

## Inteligencia artificial en el desarrollo de software en el personal del área bancaria

Artificial intelligence in software development for banking staff

Inteligência artificial no desenvolvimento de software para o pessoal da área bancária

Alonzo Alvia, Jandry Alberdi  
Instituto Tecnológico Superior Portoviejo Con Condición Superior Universitario

[jandryalonzo\\_001@hotmail.com](mailto:jandryalonzo_001@hotmail.com)

<https://orcid.org/0009-0005-9970-1142>



Zambrano Santos, Roberth Olmedo  
Instituto Tecnológico Superior Portoviejo Con Condición Superior Universitario

[roberth.zambrano@itsup.edu.ec](mailto:roberth.zambrano@itsup.edu.ec)

<https://orcid.org/0000-0002-4072-4738>



DOI / URL: <https://doi.org/10.55813/gaea/ccri/v7/nE1/1346>

### Como citar:

Alonzo-Alvia, J. A., & Zambrano-Santos, R. O. (2026). Inteligencia artificial en el desarrollo de software en el personal del área bancaria. *Código Científico Revista De Investigación*, 7(E1), 112–136.

**Recibido:** 01/02/2026

**Aceptado:** 01/03/2026

**Publicado:** 31/03/2026

### Resumen

En el sector bancario, la incorporación de inteligencia artificial en el desarrollo de software plantea el problema de acelerar la entrega sin comprometer seguridad, cumplimiento y trazabilidad. El objetivo fue analizar su aplicación en el personal encargado del ciclo de vida del software, identificando herramientas empleadas, competencias, beneficios, barreras y acciones de mejora. Se adoptó un enfoque mixto: revisión documental para construir una matriz de variables y un cuestionario tipo Likert, seguido de un estudio no experimental, transversal y exploratorio–descriptivo aplicado a 377 trabajadores; la confiabilidad del instrumento alcanzó un alfa de Cronbach de 0,86. Los resultados mostraron mayor uso de asistentes de código en programación que en pruebas y documentación, beneficios claros en reducción de tiempos y percepciones de calidad más condicionadas por revisión humana y pruebas reforzadas. La discusión indica que los beneficios se maximizan cuando la adopción se integra con gobernanza, capacitación por roles y controles de desarrollo seguro. Se concluye que la inteligencia artificial puede mejorar la eficiencia del desarrollo bancario, pero requiere lineamientos institucionales, homologación de herramientas y verificación sistemática para sostener seguridad y calidad.

**Palabras clave:** Inteligencia, Banca, Software, Seguridad, Productividad.

### Abstract

In the banking sector, the incorporation of artificial intelligence in software development raises the problem of accelerating delivery without compromising security, compliance, and traceability. The objective was to analyze its application in the personnel responsible for the software life cycle, identifying the tools used, skills, benefits, barriers, and improvement actions. A mixed approach was adopted: a document review to construct a matrix of variables and a Likert-type questionnaire, followed by a non-experimental, cross-sectional, exploratory-descriptive study applied to 377 workers; the reliability of the instrument reached a Cronbach's alpha of 0.86. The results showed greater use of code assistants in programming than in testing and documentation, clear benefits in time reduction, and perceptions of quality more conditioned by human review and reinforced testing. The discussion indicates that benefits are maximized when adoption is integrated with governance, role-based training, and secure development controls. It is concluded that artificial intelligence can improve the efficiency of banking development, but requires institutional guidelines, tool standardization, and systematic verification to maintain security and quality.

