Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Propuesta de una Herramienta de Autoevaluación para PYMEs basada en el Marco de Trabajo para la Mejora de la Infraestructura Crítica para la Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST)

Coghi Hernández Máximo.

Fernández Quesada Kattia.

Agosto 2019

Declaratoria de derechos de autor

Agradecimientos

Agradecemos a todas aquellas personas que nos apoyaron a lo largo de este proceso y de la elaboración del Trabajo Final de Graduación, su ayuda ha hecho que el trabajo se realice con éxito.

Agradecimientos por parte de Kattia:

A mi esposo, que ha sido mi apoyo estos largos 32 meses...

A mis padres y hermanos, por estar ahí siempre...

A nuestro tutor, que nunca dudó que podíamos lograrlo...

A mis amigos, esa pequeña familia que me dio la vida y que me apoyan sin tener necesidad de hacerlo...

A todos los profesores, que tanto me enseñaron...

Y finalmente a Max, porque sola, esto no hubiera sido posible.

Agradecimientos por parte de Máximo:

A mi familia, por darme su motivación en todo momento…

A nuestro tutor y lectores, que dedicaron su tiempo en la revisión y recomendaciones de este Trabajo Final de Graduación…

Y a mi compañera Kattia, por su apoyo y buen trabajo en equipo.

Tabla de Contenido

Listado de Tablas 8

Listado de Figuras 10

Resumen Ejecutivo 11

Capítulo 1. Introducción 12

1.1 Generalidades 12

1.2 Antecedentes del Problema 12

1.3 Definición y Descripción del Problema 13

1.4 Justificación 13

1.5 Viabilidad 14

1.5.1 Punto de Vista Técnico 14

1.5.2 Punto de Vista Operativo 14

1.5.3 Punto de Vista Económico 15

1.6 Objetivos 15

1.6.1 Objetivo General 15

1.6.2 Objetivos Específicos 15

1.7 Alcances y Limitaciones 16

1.7.1 Alcances 16

1.7.2 Limitaciones 16

1.8 Marco de Referencia Organizacional y Socioeconómico 16

1.9 Estado de la Cuestión 17
1.9.1 Planificación de la Revisión 17
1.9.1.1 Formulación de la Pregunta 17
1.9.1.1.1 Foco de la Pregunta 17
1.9.1.1.2 Amplitud y Calidad de la Pregunta 17
1.9.1.1.2.1 Problema 17
1.9.1.1.2.2 Pregunta de Investigación 17
1.9.1.1.2.3 Palabras Clave y Sinónimos 17
1.9.1.1.2.4 Intervención 18
1.9.1.1.2.5 Control 18
1.9.1.1.2.6 Resultado 18
1.9.1.1.2.7 Medida de Salida 18
1.9.1.1.2.8 Población 19
1.9.1.1.2.9 Aplicación 19
1.9.1.1.2.10 Diseño Experimental 19
1.9.1.2 Selección de Fuentes 19
1.9.1.2.1 Definición del Criterio de Selección de Fuentes 19
1.9.1.2.2 Lenguaje de Estudio 20
1.9.1.2.3 Identificación de Fuentes 20
1.9.1.2.3.1 Métodos de Selección de las Fuentes 20
1.9.1.2.3.2 Cadenas de Búsqueda 20
1.9.1.2.3.3 Lista de Fuentes 21

1.9.1.2.4 Selección de Fuentes Después de la Evaluación 21

1.9.1.2.5 Comprobación de las Fuentes 21

1.9.1.3 Selección de los Estudios 22

1.9.1.3.1 Procedimiento para la selección de los estudios 22

1.9.1.3.1.1 Definición del criterio de inclusión y exclusión de estudios 22

1.9.1.3.1.2 Definición de tipos de estudio 23

1.9.1.3.2 Extracción de la Información 23

1.9.2 Ejecución de la Revisión 24

1.9.2.1 Ejecución de la selección en la fuente IEEE Digital Library 24

1.9.2.2 Ejecución de la selección en la fuente Scholar Google 25

1.9.2.2.1 Evaluación de la calidad del estudio 26

1.9.2.2.2 Revisión de la selección 26

1.9.2.2.3 Extracción de información 26

1.9.2.3 Ejecución de la selección en la fuente ACM Digital Library 28

1.9.2.4 Ejecución de la Selección en la Fuente Journal of Research of NIST 28

1.9.2.4.1 Evaluación de la calidad del estudio 29

1.9.2.4.2 Revisión de la selección 29

1.9.2.4.3 Extracción de información 29

1.9.2.5 Ejecución de la Selección en la Fuente Análisis de Riesgos del INCIBE 31

1.9.2.5.1 Evaluación de la calidad del estudio 32
1.9.2.5.2 Revisión de la selección 32
1.9.2.5.3 Extracción de información 32
1.9.3 Análisis de resultados 34
1.9.3.1 Estudios Analizados 34
1.9.3.2 Presentación de Resultados 34
1.9.3.3 Resultados del Cálculo Estadístico 35
1.9.3.4 Resultados del Análisis de Sensibilidad 36
1.9.3.5 Conclusiones 36
Capítulo 2. Marco Conceptual 38
Capítulo 3. Marco Metodológico 42
3.1 Tipo de Investigación 42
3.2 Alcance Investigativo 42
3.3 Enfoque 42
3.4 Diseño 43
3.5 Población y Muestreo 43
3.6 Instrumentos de Recolección de Datos 43
3.7 Técnicas de Análisis de Información 44
3.8 Estrategia de Desarrollo de la Propuesta 44
Capítulo 4. Análisis del Diagnóstico 45
4.1 Estructura del NIST 45
4.1.1 Funciones 45

4.1.2 Categorías 46

4.1.2 Subcategorías 46

Capítulo 5. Propuesta de Solución 48

5.1 Escenarios para la Herramienta de Autoevaluación 48

5.2 Creación de las Preguntas para la Evaluación 49

5.2.1 Pregunta Sencilla 49

5.2.2 Pregunta con Frase Introductoria 50

5.2.3 Pregunta con Frase de Definición 51

5.2.4 Secuenciación de las Preguntas 52

5.2.5 Generalidad de la Herramienta 56

5.3 Respuestas de las preguntas 57

5.4 Cálculo de la nota obtenida 60

5.4.1 Valor único del Estado Actual y del Estado Deseado 60

5.4.2 Aplicar regla de tres simple 62

5.4.3 Nota global 63

5.5 Presentación de Resultados 63

5.6 Presentación de las recomendaciones. 66

Capítulo 6. Conclusiones y Recomendaciones 68

6.1 Conclusiones 68

6.2 Recomendaciones 69

Referencias 70

Listado de Tablas

Tabla 1: Formulario para la extracción de la información. 24
Tabla 2: Cadena de búsqueda adaptada a Scholar Google 25
Tabla 3: Estudios primarios obtenidos de la búsqueda de Scholar Google 25
Tabla 4: Información extraída del estudio primario Introducing OSSF: A framework for online service cybersecurity risk management 27
Tabla 5: Cadena de búsqueda adaptada a Journal of Research of NIST 28
Tabla 6: Estudios primarios obtenidos de la búsqueda del Journal of Research of NIST 29
Tabla 7: Información extraída del estudio primario Small Business Information Security: the Fundamentals 30
Tabla 8: Información extraída del estudio primario Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans 31
Tabla 9: Estudio primario obtenido de la búsqueda del INCIBE 32
Tabla 10: Información extraída de la Herramienta de Autodiagnóstico del INCIBE 33
Tabla 11: Estudios analizados 34
Tabla 12: Presentación de los estudios analizados 35
Tabla 13: Funciones del NIST vs Funciones escogidas para la Herramienta 46
Tabla 14: Categorías NIST vs Herramienta y Cantidad de Preguntas por Categoría 47
Tabla 15: Ejemplos de Preguntas para la Herramienta de Autoevaluación 52
Tabla 16: Orden de la Función Identificar 53
Tabla 17: Comparación de la Secuenciación de las Categorías en la Función Identificar 54

Tabla 18: Secuencia de 8 preguntas en la Función Identificar 55

Tabla 19: Descripción de las cuatro (4) opciones de respuesta 58

Tabla 20: Cálculos para la Función Identificación 61

Tabla 21: Obtención del valor único del Estado Actual 61

Tabla 22: Obtención del valor único del Estado Deseado 62

Tabla 23: Ejemplo de las Recomendaciones de la Herramienta de Autoevaluación 67

Listado de Figuras

Figura 1: Resultado del Análisis de Frecuencias de las palabras del Estado de la Cuestión. 38
Figura 2: Mapa del Marco Conceptual 39
Figura 3: Diagrama de Flujo de la Técnica de Análisis de la Información 44
Figura 4: Ecuación para la Nota del Estado Actual 62
Figura 5: Ecuación para la Nota del Estado Actual en Identificación 62
Figura 6: Ejemplo de Resultados presentados por Función 63
Figura 7: Ejemplo de Resultados presentados para Identificación 64
Figura 8: Ejemplo de Resultados presentados para Protección 64
Figura 9: Ejemplo de Resultados presentados para Detección 65
Figura 10: Ejemplo de Resultados presentados para Respuesta 65
Figura 11: Ejemplo de Resultados presentados para Recuperación 66

Resumen Ejecutivo

Los ciberataques incrementan año a año a nivel mundial y no discriminan entre micro, pequeñas, medianas, o grandes empresas. Cualquier empresa que utilice recursos de Tecnología de la Información es un potencial blanco para ciberatacantes sea para practicar o porque poseen información que desean.

Muchas de las lecciones aprendidas luego de un ataque apuntan hacia una desasociación entre del estado real de los esfuerzos en ciberseguridad de las organizaciones y el estado que creían tener. Esto ha sido una constante en ataques a grandes organizaciones lo cual hace pensar que las pequeñas y medianas empresas se encuentran en una situación similar o, peor aún, no han tenido recursos para hacer una evaluación de su situación actual real.

Esta situación hace surgir en los investigadores la necesidad de proponer una Herramienta de Autoevaluación para Pequeñas y Medianas Empresas (PYMEs) basada en un marco teórico identificado como mejor práctica. Fue después de realizar el análisis respectivo de las mejores prácticas existentes que se escogió el Marco de Trabajo para la Mejora de la Infraestructura Crítica para la Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST).

Capítulo 1. Introducción

1.1 Generalidades

Este es un trabajo de investigación aplicado; es decir, se desarrolló una Herramienta de Autoevaluación partiendo del Marco de Trabajo para la Mejora de la Infraestructura Crítica para la Ciberseguridad del (NIST). El contenido de este documento se considera con derechos de autor, ya que la investigación está enfocada en el desarrollo de una herramienta nueva para que cualquier PYME, independientemente de su naturaleza de negocio; tenga una herramienta para la evaluación de la seguridad informática.

1.2 Antecedentes del Problema

Los ciberataques incrementan año a año a nivel mundial y Costa Rica no es la excepción. En el 2017, el 32% de las empresas en Costa Rica habían recibido un ciberataque (Revista Summa, 2018).

Los análisis post-ataque nos hablan de que muchas de las grandes organizaciones atacadas habían detectado, a través de sus marcos de referencia de ciberseguridad, las brechas de seguridad usadas para atacarlos, pero no actuaron al respecto a veces por falta de capacidad, o por falta de presupuesto, e incluso a veces por carencia de incentivos específicos ligados a la implementación de proyectos orientados a mejorar la postura de la ciberseguridad, como el ataque sufrido por Moller-Maerks en el 2017 por el virus NotPetya (Greenberg, 2018).

1.3 Definición y Descripción del Problema

En el contexto global, los ciberataques van en aumento al igual que los atacantes que usan a pequeños países y organizaciones como sus campos de entrenamiento previo a un ataque grande.

En general, existen pequeñas y medianas empresas (PYMES) que operan sin un marco de referencia de ciberseguridad definido o que han adoptado uno, pero no tienen la capacidad interna de realizar, desde cero, una evaluación que les permita entender su estatus con respecto al marco de referencia adoptado o un marco de referencia identificado como mejor práctica (Walker, 2019).

Por lo tanto, es preciso desarrollar una herramienta de autoevaluación orientada a las pequeñas y medianas empresas (PYMES) que ayuden a sus dueños a entender el estatus actual de los esfuerzos en ciberseguridad y que oriente, según las brechas detectadas, las acciones que ayuden a cerrar dichas brechas.

