|  |  |
| --- | --- |
|  | UNIVERSIDAD VERACRUZANA  FACULTAD DE ESTADÍSTICA E INFORMÁTICA |

PROTOCOLO DEL TRABAJO:

PRÁCTICAS Y HERRAMIENTAS CRIPTOGRAFICAS ORIENTADAS AL DESARROLLO SEGURO DE SOFTWARE

MODALIDAD:

MONOGRAFIA

QUE PARA OBTENER EL GRADO DE:

LICENCIADO EN INGENIERÍA DE SOFTWARE

PRESENTA:

BRYAN JOSUÉ HERNÁNDEZ MARCIAL

DIRECTORES:

Dr. Héctor Xavier Limón Riaño

MCC. Juan Carlos Pérez Arriaga

XALAPA, VER. SEPTIEMBRE 2023

ÍNDICE

[1 Antecedentes 2](#_Toc146626588)

[2 Definición del Problema 3](#_Toc146626589)

[3 Objetivos 4](#_Toc146626590)

[4 Justificación 5](#_Toc146626591)

[5 Alcances y Limitaciones 6](#_Toc146626592)

[6 Marco Teórico 7](#_Toc146626593)

[7 Método 7](#_Toc146626594)

[8 Contenido del trabajo de investigación (índice tentativo o estructura del trabajo) 7](#_Toc146626595)

[9 Cronograma 7](#_Toc146626596)

[Cronograma de Actividades 8](#_Toc146626597)

[10 Bibliografía 9](#_Toc146626598)

[Anexos 10](#_Toc146626599)

# **Antecedentes**

La seguridad de software es un tema amplio que abarca muchos aspectos, esta se define, según Verdon et al. (2004) como ‘la capacidad del software para resistir, tolerar y recuperarse de eventos que amenazan intencionalmente la confiabilidad’. Sin embargo, para este tema, adoptaremos la definición de Devi (2013) que la describe como ‘Asegurarse que personas entrometidas no puedan leer o modificar en secreto los mensajes destinados a otros destinatarios’. Basado en el concepto anterior, se puede comprender que la seguridad de software busca la privacidad de la información. Para entender el cómo lograr esto, es importante explorar un concepto crucial en la seguridad de software: la criptografía.

De acuerdo con la información proporcionada por Amazon Web Services (2023), la criptografía es una práctica que consiste en el uso de algoritmos codificados, firmas y hashes, proteger información privada, para que exista un canal seguro para la transmisión de información privada.

La criptografía es un tópico cuya antigüedad es comparable con la de la propia escritura (Ortega et al., 2006). A su vez la criptografía se utilizó mayormente en contextos bélicos, con la finalidad de transmitir información entre aliados y evitar que el enemigo descifrara el mensaje, aun cuando lo interceptara. En pocas palabras, la criptografía es la ciencia de escribir en código secreto (Devi, 2013).

Ahora bien, en la actualidad la criptografía desempeña un papel fundamental en numerosas aplicaciones, con 5000 millones de personas conectadas a internet (I͡Ashchenko, 2002). De acuerdo con el mismo autor esto ha provocado que la criptografía sea una prioridad para el desarrollo de software, a su vez se intuye que el conocimiento criptográfico para el desarrollo de proyectos de software es importante para estudiantes de ingeniería de software y desarrolladores de software de cualquier nivel. Un ejemplo de la importancia que tiene la criptografía en la actualidad es, en aplicaciones de compras, ya que en estas aplicaciones es necesaria la información del cliente para realizar compras, por lo tanto, el cliente requiere la seguridad de que su información bancaria está protegida y que ningún externo lograra interceptar esa información (I͡Ashchenko, 2002).

(tecnologías) (por ejemplo https)

# Definición del Problema

La criptografía es un tema extenso e importante tanto para estudiantes de ingeniería de software como para desarrolladores de software de cualquier nivel, ya que, según Braga et al. (2016) el mundo está siendo testigo de un notable aumento en el uso de funciones de seguridad basadas en tecnologías criptográficas. De acuerdo con el mismo autor, ‘Casi todos los días, los desarrolladores ordinarios ejecutan tareas comunes relacionadas con la programación criptográfica’. Sin embargo, el uso incorrecto de la criptografía es una fuente frecuente de vulnerabilidades introducidas en el software durante el desarrollo. (Braga, 2019)

Dada esta situación, Hazhirpasand et al. (2021) señala que, estudios anteriores han demostrado que los desarrolladores buscan regularmente asesoramiento en foros en línea para resolver sus problemas de criptografía. Por esta razón, los desarrolladores de software a menudo participan en discusiones de estos foros para apoyar y auxiliar en los proyectos de otros desarrolladores o estudiantes de ingeniería software. Es importante destacar que plataformas como Stack Overflow a menudo contienen fragmentos de código inseguros, y los desarrolladores sin experiencia usan ciegamente dichos fragmentos (Hazhirpasand et al., 2021).