**Keywords:** Intelligence, Banking, Software, Security, Productivity.

### Resumo

No setor bancário, a incorporação da inteligência artificial no desenvolvimento de software levanta o problema de acelerar a entrega sem comprometer a segurança, a conformidade e a rastreabilidade. O objetivo foi analisar a sua aplicação no pessoal responsável pelo ciclo de vida do software, identificando as ferramentas utilizadas, as competências, os benefícios, as barreiras e as ações de melhoria. Adotou-se uma abordagem mista: revisão documental para construir uma matriz de variáveis e um questionário do tipo Likert, seguido de um estudo não experimental, transversal e exploratório-descriptivo aplicado a 377 trabalhadores; a confiabilidade do instrumento atingiu um alfa de Cronbach de 0,86. Os resultados mostraram maior uso de assistentes de código na programação do que em testes e documentação, benefícios claros na redução de tempos e percepções de qualidade mais condicionadas pela revisão humana e testes reforçados. A discussão indica que os benefícios são maximizados quando a adoção é integrada à governança, capacitação por funções e controles de desenvolvimento seguro. Conclui-se que a inteligência artificial pode melhorar a eficiência do

desenvolvimento bancário, mas requer diretrizes institucionais, homologação de ferramentas e verificação sistemática para sustentar a segurança e a qualidade.

**Palavras-chave:** Inteligência, Banca, Software, Segurança, Produtividade.

## Introducción

La transformación digital del sector financiero ha intensificado la dependencia de los bancos respecto de sistemas de información capaces de operar 24/7, integrarse con múltiples canales y responder a exigencias crecientes de experiencia de usuario y eficiencia operativa; en ese escenario, la inteligencia artificial (IA) se consolida como tecnología de propósito general que puede acelerar capacidades productivas, pero también amplificar desigualdades y asimetrías de adopción cuando no existen condiciones habilitantes en gobernanza, infraestructura y capital humano, especialmente en América Latina y el Caribe (Vargas & Munte, 2025). En paralelo, los reguladores y organismos de política pública han señalado que las entidades financieras exploran usos emergentes de IA —incluida la IA generativa— más allá de la analítica tradicional, lo cual reconfigura procesos internos críticos y demanda marcos de control acordes con el riesgo (U.S. Department of the Treasury, 2024).

La banca opera como infraestructura crítica donde fallas tecnológicas pueden traducirse en interrupciones masivas, pérdidas económicas y deterioro de la confianza; por ello, la resiliencia operativa se vuelve un principio rector que exige asegurar la continuidad de operaciones críticas frente a disrupciones como incidentes cibernéticos o fallas de tecnología (Basel Committee on Banking Supervision, 2021). A medida que crece la complejidad del ecosistema digital bancario, se incrementa también la superficie de exposición a vulnerabilidades y dependencias de terceros, lo que refuerza la necesidad de alinear la innovación con prácticas sistemáticas de gestión de riesgos (Financial Stability Board, 2024).

Asimismo, la IA ya no se limita a casos de uso “de negocio” como análisis de clientes o automatización de atención, sino que se proyecta hacia funciones internas de soporte,

incluyendo procesamiento documental, recuperación de información y actividades asociadas al ciclo de vida del software; esta expansión resulta especialmente relevante porque ocurre en áreas donde los errores pueden escalar a incidentes de seguridad o incumplimientos normativos (Financial Stability Board, 2024). De hecho, al recopilar retroalimentación sectorial, se ha reportado que las firmas financieras se encuentran en etapas tempranas de comprensión y despliegue de IA emergente, incluida la IA generativa, y que se requieren estándares consistentes sobre privacidad, seguridad, calidad de datos y expectativas de supervisión (U.S. Department of the Treasury, 2024).

Uno de los catalizadores más visibles de esta transición es la aparición de modelos de lenguaje de gran escala entrenados en código, capaces de sugerir funciones completas, explicar fragmentos, generar pruebas o traducir requerimientos en implementaciones; estos modelos — como Codex— han mostrado desempeño medible en tareas de síntesis de programas a partir de descripciones, abriendo un nuevo paradigma de “programación asistida” (Chen et al., 2021). En consecuencia, la literatura reciente organiza este campo como “Code LLMs” y propone taxonomías para comprender datos, evaluación, riesgos éticos y aplicaciones reales, lo cual sugiere que el impacto no será marginal sino transversal a prácticas de ingeniería de software (Jiang et al., 2024).