1.4 Justificación

El obtener una herramienta genérica y simple de aplicar, permitirá a cualquier PYME tener una actitud proactiva, en lugar de una actitud reactiva ante los eventos de ciberseguridad que pueden ocurrir en cualquier momento. Adicionalmente, se busca evitar un impacto negativo, por ejemplo: pérdidas económicas, daño de imagen, pérdida de oportunidades de negocio y/o clientes, entre otros, debido a un evento de ciberseguridad y un mejor manejo en los procesos digitales de la PYME.

1.5 Viabilidad

1.5.1 Punto de Vista Técnico

El Marco de Trabajo para la Mejora de la Infraestructura Crítica para la Ciberseguridad del NIST es uno de los marcos de trabajo reconocidos como mejor práctica para las empresas cuyos servicios críticos están soportados por infraestructura tecnológica.

Es un Marco de Trabajo existente, utilizado a nivel mundial y cuenta con suficiente acceso a información para proponer una herramienta de autoevaluación para PYMES basada en dicho estándar.

Adicionalmente, los investigadores han sido debidamente capacitados en el uso de este Marco de Trabajo y cuentan con experiencia laboral en el mismo. Por otra parte, se cuenta con el apoyo y guía de personas que utilizan y aplican este Marco de Trabajo en empresas de diversa índole.

1.5.2 Punto de Vista Operativo

El Estándar NIST se divide en 5 Funciones: Identificar, Proteger, Detectar, Responder y Recuperar y estas se subdividen en 23 categorías, que serán evaluadas por la herramienta.

Teniendo en cuenta que son dos investigadores para esta Tesis y que hay 3 meses para entender las 23 categorías y proponer una herramienta de autoevaluación para PYMES, se considera que cuentan con los recursos y tiempo adecuado.

Además, al momento de realizar la autoevaluación de la empresa a través de la herramienta desarrollada, no interrumpirá la operativa normal de esta.

Finalmente, la herramienta de autoevaluación podrá ser utilizada tanto por organizaciones en su formato auto-evaluativo como por consultores que quieran utilizarla al ser contratados para una evaluación de este tipo.

1.5.3 Punto de Vista Económico

El Marco de Trabajo que será utilizado es libre y de acceso gratuito por lo que no tiene un costo asociado para ser utilizado. De momento, al no tener empresa seleccionada, no se tienen costos teóricos.

Sin embargo, si durante el desarrollo de esta investigación surge un costo teórico, los costos lo asumirán los investigadores.

1.6 Objetivos

1.6.1 Objetivo General

Proponer una Herramienta de Autoevaluación para PYMEs basada en el Marco de Trabajo para la Mejora de la Infraestructura Crítica para la Ciberseguridad del NIST.

1.6.2 Objetivos Específicos

Describir la estructura y el contenido del Marco de Trabajo para la Ciberseguridad NIST.

Desarrollar una herramienta para la autoevaluación del estado de la ciberseguridad de una PYME.

Encontrar las brechas de seguridad de una PYME a través de la herramienta de autoevaluación.

Clasificar las brechas de seguridad identificadas a través de la herramienta de autoevaluación.

Proponer acciones para el cierre de las brechas de seguridad más críticas.

1.7 Alcances y Limitaciones

1.7.1 Alcances

El producto de esta investigación es desarrollar una herramienta, basada en el Marco de Trabajo para la Mejora de la Infraestructura Crítica para la Ciberseguridad del NIST, a través de una hoja de cálculo, que permita autoevaluar a una PYME. Cada empresa podrá encontrar y clasificar las brechas de seguridad informática a través de la herramienta, y al mismo tiempo, la herramienta propondrá las acciones necesarias para cerrar esas brechas de seguridad.

1.7.2 Limitaciones

Debido a que el objetivo del trabajo es el desarrollo de una propuesta de Herramienta de Autoevaluación, no se aplicará en ninguna empresa.

1.8 Marco de Referencia Organizacional y Socioeconómico

Este un trabajo de investigación aplicado en el cual se desarrollará una Herramienta de Autoevaluación la cual, según lo explicado en la sección 1.7.2, no será aplicada en ninguna empresa. Por ende, las secciones de Marco de Referencia Organizacional y Socioeconómico no serán documentadas pues no aplican a la investigación.

1.9 Estado de la Cuestión

1.9.1 Planificación de la Revisión

1.9.1.1 Formulación de la Pregunta

1.9.1.1.1 Foco de la Pregunta

En esta revisión sistemática se pretende identificar trabajos centrados en herramientas de autoevaluación para PYMEs en materia de seguridad informática.

1.9.1.1.2 Amplitud y Calidad de la Pregunta

1.9.1.1.2.1 Problema

Como fue comentado anteriormente, los ciberataques van en aumento y ningún tipo de empresa se escapa de esta amenaza. Proponer una herramienta de autoevaluación para las PYMES es contribuir a la solución ante esta amenaza. De este modo, el problema se centra en el estudio de los trabajos hechos previamente sobre herramientas de autoevaluación del estado actual en materia de ciberseguridad para PYMES.

1.9.1.1.2.2 Pregunta de Investigación

La pregunta de investigación sería la siguiente: ¿Cuáles herramientas de autoevaluación sobre el estado actual en materia de ciberseguridad existen para PYMES?

1.9.1.1.2.3 Palabras Clave y Sinónimos

A continuación, se definen un conjunto de palabras clave para localizar los trabajos hechos anteriormente, y que al mismo tiempo permitan realizar consultas a las fuentes más relevantes:

Ciberseguridad: Cybersecurity

Seguridad de la información: Information security

Pequeña y mediana empresa: Small and Medium Business

Estándares de seguridad informática: NIST, Framework, Standard, Guide

Autoevaluación: Self-assessment.

1.9.1.1.2.4 Intervención

Como parte de la revisión sistemática, se van a revisar las herramientas existentes sobre la autoevaluación de las PYMEs en materia de ciberseguridad, obteniendo así las más relevantes y luego se realizará el análisis de las herramientas.

1.9.1.1.2.5 Control

En este caso, no se considera un dato o trabajo inicial que deba estar incluido en el conjunto de resultados.

1.9.1.1.2.6 Resultado

El resultado de esta revisión es conocer las propuestas o herramientas existentes sobre la autoevaluación de las PYMEs en materia de ciberseguridad.

1.9.1.1.2.7 Medida de Salida

La medida de salida de los resultados obtenidos se enfocará en la cantidad de propuestas encontradas según el criterio de búsqueda definido anteriormente.

1.9.1.1.2.8 Población

La población que se va a analizar son las publicaciones que se encuentran en los repositorios de las fuentes seleccionadas y que tengan relación con el objetivo de esta revisión.

1.9.1.1.2.9 Aplicación

Los beneficiarios de esta revisión sistemática serán los dueños de las PYMEs y el personal encargado o departamento que administre los recursos de TI de la organización. Al mismo tiempo, beneficiará a cualquier persona que esté interesada en conocer el estado actual de negocio en materia de ciberseguridad.

1.9.1.1.2.10 Diseño Experimental

El meta-análisis de la revisión está enfocado a analizar las herramientas de autoevaluación en materia de ciberseguridad presentes en los estudios primarios. Esto permitirá conocer sobre las tendencias actuales y presentación de resultados de autoevaluación. Al mismo tiempo permite comparar las características de las herramientas más significativas identificadas en la revisión.

1.9.1.2 Selección de Fuentes

1.9.1.2.1 Definición del Criterio de Selección de Fuentes

Los criterios para la selección de las fuentes de búsqueda basan en la opinión y experiencia profesional de los autores de este trabajo. Las fuentes deben ser accesibles vía web y deben tener los elementos necesarios para ser incluidas en los motores de búsqueda tradicionales con capacidad de consultas avanzadas,

como los son por ejemplo Google o Bing. No se utilizarán fuentes que residan en la internet profunda o la internet oscura.

1.9.1.2.2 Lenguaje de Estudio

El lenguaje primario de los estudios será el inglés y los mismos serán extraídos mediante consultas con palabras claves en inglés; sin embargo, se tiene planeado buscar estudios cuyo lenguaje primario sea el español y serán extraídos mediante consultas con palabras claves en español. No se tiene claridad de si se encontrarán estudios relevantes en este último idioma; sin embargo, de encontrarles, se incluirán en el informe de la revisión sistemática el cual será realizado en español.

1.9.1.2.3 Identificación de Fuentes

1.9.1.2.3.1 Métodos de Selección de las Fuentes

La experiencia profesional y educacional de los autores será el criterio principal para la selección de las fuentes que ofrecen información de calidad en el área de herramientas de autoevaluación sobre el estado actual en materia de ciberseguridad para PYMES.

1.9.1.2.3.2 Cadenas de Búsqueda

Se utilizarán términos de búsqueda avanzados en conjunción con las palabras claves y/o conceptos relacionados con el Objetivo General de este trabajo. Entre los términos de búsqueda avanzados que se utilizarán están:

“”: para especificar cadenas de múltiples palabras

AND: para buscar fuentes que tengan todas las palabras claves solicitadas

OR: para buscar fuentes que tengan alguna de las palabras o cadenas claves

-: para buscar fuentes que tengan una palabra o cadena clave pero que no contengan otra palabra o cadena clave indicadas

~: para buscar fuentes con contenido relacionado a la palabra clave.

1.9.1.2.3.3 Lista de Fuentes

La lista de fuentes que se utilizarán para realizar la revisión sistemática es la siguiente:

IEEE Digital Library

Scholar Google

ACM Digital Library

Journal of Research of the NIST

Instituto Nacional de Ciberseguridad de España.

1.9.1.2.4 Selección de Fuentes Después de la Evaluación

Una vez realizadas la revisión de la lista de fuentes, se seleccionarán solamente aquellas en donde se encontraron estudios primarios relevantes según la experiencia profesional y educacional de los autores.

1.9.1.2.5 Comprobación de las Fuentes

Las fuentes se revisarán en primera instancia a través de Scimago Journal & Country Rank (del sitio web www.scimagojr.com) y el Índice H será usado como

referencia de comprobación. Posteriormente, aquellas fuentes que tengan un Índice H elevado, serán revisadas en conjunto con el tutor de la tesis. Utilizando el criterio experto de los autores de este trabajo y con el consentimiento del tutor, se decidió añadir una nueva fuente, sin necesidad de comprobarla, la cual es el Análisis de Riesgos del Instituto Nacional de Ciberseguridad de España (INCIBE).

1.9.1.3 Selección de los Estudios

Seguidamente se procederá a describir el proceso y el criterio que se utilizarán en la ejecución de la revisión para seleccionar y evaluar los estudios primarios.

1.9.1.3.1 Procedimiento para la selección de los estudios

Para seleccionar los estudios encontrados como primarios, se utilizará un procedimiento iterativo por cada una de las fuentes que se listaron anteriormente. El procedimiento consiste en ejecutar la consulta en motor de búsqueda en la fuente seleccionada. Para seleccionar un conjunto inicial de estudios, se leerán los títulos y el Resumen Ejecutivo de los estudios obtenidos de las búsquedas y se evaluarán según el criterio de inclusión y exclusión.

1.9.1.3.1.1 Definición del criterio de inclusión y exclusión de estudios

El criterio de inclusión se aplica a los resultados obtenidos después de ejecutar la consulta en el motor de búsqueda en la fuente seleccionada, esto permite obtener una primera selección de documentos que podrían ser candidatos a estudios primarios. Este criterio consiste en analizar el título, concordancia con las

palabras clave y el Resumen Ejecutivo de cada documento. En este criterio se localiza y elimina la mayor parte de los resultados obtenidos.

El criterio de exclusión se aplica al subconjunto de documentos obtenidos en la fase anterior, lo que permite obtener el conjunto de estudios primarios. Este criterio, involucra principalmente la lectura y el análisis del Resumen Ejecutivo y las conclusiones. También se realizará una lectura detallada sobre las otras partes del documento.

1.9.1.3.1.2 Definición de tipos de estudio

Los tipos de estudio primarios que se van a seleccionar durante esta revisión sistemática son los artículos que se encuentran en las fuentes listadas anteriormente, y que al mismo tiempo cumplan con los criterios de inclusión y exclusión.

1.9.1.3.2 Extracción de la Información

Se utilizará el siguiente formulario para documentar la información extraída de cada estudio primario que incluye:

Información de identificación del estudio (título, publicación, autores y referencia)

Descripción (área del estudio y resumen)

Aspectos por destacar.

Identificación	
Título	
Publicación	
Autores	
Referencia	
Descripción	
Área del Estudio	
Resumen	
Aspectos a Destacar	

Tabla 1: Formulario para la extracción de la información.