De acuerdo con una exploración del tema, se percibe que no se cuenta con una recopilación de herramientas y prácticas para el desarrollo seguro de software con un enfoque en la criptografía, ya que la información referente a este tema se encuentra dispersa en diversas fuentes, esto puede dificultar el acceso a la información tanto a desarrolladores como para estudiantes.

# Objetivos

Objetivo general: Analizar el estado del arte de la seguridad en términos criptográficos en el contexto de desarrollo seguro de software por medio de una revisión de la literatura con el propósito de ofrecer a estudiantes y desarrolladores una fuente de conocimiento que les permita contar con una fuente de información respecto a este tema.

OE1: Identificar las buenas prácticas para el desarrollo del software seguro aplicado a la criptografía.

OE2: Identificar herramientas que apoyen en el desarrollo del software seguro aplicado a la criptografía.

OE3: Identificar malas prácticas o anti-patrones y sus consecuencias en términos de seguridad.

OE4: Identificar los conocimientos de criptografía que requiere un desarrollador de software.

# Justificación

En la actualidad, la criptografía se ha convertido en un componente esencial para mitigar los problemas de seguridad en las aplicaciones y sistemas de software en un entorno cada vez más digitalizado. Sin embargo, hasta donde hemos explorado existe una carencia en la disponibilidad de recursos centralizados que ofrezcan una recopilación sobre las prácticas y herramientas necesarias para implementar la criptografía de manera segura en el desarrollo de software.

Este proyecto de investigación se propone abordar esta problemática al recopilar y organizar la información sobre prácticas y herramientas para el desarrollo seguro del software aplicadas a la criptografía. Con este estudio se pretende apoyar a los desarrolladores y estudiantes en temas relacionados con desarrollo seguro enfocado en criptografía.

(Recordar el problema principal)-> los desarrolladores toman codifos malos y esto generara la problemática, y que la información esta dispersa

Esta investigación podría ayudar a tal gente

# Alcances y Limitaciones

**Alcances**:

**Exclusión de Aspectos Matemáticos y de Hardware:** Esta investigación no profundizará en los aspectos matemáticos subyacentes de la criptografía ni en detalles específicos relacionados con hardware criptográfico. Se centrará en las implicaciones prácticas y en cómo los desarrolladores de software pueden implementar de manera segura soluciones criptográficas en sus proyectos.

**Área de Enfoque**: Se explorarán temas relacionados con la criptografía y su aplicación en el desarrollo seguro de software, con un énfasis en las consideraciones prácticas y las recomendaciones relevantes para implementar soluciones criptográficas en aplicaciones y sistemas de software. (y no en el uso de la criptografía)

**Investigación de los últimos 10 años**: La investigación se limitará a fuentes publicadas en los últimos 10 años, lo que garantizará la inclusión de las tendencias y avances más actuales en el campo de la criptografía aplicada al desarrollo de software.

**Investigación en idioma inglés:** Solo se tomará en cuenta fuentes de información de literatura gris y blanca en idioma inglés.

**No Profundización Extrema en Criptografía:** A pesar de su enfoque en la aplicación criptográfica, esta investigación no profundizará en aspectos altamente técnicos de la criptografía que requieran conocimientos matemáticos avanzados o experiencia en criptografía teórica, ya que no se cuenta con experiencia profesional sobre la criptografía.

**Enfoque en Desarrollo Seguro**: Aunque se abordará la criptografía en el contexto del desarrollo seguro de software, esta investigación no se adentrará en otros aspectos de seguridad de software, como pruebas de penetración o gestión de vulnerabilidades. Su objetivo principal es proporcionar información sobre prácticas y herramientas para el desarrollo seguro con enfoque en la criptografía.

**Limitaciones**:

**Investigación Bibliográfica**: No se podrá abordar otras fuentes de información que no son cubiertas por la Universidad Veracruzana.

**Investigación en idioma inglés:** A pesar de que solo serán tomado en cuenta literaturas del idioma inglés, esto también se puede contar como una limitante por no tener mucha experiencia con el idioma inglés.

# Marco Teórico

Explicación breve de los elementos teóricos (o teorías o disciplinas) empleados con el fin de ubicar al lector en la potencialidad del trabajo. El contenido de este apartado dependerá principalmente del tipo de trabajo. En tesis, tesinas, monografías y trabajos prácticos-científicos es de suma importancia ya que además en este apartado se buscará apoyo en todos aquellos trabajos alusivos al tema a desarrollar, que sean resultado de investigaciones con un alto rigor, provenientes de centros de investigación, instituciones, universidades, grupos de investigación reconocidos (es decir APORTACIONES DE OTRAS INVESTIGACIONES).

En otro tipo de trabajos, un marco contextual es suficiente. En este marco contextual deben establecerse el ámbito en el que se da el problema y la propuesta.

Cubrir conceptos, que es la criptografía, áreas principales, desarrollo seguro, programación segura, metodologías

La seguridad es un tema amplio y cubre una multitud de pecados. En su forma más simple, se ocupa de asegurarse de que las personas entrometidas no puedan leer, o peor aún, modificar en secreto los mensajes destinados a otros destinatarios. Se refiere a las personas que intentan acceder a servicios remotos que no están autorizados a usar. La mayoría de los problemas de seguridad son causados intencionalmente por personas malintencionadas que intentan obtener algún beneficio, llamar la atención o dañar a alguien.

