Pontificia Universidad Católica del Ecuador Sede Esmeraldas (PUCESE)

ESCUELA DE HÁBITAT, INFRAESTRUCTURA Y CREATIVIDAD

CARRERA:
INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

LÍNEA DE INVESTIGACIÓN:
INGENIERÍA DE SOFTWARE, INNOVACIÓN Y EMPRENDIMIENTO EN TIC

TÍTULO DEL ARTÍCULO CIENTÍFICO:
SEGURIDAD EN EL CÓDIGO SUGERIDO POR GITHUB COPILOT: ESTUDIO SISTEMÁTICO CON HERRAMIENTAS DE ANÁLISIS ESTÁTICO

TÍTULO PROFESIONAL:
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR:
Abel Roberson Ávila Ospina

ASESOR:
Msc. Xavier Quiñonez Ku

ESMERALDAS, 2026

SEGURIDAD EN EL CÓDIGO SUGERIDO POR GITHUB COPILOT: ESTUDIO SISTEMÁTICO CON HERRAMIENTAS DE ANÁLISIS ESTÁTICO

First A. Author, Second B. Author, Third C. Author

Name of authors' institution, city (Country)

ABSTRACT

La adopción de asistentes de codificación basados en inteligencia artificial, como GitHub Copilot, ha incrementado la productividad en el desarrollo de software, pero también ha introducido nuevas preocupaciones de seguridad. Este estudio presenta un análisis empírico y cuantitativo de la seguridad del código sugerido por GitHub Copilot mediante análisis estático. Se evaluaron setenta y dos fragmentos de código provenientes de treinta y ocho repositorios públicos en JavaScript, TypeScript y Python, seleccionados bajo criterios de evidencia explícita de uso de Copilot. El análisis se realizó con CodeQL y sus suites de seguridad, empleando métricas de frecuencia, severidad y recurrencia. Los resultados evidencian vulnerabilidades de severidad media y alta, principalmente relacionadas con inyecciones, manejo inseguro de entradas y exposición de datos sensibles, destacando TypeScript como el lenguaje con mayor concentración de vulnerabilidades críticas. Con base en estos hallazgos, se proponen recomendaciones alineadas con los estándares OWASP, CWE e ISO, orientadas a promover un uso seguro y responsable de herramientas de generación automática de código. Este trabajo aporta evidencia empírica verificable sobre los riesgos de seguridad asociados al código generado por IA y resalta la necesidad de integrar análisis de seguridad sistemáticos en entornos de desarrollo asistidos por inteligencia artificial.

KEYWORDS

CodeQL, Generative artificial intelligence, GitHub Copilot, Software security, Static analysis.

Security in GitHub Copilot Suggested Code: A Systematic Empirical Study Using Static Analysis Tools

Abel Roberson Avila Ospina (https://orcid.org/0009-0009-2743-5817), Esteban Fabricio Gonzabay-Jiménez (https://orcid.org/0009-0000-5224-1568), José Luis Carvajal Carvajal (https://orcid.org/0000-0001-9498-8088), Xavier Quiñonez-Ku (https://orcid.org/0000-0002-8653-6214)

Pontificia Universidad Católica del Ecuador, Esmeraldas campus, Esmeraldas (Ecuador).

ABSTRACT

The adoption of AI-based coding assistants, such as GitHub Copilot, has increased productivity in software development, but it has also introduced new security concerns. This study presents an empirical and quantitative analysis of code security suggested by GitHub Copilot using static analysis. Seventy-two code snippets from thirty-eight public repositories in JavaScript, TypeScript and Python were evaluated, selected under criteria of explicit evidence of Copilot use. The analysis was carried out with CodeQL and its security suites, using frequency, severity and recurrence metrics. The results show vulnerabilities of medium and high severity, mainly related to injections, insecure handling of inputs and exposure of sensitive data, highlighting TypeScript as the language with the highest concentration of critical vulnerabilities. Based on these findings, recommendations aligned with the OWASP, CWE and ISO standards are proposed, aimed at promoting the safe and responsible use of automatic code generation tools. This work provides verifiable empirical evidence on the security risks associated with AI-generated code and highlights the need to integrate systematic security analyses into AI-assisted development environments.

KEYWORDS

CodeQL, generative artificial intelligence, GitHub Copilot, software security, static analysis.