1.9.2 Ejecución de la Revisión

En esta sección se ejecutará la revisión sistemática en cada una de las fuentes seleccionadas, siguiendo los lineamientos especificados con anterioridad.

1.9.2.1 Ejecución de la selección en la fuente IEEE Digital Library

La búsqueda se realizó seleccionando las siguientes opciones:

Búsqueda en: Journals and Magazines.

Frases o palabras claves: **self assessment cybersecurity framework smb**.

La cadena de búsqueda se ajustó de diversas maneras debido a que se notó que pocos estudios contienen las palabras claves.

La ejecución de la búsqueda en IEEE Digital Library encontró 1 estudio. Al realizar el criterio de inclusión sobre el mismo; es decir, la revisión del título, concordancia con las palabras clave y el Resumen Ejecutivo, el mismo fue excluido.

De esta manera, la fuente IEEE Digital Library no contiene estudios a ser utilizados en esta revisión sistemática.

1.9.2.2 Ejecución de la selección en la fuente Scholar Google

La búsqueda se realizó seleccionando las siguientes opciones:

Frases o palabras claves: **self assessment cybersecurity framework**.

La cadena de búsqueda se ajustó para adaptarla con la sintaxis de la fuente y para que los estudios encontrados sean los más relevantes para la revisión.

self-assessment cybersecurity framework

Tabla 2: Cadena de búsqueda adaptada a Scholar Google

La ejecución de la búsqueda en Scholar Google encontró 2,670 estudios por lo que se decidió revisar los 20 más relevantes. Al realizar el criterio de inclusión sobre los mismos; es decir, la revisión del título, concordancia con las palabras clave y el Resumen Ejecutivo y posteriormente realizar el criterio de exclusión, se decidió considerar un estudio primario.

1	**Introducing OSSF: A framework for online service cybersecurity risk management.** Computers & Security, March 2017. Meszaros, J., & Buchalcevova, A.

Tabla 3: Estudios primarios obtenidos de la búsqueda de Scholar Google

1.9.2.2.1 Evaluación de la calidad del estudio

Se evaluó la calidad de Computers & Science utilizando Scimago Journal & Country Ranking y la revista tiene un Índice H de 72. Este índice indica que esta fuente tiene estudios de calidad que pasan por una serie de filtros y evaluaciones para ser publicados.

1.9.2.2.2 Revisión de la selección

Esta selección fue validada por los autores de este trabajo y el interés en su contenido hizo que se incluya en el mismo.

1.9.2.2.3 Extracción de información

Con el formato ya definido, se extrajo la información de este estudio primario.

Identificación	
Título	Introducing OSSF: A framework for online service cybersecurity risk management.
Publicación	Computers & Security Volumen 65, Marzo 2017. Páginas 300-313.
Autores	Meszaros, J., & Buchalcevova, A.
Referencia	(Meszaros & Buchalcevova, 2017)
Descripción	
Área del Estudio	Marco de trabajo para el manejo de los riesgos de ciberseguridad.
Resumen	Propuesta de un nuevo marco de trabajo para el manejo de los riesgos de ciberseguridad con dos componentes claves: el modelo de amenazas y el modelo de riesgos.
Aspectos a Destacar	

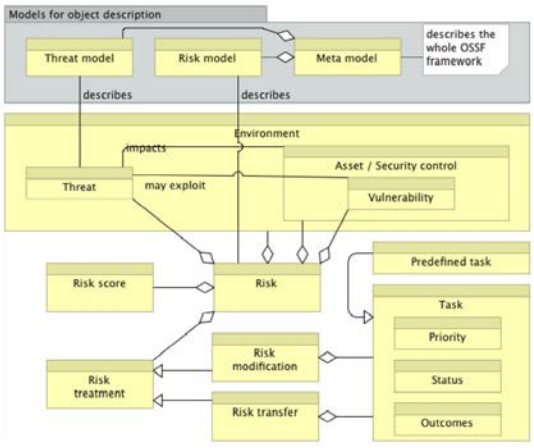

Fig. 1 – Components of the OSSF (ArchiMate notation, information structure viewpoint).

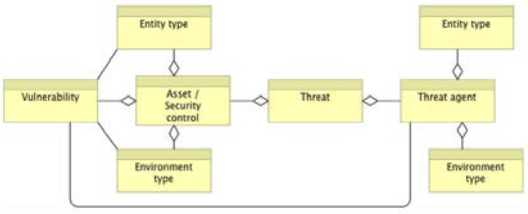

Fig. 2 – Threat model of the OSSF (ArchiMate notation, information structure viewpoint).

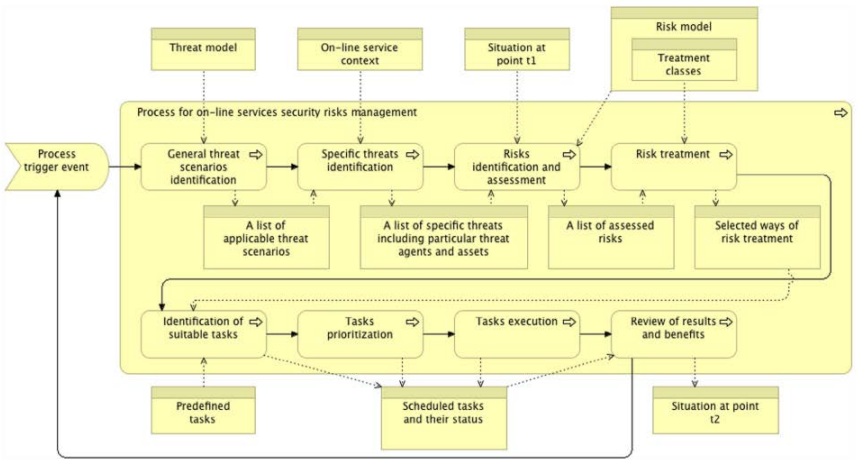

Fig. 3 – Risk management process of the OSSF (ArchiMate notation, business process viewpoint).

Tabla 4: Información extraída del estudio primario Introducing OSSF: A framework for online service cybersecurity risk management.

1.9.2.3 Ejecución de la selección en la fuente ACM Digital Library

La búsqueda se realizó seleccionando las siguientes opciones:

Búsqueda en: todo.

Frases o palabras claves: **self assessment cybersecurity framework smb**.

La cadena de búsqueda se ajustó de diversas maneras dejó de esta manera debido a que se obtenían pocos o ningún estudio con todas las palabras claves.

La ejecución de la búsqueda en ACM Digital Library no dio como resultado ningún estudio primario que deba ser evaluado en esta revisión sistemática.

1.9.2.4 Ejecución de la Selección en la Fuente Journal of Research of NIST

La búsqueda se realizó seleccionando las siguientes opciones:

Búsqueda en el motor de búsqueda del Journal

Frases o palabras clave: **small business security self assessment**

Small business security self assessment

Tabla 5: Cadena de búsqueda adaptada a Journal of Research of NIST

La ejecución de la búsqueda en Journal of Research of NIST encontró 1,989,196 estudios por lo que se decidió revisar los 10 más relevantes. Al realizar el criterio de inclusión sobre los mismos; es decir, la revisión del título, concordancia con las palabras clave y el Resumen Ejecutivo y posteriormente realizar el criterio de exclusión, se identificaron dos documentos como primarios.

1	**Small Business Information Security: the Fundamentals** NIST Interagency/Internal Report (NISTIR) - 7621 Rev 1, Noviembre 03, 2016
2	**Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans** Special Publication (NIST SP) - 800-53A Rev 4. Diciembre 11, 2014

Tabla 6: Estudios primarios obtenidos de la búsqueda del Journal of Research of NIST

1.9.2.4.1 Evaluación de la calidad del estudio

Para evaluar la calidad de los documentos ubicados en el Journal of Research of NIST, se realizó la consulta en el sitio web Scimago Journal & City Rank. El resultado de la búsqueda indicó que este Journal tiene un índice H de 49. Este índice indica que esta fuente tiene estudios de calidad que pasan por una serie de filtros y evaluaciones para ser publicados.

1.9.2.4.2 Revisión de la selección

Esta selección fue validada por los autores de este trabajo y el interés en su contenido hizo que se incluya en el mismo.

1.9.2.4.3 Extracción de información

Al igual que las fuentes anteriores, se utilizará el formulario para documentar la información extraída de cada estudio primario.

Identificación	
Título	Small Business Information Security: the Fundamentals
Publicación	NIST Interagency/Internal Report (NISTIR) - 7621 Rev 1 Noviembre 03, 2016
Autores	Celia Paulsen Patricia Toth
Referencia	(Toth & Paulsen, 2016)
Descripción	
Área del estudio	Seguridad de la información, ciberseguridad, pequeña empresa
Resumen	El documento es un informe que desarrolló NIST como guía de referencia sobre ciberseguridad para pequeñas empresas. Presenta los fundamentos para un programa de seguridad de información para pequeña empresa en lenguaje no técnico.
Aspectos a Destacar	
▪ El documento explica por qué se da su enfoque a pequeña empresa ▪ Explica además sobre la administración de riesgos y cómo abarcarlo ▪ Menciona cómo se debe abarcar la seguridad de información según los cinco dominios de NIST ▪ Al final del documento presenta una serie de plantillas para que la pequeña empresa puede llenar con su información.	

Tabla 7: Información extraída del estudio primario Small Business Information Security: the Fundamentals

Identificación	
Título	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
Publicación	Special Publication (NIST SP) - 800-53A Rev 4. Diciembre 11, 2014
Autores	Ronald S. Ross
Referencia	(Ross, 2014)
Descripción	
Área del estudio	Seguridad de la información, ciberseguridad, evaluación, controles de seguridad, gestión de riesgos
Resumen	El documento proporciona un conjunto de procedimientos para realizar evaluaciones de controles de seguridad en los sistemas de información y organizaciones federales
Aspectos a Destacar	
▪ Los procedimientos de evaluación se ejecutan en varias fases del ciclo de vida del desarrollo del sistema de información ▪ Los procedimientos son personalizables y se pueden adaptar a cada organización ▪ Se realizan evaluaciones sobre controles de seguridad y evaluación sobre controles de privacidad. Al mismo tiempo se comparan con la tolerancia de riego que desee manejar la organización ▪ Al final del documento se proporciona una lista de verificación para que se pueda aplicar a cada organización	

Tabla 8: Información extraída del estudio primario Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans

1.9.2.5 Ejecución de la Selección en la Fuente Análisis de Riesgos del INCIBE

Debido al conocimiento experto de los autores de este trabajo y del tutor de este, no fue necesaria ninguna búsqueda ya que se conoce la dirección de este Análisis de Riesgos: https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos

Una vez encontrado el Análisis de Riesgos, al realizar el criterio de inclusión sobre el mismo; es decir, la revisión del título, concordancia con las palabras clave y el Res Ejecutivo titulado ¿Conoce sus Riesgos?, se identificó el mismo como documento como primario.

1	**Herramienta de Autodiagnóstico** Instituto Nacional de Ciberseguridad de España (INCIBE), sin fecha

Tabla 9: Estudio primario obtenido de la búsqueda del INCIBE

1.9.2.5.1 Evaluación de la calidad del estudio

Debido a que este Análisis de Riesgos fue incluido por el criterio experto de los autores de este trabajo y el tutor del mismo, no se realizó evaluación de la calidad del estudio.

1.9.2.5.2 Revisión de la selección

Esta selección fue validada por los autores de este trabajo y el interés en su contenido hizo que se incluya en el mismo.

1.9.2.5.3 Extracción de información

Al igual que las fuentes anteriores, se utilizará el formulario para documentar la información extraída del Análisis de Riesgos del INCIBE.

Identificación	
Título	Herramienta de Autodiagnóstico
Publicación	Instituto Nacional de Ciberseguridad de España (INCIBE), sin fecha
Autores	Desconocidos
Referencia	(INCIBE, s.f.)
Descripción	
Área del estudio	Análisis de Riesgos de Ciberseguridad
Resumen	Es una Herramienta de Autodiagnóstico que calcula el riesgo del negocio y da recomendaciones genéricas
Aspectos a Destacar	

- Doce (12) preguntas y respuestas sencillas
- Indica el porcentaje de completitud según la cantidad de preguntas contestadas
- Provee un resumen del diagnóstico y un resultado de manera visual que se capturó al final de esta sección
- Evalúa el riesgo general y el riesgo individual en las áreas de Personas, Procesos y Tecnología
- Provee consejos según el nivel del riesgo general en cada una de las tres áreas mencionadas anteriormente

Tabla 10: Información extraída de la Herramienta de Autodiagnóstico del INCIBE

1.9.3 Análisis de resultados

Una vez ejecutadas las revisiones de todas las fuentes identificadas y con el conjunto de estudios primarios, se presentan las conclusiones del análisis de estos.

