemática.

3) Extracción de datos y síntesis

Para extraer la información importante de cada artículo, se diseñó un formulario. El formulario contiene los siguientes campos: (1) identificación del artículo, (2) bibliografía (título, autor, año), (3) tipo de artículo (caso de estudio, encuesta, experimento, investigación), (4) objetivo del estudio, (5) contexto en que se desarrolla el estudio, (6) tipo de estudio (mejora, despliegue o ambos), (7) nivel de profundidad del análisis (alto, medio, bajo), (8) modelos de madurez en ciberseguridad nombrados, (9) frecuencia de nombrado, y (10) conclusiones.

Por cada artículo seleccionado, después de leerse el texto completo, se procedió a registrar la información en el formulario, el cual permitió realizar el análisis posterior de los resultados. Los campos "modelos de madurez" y "frecuencia de nombrado" resumen los aspectos que responden a la pregunta planteada y las conclusiones que presenta el estudio.

IV. ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS DE LA REVISIÓN SISTEMÁTICA

Al concluir la ejecución de la revisión sistemática, los resultados se resumieron y analizaron. En el análisis, se usan herramientas estadísticas para determinar la frecuencia del nombrado de los modelos de madurez en ciberseguridad. Para realizar el resumen, los estudios fueron clasificados en estudios relacionados con: (1) modelos de madurez en ciberseguridad, (2) modelos más nombrados en los estudios y (3) variantes de los modelos de madurez en ciberseguridad.

Los artículos contienen casos de estudio, experimentos, encuestas, presentados a continuación y clasificados de acuerdo a los criterios de Petersen [18]:

TABLA III. ESTUDIOS CLASIFICADOS EN BASE A LA CATEGORIZACIÓN DE PETERSEN

Clasificación	*Referencia*
Propuestas de solución	[6],[8],[12]
Búsquedas de evaluación	[7],[9],[10],[15]
Artículos de opinión	[11],[16], [17]
Artículos de experiencia	[13]
Artículos filosóficos	[14]

A continuación, se presentan los resultados de la revisión sistemática.

A. Modelos de Madurez en Ciberseguridad Utilizados en los Estudios

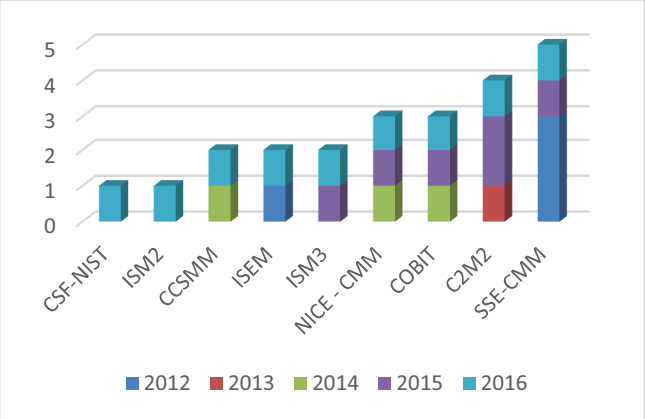
Con el fin de conocer los modelos de madurez en ciberseguridad que se utilizan en los estudios de investigación, se seleccionaron los modelos identificados en los estudios primarios (véase Tabla IV).

TABLA IV. MODELOS DE MADUREZ EN CIBERSEGURIDAD IDENTIFICADOS

Modelos	*Referencias*
CCSMM (Community Cyber Security Maturity Model)	[7], [9]
COBIT (Control Objectives for Information and related Technology)	[7], [15], [16]
CSF-NIST (Cybersecurity Capability Maturity Model – National Institute of Standards and Technology)	[7]
C2M2 (Cybersecurity Capability Maturity Model)	[6], [7], [8], [17],
ISEM (Information Security Evaluation Maturity Model)	[7], [14]
ISM2 (Information Security Maturity Model)	[7]
ISM3 (Information Security Management Maturity Model)	[7], [11]
NICE-CMM (National Initiative for Cybersecurity Education – Capability Maturity Model)	[7], [9], [10]
SSE-CMM (Systems Security Engineering Capability Maturity Model)	[7], [11], [12], [13], [14]

B. *Frecuencia de Nombrado de los Modelos de Madurez en Ciberseguridad*

En la Fig. 1 se muestra la frecuencia de nombrado de los modelos de madurez en ciberseguridad por año. En los estudios



de investigación, se puede observar que el más utilizado es el SSE-CMM que ha sido adoptado para ciberseguridad.

Figura 1. Frecuencia del nombrado de los Modelos de Madurez en Ciberseguridad identificados por año

C. *Variantes de los Modelos de Madurez en Ciberseguridad*

Debido a que no existen en el mercado modelos de madurez en ciberseguridad por cada área de la industria, muchos de los modelos han sufrido variantes y modificaciones, e inclusive adaptaciones de otros modelos que no fueron elaborados inicialmente para ese propósito. Dentro de los estudios primarios se encontraron variantes de los modelos. Por ejemplo, el modelo de ciberseguridad C2M2 tiene 2 variantes: el Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) que está enfocado al sector eléctrico y el Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) enfocado al servicio de gas y combustibles.

