



Universidad Veracruzana

Facultad de Estadística e Informática

Región Xalapa

Licenciatura en Ingeniería de Software

Análisis de prácticas de seguridad en ASP.NET Core: una Revisión de la Literatura Gris

Práctico - Técnico para la experiencia educativa de Proyecto Guiado

Presentan:

Paloma Osiris Báez Lara
Alejandro Sánchez Marín

Directores:

Dr. Héctor Xavier Limón Riaño
Dra. María Karen Cortés Verdín
Dra. Lizbeth Alejandra Hernández González

Octubre de 2024

“Lis de Veracruz: Arte, Ciencia, Luz”



Universidad Veracruzana

Facultad de Estadística e Informática
Región Xalapa

Licenciatura en Ingeniería de Software

Propuesta de modelo de seguridad enfocado en sistemas web

Protocolo de investigación para acreditar Proyecto Guiado

Presentan:

Paloma Osiris Báez Lara

Alejandro Sánchez Marín

Directores:

Dr. Héctor Xavier Limón Riaño

Dra. María Karen Cortés Verdín

Dra. Lizbeth Alejandra Hernández González

Índice

Índice	3
1. Introducción	4
2. Preguntas de investigación	5
3. Selección del tipo de revisión.....	6
4. Estrategia de búsqueda.....	8
4.1 Términos de búsqueda.....	8
4.2 Cadenas de búsqueda	9
4.3 Selección de fuentes	10
5. Selección de los estudios primarios	10
5.1 Criterios de selección de estudios primarios	10
5.2 Evaluación de la calidad de estudios de la literatura gris	12
5.3 Procedimiento de selección de estudios primarios	12
6. Extracción de los datos.....	13
7. Estrategia para la síntesis de datos	14
8. Limitaciones	14
9. Informe	15
10. Gestión de la revisión	15
Referencias.....	16

I. Introducción

El desarrollo de software es fundamental para la creación de aplicaciones y sistemas que cumplan con las necesidades tecnológicas, así como para que se adapten a los diferentes requerimientos de los usuarios y entornos de ejecución. (Shaefer et al., 2012). Además, la seguridad en el software es cada vez más importantes debido a la creciente digitalización. A medida que los datos y la información se acoplan de manera más profunda en los sistemas, se vuelve fundamental asegurar estos sistemas contra ciberataques.

Dada la necesidad de que el software cumpla con requisitos de calidad específicos como lo es la seguridad, los desarrolladores de software recurren a los *frameworks* de desarrollo. Estas herramientas mejoran la eficiencia, garantizan la confiabilidad y satisfacen la creciente complejidad de las aplicaciones web. Los *frameworks* de desarrollo de software mejoran el proceso de desarrollo al proporcionar módulos y estructuras preconstruidos, lo que reduce significativamente el tiempo y los recursos necesarios para la ejecución del proyecto (Selivorstova et al., 2020).

Frameworks como ASP. NET Core, integran mecanismos de seguridad en su entorno, como por ejemplo autenticación y autorización, sin embargo, aunque algunos *frameworks* proveen aspectos de seguridad, muchos desarrolladores carecen de las habilidades necesarias para manejar estos *frameworks* adecuadamente, especialmente en los aspectos de seguridad que estos *frameworks* proporcionan. En consecuencia, esta carencia se vuelve un aspecto crítico, porque los *frameworks* de desarrollo de software presentan una complejidad intrínseca, su efectividad está significativamente influenciada tanto por las buenas como por las malas prácticas (Slaughter, 1996). El desconocimiento puede generar malas prácticas que podrían llevar a causar problemas, por otro lado, las buenas prácticas mitigan la complejidad al promover la claridad y la capacidad de mantenimiento (Banker et al., 1998)

Esta Revisión de la Literatura Gris (RLG) tiene como objetivo identificar y analizar los mecanismos de seguridad que ofrecen el *framework* de desarrollo de software de ASP.NET Core, de modo que permitirá determinar los escenarios en los que estos mecanismos son aplicables, así como las amenazas o vulnerabilidades a las que están asociados, de igual forma se podrán identificar las practicas que facilitan, dificultan y comprometen la implementación de estos *frameworks*. Asimismo, esta RLG proporcionara

hallazgos confiables, que permitirán extraer conclusiones y tomar decisiones que aportaran para el desarrollo de un modelo de seguridad enfocado a ASP.NET Core.