1.9.3.1 Estudios Analizados

En la Tabla 11 se muestra un resumen de los estudios analizados por cada fuente, cuántos fueron considerados relevantes, cuántos fueron seleccionados como primarios. En esta primera etapa del trabajo no se ha realizado un refinado del análisis de las fuentes por lo que la columna de refinado muestra que aún no aplica.

Fuentes	Estudios	Relevantes	Primarios	Primarios (refinado)
IEEE Digital Library	1	0	0	N/A
Scholar Google	20	20	1	N/A
ACM Digital Library	0	0	0	N/A
Journal of Research of the NIST	10	10	2	N/A
INCIBE	1	1	1	N/A
TOTAL	32	31	4	N/A

Tabla 11: Estudios analizados

1.9.3.2 Presentación de Resultados

La presentación de los resultados obtenidos se agrupa en tres áreas que fueron consideradas un aporte importante para el desarrollo de una Herramienta de Autoevaluación para PYMEs basada en el Marco de Trabajo para la Mejora de la Infraestructura Crítica para la Ciberseguridad del NIST. Las áreas consideradas son:

Trabajos orientado proceso adecuado a seguir para una evaluación.

Trabajos orientados a herramientas de autoevaluación de seguridad informática.

Trabajos orientados a pequeña y mediana empresa.

En la Tabla 12 se muestra un resumen de los estudios primarios revisados y su relevancia para cada una de las áreas consideradas.

Estudio	Trabajos orientado proceso adecuado a seguir para una evaluación	Trabajos orientados a herramientas de autoevaluación de seguridad informática	Trabajos orientados a pequeña y mediana empresa
Introducing OSSF: A framework for online service cybersecurity risk management.	X		
Small Business Information Security: the Fundamentals		X	X
Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans		X	
Herramienta de Autodiagnóstico del INCIBE		X	

Tabla 12: Presentación de los estudios analizados

1.9.3.3 Resultados del Cálculo Estadístico

Para el análisis del Estado de la Cuestión de este trabajo, no se realizó un Cálculo Estadístico sobre los estudios primarios seleccionados.

1.9.3.4 Resultados del Análisis de Sensibilidad

Para el análisis del Estado de la Cuestión de este trabajo, no se realizó un Cálculo Estadístico sobre los estudios primarios seleccionados.

1.9.3.5 Conclusiones

Analizados los estudios primarios seleccionados y habiendo realizado una comparación entre los mismos, se llega a las siguientes conclusiones:

Existen trabajos realizados que ayudan a conceptualizar puntos importantes a tener en cuenta al desarrollar una herramienta de evaluación.

Existen herramientas de autoevaluación basadas en el Marco Trabajo para la Mejora de la Infraestructura Crítica para la Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST).

Una de las herramientas de autoevaluación identificadas es sencilla en demasía, no tiene mayor explicación o ayuda, y no provee propuestas para el cierre de brechas identificadas.

Otra de las herramientas de autoevaluación identificada es compleja, asume un alto nivel de conocimiento de los conceptos de Tecnología de la Información, y tampoco provee propuestas para el cierre de las brechas que identifique.

La herramienta de autodiagnóstico del INCIBE es sencilla, no asume un alto nivel de conocimiento de los conceptos de Tecnología de la Información y provee propuestas para reducir los riesgos de la empresa; sin embargo, es cuestionable la robustez del análisis de riesgos realizado

a través de 12 preguntas solamente y no es un análisis comprehensivo del estado completo de la organización en materia de la Mejora de la Infraestructura Crítica.

Capítulo 2. Marco Conceptual

Este es un trabajo de investigación en el cual no se expondrán y contrastarán teorías ni se generará una teoría nueva, sino que se expondrán y utilizarán conceptos existentes e identificados durante la revisión sistémica realizada en el Estado de la Cuestión.

Para representar a través de un mapa los conceptos claves de esta investigación, el Estado de la Cuestión completo se procesó a través de un software que analiza la frecuencia de las palabras en un texto, en este caso se utilizó la herramienta en línea TagCrowd (TagCrowd, s.f.). Existen palabras que son artículos o preposiciones como “a”, “de”, “la”, “el”, entre otras; las cuales tienen una alta frecuencia de utilización, pero ninguna relevancia para el Marco Conceptual. Los resultados arrojados por TagCrowd se depuraron para obtener las 13 palabras de mayor frecuencia en el Estado de la Cuestión, las cuales pueden observarse junto con sus respectivas frecuencias en la Figura 1: Resultado del Análisis de Frecuencia de palabras del Estado de la Cuestión.

Figura 1: Resultado del Análisis de Frecuencias de las palabras del Estado de la Cuestión.

Partiendo de la relevancia de cada una de estas palabras para el Marco Conceptual de esta investigación, se encontró que el conocimiento existente se puede representar a través de la Figura 2: Mapa del Marco Conceptual realizado por los investigadores:

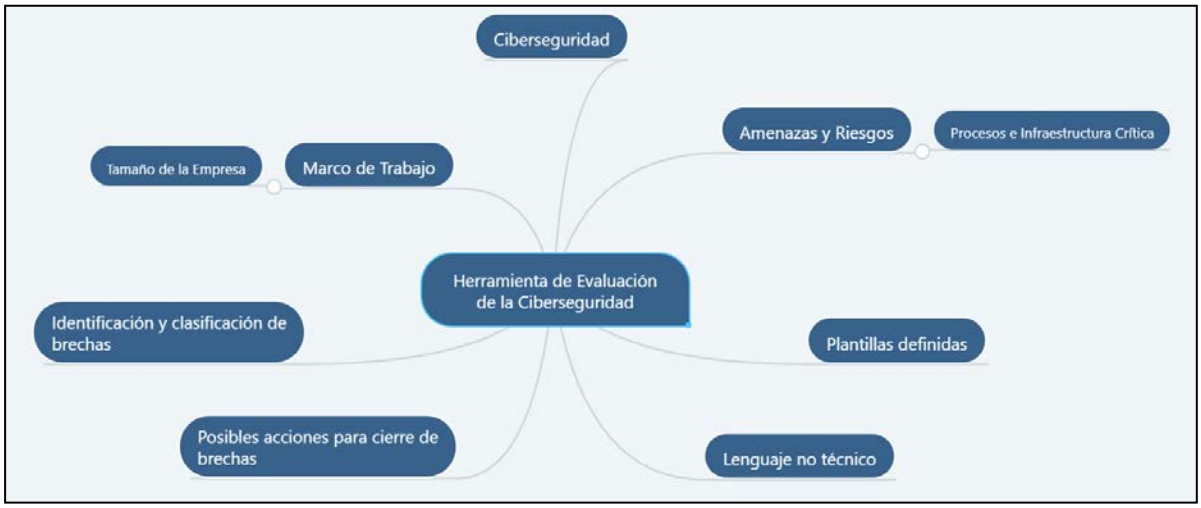

Figura 2: Mapa del Marco Conceptual

La ciberseguridad se conoce, en su forma más simplista, como la seguridad de la Tecnología de la Información (TI) o seguridad de la información electrónica (Kaspersky Lab, s.f.) y es de esta manera en que se diferencia de la seguridad física.

La evaluación de la ciberseguridad de una empresa empieza por el Marco de Trabajo que haya sido escogido por la misma para ser implementado o, en su defecto, como estándar establecido o mejor práctica del mercado para determinar el estatus de la ciberseguridad.

En términos generales, se reconocen cuatro (4) como los estándares más robustos y de mayor uso (Watson, 2019):

El Marco de Trabajo para la Mejora de la Infraestructura Crítica para la Seguridad del NIST.

PCI DSS

ISO 27001/27002

Controles de Seguridad Críticos CIS.

Una vez escogido el Marco de Trabajo, el mismo se ajustada teniendo en cuenta las características significativas de la organización, una de las cuales es el tamaño de esta (Ross, 2014). En Costa Rica, el tamaño de la empresa se determina “mediante la ponderación matemática de una fórmula que las clasifica según actividad empresarial, y que contempla el personal promedio contratado en un período fiscal, el valor de los activos, el valor de ventas anuales netas y el valor de los activos totales netos” (MEIC, s.f.). Según el resultado obtenido de la fórmula las PYMES se subclasifican en Microempresa, Pequeña Empresa, Mediana Empresa.

El ajuste al Marco de Trabajo debe también estar dirigido por criterios con base los riesgos y las amenazas identificadas con potencial impacto a los procesos e infraestructura crítica de la empresa para evitar situaciones en las que los controles de seguridad implementados estén desalineados con la criticidad de la infraestructura (Meszaros & Buchalcevova, 2017).

Una herramienta que funcione en modalidad autoevaluativa para una PYME debe contar con dos características claves para que pueda ser utilizada en formato autoevaluativo (Toth & Paulsen, 2016) (Ross, 2014):

i. Proveer plantillas definidas para la evaluación

ii. Estar realizada en lenguaje no técnico

Las plantillas pre-definidas son la herramienta ya lista para ser utilizada por la empresa, sin tener que invertir en entender cómo ajustar el Marco de Trabajo, cómo evaluarlo y el lenguaje no técnico es la clave para que todas aquellas organizaciones que no cuentan con un especialista en TI o cuyo especialista no tiene conocimientos profundos de ciberseguridad puedan aplicarla sin problemas.

La innovación de esta investigación consiste en incorporar, como paso final, la información necesaria para que las empresas puedan clasificar las brechas identificadas por la herramienta de autoevaluación al igual que posibles acciones para el cierre de las brechas identificadas.

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

En este trabajo se utilizará la investigación de tipo aplicada ya que se emplearán las mejoras prácticas en el ámbito de la ciberseguridad que propone el Marco de Trabajo NIST, con el objetivo de atender las brechas de seguridad que podrían presentar las PYMES.

3.2 Alcance Investigativo

El alcance investigativo de este trabajo es descriptivo ya que se utiliza el perfil de las PYMES y se basa en la tendencia de las mismas de operar sin un Marco de Trabajo de ciberseguridad definido.

Como se ha mencionado anteriormente, la intención de este trabajo es que cualquier PYME pueda hacer uso de la herramienta y contrastar el estado actual versus las buenas prácticas que propone el Marco de Trabajo del NIST.

3.3 Enfoque

Para el desarrollo de este trabajo se utilizará un enfoque cualitativo ya que este tipo de enfoque se adapta mejor al contexto de investigación. Este enfoque es muy utilizado en el área de la Informática y, al mismo tiempo, es muy utilizado en la implementación de estándares. Además, no se depende de variables para comprobar una teoría como tal, sino que el enfoque será proponer acciones para el cierre de las brechas de seguridad identificadas en una PYME.

3.4 Diseño

Este trabajo emplea un enfoque cualitativo utilizando una investigación evaluativa. Las características de la investigación evaluativa se adaptan para la implementación de estándares dentro de una organización y, al mismo tiempo, permite evaluar la eficiencia de una organización en términos de seguridad informática.

3.5 Población y Muestreo

Al ser este un trabajo de enfoque cualitativo, y al mismo tiempo una investigación aplicada al desarrollo de la herramienta, se utilizará la técnica de muestreo no probabilístico basado en método intencional o por conveniencia donde el individuo que conviene investigar la PYME y su situación en materia de Infraestructura Crítica para la Ciberseguridad (Universo Fórmulas, s.f.)

3.6 Instrumentos de Recolección de Datos

Al tratarse de un enfoque cualitativo, el elemento de recolección de datos será la entrevista a través de plantillas predefinidas donde se realizarán una serie de preguntas relacionadas con los aspectos de ciberseguridad de la PYME. El resultado se analizará con el objetivo de identificar brechas de seguridad según el Marco de Trabajo del NIST y proponer soluciones según la severidad de las brechas.