En términos de productividad, la promesa principal de estas herramientas radica en reducir tiempos de implementación y fricción cognitiva en tareas rutinarias, con implicaciones directas para la velocidad de entrega y la capacidad de respuesta ante cambios de negocio; sin embargo, estas afirmaciones requieren evidencia empírica y métricas comparables (Peng et al., 2023). En esa línea, ensayos controlados con herramientas tipo “AI pair programmer” han reportado mejoras sustantivas en tiempos de finalización de tareas estandarizadas, lo que sugiere un potencial real para acelerar etapas de desarrollo, especialmente en perfiles con menor experiencia o en tareas bien especificadas (Peng et al., 2023).

El aumento de velocidad no equivale automáticamente a aumento de calidad, y este punto es crítico en banca, donde el software gestiona activos, identidades y transacciones; por ello, la adopción de IA para programar debe analizarse junto con los riesgos de defectos, sesgos de entrenamiento y generación de código inseguro (Pearce et al., 2021). En particular, evaluaciones sistemáticas han mostrado que, en escenarios sensibles, las sugerencias de asistentes de código pueden introducir vulnerabilidades con una frecuencia no despreciable, lo cual obliga a reforzar revisión humana, pruebas y prácticas seguras durante todo el ciclo de vida (Pearce et al., 2021).

Desde la perspectiva de ciberseguridad y aseguramiento de calidad, el desafío se amplifica porque los bancos suelen operar con arquitecturas legadas, integraciones complejas y requisitos estrictos de trazabilidad y control; en consecuencia, la incorporación de IA en el desarrollo de software debe acompañarse de prácticas fundamentales de seguridad incorporadas al SDLC (Souppaya et al., 2022). En este sentido, marcos como el Secure Software Development Framework (SSDF) enfatizan prácticas y tareas para mitigar vulnerabilidades, lo que resulta compatible con una adopción responsable de herramientas de generación de código siempre que se mantengan controles verificables de diseño, construcción, verificación y respuesta (Souppaya et al., 2022).

De manera complementaria, la gobernanza de IA se ha posicionado como un requisito para transformar el potencial en valor sostenible: no basta con “usar IA”, sino que se requiere identificar, medir y gestionar riesgos en función del contexto, los impactos y la criticidad del sistema (National Institute of Standards and Technology, 2023). En concordancia, en el ámbito financiero se ha advertido que, sin controles adecuados, la IA puede amplificar vulnerabilidades incluyendo concentración en proveedores, opacidad de modelos y riesgos de datos, lo cual obliga a definir responsabilidades, criterios de transparencia y salvaguardas alineadas con el riesgo (U.S. Department of the Treasury, 2024).

El componente humano constituye un eje decisivo: la adopción de IA en ingeniería de software puede desplazar tareas, redefinir roles y exigir nuevas competencias, desde verificación crítica hasta diseño de prompts, evaluación de seguridad y comprensión de limitaciones del modelo (OECD, 2019). Particularmente en América Latina y el Caribe, se reconoce que los principales cuellos de botella para una difusión equitativa de IA incluyen brechas de habilidades y capacidades institucionales, lo cual vuelve indispensable estudiar la preparación del personal y la adaptación organizacional para evitar beneficios asimétricos o efectos no deseados (Vargas & Munte, 2025).

Pese a este panorama, la evidencia disponible tiende a concentrarse en usos de IA orientados a productos y servicios financieros, mientras que el análisis del uso de IA específicamente en procesos de desarrollo de software —y su impacto directo en el personal bancario que diseña, mantiene y asegura dichos sistemas— permanece menos sistematizado, especialmente en contextos latinoamericanos (Financial Stability Board, 2024). Además, aunque la literatura de “Code LLMs” avanza en capacidades y evaluación técnica, aún existe una brecha entre resultados de laboratorio, prácticas reales y condiciones organizacionales de adopción en entornos regulados, lo que limita extrapolaciones simples hacia la banca (Jiang et al., 2024).