2. Preguntas de investigación

En la Tabla 1 se definieron seis Preguntas de Investigación (PI) donde cada una tiene una motivación que dice por qué son de valor para esta investigación. De igual manera, estas preguntas están alineadas con los objetivos específicos y a partir de estas se busca determinar la información que se espera recopilar.

Tabla 1. Preguntas de investigación		
ID	Pregunta de investigación	Motivación principal
PI-1	¿Qué mecanismos de seguridad provee ASP.NET Core?	Permite identificar los mecanismos de seguridad que hay disponibles en los <i>frameworks</i> más utilizados por los estudiantes, esto permitirá analizar y evaluar el alcance que proveen estos <i>frameworks</i> para el desarrollo seguro de aplicaciones web.
PI-2	¿En qué posibles contextos o escenarios se utilizan los mecanismos de seguridad en ASP.NET Core?	Ayuda a definir situaciones específicas bajo cierto ambiente en las que serían útiles y efectivas aplicar los mecanismos de seguridad.
PI-3	¿Qué amenazas y/o vulnerabilidades están asociadas a cada uno de los mecanismos de seguridad en ASP.NET Core?	Es importante analizar las posibles amenazas que estos mecanismos de seguridad buscan mitigar, esto ayudará a abordar los riesgos de seguridad durante el desarrollo de software.
PI-4	¿Qué buenas prácticas se asocian a los mecanismos de seguridad en ASP.NET Core?	Entender las decisiones y acciones que llevan a implementaciones adecuadas de los mecanismos de seguridad, permite identificar los pasos clave para aplicar adecuadamente el mecanismo.
PI-5	¿Qué malas prácticas se asocian a los mecanismos de seguridad en ASP.NET Core?	Analizar las malas prácticas y sus consecuencias para saber cómo evitarlas y tener adecuadas implementaciones
PI-6	¿Qué retos plantea el uso de los mecanismos de seguridad identificados en A SP.NET Core?	Identificar que es lo más complejo, permitirá saber cómo anticiparse a posibles dificultades en el uso de mecanismos de seguridad.

3. Selección del tipo de revisión

El propósito de esta sección es justificar la elección del tipo de revisión utilizada para la investigación. Al tratarse en un principio de una RSL, se seleccionó la metodología sistemática del Quasi-Gold Standard que propone Zhang et al., (2011) debido a su enfoque para evaluar la precisión y retorno de los estudios relevantes. En la Figura 1 se muestra un diagrama de actividades que muestra el proceso para evaluar la integridad de la búsqueda.

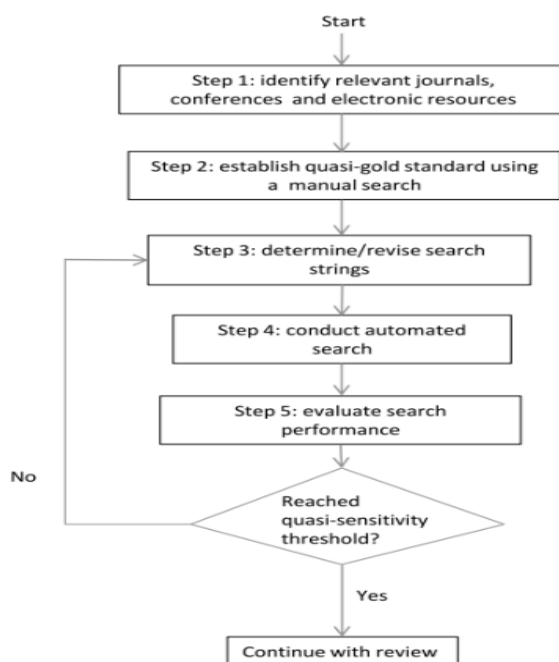


Figura 1.Flujo de trabajo del proceso de búsqueda sistemática propuesto (Zhang et al., 2011)

Para el proceso de identificación de las cadenas de búsqueda siguiendo la actividad número dos propuesto por Zhang, se llevó una búsqueda manual en donde se seleccionaron los trabajos más relevantes en base a la inclusión de estos en base a su título y el resumen del artículo. En la Tabla 2 se muestra los estudios obtenidos.