3.7 Técnicas de Análisis de Información

Para realizar el respectivo análisis de información, se utilizará el proceso presentado en la Figura 3: Diagrama de Flujo de la Técnica de Análisis de la Información:

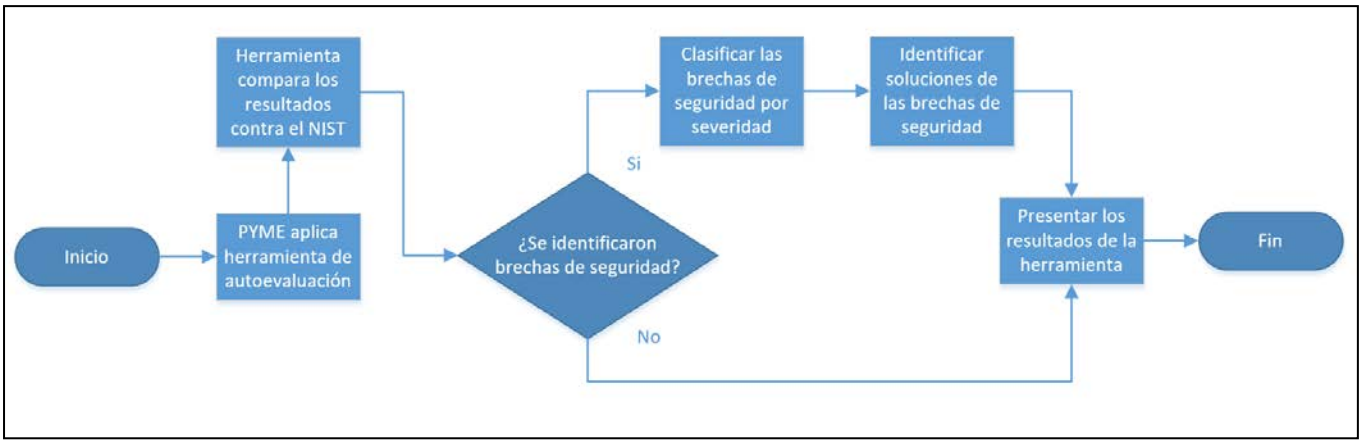

Figura 3: Diagrama de Flujo de la Técnica de Análisis de la Información

3.8 Estrategia de Desarrollo de la Propuesta

Las plantillas que se presentarán a la PYME estarán basadas en los cinco dominios que define el Marco de Trabajo del NIST. Para asegurar la mayor compatibilidad y facilidad de uso, se analizarán varios escenarios y se escogerá el que permita mayor flexibilidad.

Capítulo 4. Análisis del Diagnóstico

4.1 Estructura del NIST

4.1.1 Funciones

En primera instancia, el NIST se divide en cinco (5) funciones con el objetivo de que la empresa piense en sus riesgos organizadamente y vea que una adecuada comprensión y gestión en las primeras funciones repercute positivamente en las siguientes. Estas cinco funciones y su descripción son:

1. **Identificar:** donde se incorporan los aspectos de compresión organizacional
2. **Proteger:** donde se analizan los servicios críticos y las medidas de seguridad necesarias para la operación de estos
3. **Detectar:** donde se consideran las actividades que permiten identificar intrusiones o incidentes
4. **Responder:** donde se revisan las actividades apropiadas para contener y reaccionar ante una intrusión o incidente
5. **Recuperar:** donde se enfocan las acciones para la recuperación luego de un incidente o intrusión.

Utilizando el criterio experto de los autores y el tutor del este trabajo, se tomó la decisión de utilizar estas cinco funciones para organizar la Herramienta de Autoevaluación; sin embargo, se utilizarán las palabras en acción y no en verbo; es decir, en lugar de Identificar, se usará Identificación. La Tabla 13 muestra la relación entre las funciones del NIST y las funciones que utilizarán en la Herramienta de Autoevaluación.

	Función 1	Función 2	Función 3	Función 4	Función 5
NIST	Identificar	Proteger	Detectar	Responder	Recuperar
Herramienta	Identificación	Protección	Detección	Respuesta	Recuperación

Tabla 13: Funciones del NIST vs Funciones escogidas para la Herramienta

4.1.2 Categorías

Las cinco (5) funciones del NIST se subdividen en veintitrés (23) categorías en total que evalúan aspectos específicos de las funciones. Utilizando el criterio experto de los autores y el tutor del este trabajo, se tomó la decisión de utilizar la misma cantidad de categorías para organizar la Herramienta de Autoevaluación; sin embargo, se realizaron ajustes a sus nombres con el fin de facilitar la comprensión por parte del personal de las PYMES.

4.1.2 Subcategorías

Cada una de las categorías del NIST se subdivide en subcategorías que son las que evalúan aspectos puntuales de cada categoría. Estas subcategorías se convirtieron en preguntas específicas en la Herramienta de Autoevaluación para que la PYME evalúe su estado actual y su estado deseado. Se escogió realizarlo en forma de pregunta con el fin de facilitar la comprensión del aspecto específico que está siendo evaluado, resultando un total de ciento nueve (109) preguntas específicas a ser realizadas para la Autoevaluación.

La Tabla 14 muestra la relación entre las funciones de la Herramienta de Autoevaluación, las categorías del NIST, los nombres que se utilizarán en las Categorías de la Herramienta de Autoevaluación y la cantidad de preguntas de evaluación que resultó en cada una de estas categorías. Las preguntas específicas se podrán encontrar en la Herramienta de Autoevaluación misma.

Función Herramienta	Categoría NIST	Categoría Herramienta	Cantidad de Preguntas
Identificación	Entorno empresarial	Entorno empresarial	5
	Gobernanza	Gobernanza	4
	Estrategia de gestión de riesgos	Gestión de Riegos	3
	Gestión de activos	Gestión de Activos	6
	Evaluación de riesgos	Riesgos Organizacionales	6
	Gestión del riesgo de la cadena de suministro	Riesgos en Cadena Suministros	5
Protección	Conciencia y capacitación	Capacitación	5
	Procesos y procedimientos de protección de la información	Procesos y Procedimientos	12
	Gestión de identidad y control de acceso	Control de Acceso	8
	Seguridad de datos	Seguridad de Datos	8
	Mantenimiento	Mantenimiento	2
	Tecnología protectora	Tecnología de Protección	5
Detección	Anomalías y eventos	Detección de Intrusiones	5
	Vigilancia continua de seguridad	Monitoreo Continuo	8
	Procesos de detección	Proceso para Detección de Intrusiones	5
Respuesta	Planificación de respuesta	Proceso de Respuesta	1
	Comunicaciones	Comunicación de Incidentes	5
	Análisis	Análisis de Incidentes	5
	Mitigación	Mitigación de Incidentes	3
	Mejoras	Mejora del Proceso de Respuesta	2
Recuperación	Planificación de recuperación	Proceso de Recuperación	1
	Mejoras	Mejora del Proceso de Recuperación	2
	Comunicaciones	Comunicación de la Recuperación	3

Tabla 14: Categorías NIST vs Herramienta y Cantidad de Preguntas por Categoría

Capítulo 5. Propuesta de Solución

5.1 Escenarios para la Herramienta de Autoevaluación

Para llevar a cabo la autoevaluación se utilizan las preguntas resultantes de la conversión de las subcategorías del Marco de Trabajo para la Mejora de la Infraestructura Crítica del NIST, las cuales se adoptaron a un nivel de compresión para una PYME, se presentan los resultados de la autoevaluación y posteriormente se brindan recomendaciones para cerrar las brechas de seguridad identificadas.

Sin embargo, la forma de implementar este cuestionario, presentar los resultados y brindar recomendaciones plantea distintos escenarios, especialmente en la forma para que el usuario complete las preguntas de la herramienta.

El primer escenario que se presenta es imprimir las preguntas del cuestionario y dar las hojas para que el usuario proceda con la autoevaluación. El problema con esta propuesta es el ingreso manual de datos, además existe el riesgo de cometer errores cuando se realicen los cálculos manualmente. Adicionalmente, no se presentan los resultados de manera inmediata.

El segundo escenario que se presenta es transcribir las preguntas del cuestionario en una hoja de cálculo. La ventaja de esta propuesta es que permite procesar los cálculos de manera automática y dar los resultados al instante. A pesar de que no se aprovecha al máximo el uso de la tecnología, por ejemplo, una página web, este escenario cumple con los objetivos.

El tercer escenario que se presenta es darle al usuario un enlace para que pueda llenar el cuestionario en una página web. La desventaja con la implementación de este modelo es que conlleva una la complejidad técnica mayor que la hoja de cálculo, lo que consume más tiempo de implementación.

Adicionalmente, se deben considerar más variables en el diseño, por ejemplo, tipo de servidor, hospedaje de la página, requisitos de seguridad, entre otros.

Por lo tanto, con el objetivo de dar una propuesta de una herramienta de autoevaluación en materia de ciberseguridad para PYME, se decidió transcribir la estructura y preguntas resultantes del NIST en una hoja de cálculo, ya que esta solución permite mostrar los resultados y las recomendaciones al instante, de igual forma, el tiempo de implementación es menor que desarrollar una aplicación web.

5.2 Creación de las Preguntas para la Evaluación

Para el desarrollo de la herramienta, no se partirá de cero sino que se usará el Marco de Trabajo para la Mejora de la Infraestructura Crítica para la Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST). En la sección 1.5 Viabilidad se desarrollaron las razones de la escogencia de este Marco de Trabajo, por lo cual, no se desarrollarán de nuevo sino que se referencia esta sección. Una de las fortalezas que tiene este Marco de Trabajo es su robustez; sin embargo, esta fortaleza es a la vez su más grande debilidad a la hora de utilizarlo en una PYME la cual, dependiendo de su tamaño y su enfoque, puede contar con recursos de TI o puede no tener personal de TI del todo.

5.2.1 Pregunta Sencilla

El primer aspecto clave para la herramienta que se desarrolló es formular preguntas a través de las cuales se haga la evaluación de la PYME y que estas sean, no solamente en español, sino en un lenguaje entendible por una persona sin conocimientos profundos o formación en Tecnologías de la Información haciendo

que la herramienta sea sencilla de usar y pueda, por ende, funcionar en modo autoevaluación; es decir, sin ayuda de un consultor o especialista de TI.

A esta técnica se le puede llamar **Pregunta Sencilla** y se puede tomar, por ejemplo, la Categoría ID.BE-5 del Marco de Trabajo del NIST para ilustrar la necesidad de usar un lenguaje entendible por cualquier persona. Esta categoría indica: ***"ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales)"***. Al hablar de resiliencia en términos organizacionales se está hablando de la cantidad máxima de tiempo que una organización puede tener servicios críticos fuera del línea o caídos de tal forma que pueda recuperarse y volver a operar antes de sufrir una pérdida tal que sea imposible la recuperación de esta. Una vez analizada la categoría y su objetivo, se tomó la decisión de formular la pregunta de la siguiente manera: ***"¿La organización identificó tiempos máximos de recuperación en caso de caída de los servicios críticos?"*** De esta forma, la pregunta es clara y específica.

5.2.2 Pregunta con Frase Introductoria

Otra técnica que se utilizó para la formulación de preguntas que sean fáciles de entender, es comenzar la pregunta con una frase introductoria que ayude al lector a ubicarse en el contexto de la pregunta y poder así no sólo entenderla sino escoger la mejor respuesta.

A esta técnica se le puede llamar **Pregunta con Frase Introductoria** y se puede usar como ejemplo la Categoría ***"PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo,***

desaprovisionamiento, selección del personal)”. Si bien se podría decir que el lenguaje de esta categoría es más fácil de entender que el primer ejemplo, todavía tiene campo para formular la pregunta en lenguaje menos técnico. La pregunta se formuló de la siguiente manera: “***En los procesos de Recursos Humanos (contrataciones, despidos, cambios de puestos, etc.) ¿Se incluyen los aspectos necesarios para la Seguridad de TI (cambios o eliminación de accesos, etc.)?”*.**

5.2.3 Pregunta con Frase de Definición

De manera similar, algunas preguntas se iniciaron con una frase introductoria que define el concepto que se quiere evaluar. Esta técnica se utilizó en los casos en que un concepto conocido de TI pueda generar ambigüedad en lenguaje no técnico y se le puede llamar Pregunta con Frase de Definición.

Se puede utilizar como ejemplo la Categoría ***“RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente”*** para la cual se tomó la decisión de formular la pregunta de la siguiente manera: ***“Entendiendo incidente como una interrupción parcial o total en un servicio de la organización, ¿Se tiene un Plan de Respuesta a Incidentes que se ejecute o siga al inicio y durante el incidente?”***.

La Tabla 15 provee más ejemplos de cada una de las técnicas descritas anteriormente y utilizadas a través de las preguntas de la Herramienta de Autoevaluación.