2.- Evidencias de envío a medio científico

1. **Documento de aprobación del asesor para realizar el envío del artículo científico (formato similar al usado para las tesis donde se especifica el porcentaje de similitud).**

INFORME DEL DOCENTE - DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CARRERA INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Esmeraldas, 10 de abril de 2026

Mgt. Homero Velasteguí
COORDINADOR DE CARRERA INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

De mis consideraciones:

Se envía el informe correspondiente a la tutoría realizada al Trabajo de Titulación que se detalla a continuación:

TITULO DEL TRABAJO DE INTEGRACIÓN CURRICULAR	SEGURIDAD EN EL CÓDIGO SUGERIDO POR GITHUB COPILOT: ESTUDIO SISTEMÁTICO CON HERRAMIENTAS DE ANÁLISIS ESTÁTICO	
DIRECTOR	Nombre	Cédula
	Xavier Quiñonez Ku	0801628207
ESTUDIANTE(S)	Nombre	Cédula
	Abel Roberson Ávila Ospina	0850478645

Se informa que el trabajo ha cumplido con todos los parámetros establecidos, mediante el cual el estudiante demuestra el desarrollo de competencias en el campo de conocimiento de su profesión y presenta una propuesta en el área de conocimiento, con un nivel de argumentación coherente.

Dando por concluida esta tutoría de trabajo de titulación, CERTIFICO, para los fines pertinentes, que el (los) estudiante(s) está(n) apto(s) para continuar con el proceso de LECTURA.

Atentamente,

DIRECTOR/TUTOR DE TRABAJO DE TITULACIÓN
C.I. 0801628207
NOMBRE: Msc. Xavier Quiñonez Ku
FECHA: 10-04-2026

2. Datos del medio científico enviado a revisión por pares o ya publicado

Para artículos en proceso de publicación. Un artículo está en proceso de publicación cuando se ha enviado a la plataforma de la revista científica seleccionada para que el editor inicie su análisis y luego proceda a iniciar el proceso de revisión por pares.

Nombre de la revista científica: International Journal of Interactive Multimedia and Artificial Intelligence (IJIMAI)

Enlace (URL) de la revista: https://www.ijimai.org/index.php/ijimai/

ISSN de la revista: ISSN: 1989-1660 (Online)

Medio(s) de indexación:

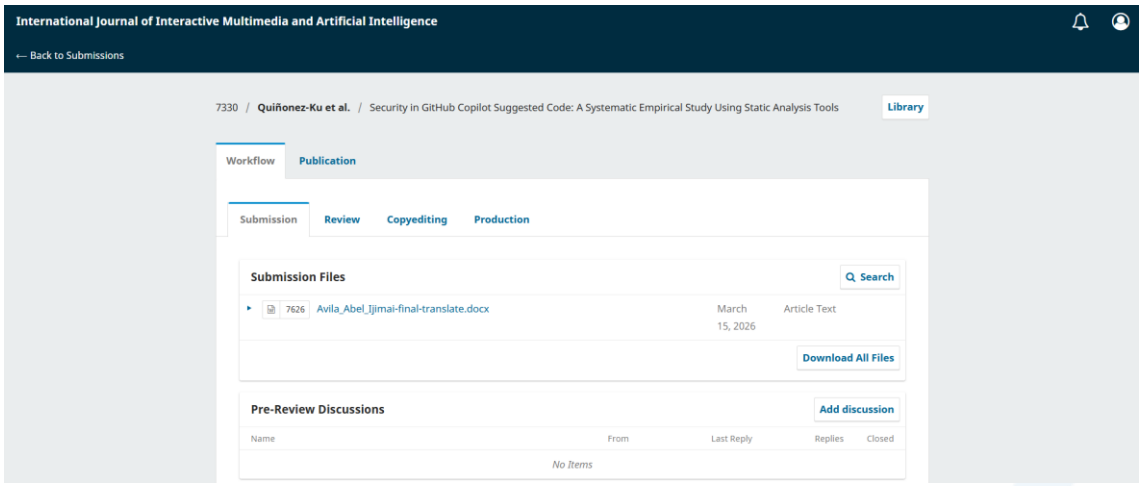
[X] Scopus
[ ] Scielo Ecuador
[X] Emerging Source Citation Index (ESCI - Web of Science)
[X] Google Scholar
[ ] Base Search
[ ] Copernicus Index
[ ] EBSCO. Applied Science & Technology Source Ultimate
[ ] Latam +
[ ] Scientific Indexing Services
[ ] Europub
[ ] ScienceGate
[X] Latindex 2.0

Nombre del editor de la revista: Dra. Elena Verdú

Correo electrónico del editor de la revista: journal@ijimai.org

Fecha de envío del artículo a la revista: 15-03-3026

3. **Captura de pantalla de plataforma de la revista en la que se sube el artículo.**



4. **Captura de pantalla del correo recibido por la plataforma o editor de la revista.**