Tabla 2. Estudios relevantes conocidos		
ID	Título	Referencia
1	Descriptive Analysis of Built-in Security Features in Web Development Frameworks	Aborujilah, A., Adamu, J., Shariff, S. M., & Long, Z. A. (2022). Descriptive Analysis of Built-in Security Features in Web Development Frameworks. 2022 16th International Conference On Ubiquitous Information Management And Communication (IMCOM). https://doi.org/10.1109/imcom53663.2022.9721750

Las cadenas de búsqueda fueron hechas en base a los términos identificados en las Preguntas de Investigación, estas fueron ingresadas en el motor de búsqueda de IEEE Xplore con la finalidad de seguir con la actividad número cinco, es decir, la evaluación del rendimiento de acuerdo con el Quasi-Gold Standard previamente definido. Zhang sugiere que se podría utilizar un umbral de sensibilidad de entre un 70% y 80% para saber si continuar o no con la siguiente etapa de revisión.

En la Tabla 3 se muestran las cadenas que fueron probadas.

Tabla 3. Cadenas probadas con el Quasi-Gold Standar					
ID	Cadena	Estudios encontrados	Estudios relevantes encontrados	Retorno	Precisión
1	"ASP.NET Core" AND Feature AND Security	324	1	1/1=1	1/324=0.0030
2	"ASP.NET Core" AND (Feature OR Mechanisms) AND Security	771	1	1/1=1	1/771=0.0012
3	"ASP.NET Core" AND (Threat OR Vulnerability OR Weakness OR Attack) AND Security	782	1	1/1=1	1/782=0.0012

Como se observa, la cantidad de literatura blanca obtenida es muy poca y aunque se encontraron otras fuentes que probablemente hubieran sido de utilidad, estas no eran de acceso libre y se debía pagar. Debido a esto, se optó al uso exclusivo de la literatura gris en base a los cuestionamientos que menciona Garousi et al., (2019) tal como está en la Tabla 4.

Tabla 4. Preguntas para decidir cuándo usar literatura gris		
ID	Pregunta	Posible respuesta (Sí/No)
1	¿Es el tema "complejo" y no se puede resolver considerando únicamente la literatura formal?	Sí
2	¿Existe una falta de volumen o de calidad de las pruebas, o una falta de consenso sobre la medición de los resultados en la bibliografía oficial?	Sí
3	¿Es importante la información contextual para el tema estudiado?	Sí
4	¿Se trata de validar o corroborar los resultados científicos con experiencias prácticas?	Sí

5	¿Es el objetivo cuestionar los supuestos o falsificar los resultados de la práctica utilizando la investigación académica o viceversa?	No
6	¿Sería útil para una o ambas comunidades una síntesis de los conocimientos y pruebas de la comunidad industrial y académica?	Sí
7	¿Existe un gran volumen de fuentes profesionales que indique un elevado interés de los profesionales por un tema?	No

Como resultado de la evaluación inicial, se decidió cambiar el enfoque a uno que sea exclusivo de la literatura gris. Esta decisión fue tomada debido a la escasez de literatura blanca relevante y que fuera accesible. Las pautas que define Garousi fueron de utilidad para justificar este cambio de literatura y al centrarse únicamente a estos se espera acceder a información más amplia y práctica.

4. Estrategia de búsqueda

Para la identificación de los estudios primarios se seguirá con la estrategia de búsqueda para la investigación, el proceso sistemático Quasi-Gold Standard que propone Zhang et al., (2011). Siguiendo las cinco etapas del flujo de trabajo, pero enfocado a la literatura gris únicamente:

- I. Identificar libros, revistas, reportes de gobiernos y documentos técnicos relevantes (Literatura gris de primer, segundo nivel y blogs).
- II. Determinar las cadenas de búsqueda.
- III. Conducir la búsqueda automatizada.