Técnica Utilizada	Categoría Marco de Trabajo NIST	Pregunta Herramienta Autoevaluación
Pregunta simple	DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	¿Se monitorean las actividades realizadas por los empleados en las computadoras?
Pregunta simple	ID.BE-3: Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.	¿La empresa tiene misión, visión y objetivos todo documentado?
Pregunta con Frase Introductoria	RC.RP-1: El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	Una vez contenido y mitigado el incidente, ¿Se tienen un Plan de Recuperación de Incidentes que se ejecute para restaurar los servicios afectados por el incidente?
Pregunta con Frase Introductoria	RS.IM-2: Se actualizan las estrategias de respuesta.	Si hay lecciones aprendidas, ¿se incorporan en el Plan de Recuperación para mejorarlo?
Pregunta con Frase de Definición	ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.	Entendiendo tolerancia o apetito al riesgo como el nivel de riesgo que la empresa está dispuesta a aceptar para conseguir su misión, visión y objetivos, ¿La tolerancia o apetito al riesgo de la organización está definida y documentada?
Pregunta con Frase de Definición	ID.RA-1: Se identifican y se documentan las vulnerabilidades de los activos.	Entendiendo vulnerabilidad como un defecto o característica que puede usarse para un ataque, ¿Se conocen las vulnerabilidades de los equipos de cómputo y sistemas?

Tabla 15: Ejemplos de Preguntas para la Herramienta de Autoevaluación

5.2.4 Secuenciación de las Preguntas

Al analizar el Marco de Trabajo escogido, se notó que las áreas que son evaluadas son comprehensivas, pero no fueron creadas con una secuencia lógica

que facilite una autoevaluación por parte de personal no técnico. Si se analiza en detalle la función de Identificar, por ejemplo, se observa que las categorías a evaluar “saltan” o “brincan” entre ellas o de una a otra y no siguen un orden lógico partiendo de lo general hacia lo más específico ni viceversa.

La Tabla 16 lista las categorías de la Función identificar y provee un buen ejemplo de estos “saltos” o “brincos” lógicos entre las áreas ya que, siguiendo el orden en que el Marco de Trabajo las lista, primero se evaluan el inventario de los activos, luego se pasan a dos áreas diferentes, para retornar y evaluar cómo están los riesgos de esos activos y, posteriormente evaluar cómo se definió el proceso de Gestión de Riesgos con el que se gestionan los riesgos que ya fueron evaluados.

Identificador de Categoría	Categoría	Descripción
ID.AM	Gestión de activos	Evaluación del inventario de activos, priorización según criticidad y valor, roles y responsabilidades en Seguridad de TI
ID.BE	Entorno empresarial	Evaluación de la empresa y el ambiente con que se relaciona
ID.GV	Gobernanza	Evaluación de los aspectos de la gobernanza de la empresa
ID.RA	Evaluación de riesgos	Evaluación de los resultados de la gestión de riesgos
ID.RM	Estrategia de gestión de riesgos	Evaluación de la definición del Proceso de Gestión de Riesgos
ID.SC	Gestión del riesgo de la cadena de suministro	Evaluación de la empresa y sus proveedores

Tabla 16: Orden de la Función Identificar

Pensando en la facilidad para la persona que realice la autoevaluación, se tomó la decisión de reorganizar las categorías de las más general a las más

específicas y, no hacerlo solamente a nivel de categorías sino a nivel de preguntas individuales, colocando las mismas en el mejor orden lógico posible, aunque esto signifique intercalar preguntas de distintas categorías.

Utilizando la función de Identificar como ejemplo, la Tabla 17 hace una comparación entre el orden de las categorías en el Marco de Trabajo y el orden en que se decidió colocarlas para la Herramienta de Autoevaluación. La Tabla 18 utiliza una pequeña sección de la Herramienta de Autoevaluación como ejemplo del resultado al organizar las preguntas siguiendo el propuesto orden de las categorías, pero insertando preguntas específicas, aunque sean de otra categoría, cuando tiene sentido lógico. Al revisar el orden en que las preguntas se colocaron, se nota que primero se encuentran las de la categoría Entorno empresarial pero las preguntas van en orden 3, 2, 4, 5, 1 en lugar del orden 1, 2, 3, 4 y 5; posteriormente se comienza con la pregunta 1 de Gobernanza, se intercala la pregunta 6 de Gestión de activos, para continuar con la 2 de Gobernanza.

Identificador de Categoría	Categoría – Orden según NIST	Identificador de Categoría	Categoría – Orden según Herramienta
ID.AM	Gestión de activos	ID.BE	Entorno empresarial
ID.BE	Entorno empresarial	ID.GV	Gobernanza
ID.GV	Gobernanza	ID.RM	Estrategia de gestión de riesgos
ID.RA	Evaluación de riesgos	ID.AM	Gestión de activos
ID.RM	Estrategia de gestión de riesgos	ID.RA	Evaluación de riesgos
ID.SC	Gestión del riesgo de la cadena de suministro	ID.SC	Gestión del riesgo de la cadena de suministro

Tabla 17: Comparación de la Secuenciación de las Categorías en la Función Identificar

Pregunta Herramienta Autoevaluación	Subcategoría según NIST
¿La empresa tiene misión, visión y objetivos todo documentado?	**ID.BE-3:** Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.
¿La empresa provee infraestructura crítica usada por todo su sector de la industria?	**ID.BE-2:** Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.
¿La empresa tiene servicios y funciones críticas, y las dependencias entre ellas, todo documentado?	**ID.BE-4:** Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.
¿La empresa identificó tiempos máximos de recuperación en caso de caída de los servicios críticos?	**ID.BE-5:** Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).
¿Los proveedores conocen lo que hace la empresa?	**ID.BE-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.
¿Hay una Política de Seguridad de TI definida?	**ID.GV-1:** Se establece y se comunica la Política de seguridad cibernética organizacional.
¿Existen roles y responsabilidades para la Seguridad de TI definidos?	**ID.AM-6:** Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.
¿Los empleados y terceros (proveedores y/o socios) quienes tienen roles y responsabilidades en la Seguridad de TI lo saben?	**ID.GV-2:** Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos

Tabla 18: Secuencia de 8 preguntas en la Función Identificar

Este es tan sólo un breve ejemplo del esfuerzo realizado para que la Herramienta de Autoevaluación desarrollada tenga una mejor secuenciación en las preguntas.

5.2.5 Generalidad de la Herramienta

Existen algunas áreas evaluadas por el Marco de Trabajo del NIST que tal vez no aplican a ciertas PYMEs, incluso algunas no aplican a la mayoría de las empresas. Esta situación se discutió y se tomó la decisión de incluirlas en la Herramienta de Autoevaluación, pero proveer la forma de que la organización indique que “No Aplican”.

Para esto, una de las opciones de las posibles respuestas para cada pregunta siempre es el equivalente a decir: “la empresa no tiene o no hace lo que se pregunta”. Por ejemplo, en la pregunta: ***“¿La empresa provee infraestructura crítica usada por todo su sector de la industria?”***, la primera respuesta es: ***“1. La empresa no provee infraestructura crítica a su industria”***.

De la mano, las instrucciones de la Herramienta de Autoevaluación indican que: ***“Hay preguntas acerca de temas que podrían no aplicar a su empresa (su PYME no provee infraestructura crítica para todo el sector de PYMEs o su PYME no desarrolla sistemas). Para estas preguntas, la respuesta debe ser 1 en Estado Actual y Estado Deseado”***.

De esta manera, la Herramienta de Autoevaluación puede ser utilizada por cualquier PYME y son las características individuales de la empresa; es decir, sólo aquellas preguntas que sí aplican, las que serán evaluadas para obtener tanto el resultado del Estado Actual como del Estado Deseado.

Igualmente, es probable que la PYME cuando esté contestando las preguntas y seleccionando los niveles deseados a futuro, quiera escoger el nivel más alto en todas las opciones con tal de estar protegido en el mayor nivel posible. Para llegar al nivel de madurez más alto se deben asignar una cantidad relevante de recursos y, en una PYME, esta acción podría descuidar otras áreas del negocio. Es por esta razón, que se tomó la decisión de incluir en la herramienta la recomendación de seleccionar el nivel donde la empresa se sienta más cómoda y aplicar el nivel más alto deseado en las áreas más críticas del negocio indicando lo siguiente en las instrucciones: ***"Tenga en cuenta que la Respuesta 4 (el nivel más alto) no es necesariamente el ideal para su empresa. Usted es quien mejor la conoce y quien mejor sabe en qué nivel se siente cómodo(a) y en qué nivel es suficiente para su empresa. Algunos aspectos no aplican para su empresa y nunca lo harán. En algunos aspectos, realizar lo que indica la pregunta sólo para los casos o elementos más críticos es suficiente y en algunos aspectos, realizarlo en todos los casos o elementos, aunque no sea de forma estandarizada también es suficiente"***.

5.3 Respuestas de las preguntas

Con el objetivo de llevar a cabo la autoevaluación, se tomó la decisión de solicitar al usuario responder dos aspectos por cada pregunta: el primero es el Estado Actual de la empresa y el segundo es el Estado Deseado. Tal y como su nombre lo indica, el Estado Actual se refiere a la situación al momento de contestar las preguntas, mientras que el Estado Deseado se refiere donde la organización planea estar en un futuro determinado. El plazo para cumplir el Estado Deseado

deberá ser establecido por cada entidad que llene la autoevaluación según su capacidad de operación.

Para mayor facilidad para quien realice la autoevaluación, las respuestas del Estado Actual y del Estado Deseado se encuentran predefinidas en una lista con valores que van del 1 al 4, la respuesta es única para ambos estados. Éstos valores determinan el nivel de la seguridad cibernética según los niveles que define el estándar NIST.

Adicionalmente, la hoja de cálculo cuenta con una columna donde explica el significado de cada nivel, para utilizarla como referencia al momento de seleccionar el Estado Actual y el Estado Deseado. La Tabla 19 muestra la descripción genérica de las cuatro posibles opciones de respuesta. Es importante mencionar que las opciones de respuesta se adaptaron según la pregunta que se formula.

La primera opción de respuesta es la más básica y se debe seleccionar cuando la empresa no implementa un control en específico. Por ejemplo, para la pregunta "***¿Existe un inventario de los equipos de cómputo de la organización?"***, la opción de respuesta es: ***"1. No existe un inventario"***.

Nivel	Descripción genérica de la opción de respuesta
1	La empresa no cumple con lo que plantea la pregunta
2	La empresa cumple parcialmente que plantea la pregunta
3	La empresa cumple en gran medida lo que plantea la pregunta, pero no de forma estandarizada
4	La empresa cumple con todo lo que plantea la pregunta de manera estandarizada, además realiza revisiones periódicas y se incluyen lecciones aprendidas de la última revisión

Tabla 19: Descripción de las cuatro (4) opciones de respuesta

La segunda opción de respuesta determina si la empresa cumple con la pregunta, pero lo realiza de manera parcial. Si se toma nuevamente la pregunta anterior: "***¿Existe un inventario de los equipos de cómputo de la organización?"***, la opción de respuesta es: ***"2. Algunos equipos se han inventariado, pero no todos"***.

La siguiente opción determina si una empresa realiza todo lo que formula la pregunta, pero no existe un seguimiento estandarizado ni seguimiento continuo. Continuando con el ejemplo anterior, la opción de respuesta es: ***"3. Todos los equipos están identificados, inventariados y se revisan, pero no de forma estándar en toda la organización***".

La última opción permite saber si la empresa cumple con todo, y al mismo tiempo realiza esta tarea de manera estandarizada con una periodicidad establecida y en cada revisión se incluyen las lecciones aprendidas desde la última revisión. Retomando el ejemplo anterior, la opción de respuesta es: ***"4. Todos los equipos están identificados, inventariados y se revisan siguiendo un proceso estándar para toda la organización. La revisión se hace con la periodicidad establecida y se incorporan mejoras derivadas de lecciones aprendidas"***.

El proceso de adaptar la descripción genérica de las opciones de respuesta se realizó para cada una de las preguntas del cuestionario.

Al momento de terminar la autoevaluación, los valores seleccionados se utilizan para mostrar una calificación por cada una de las Funciones evaluadas, es decir, la nota obtenida en Identificación, en Protección, en Detección, en Respuesta y en Recuperación. Adicionalmente, se muestra una nota global de toda la autoevaluación. Presentar los resultados por Función permite identificar las áreas que necesitan mayor enfoque según las necesidades de la empresa.