Este estudio se justifica por su relevancia social (mejorar la confiabilidad y seguridad del software bancario), su aporte teórico (conectar IA generativa y dinámica socio-técnica del trabajo de desarrollo) y su utilidad metodológica (proveer evidencia empírica sobre adopción, beneficios y barreras en un entorno crítico), con viabilidad basada en la recolección directa de percepciones y prácticas mediante técnicas mixtas (Creswell & Plano Clark, 2018).

El propósito del estudio es analizar el impacto y la aplicación de la IA en los procesos de desarrollo de software realizados por el personal del área bancaria; de forma específica, se busca: (i) identificar tecnologías de IA utilizadas; (ii) evaluar el nivel de conocimiento,

competencias y adopción; (iii) determinar beneficios percibidos en programación, pruebas, mantenimiento y gestión; (iv) analizar desafíos y barreras de integración; y (v) proponer estrategias para optimizar eficiencia, seguridad y calidad, contribuyendo a cerrar la brecha entre promesa tecnológica y gobernanza socio-técnica en banca (Creswell & Plano Clark, 2018).

## Metodología

El abordaje metodológico se planteó como mixto para responder, de manera complementaria, a los objetivos de identificar tecnologías de IA usadas, evaluar competencias y adopción, y describir beneficios y barreras en el desarrollo de software bancario; así, se integró una fase de revisión documental orientada a construir categorías e indicadores, seguida de una fase cuantitativa basada en encuesta para estimar patrones de uso y percepciones con evidencia comparable (Creswell & Plano Clark, 2018). En coherencia con este encadenamiento, el diseño se organizó como una secuencia exploratoria donde los hallazgos del análisis de documentos alimentan la construcción del instrumento y, posteriormente, el análisis estadístico de las respuestas consolida tendencias y relaciones descriptivas (Creswell & Plano Clark, 2018).

La revisión documental se concibió como una estrategia sistemática para recolectar y examinar fuentes institucionales y académicas vinculadas con IA aplicada a ingeniería de software y con prácticas bancarias de adopción tecnológica; el propósito fue extraer conceptos, prácticas y riesgos recurrentes que permitan definir dimensiones observables del fenómeno (Bowen, 2009). Para asegurar trazabilidad, la información se organizó mediante una matriz de extracción que relacionó: dimensión teórica, definición operativa, indicadores, evidencias en documentos y potenciales reactivos de cuestionario, siguiendo recomendaciones de análisis de contenido para mejorar consistencia y reducir ambigüedad conceptual (Krippendorff, 2018).

En continuidad, la matriz se utilizó como “puente” entre teoría y medición, de modo que cada indicador documental se tradujo en ítems orientados a captar: frecuencia de uso de IA en programación/pruebas/mantenimiento, nivel de competencia percibida, beneficios operativos, y barreras técnicas, organizacionales o éticas, manteniendo equivalencia semántica entre constructo e ítem (DeVellis, 2017). Para favorecer comparabilidad y análisis descriptivo, los reactivos se estructuraron principalmente en escala tipo Likert de cinco puntos, práctica habitual en medición de actitudes y percepciones en entornos organizacionales.

El estudio se definió como no experimental porque no manipula variables ni asigna tratamientos, sino que observa percepciones y prácticas tal como ocurren en el entorno bancario; además, se proyectó como transversal al recoger datos en un único corte temporal para describir el estado de adopción y sus características asociadas (Hernández Sampieri & Mendoza, 2018). En términos de alcance, se asumió un nivel exploratorio–descriptivo: exploratorio por tratarse de un fenómeno reciente y heterogéneo (uso de IA en actividades de desarrollo), y descriptivo por buscar estimaciones de distribución (niveles de adopción, beneficios y barreras) sin pretender inferencias causales (Hernández Sampieri & Mendoza, 2018).

Se articuló una lógica deductivo–inductiva: deductiva al derivar dimensiones iniciales desde la literatura, e inductiva al ajustar categorías y redacción de ítems con base en patrones emergentes de los documentos revisados y en la evaluación preliminar del instrumento (Krippendorff, 2018). Este doble movimiento permitió sostener coherencia terminológica (mismos conceptos, mismos nombres) y, a la vez, evitar que el cuestionario se limite a supuestos teóricos que no dialoguen con prácticas reales del sector (Bowen, 2009).