En la etapa cinco, habrá una modificación, ya que no se evaluará la precisión del Quasi-Gold, esto debido a la naturaleza de la investigación, al ser literatura gris y que los motores de búsqueda que se usarán arrojan una cantidad grande de resultados, no cobra sentido medir la precisión, ya que esta será demasiado baja, lo que lo vuelve un dato irrelevante para la evaluación del desempeño de la búsqueda.

4.1 Términos de búsqueda

La Tabla 5 que se muestra a continuación ilustra los conceptos que fueron obtenidas a partir de las Preguntas de Investigación (PI) previamente mostradas. De igual manera, estos términos ayudarán a realizar las cadenas de búsqueda.

Tabla 5. Términos de búsqueda		
Concepto	Concepto en inglés	Términos relacionados
Framework	Framework	
ASP.NET Core	ASP.NET Core	
Buenas prácticas	Best practice	
Malas prácticas	Bad practice	Anti-pattern, Smell
Amenazas	Threat	Risk, vulnerability, exploit
Mecanismo de seguridad	Security Mechanism	Feature
Seguridad	Security	Cybersecurity
Escenario	Scenario	Security context, application
Reto	Challenge	Difficulty, limitation, disadvantage

4.2 Cadenas de búsqueda

Debido a la naturaleza de la literatura gris, no fue posible llevar a cabo la construcción de un Quasi-Gold Standard que es lo que propone Zhang et al. (2011). Sin embargo, se tomó como referencia un artículo correspondiente a la documentación oficial del *framework* de ASP.NET Core, es decir, de Microsoft. Dicha fuente es la siguiente:

<https://learn.microsoft.com/en-us/aspnet/core/security/?view=aspnetcore-9.0>

En esta se mencionan distintos temas de seguridad entre las que destacan los mecanismos de seguridad y amenazas que este *framework* mitiga, mencionado esto, para llevar a cabo la construcción de las cadenas de búsqueda se tomó como referencia estos mecanismos que se mencionan y de igual manera se tomó en cuenta dos amenazas que mitiga, se colocó en la cadena la amenaza en lugar del mecanismo de seguridad que la mitiga debido a que en la literatura se referencia más a la amenaza. De igual manera, se construyó una cadena de búsqueda en general que corresponde a una mezcla de todas y donde se incluyen los términos de búsqueda, pero se limitó a tres fuentes de información las cuales son blogs y sitios donde se suelen hacer mención temas de desarrollo y seguridad de software.

A continuación, en la Tabla 7 se presentan las cadenas de búsqueda.

Tabla 7. Cadenas probadas con el Quasi-Gold Standard de literatura gris para ASP.NET Core

ID	Cadenas Google Search	Estudios relevantes encontrados	Retorno
CB-1	"ASP.NET Core" AND Security AND "Authentication"		
CB-2	"ASP.NET Core" AND Security AND "Authorization"		
CB-3	"ASP.NET Core" AND Security AND "Data Protection"		
CB-4	"ASP.NET Core" AND Security AND "HTTPS Enforcement"		
CB-5	"ASP.NET Core" AND ("Safe Storage of App Secrets" OR "Secrets Management" OR "App Secrets Security") AND Security		
CB-6	"ASP.NET Core" AND Security AND (Cross-site request forgery OR CSRF OR XSRF)		
CB-7	"ASP.NET Core" AND Security AND "CORS"		
CB-8	"ASP.NET Core" AND Security AND (Cross-Site Scripting OR XSS)		
CB-9	"ASP.NET Core" AND (Feature OR Mechanisms) AND Security AND (Good Practices OR Bad Practices OR "Anti-Pattern") AND (Authentication OR Authorization OR "Data protection" OR HTTPS Enforcement OR App Secrets Management OR CSRF OR CORS OR XSS) AND (site:medium.com OR site:microsoft.com OR site:linkedin.com)		
	Cadena Google Scholar		
CB-10	"ASP.NET Core" AND (Feature OR Mechanisms) AND Security AND (Good Practices OR Bad Practices OR "Anti-Pattern")		

4.3 Selección de fuentes

Para la recuperación de recursos de literatura gris se tomarán los resultados del motor de búsqueda Google Search y Google Scholar, ya que en estos motores de búsqueda se encuentran las publicaciones que pertenecen a los tres niveles de literatura gris.

5. Selección de los estudios primarios

A continuación, se describen los criterios de inclusión y exclusión para estudios primarios de literatura gris, además siguiendo lo propuesto por Garousi (2019) para una revisión de literatura gris, se plantearon criterios de paro, así como un *checklist* para la evaluación de la calidad de la literatura gris. Por último, se describe el procedimiento de selección.

5.1 Criterios de selección de estudios primarios

Se plantearon seis criterios de inclusión, tres criterios de exclusión y dos criterios de paro para la selección de los estudios primarios:

Criterios de inclusión:

- CI-1. Resultados publicados entre 2022 y 2024 o publicaciones hechas de ASP.NET Core en sus versiones 7.0 y 8.0.
- CI-2. La publicación fue escrita originalmente en idioma inglés.
- CI-3. En la publicación se puede identificar el nombre del autor u organización.
- CI-4: El título presenta indicios de tener relación con al menos una pregunta de investigación.
- CI-5: Tras leer la publicación, se debe confirmar que este responde a una o más de las preguntas de investigación.
- CI-6: La publicación cumple con los criterios de la evaluación del aseguramiento de calidad para literatura gris.

Criterios de exclusión

- CE-1. La publicación no contiene fecha de publicación ni especifica las versiones del *framework*.
- CE-2: La publicación no es un blog y pertenece al tercer nivel de literatura gris, así como esta no debe tener como objetivo la promoción o venta de algún tipo de herramienta, servicio o vacante de empleo.
- CE-3. La publicación sea duplicada.

Criterios de Paro

Dada la naturaleza de una RLG y que los motores de búsqueda de dicha literatura arrojan miles de millones de resultados, se ve la necesidad de plantear criterios de paro con el fin de no invertir esfuerzo en resultados que no contribuyan a la investigación y así obtener la mayor información útil posible.

- CP-1. Saturación teórica: Los resultados no presentan nuevos conceptos tras analizar diez resultados consecutivos que dejan de aportar información relevante.
(MODIFICAR)
- CP-2. Esfuerzo Limitado: Se han alcanzado los 200 resultados.

5.2 Evaluación de la calidad de estudios de la literatura gris

Siguiendo lo propuesto por Garousi (2019), se realizará el aseguramiento de la calidad de la literatura gris, para esto se tomará como base el *checklist* propuesto por Garousi et al, con modificaciones para que se adapte al contexto de esta revisión sistemática. En la Tabla 6 se muestra el *checklist* modificado, el cual cuanta con una sumatoria total de 6.5, cada pregunta de los criterios podrá ser evaluados en una escala, donde 0 = No, 0.5 = Parcialmente y 1 = Sí. Se normalizará aplicando una sumatoria de cada criterio por estudio dividiéndolo entre el número total de puntos (6.5), y los criterios de aceptación del *checklist* será 4.0 sobre el valor normalizado. Aquellas fuentes que proporcionan un alto valor de profundidad se decidió agregar una bonificación equivalente a 1.5 puntos sobre aquellas que no ofrecían tanto para este criterio.

Tabla 8. Criterios de calidad de los estudios		
Criterio	Pregunta	Puntos
Autoridad del productor 1. ¿La fuente del recurso es confiable y reconocida en el área?	1.1 ¿El autor cuenta con experiencia demostrable o un título en el área de seguridad o desarrollo de software?	
	1.2 ¿La organización o empresa es reconocida por su experiencia o autoridad en el área de seguridad o desarrollo de software?	
Objetividad	2. ¿El recurso es objetivo, o se basa meramente en una opinión?	
Fuentes relacionadas	3. ¿El recurso ha sido referenciado por otros recursos?	
Profundidad del tema	5. ¿El recurso analiza el tema en profundidad o lo trata de manera superficial?	
Tipo de fuente	<ul style="list-style-type: none"> Libro, revista, tesis, reporte de gobierno, White paper (1 punto) Reporte anual, artículo de noticias, sitios de pregunta/respuesta, artículo de wiki, Blog (0.5 puntos) 	

5.3 Procedimiento de selección de estudios primarios

El procedimiento seguido para la selección de los estudios primarios se basa en 4 etapas, las cuales se basan en los criterios de exclusión e inclusión con el objetivo de realizar un proceso de búsqueda adecuado: filtrando y buscando no perder fuentes de información relevantes. Se muestra en la Figura 2.