5.4 Cálculo de la nota obtenida

Al momento de contestar todas las preguntas, la herramienta realiza una serie de cálculos con el objetivo de brindar una nota por Función y dar una nota global de los resultados. El valor de las notas se ubica entre los números 0 y 100, y la nota representa una relación proporcional del estado actual con base en el estado deseado. Se decidió utilizar este rango de valores, ya que es un sistema muy utilizado a nivel costarricense para brindar una calificación.

Por lo tanto, para conseguir la nota de cada Función se necesita obtener un valor único para el estado actual y otro para el estado deseado según las respuestas del cuestionario asociadas a esta Función. Una vez obtenidos los valores se utiliza una regla de tres simple, donde el valor del estado deseado obtenido se considera la nota más alta, es decir, el valor del estado deseado equivale a la nota con valor 100.

5.4.1 Valor único del Estado Actual y del Estado Deseado

Para obtener el valor único del estado actual y del estado deseado, primero se realiza una sumatoria por niveles, es decir, se cuentan las respuestas que pertenecen al nivel 1, cuántas pertenecen al nivel 2 y sucesivamente hasta el nivel 4. La Tabla 20 muestra un ejemplo de la sumatoria de la Función Identificación, donde el resultado son 9 respuestas de nivel 1 del estado actual, del nivel 2 corresponden 18, del nivel 3 corresponden 2 y ninguna respuesta en el nivel 4. Mientras que, 5 respuestas son parte del nivel 1 del estado deseado, en el nivel 2 no hay respuestas, en el nivel 3 se seleccionaron 21 respuestas y para el nivel 4 se seleccionaron 3 respuestas.

		Nivel Estado Actual				Nivel Estado Deseado			
Función	**Subcategoría**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Identificación	Entorno Empresarial	0	3	2	0	0	0	2	3
	Gobernanza	4	0	0	0	0	0	4	0
	Gestión de Activos	0	3	0	0	0	0	3	0
	Gestión de Riesgo	0	6	0	0	0	0	6	0
	Riesgos Organizacionales	0	6	0	0	0	0	6	0
	Riesgos en Cadena Suministros	5	0	0	0	5	0	0	0
	Total	**9**	**18**	**2**	**0**	**5**	**0**	**21**	**3**

Tabla 20: Cálculos para la Función Identificación

Una vez obtenida la sumatoria por niveles, se procede a convertir estos resultados es un valor único para el estado actual y otro para el estado deseado. Para llevar a cabo este proceso, se decidió multiplicar los resultados de los niveles por una puntuación del 0 al 3 respectivamente, es decir, los valores del nivel 1 se multiplican por 0, los valores del nivel 2 se multiplican por 1, y así sucesivamente hasta el nivel 4. Las Tablas 21 y 22 muestran cómo se obtienen los valores únicos del estado actual y del estado deseado.

Estado Actual	Valor obtenido	Puntuación	Resultado Multiplicación
Nivel 1	9	0	0
Nivel 2	18	1	18
Nivel 3	2	2	4
Nivel 4	0	3	0
		Total	**22**

Tabla 21: Obtención del valor único del Estado Actual

Estado Deseado	Valor obtenido	Puntuación	Resultado Multiplicación
Nivel 1	5	0	0
Nivel 2	0	1	0
Nivel 3	21	2	42
Nivel 4	3	3	9
		Total	**51**

Tabla 22: Obtención del valor único del Estado Deseado

5.4.2 Regla de tres simple

Por último, se utiliza la regla de tres simple para obtener una nota. El valor del estado deseado equivale a una nota de 100. De esta manera se obtiene la nota por Función. La regla de tres simple corresponde a la siguiente fórmula:

$$\left.\begin{array}{rl} Nota\ Deseada & \rightarrow 100 \\ Nota\ Actual & \rightarrow X \end{array}\right\} \rightarrow X = \frac{Nota\ Actual\ \cdot 100}{Nota\ Deseada}$$

Figura 4: Ecuación para la Nota del Estado Actual

Continuando con el ejemplo que se ha venido desarrollando y después de aplicar la fórmula, la nota de la Función Identificación da como resultado 43.

$$X = \frac{22\ \cdot 100}{51} = 43$$

Figura 5: Ecuación para la Nota del Estado Actual en Identificación

Es importante mencionar que, este proceso se realiza para las cinco Funciones de la Herramienta de Autoevaluación.

5.4.3 Nota global

Además de presentar las notas obtenidas por las Funciones, la herramienta muestra una nota global, es decir, una nota de toda la autoevaluación. Para llevar a cabo este proceso, se realiza el mismo procedimiento descrito en los puntos 5.3.1 y 5.3.2 de esta sección. La diferencia consiste en aplicar los cálculos para todas las preguntas y no separarlas por Función. De esta forma, se consigue una nota general de toda la autoevaluación.

5.5 Presentación de Resultados

Los resultados que muestra la herramienta es la nota general de toda la autoevaluación y la calificación por cada una de las Funciones evaluadas. Es importante mencionar que cada nota está acompañada de un gráfico de barras con el objetivo de visualizar mejor los resultados. La Figura 6 ejemplifica la presentación de los resultados para cada una de las Funciones evaluadas.

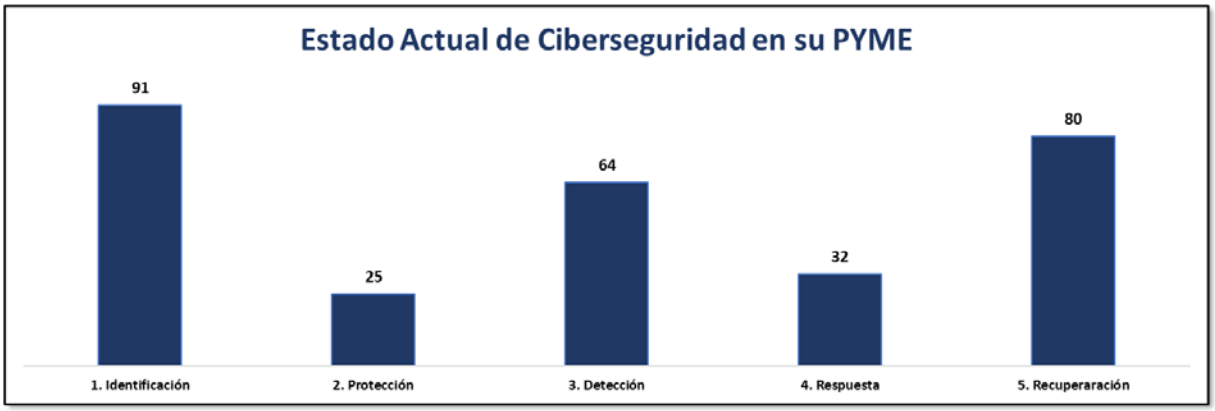

Figura 6: Ejemplo de Resultados presentados por Función

La presentación de resultados de la Función Identificación abarca las categorías del Entorno Empresarial, Gobernanza, Gestión de Riesgos, Gestión de Activos, Riesgos Organizacionales y los Riesgos de la Cadena de Suministros.

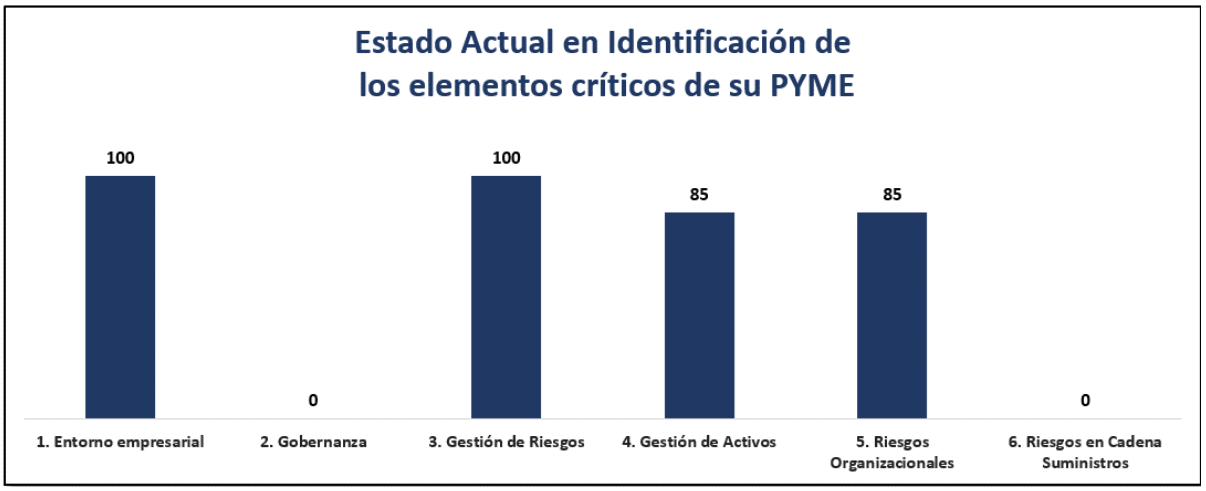

Figura 7: Ejemplo de Resultados presentados para Identificación

En el caso de la Función Protección, abarca las categorías: Capacitación, Procesos y Procedimientos, Control de Acceso, Seguridad de Datos, Tecnologías de Protección y Mantenimiento.

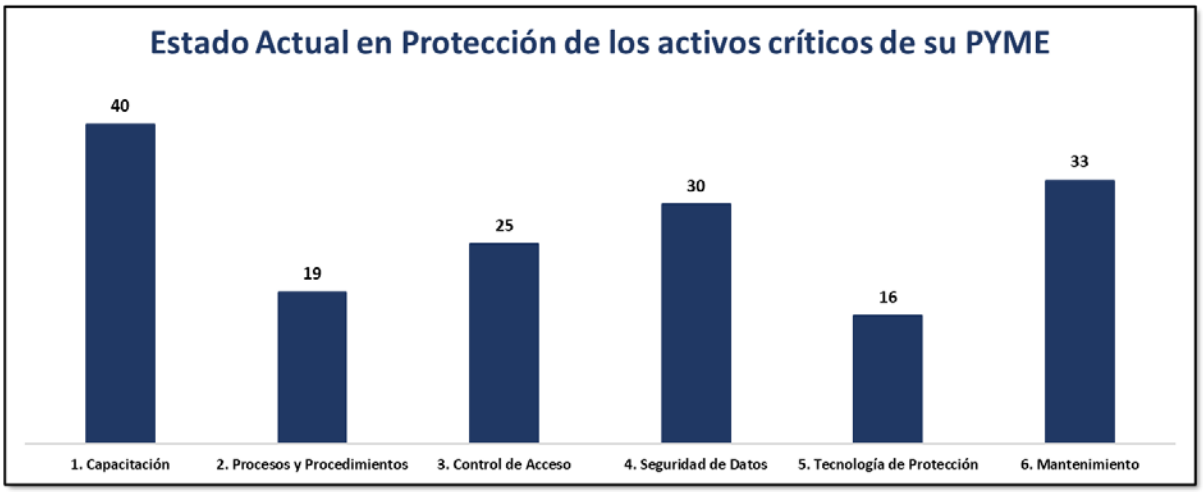

Figura 8: Ejemplo de Resultados presentados para Protección

Por otra parte, la presentación de resultados de la Función Detección abarca las categorías: Proceso para detección de intrusiones, Monitoreo Continuo y Detección de Intrusiones.

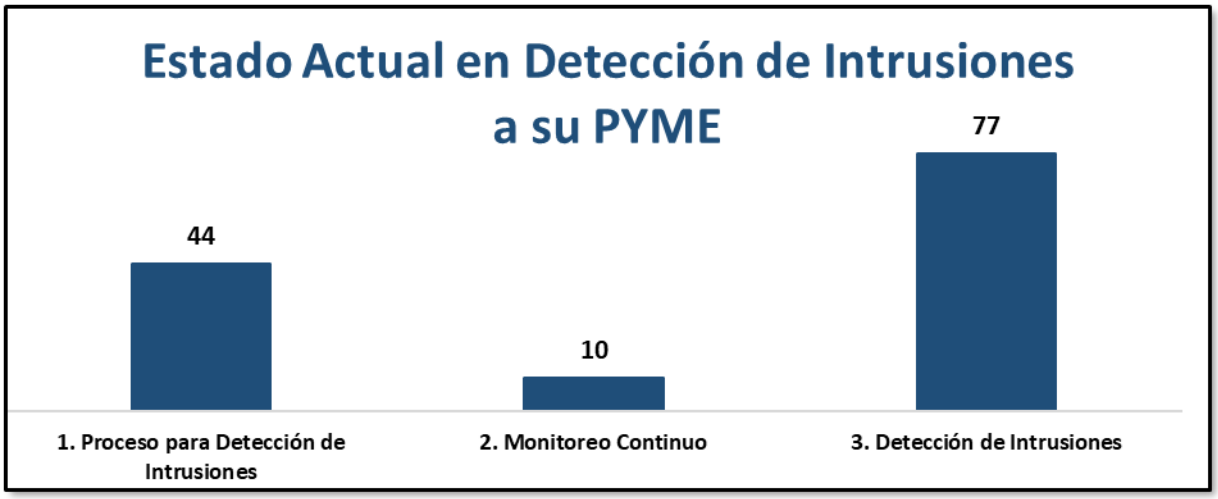

Figura 9: Ejemplo de Resultados presentados para Detección

Respecto la Función Respuesta, se toman en cuenta los resultados de las categorías: Proceso de respuesta, Análisis de incidentes, Mitigación de incidentes, comunicación de incidentes y mejora del proceso de respuesta.