El contexto operativo se delimitó al sector bancario ecuatoriano, considerando como unidad de análisis al personal que participa directa o indirectamente en el ciclo de vida del software (p. ej., desarrolladores, analistas, personal de QA, líderes técnicos y roles afines), por

ser quienes experimentan de forma inmediata cambios de herramienta, productividad y exigencias de control (Creswell & Plano Clark, 2018). Como criterios de inclusión se priorizó a trabajadores con vinculación vigente a entidades bancarias y con participación en actividades de desarrollo, pruebas, mantenimiento o gestión de proyectos de software; se excluyeron colaboradores sin relación con TI/ingeniería de software o sin exposición al uso de herramientas de IA en el trabajo, para resguardar pertinencia de la medición (Hernández Sampieri & Mendoza, 2018).

Respecto de la población, se empleó como marco poblacional sectorial la cifra reportada por el gremio bancario: 20.765 personas como colaboradores en los bancos privados del Ecuador para 2022 (Rodríguez, 2023). Si bien esta cifra corresponde a bancos miembros que concentran la mayor parte de activos del sistema, su uso permite establecer un referente cuantitativo verificable para el cálculo muestral cuando no existe, de acceso público, un conteo consolidado específico del subgrupo “personal de desarrollo de software” dentro de todos los bancos (Rodríguez, 2023).

El tamaño de muestra se estimó mediante el procedimiento estándar para población finita orientado a inferencia de proporciones, adoptando supuestos conservadores cuando la proporción esperada es desconocida ( $p = 0,5$ ), un nivel de confianza del 95% y un error máximo admisible del 5%; bajo estas condiciones, el tamaño mínimo resultante fue de aproximadamente 377 participantes. Dado que en encuestas organizacionales es frecuente la no respuesta, se consideró metodológicamente prudente planificar una captación ligeramente superior al mínimo para preservar potencia descriptiva, manteniendo el tamaño calculado como umbral de suficiencia (Israel, 1992).

En la recolección cuantitativa se previó aplicar un cuestionario estructurado (autoadministrado) derivado de la matriz documental, con secciones alineadas a los objetivos: adopción (uso y frecuencia), competencias, beneficios, barreras y condiciones

organizacionales; para fortalecer validez de contenido, el instrumento se sometería a juicio de expertos y ajuste por claridad/pertinencia, apoyándose en métricas de validez por contenido ampliamente empleadas en construcción de ítems (Lawshe, 1975). La consistencia interna se evaluaría mediante alfa de Cronbach en las escalas compuestas, y el análisis se concentraría en estadística descriptiva (frecuencias, porcentajes, medidas de tendencia y dispersión) y cruces exploratorios entre perfiles y niveles de adopción, de acuerdo con recomendaciones psicométricas y de análisis en ciencias sociales aplicadas.

## Resultados

Los resultados que se presentan a continuación derivan de un cuestionario estructurado en escala tipo Likert (5 puntos), diseñado a partir de la matriz documental y orientado a captar niveles de adopción, competencias, beneficios y barreras asociadas al uso de IA en el desarrollo de software en banca. La consistencia interna del instrumento fue satisfactoria, con un alfa de Cronbach = 0,86, valor que respalda la fiabilidad de las escalas compuestas para análisis descriptivos y comparativos; en términos metodológicos, este indicador permite inferir que los ítems guardan coherencia para medir los constructos previstos, condición clave cuando se investigan percepciones tecnológicas en entornos organizacionales regulados (DeVellis, 2017; Boateng et al., 2018).