V. Informe de Resultados de la Revisión Sistemática

Una vez seleccionados y analizados cada uno de los estudios primarios, se identificaron los modelos de madurez en ciberseguridad más nombrados en los estudios de investigación y se elaboró una matriz de modelos de madurez en ciberseguridad por número de veces nombrados en los estudios. Durante la revisión de la matriz, se observó que algunos modelos de madurez están basados en otros modelos, pero no todos están relacionados con la ciberseguridad. Por ejemplo, se basan en el CMMI para poder adaptarlos a sus necesidades, inclusive se encontraron algunos modelos adaptados a un enfoque forense [5] como: Digital Forensic Organization Core Capability (DFOCC) y Digital Forensic Management Framework (DFMF).

Considerando que hay un número de veces que aparece repetido un mismo modelo de madurez en ciberseguridad en los estudios, mediante un procedimiento de conteo se determinó el número de veces que el modelo de madurez se repite. Al tabular los datos, se obtiene la lista de modelos de madurez en ciberseguridad que son más nombrados en los estudios, obteniéndose los modelos de madurez empleados en ciberseguridad ordenados por la frecuencia con que han sido mencionados por los autores. Se identificaron los principales modelos de madurez en ciberseguridad, de acuerdo a la distribución de frecuencias. Del análisis realizado de los modelos de madurez en ciberseguridad para implementarlos en la industria, se observó lo siguiente:

- "C2M2" Cybersecurity Capability Maturity Model. Es un modelo que está enfocado a ciberseguridad y que debido a su importancia se crearon dos variantes, una para el sector energético [6], [7], [8], y otra para el sector de gas y combustibles [7] de los Estados Unidos de Norteamérica [17].
- "NICE" Capability Maturity Model (CMM). Es un modelo de ciberseguridad, enfocado en la gestión de la planificación del trabajo de todos los participantes en la gestión de la ciberseguridad, y en los objetivos de la organización [7], [9], [10].
- "SSE-CMM" Systems Security Engineering Capability Maturity Model. Origen de la Norma ISO/IEC 21827:2002 Information Technology – Systems Security Engineering – Capability Maturity Model. Es una de las normas más utilizadas internacionalmente en relación con la definición e implantación de los procesos de seguridad, ya que define en detalle los procesos que deben tenerse en cuenta en cualquier organización que desea implantar un "Proceso Global de Seguridad". Este modelo es el más mencionado en los trabajos de investigación y es un modelo aplicado a seguridad de la información, pero se ha acoplado en los diferentes trabajos para abordar ciberseguridad [7], [11], [12], [13], [14].
- "ISEM" Information Security Evaluation Maturity Model. Es un modelo que nombran los autores por ser uno de los primeros modelos de madurez aplicados a seguridad de la información. Se ha utilizado como parámetro para desarrollar otros modelos de madurez aplicados a ciberseguridad, pero solo se nombra y no se realiza un análisis a fondo por los nuevos paradigmas de tecnología y porque ya existen nuevos modelos de madurez aplicados a diferentes sectores [7], [14].
- "COBIT" Control Objectives for Information and related Technology. Es un modelo conocido y aplicado en TI, desarrollado por ISACA, donde se manejan 5 niveles de madurez. Se desarrolló para medir el nivel de madurez en el dominio de gobierno de TI, pero se ha usado de referencia en los trabajos investigados que incluyen al gobierno de TI como uno de los factores claves de la ciberseguridad, complementando COBIT con otros modelos [7], [15], [16].
- "ISM3" Information Security Management Maturity Model. Lo relevante de este modelo es que se manejan métricas de Seguridad de la Información, que ayudan a

mantener a la organización en un nivel de riesgo aceptable, se ajusta tanto a pequeñas como a grandes organizaciones, es muy utilizado y adaptable para necesidades específicas como ciberseguridad [7], [11].

- "CCSMM" Community Cyber Security Maturity Model. Este modelo fue desarrollado por la Universidad de San Antonio Texas, es un modelo holístico que determina la postura de ciberseguridad en organizaciones, comunidades y naciones [7], [9].

VI. Conclusiones

En este artículo se han presentado los resultados de la revisión sistemática. Con lo anterior, podemos diferenciar los modelos que están enfocados a ciberseguridad y aquellos que se han adaptado para su aplicación en ciberseguridad, así como también cuáles son los que se utilizan actualmente en nuevas investigaciones. Se puede indicar que: (1) todos los modelos toman como referencia el modelo CMM; (2) los modelos de ciberseguridad actuales son adaptaciones de otros modelos; (3) los modelos principales usados para ciberseguridad tienen variantes; (4) no existe una tendencia por un modelo de ciberseguridad, si no que el modelo más mencionado es un modelo de madurez aplicado a seguridad de la información SSE-CMM; y (5) la mayoría de modelos de madurez son elaborados y auspiciados por entidades estatales y organizaciones de estandarización internacionales.