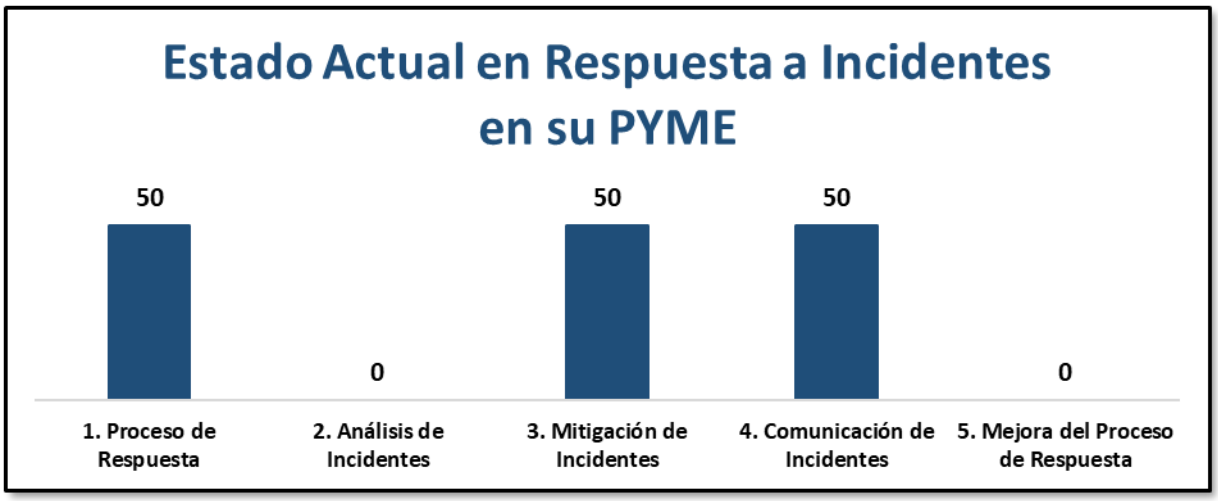

Figura 10: Ejemplo de Resultados presentados para Respuesta

Por último, se mostrará la nota de la Función Recuperación, donde se toman los valores obtenidos en las categorías del Proceso de Recuperación, Comunicación de la Recuperación y la Mejora del Proceso de Recuperación.

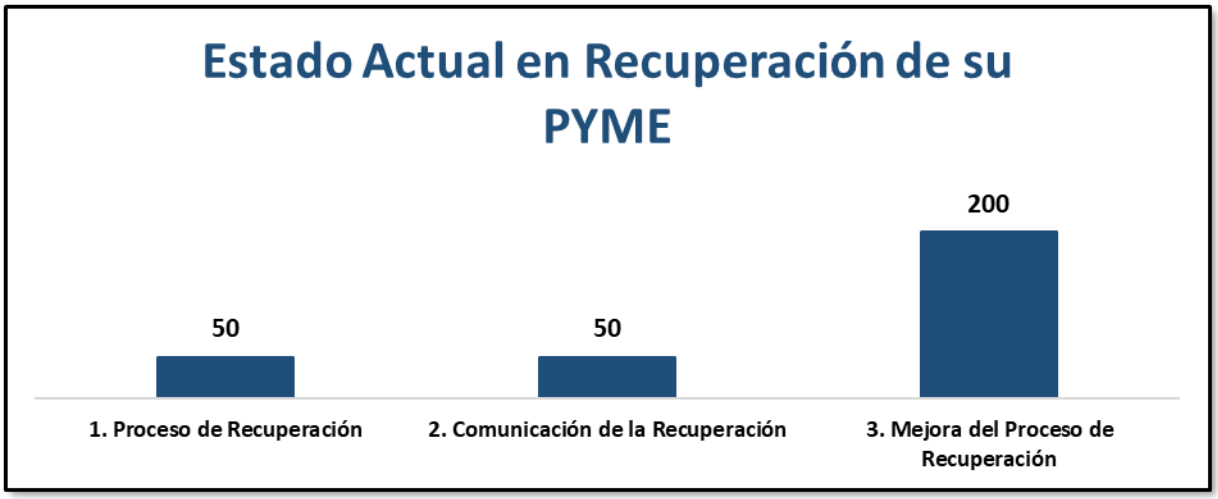

Figura 11: Ejemplo de Resultados presentados para Recuperación

5.6 Presentación de las recomendaciones.

Además de presentar el resultado de la autoevaluación, se decidió que la herramienta mostrara al usuario una serie de recomendaciones con el objetivo de cerrar las brechas de seguridad que se identificaron después de contestar las preguntas.

Las recomendaciones están separadas por las categorías del estándar NIST, y menciona las acciones más críticas parar cerrar las brechas de seguridad.

Con el objetivo de que la PYME pueda enfocarse en las áreas más críticas, las recomendaciones se muestran en una lista, donde el primer elemento de la lista es la subcategoría que obtuvo la nota más baja después de completar la autoevaluación. Además, la herramienta recomienda a la empresa utilizar otros criterios secundarios, como por ejemplo las categorías más importantes para la PYME, con el objetivo de priorizar, dentro de todas las recomendaciones recibidas, cuales son las que se deben implementar a corto plazo.

Continuando con el ejemplo utilizado y tomando como referencia los resultados de la Figura 7, se observa que las categorías Gobernanza y Riesgos de

la cadena de suministros tiene la nota más baja, por lo tanto, en la lista de recomendaciones estas categorías se muestran de primero. La Tabla 23 ejemplifica la presentación de las recomendaciones ordenadas por la nota obtenida.

Adicionalmente, para algunas recomendaciones, se presenta una lista de herramientas gratuitas que el usuario puede utilizar con el fin de proteger a su empresa.

No.	Sub categoría	Recomendación
1	Gobernanza	1. Crear y comunicar los lineamientos sobre la Seguridad de TI a todos los empleados de la empresa 2. Identificar requisitos legales y regulatorios respecto a la Seguridad de TI
2	Análisis de Incidentes	1. Investigar las notificaciones y alertas de los sistemas de detección 2. Es necesario comprender el impacto del incidente de ciberseguridad cuando se presente 3. Es recomendable implementar las medidas necesarias para realizar un análisis forense 4. Se recomienda realizar una clasificación de los incidentes de acuerdo con los planes de respuesta 5. Es recomendable establecer los procesos para recibir, analizar y responder a las vulnerabilidades identificadas desde fuentes internas y externas

Tabla 23: Ejemplo de las Recomendaciones de la Herramienta de Autoevaluación

Existe además una recomendación general que se da a la PYME en caso de que se detecte que el Estado Actual en alguna Categoría o Función sea mayor al Estado Deseado. En este caso, se dará una recomendación que indica ***"Los resultados de la Autoevaluación muestran que su PYME tiene un Estado Actual mayor al Estado Deseado. Se recomienda que mantenga el nivel de esfuerzo realizado actualmente en lugar de bajarlo al Estado Deseado; sin embargo, es importante que determine si los recursos que requiere mantener el Estado Actual prefiere enfocarlos en otras áreas"***.

Capítulo 6. Conclusiones y Recomendaciones

6.1 Conclusiones

Los autores de este trabajo llegan a las siguientes conclusiones detalladas:

El estudio profundo de la estructura y el contenido del Marco de Trabajo para la Ciberseguridad del NIST permitió concluir que, desde un punto de vista de organización, la estructura es robusta, bien organizada y utilizable sin mayores alteraciones; sin embargo, desde un punto de vista de facilidad de entendimiento por una persona con pocos conocimientos de Tecnología de la Información de las Subcategorías a evaluar, la usabilidad es baja en su estado nativo y se requirió bastante ajuste para que las preguntas fueran fáciles de entender por cualquier persona.

Utilizando la estructura del Marco de Trabajo de NIST y ajustando las subcategorías a preguntas en lenguaje comprensible para cualquier persona sin conocimientos profundos de Tecnología de la Información, fue totalmente viable desarrollar una Herramienta de Autoevaluación.

Cuando se solicita a la PYME la información sobre el Estado Actual y el Estado Deseado en cada Categoría, esta información permite identificar la brecha entre el Estado Deseado y el Estado Actual por Categoría. Esta información permite, a su vez, determinar cuáles son las mayores brechas según el Estado Actual y permite clasificar qué áreas deben recibir mayor cantidad de recursos para el cierre de las brechas.

La herramienta permite identificar las áreas de mayor brecha y, a su vez, mostrar una lista de recomendaciones para cerrar las brechas. Existen muchas herramientas y guías gratuitas que fueron documentadas para

pasar ese conocimiento a la PYME y que puedan ser exploradas como una posibilidad para el cierre de brechas.

6.2 Recomendaciones

Para un trabajo de investigación que utilice un estándar internacional como los son ISO, COSO, COBIT, ITIL, NIST, GDPR, entre otros, se recomienda a los futuros investigadores utilizar, como punto de inicio, la traducción oficial del estándar al idioma español (siempre y cuando esté disponible) ya que muchos de estos estándares surgen en idioma inglés. Son dos los beneficios que puede traer el uso del estándar en el idioma natal de los investigadores:

1. Ahorro de tiempo en la traducción de los términos o áreas a ser utilizadas
2. Evita errores o malentendidos en los conceptos bases que soportarán el trabajo de investigación.

Referencias

Greenberg, A. (2018). *The untold story of NotPetya, the most devastating cyberattack in history.* Obtenido de WIRED: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Herramienta de Autodiagnóstico. (n.d.). Retrieved from Instituto Nacional de Ciberseguridad (INCIBE): www.incibe.es

INCIBE. (s.f.). *Herramienta de Autodiagnóstico.* Retrieved from Instituto Nacional de Ciberseguridad de España: https://adl.incibe.es/

Kaspersky Lab. (s.f.). *What is Cyber-Security.* Retrieved from Kaspersky Lab: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

MEIC. (s.f.). *PYMES Costa Rica.* Retrieved from Ministerio de Economía, Industria y Comercio: http://www.pyme.go.cr/cuadro5.php?id=1

Meszaros, J., & Buchalcevova, A. (2017). *Introducing OSSF: A framework for online service cybersecurity risk management.* Retrieved from Computers & Security: https://www.sciencedirect.com/science/article/pii/S0167404816301791

Revista Summa. (2018). *Ciberataques ganan terreno en Costa Rica y urge aplicar mecanismos para detenerlos.* Obtenido de Revista Summa: http://revistasumma.com/ciberataques-ganan-terreno-en-costa-rica-y-urge-aplicar-mecanismos-para-detenerlos/.

Ross, R. S. (2014). *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.* Obtenido de Journal of Research of the NIST:

https://www.nist.gov/publications/assessing-security-and-privacy-controls-federal-information-systems-and-organizations

TagCrowd. (s.f.). *TagCrowd*.

Toth, P. R., & Paulsen, C. (2016). *Small Business Information Security: The Fundamentals.* Obtenido de Journal of Research of the NIST: https://www.nist.gov/publications/small-business-information-security-fundamentals

Universo Fórmulas. (s.f.). *Muestreo No Probablilístico.* Retrieved from Universo Fórmulas: https://www.universoformulas.com/estadistica/inferencia/muestreo-no-probabilistico/

Walker, I. (2019). *Forbes.* Retrieved from Forbes: https://www.forbes.com/sites/ivywalker/2019/01/31/cybercriminals-have-your-business-their-crosshairs-and-your-employees-are-in-cahoots-with-them/#482409d81953

Watson, M. (2019). *Top 4 cybersecurity frameworks.* Retrieved from IT Governance: https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks