Buenas prácticas para la Seguridad Informática en PyMES

Tomás Alcántara, Marisa Panizzi[1], Iris Sattolo[1]

[1]Escuela Superior de Ingeniería, Informática y Ciencias Agroalimentarias Universidad de Morón. Cabildo 134 (B1708JPD), Partido de Morón, Argentina.
talcantara1995@gmail.com, marisapanizzi@outlook.com, iris.sattolo@gmail.com

Resumen. Actualmente la seguridad informática es uno de los principales desafíos dentro de las empresas ya que un ataque podría arruinar la reputación de esta ocasionando pérdidas a nivel económico y confiabilidad. A su vez dentro de la economía mundial muchas de las empresas son PyMES, con lo cual juegan un rol muy importante en la economía de cada país, así como también en el área laboral de los ciudadanos. El presente trabajo de tesis de la carrera Licenciatura en Sistemas de la UM pretende desarrollar un conjunto de buenas prácticas de seguridad informática para PyMES. Antes de comenzar con el diseño de la solución, se elaboró el estado del arte respecto a la seguridad informática en PyMES mediante un mapeo sistemático de la literatura (en inglés *systematic mapping study* o SMS). Se presentan los resultados del SMS y las actividades planificadas para la finalización de la tesis.

Palabras claves: Seguridad informática, PyMES, buenas prácticas, SMS.

1 Introducción

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable [1].

La seguridad informática ha tomado un rol muy importante en el ámbito de la tecnología. La mayoría de las empresas y los organismos estatales comenzaron a incorporar personal especializado en seguridad en sus equipos ya que deben asegurar su infraestructura para disminuir la posibilidad de un ataque que perjudique su imagen corporativa o que sufran un perjuicio económico.

En ese sentido si hablamos de las de las organizaciones uno de los motores principales de las economías en los países son las PyMES. En Argentina según los últimos datos de la SEPYME hay más de 1.633.000 de empresas registradas bajo la modalidad de PyMES [2]. Muchas de estas empresas suelen brindar servicios a otras empresas u organismos, con lo cual en varias ocasiones son los puntos de entrada de ataques ya que al brindar servicios a otras empresas suelen tener ciertos privilegios sobre otras infraestructuras. Muchas veces es más simple y rápido realizar un ataque sobre las mismas PyMES que sobre las empresas de mayor tamaño, esto se debe a que en las empresas

chicas no suelen tener personal idóneo en el área de seguridad y muchas veces ven este área o soluciones de seguridad como un costo y no como una inversión.

La motivación principal de esta investigación es que durante el 2021 se duplicaron los ataques informáticos con respecto al 2020 según el Equipo de Respuesta ante Emergencias Informáticas Nacional (CERT, por su sigla en inglés) de la Dirección Nacional de Ciberseguridad de Argentina [3]. Con respecto a los números que manejan las principales empresas de seguridad se puede observar que según el informe de la empresa Kaspersky [4] al menos el 15,45% de los usuarios de internet fue afectado por malware.

Dada las altas tasas de ataques informáticos informados por organismos y empresas reconocidas, el trabajo de la tesis se focalizó en el diseño de un conjunto de prácticas a nivel seguridad informática que pueda ser utilizado en PyMES de Argentina Antes de comenzar con el diseño de la solución se realizó la construcción del estado del arte respecto a la seguridad informática en PyMES mediante un mapeo sistemático de la literatura (en inglés, *Systematic Mapping Studies* o SMS)

Dada la situación actual de las PyMES y del auge de la seguridad informática se decide realizar un análisis de la situación actual con respecto a la problemática de seguridad informática en PyMES Para realizar el SMS se siguieron los lineamientos propuestos por Kitchenham *et al.* [5] y por Petersen *et al.* [6].

El artículo se estructura de la siguiente manera: en la Sección 2 se describe la planificación del SMS, en la Sección 3 se describe su ejecución. Los resultados se presentan en la Sección 4. En la Sección 5 se exponen las conclusiones y trabajos futuros.

2 Planificación del SMS

En esta sección se presenta la definición del protocolo de revisión del SMS: preguntas de investigación (PI), estrategia de búsqueda, selección de los estudios, criterios y proceso de selección, formulario de extracción y el proceso de síntesis de los datos.