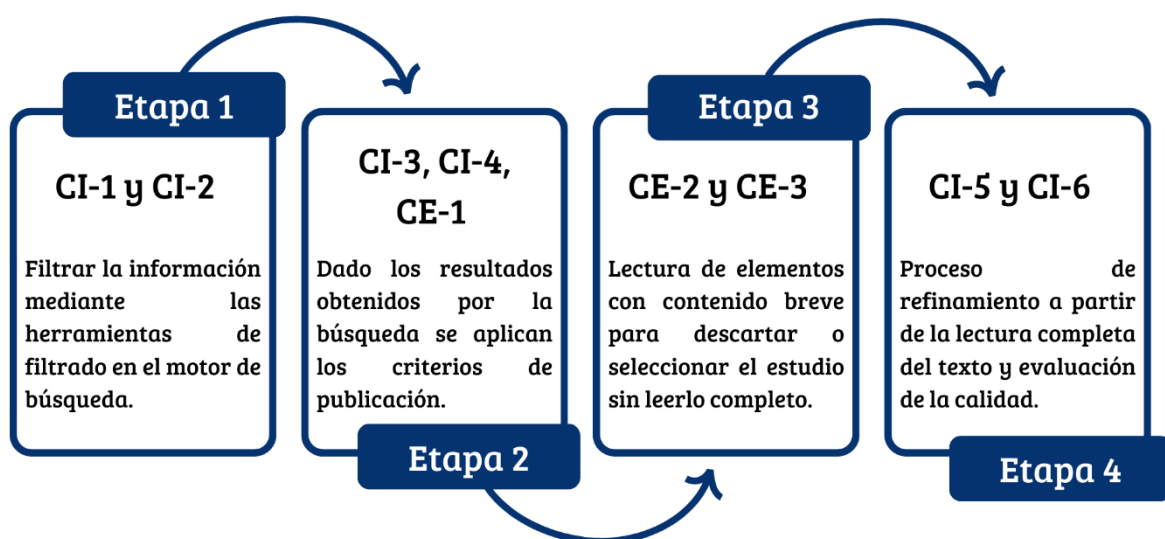


Figura 2. Proceso de selección de estudios primarios

6. Extracción de los datos

En este punto se abordarán los formatos que se deben tener para la extracción de los datos, esto con el objetivo de estandarizar la recopilación de datos y facilitar su análisis.

Tabla 9. Formato para la extracción de la información

Datos generales						
Título						
Autores						
Año						
Fuente						
Tipo de publicación (libro, revista, tesis, etc.)						
Referencia o detalles de la publicación						
Pregunta de investigación que responde	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6
Datos para la síntesis						
PI-1 Mecanismos de seguridad que provee ASP.NET Core	Nombre mecanismo					
	Descripción mecanismo					
PI-2 Contextos o escenarios donde se utilizan los mecanismos de seguridad en ASP.NET Core	Escenario					
	Descripción					
PI-3	Nombre de la amenaza asociada al mecanismo					

Amenazas y/o vulnerabilidad están asociadas a cada uno de los mecanismos de seguridad en ASP.NET Core	Descripción amenaza	
PI-4 Buenas prácticas que se asocian a los mecanismos de seguridad en ASP.NET Core	Buena práctica asociada al mecanismo	
	Descripción de la buena práctica	
PI-5 Malas prácticas que se asocian a los mecanismos de seguridad en ASP.NET Core	Mala práctica asociada al mecanismo	
	Descripción de la mala práctica	
PI-6 Retos que plantea el uso de los mecanismos de seguridad identificados en ASP.NET Core	Reto	
	Descripción	

7. Estrategia para la síntesis de datos

Para la síntesis de los datos recabados en la RLG, se realizará una síntesis narrativa, siguiendo el proceso del marco de trabajo propuesto por Popay et al. (2006).