La criptografía proviene de las palabras griegas para "escritura secreta". Tiene una larga y colorida historia que se remonta a miles de años. Los profesionales hacen una distinción entre cifrados y códigos. Un cifrado es una transformación carácter por carácter o bit por bit, sin tener en cuenta la estructura lingüística del mensaje. Por el contrario, un código reemplaza una palabra por otra palabra o símbolo. Los códigos ya no se usan, aunque tienen una historia gloriosa. En los datos y las telecomunicaciones, la criptografía es necesaria cuando se comunica a través de cualquier medio confiado, lo que incluye casi cualquier red, en particular Internet. La criptografía, entonces, no solo protege los datos contra robos o alteraciones. En general, hay tres tipos de esquemas criptográficos que se utilizan normalmente para lograr estos objetivos:

1. Criptografía de clave secreta (o simétrica): Utiliza una sola clave tanto para el cifrado como para el descifrado.
2. Criptografía de clave pública (o asimétrica): Utiliza una clave para el cifrado y otra para el descifrado
3. Funciones hash: Utiliza una transformación matemática para "cifrar" información de forma irreversible. (Davi, 2013)

sino que también se puede utilizar para la autenticación de usuarios.

# Método

Una SLR es un tipo de revisión de la literatura que recopila y analiza críticamente múltiples estudios o trabajos de investigación a través de un proceso sistemático, por lo cual se tomará el proceso de RSL propuesto por Kitchenham por lo cual será:

1.Planificar la SRL.

2.Especificar preguntas de investigación.

3.Desarrollar protocolo de revisión.

4.Conducir la SRL.

5.Validar protocolo de revisión.

6.Identificar fuentes/Estudios relevantes.

7.Seleccionar Estudios Primarios.

8.Evaluar la calidad de los estudios.

9.Extraer Datos Requeridos.

10.Sintetizar Datos.

11. Documentar la SRL.

12. Escribir informe del SRL.

13.Validar Informe.

# Contenido del trabajo de investigación (índice tentativo o estructura del trabajo)

Una idea de la organización del trabajo, con objeto de ayudar al lector a captar la relación que existe entre sus diversas partes.

# Cronograma

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cronograma de Actividades** | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| **Actividades** | **MESES** | | | | | | | | | | | | |
| **2023** | | | | **2024** | | | | | | | | |
| **Sep.** | **Oct** | **Nov** | **Dic** | **Ene** | **Feb** | **Mar** | **Arb** | **May** | **Jun** | **Jul** | **Ago.** | **Sep.** |
| Primera Entrega |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Primera Defensa |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Revisión de literatura |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Defensa de la Revisión de la literatura |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Primera Entrega de la monografía y corrección de la RSL |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Realización de la Monografía |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Realización del Articulo |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Defensa de la monografía |  |  |  |  |  |  |  |  |  |  |  |  |  |

# Bibliografía

Braga, A., Dahab, R., Antunes, N., Laranjeiro, N., & Vieira, M. (2019). Understanding how to use static analysis tools for detecting cryptography misuse in software. IEEE Transactions on Reliability, 68(4), 1384-1403.

Hazhirpasand, M., & Ghafari, M. (2021, November). Crypto Experts Advise What They Adopt. In 2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW) (pp. 179-184). IEEE.

Braga, A., Dahab, R., Antunes, N., Laranjeiro, N., & Vieira, M. (2017, October). Practical evaluation of static analysis tools for cryptography: Benchmarking method and case study. In 2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE) (pp. 170-181). IEEE

Braga and R. Dahab, "Mining Cryptography Misuse in Online Forums," 2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Vienna, Austria, 2016, pp. 143-150, doi: 10.1109/QRS-C.2016.23.

T. R. Devi, "Importance of Cryptography in Network Security," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, India, 2013, pp. 462-467, doi: 10.1109/CSNT.2013.102.

D. Verdon y G. McGraw, "Risk analysis in software design", IEEE Secur. Privacy Mag., vol. 2, núm. 4, págs. 79 a 84, julio de 2004.

Amazon Web Services. (2023). What Is Cryptography? https://aws.amazon.com/es/what-is/cryptography

Ortega Triguero, J. & López Guerrero, M. Á. (2006). Introducción a la criptografía: historia y actualidad.. Ediciones de la Universidad de Castilla-La Mancha. https://elibro.net/es/lc/bibliotecauv/titulos/54964

I͡Ashchenko. (2002). Cryptography: an Introduction. En Student mathematical library (ilustrada ed.). American Mathematical Soc., 2002. <https://doi.org/10.1090/stml/018>

V. H. Guthrie and P. B. Parikh, "Software safety analysis: using the entire risk analysis toolkit," Annual Symposium Reliability and Maintainability, 2004 - RAMS, Los Angeles, CA, USA, 2004, pp. 272-279, doi: 10.1109/RAMS.2004.1285460.

# Anexos