El objetivo de este SMS es responder la siguiente pregunta de investigación (PI): *¿Cuál es el estado del arte respecto a la existencia de un modelo de mejores prácticas de seguridad informática en PyMES argentinas?* Esta pregunta principal (PI) se descompone en un conjunto de sub-preguntas (PI1-3), las cuales se presentan a continuación:

- *PI1: ¿Qué tipo de contribuciones existen respecto a la seguridad informática en PyMES?*
- *PI2: ¿En qué capa de seguridad se realiza la contribución?*
- *PI3: ¿Qué tipos de investigación se encuentra en los artículos?*

Se decide realizar la búsqueda en las siguientes bibliotecas y repositorios digitales: *Google Schoolar, Scielo, Dialnet* considerando publicaciones de congresos y revistas. La búsqueda se realizó en un período comprendido entre enero del 2010 a mayo del 2022.

La cadena de búsqueda utilizada es:

(Seguridad informática) and (PyMES) and (estándar OR modelo OR arquitectura OR esquema OR guía OR procedimiento)

Los criterios de inclusión y exclusión utilizados para el proceso de selección de artículos se presentan en la Tabla 1.

Tabla 1. Criterios de inclusión y exclusión.

Criterios de inclusión	Criterios de exclusión
Artículos vinculados a las PI.	Artículos que no estén accesible para su lectura completa.
Artículos publicados a partir de enero del 2010 hasta mayo del 2022.	Libros, tesis, presentaciones en power point, informes técnicos, artículos que cuenten solo con el resumen.
Artículos en el idioma español.	

Para dar respuesta a cada una de las preguntas de investigación (PI) se definió un esquema de clasificación, que por restricciones de espacio se presenta en un apéndice en [7], junto con el formulario de extracción de datos. Se utiliza una síntesis temática basada en el esquema de clasificación que se representará a través de gráficos.

El proceso de selección de los estudios consistió en los siguientes pasos: 1) realizar la búsqueda en las fuentes definidas aplicando la cadena en el título y/o en el resumen, 2) eliminar los artículos duplicados, 3) aplicar los criterios de inclusión y exclusión en el título, resumen y palabras clave, 4) aplicar los criterios de inclusión y exclusión al texto completo. Este proceso permitió la selección de los estudios primarios que se analizaron para dar respuesta a las preguntas de investigación (PI) formuladas.

3 Ejecución del SMS

Por restricciones de espacio, la cantidad de artículos encontrados en cada uno de las librerías, plataformas y repositorios digitales definidos en el protocolo de revisión se encuentran en un apéndice en [7] junto con el listado de los 10 estudios primarios analizados.

4 Resultados del SMS

A continuación, se pretende dar respuesta a las preguntas de investigación (PI) en base a la literatura analizada mediante la utilización de gráficos.

PI1: ¿Qué tipos de contribuciones existen respecto a la seguridad informática en PyMES?

El estándar más mencionado en los estudios primarios es ISO 27001. En la mayoría de los estudios se encontró que para resolver las problemáticas de seguridad en las PyMES se utilizan soluciones que son para empresas de más envergadura, como por ejemplo, COBIT, ITIL y los estándares de ISO (Ver Figura 1).

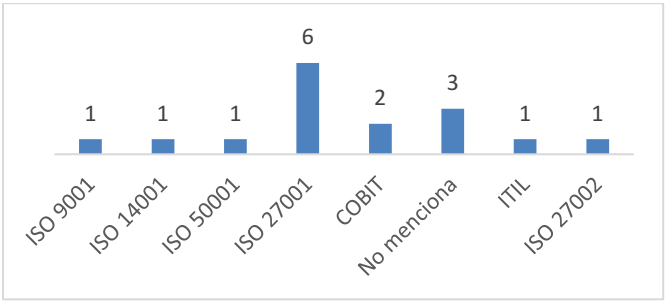

Fig. 1. Estándares utilizados.

PI2: ¿En qué capa de seguridad se realiza la contribución?
En los estudios analizados se encontró que en un mismo artículo se resuelven problemas de diferentes capas de seguridad. Las capas de seguridad a las cuales hacen referencia la mayoría de los estudios son "aplicaciones" y "red" (Ver Figura 2).