El proceso por seguir consta de tres etapas:

- I. Desarrollo de un modelo teórico: describir cómo y por qué se espera que los estudios incluidos en la revisión respondan a las preguntas de investigación.
- II. Desarrollo de síntesis preliminar: organizar la información para describir patrones en los estudios.
- III. Explorar relaciones en los datos: identificar factores de desviación en los estudios seleccionados.

8. Limitaciones

Las limitaciones que presenta la revisión sistemática de la literatura son la siguientes:

- LI-1. Aunque se analizan amenazas y vulnerabilidades conocidas en la literatura, la rápida evolución de las amenazas de seguridad limita el alcance de los resultados obtenidos.
- LI-2. Dada la naturaleza de la literatura gris que se usará en esta revisión, es posible que algunos de los estudios importantes, queden fuera de este trabajo.
- LI-3. Está limitado a literatura gris.

9. Informe

Como último paso de la RLG, se realizará un reporte que contenga los resultados obtenidos. Cómo índice tentativo o estructura de trabajo se propone el siguiente:

Tabla de contenido

Resumen.....	1
Palabras clave.....	2
Introducción	3
Conducción del método	4
Preguntas de investigación	5
Procedimiento de búsqueda	6
Cadena de búsqueda.....	7
Criterios de selección	8
Evaluación de la calidad	9
Estudios primarios seleccionados	10
Extracción y síntesis de datos.....	11
Resultados	12
Respuestas a preguntas de investigación	13
Conclusiones	14
Referencias.....	15

10. Gestión de la revisión

Las herramientas de soporte que se utilizarán para desarrollar la RLG son:

- Microsoft Word: procesador de texto para la redacción del reporte de la RLG
- Microsoft Excel: hoja de cálculo para la gestión de datos

En la Tabla 10, se muestra un cronograma con las fechas aproximadas para el desarrollo de la RLG:

Tabla 10. Cronograma de trabajo					
Actividades	Meses				
	Septiembre	Octubre	Noviembre	Diciembre	Enero
	Semanas	Semanas	Semanas	Semanas	Semanas

	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Definición del protocolo de RLG																				
Tercera presentación de avances																				
Conducción de la revisión																				
Elaboración del informe de la RLG																				
Presentación de resultados en el seminario																				

Referencias

- Garousi, V., Felderer, M., & Mäntylä, M. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information & Software Technology*, 106, 101-121. <https://doi.org/10.1016/j.infsof.2018.09.006>
- Ina, Schaefer., Rick, Rabiser., Dave, Clarke., Lorenzo, Bettini., David, Benavides., Goetz, Botterweck., Animesh, Pathak., Salvador, Trujillo., Karina, Villela. (2012). Software diversity: state of the art and perspectives. *International Journal on Software Tools for Technology Transfer*, 14(5):477-495. doi: 10.1007/S10009-012-0253-Y
- Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., Britten, N., Roen, K. y Duffy, S. (2006). Guidance on the conduct of narrative synthesis in systematic reviews: A product from the ESRC Methods Programme. <https://doi.org/10.13140/2.1.1018.4643>
- Rajiv, D., Banker., Gordon, B., Davis., Sandra, A., Slaughter. (1998). Software Development Practices, Software Complexity, and Software Maintenance Performance: a Field Study. *Management Science*, 44(4):433-450. doi: 10.1287/MNSC.44.4.433
- Sanora, Ann, Slaughter. (1996). Software development practices and software maintenance performance: a field study.
- Yuliia, Romanivna, Selivorstova., Iryna, Victorivna, Liutenko., Sergey, Valerievich, Orekhov. (2020). Frameworks analysis and evaluation used in the web-application development. 44-50. doi: 10.20998/2079-0023.2020.02.08
- Zhang, H., Babar, M. A., & Tell, P. (2011). Identifying relevant studies in software engineering. *Information and Software Technology*, 53(6), 625-637. <https://doi.org/10.1016/j.infsof.2010.12.010>



“Lis de Veracruz: Arte, Ciencia, Luz”

www.uv.mx