Durante el análisis de los estudios, se ha observado que cada autor usa un vocabulario diferente para un mismo significado. También se identificó que los modelos de ciberseguridad existentes actualmente no son adaptables completamente a las necesidades particulares de las organizaciones. Por ello, se han creado diferentes variantes, donde solo las principales han sido mencionadas en esta revisión, pues la gran mayoría de modelos no están diseñados para abordar de manera única los riesgos de ciberseguridad.

Del análisis realizado, se desprende que el número de modelos mencionados por los autores es muy reducido, identificando que existe un campo no explotado en la actualidad sobre ciberseguridad, ya que entre los artículos revisados solamente una minoría abordaban modelos aplicados a la problemática de ciberseguridad.

A destacar que el modelo ISEM solamente es mencionado porque muchos modelos lo tomaron como referencia, pero no es aplicado actualmente en la industria.

De igual manera, el modelo de COBIT es muy mencionado en los artículos, pero es un modelo que no aborda de manera completa la problemática de ciberseguridad, siendo su enfoque de gobierno de seguridad de TI, pero se ha forzado su uso por la sencillez y facilidad de su implementación.

Como conclusión final, podemos indicar que en la actualidad existe una deficiencia de modelos de madurez que sean totalmente enfocados en ciberseguridad, de fácil implementación y adaptables a diferentes tipos de organizaciones.

Referencias

[1] Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam. New York, NY: "Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats", pp 24-25, 2015.

[2] ACIS VIII Jornada Nacional de Seguridad Informática, "http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/05-ModelosMadurezSeguridadInformatica.pdf, consultado el 21 de febrero de 2017, 10 am.

[3] B. Kitchenham, T. Dybå and M. Jørgensen, "Evidence-based software engineering," Proceedings of the International Conference on Software Engineering, pp. 273–281, 2004.

[4] B. Kitchenham, "Guidelines for performing systematic literature reviews in software engineering," EBSE Technical Report EBSE-2007-01, Keele University, 2007.

[5] G. Peterson and S. Shenoi, Advances in Digital Forensics VII, *361*(January), 3–21. https://doi.org/10.1007/978-3-642-24212-0, 2012.

[6] S.H.B. Von Solms, A maturity model for part of the African Union Convention on Cyber Security. Proceedings of the 2015 Science and Information Conference, SAI 2015, 1316–1320. https://doi.org/10.1109/SAI.2015.7237313, 2015.

[7] N.T. Le and D.B. Hoang, "Can maturity models support cyber security ?," University Tecchnology of Sydney, Faculty of Engineering & IT, 2016

[8] R.M. Adler, A dynamic capability maturity model for improving cyber security. 2013 IEEE International Conference on Technologies for Homeland Security (HST), 230–235. https://doi.org/10.1109/THS.2013.6699005, 2013.

[9] C. Barclay, Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?, K 2014, 275–282. https://doi.org/10.1109/Kaleidoscope.2014.6858466, 2014.

[10] M. Bishop, N. Miloslavskaya and M. Theocharidou, Information Security Education Across the Curriculum: 9th IFIP WG 11.8 World Conference, WISE9 Hamburg, Germany, May 26-28, 2015 Proceedings. IFIP Advances in Information and Communication Technology, 453, 53–63. https://doi.org/10.1007/978-3-319-18500-2, 2015.

[11] A.I. Hohan, M. Olaru and I.C Pirnea, Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. Procedia Economics and Finance, 32(15), 352–359. https://doi.org/10.1016/S2212-5671(15)01404-5, 2015.

[12] M. Ouedraogo, H. Mouratidis, E. Dubois and D. Khadraoui, Information systems security criticality and assurance evaluation. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6059 LNCS, 38–54. https://doi.org/10.1007/978-3-642-13577-4_4, 2012.

[13] M.T. Siponen, Maturity Criteria for Developing Secure {IS} and {SW:} Limits, and Prospects. Sec, 214, 91–108. https://doi.org/10.1007/978-0-387-35586-3_7, 2012.

[14] S. Lee, T. Chung and M. Choi, An empirical study of quality and cost based security engineering. Information Security Practice and Experience, 379–389. Retrieved from http://link.springer.com/chapter/10.1007/11689522_35, 2012.

[15] Y. Goksen, E. Cevik and H. Avunduk, A Case Analysis on the Focus on the Maturity Models and Information Technologies. Procedia Economics and Finance, 19(15), 208–216. https://doi.org/10.1016/S2212-5671(15)00022-2, 2015.

[16] F.B. Bergmann and M.S. Silveira, Human Aspects of Information Security, Privacy, and Trust. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8533, 387–399. https://doi.org/10.1007/978-3-319-07620-1, 2014.

[17] J. Payette, E. Anegbe, E. Caceres and S.Muegge, Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects, 26–34., 2015.

[18] Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008). Systematic Mapping Studies in Software Engineering. 12Th International