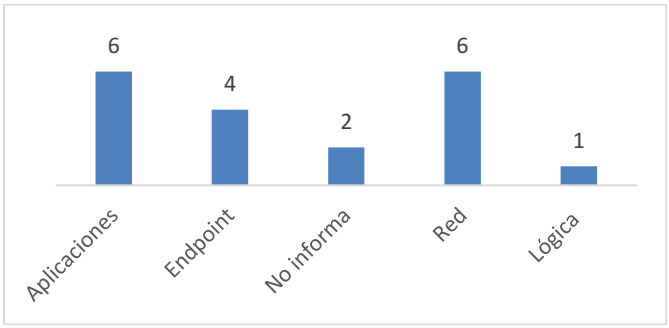

Fig. 2. Capas de seguridad.

PI3: ¿Qué tipos de investigación se encuentra en los artículos?
Dentro de los hallazgos se logró evidenciar que la mayoría de los estudios se corresponden a validaciones (6 en total). Y dos estudios son del tipo de investigación "evaluación" y dos estudios del tipo "propuesta de solución" (Ver Figura 3).

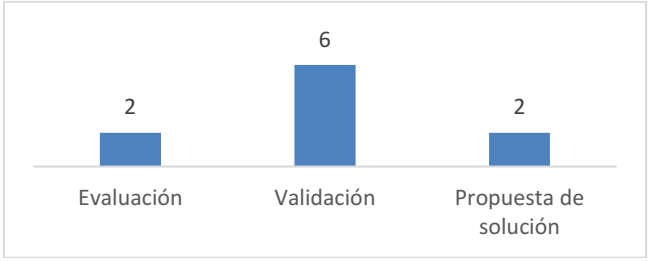

Fig. 3. Tipos de investigación según la clasificación propuesta por Wieringa [8].

5 Conclusiones y trabajos futuros

Se logró construir el estado del arte respecto a la situación de soluciones de seguridad informática utilizada en PyMES mediante el desarrollo de un SMS. Se analizaron 10 estudios primarios recuperados de las fuentes de búsqueda definidas en el protocolo de revisión cuyo período de búsqueda ha sido comprendido entre enero del 2010 y mayo del 2022. Una vez analizados los estudios primarios, se concluye que:

- La mayoría de las contribuciones hacen referencia a la utilización de estándares definidos por ISO siendo la mayoría correspondiente a la ISO 27001.
- Se pudo evidenciar que la mayoría de las investigaciones abordan la problemática de la seguridad informática sobre redes, aplicaciones y endpoint. En ese sentido se puede analizar que los principales vectores de ataques se encuentran sobre estas capas. También es importante destacar que el principal problema de seguridad informática es el usuario, que pueden llegar a ser un punto de ataque por desconocimiento del tema o por un mal uso de la tecnología. Estas tres capas mencionadas anteriormente son los primeros puntos por proteger en una organización, serían como los pasos iniciales a revisar al momento de plantear una arquitectura segura.
- Se logró evidenciar la ausencia de una solución específica para PyMES dado que en las investigaciones se utilizan estándares, prácticas y las contextualizan para resolver problemas de seguridad informática en este tipo de empresas.

Las futuras actividades para continuar con el desarrollo de la tesis son: 1) el desarrollo de un conjunto de buenas prácticas que pueda ser utilizadas en PyMES de Argentina y 2) Validar la solución en diferentes estudios de casos en PyMES de Argentina.

Referencias

1. López Purificación A. Seguridad informática. Editex. ISBN 978-84-9771-657-4 (2010).
2. Ministerio de desarrollo productivo, Más de 16 millones de empresas ya se incorporaron al registro MiPyME. Disponible: https://www.argentina.gob.ar/noticias/mas-de-16-millones-de-empresas-ya-se-incorporaron-al-registro-mipyme (2022).
3. Dirección Nacional de Ciberseguridad. Informe del CERT.ar. Disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-3 (2020).
4. Kaspersky. Boletín de Seguridad de Kaspersky. Estadísticas 2021. Disponible en: https://securelist.lat/kaspersky-se2021)curity-bulletin-2021-statistics/96099 (2021).
5. Kitchenham B., Chartes, S. Guidelines for performing systematic literature reviews in software engineering, Keele University, EBSE-2007-01 (2007).
6. Petersen K. Wohlin C.: Context in industrial software engineering research. Third International Symposiumm on Empirical Software Engineering and Measurement (2009).
7. Alcantara T., Panizzi M., Sattolo I. Apéndice- Buenas Prácticas para la Seguridad Informática en PyMES (Camera Ready). Disponible en: https://doi.org/10.6084/m9.figshare.20514780.v5 (2022).
8. Wieringa R., Maiden N., Mead N., Rolland C. Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. Requirements Engineering, 11(1), pp. 102-107 (2006).