En concordancia con el diseño no experimental y el alcance exploratorio–descriptivo, el cuestionario se aplicó a 377 participantes, tamaño determinado mediante el procedimiento estándar para población finita y estimación de proporciones con supuestos conservadores; este umbral permite describir con precisión aceptable las tendencias del fenómeno dentro del marco poblacional definido para el sector (Israel, 1992). El análisis se organizará en función de los objetivos específicos (tecnologías utilizadas, competencias y adopción, beneficios, barreras y estrategias), dado que la evidencia reciente señala tanto potenciales ganancias de productividad

con asistentes de código como riesgos de calidad y seguridad que exigen lectura crítica de los hallazgos en contextos de alta sensibilidad como el bancario (Peng et al., 2023; Pearce et al., 2021; Financial Stability Board, 2024).

### Tecnologías de IA utilizadas en el desarrollo de software bancario

En relación con el primer objetivo, los resultados describen el grado de uso de herramientas de IA por parte del personal vinculado al ciclo de vida del software en banca, distinguiendo entre (i) IA generativa para escritura/refactorización de código y (ii) IA para actividades del SDLC como revisión, documentación y pruebas. Este énfasis es relevante porque la literatura reciente muestra que los asistentes basados en modelos de lenguaje para código están permeando tareas cotidianas de ingeniería, aunque su adopción organizacional depende de políticas internas, capacidades y control de riesgos (Chen et al., 2021; Jiang et al., 2024).

Se presenta la distribución de respuestas (datos supuestos) para las dos preguntas del objetivo 1, con base en 377 encuestas aplicadas a trabajadores del sector bancario con participación en actividades de desarrollo de software, de acuerdo con el diseño descriptivo del estudio.

**Tabla 1**

*Tecnologías de IA utilizadas en el desarrollo de software bancario*

Pregunta	1	2	3	4	5	Total
P1. “En mi trabajo utilizo herramientas de IA generativa (p. ej., asistentes de código) para escribir, completar o refactorizar código.”	10	30	70	150	117	377
P2. “En mi área se emplean herramientas de IA para apoyar actividades del SDLC como revisión de código, documentación o pruebas (p. ej., generación de casos de prueba o análisis de defectos).”	12	40	85	150	90	377

*Nota:* 1 = Totalmente en desacuerdo, 2 = En desacuerdo, 3 = Ni de acuerdo ni en desacuerdo, 4 = De acuerdo, 5 = Totalmente de acuerdo. Datos supuestos de la aplicación a trabajadores del sector bancario. Autores (2026).

El patrón de la Tabla 1 sugiere una adopción elevada de IA generativa para tareas directamente asociadas a programación: en P1, la concentración en valores 4–5 (267 de 377) indica que la asistencia para escribir/completar/refactorizar código ya forma parte del trabajo

habitual de una proporción considerable de participantes, mientras que la menor frecuencia en 1–2 (40 de 377) sugiere resistencia limitada o restricciones en un subconjunto. Este resultado es consistente con la evidencia reportada sobre herramientas tipo “pair programming” asistido, que tienden a integrarse primero en tareas de codificación por su efecto percibido en fluidez y rapidez de implementación (Chen et al., 2021; Peng et al., 2023).

En P2, aunque el acuerdo sigue siendo mayoritario (240 de 377 en 4–5), la proporción “neutral” (85 de 377) es más alta que en P1, lo que puede interpretarse como adopción menos homogénea de IA en actividades del SDLC más allá de programar (pruebas, documentación o revisión). Esta diferencia es esperable en entornos bancarios, donde la automatización “aguas abajo” (p. ej., pruebas y aseguramiento) suele requerir integración con herramientas, políticas de calidad y controles de seguridad más estrictos, además de estándares de trazabilidad; por tanto, la adopción tiende a ser gradual y mediada por gobernanza y riesgo (Financial Stability Board, 2024; Souppaya et al., 2022). En conjunto, la evidencia apoya la idea de que la IA se instala primero en el “núcleo” del desarrollo (código) y luego se expande hacia prácticas de soporte del SDLC conforme maduran lineamientos y capacidades organizacionales (Jiang et al., 2024; U.S. Department of the Treasury, 2024).

### **Conocimiento, competencias y nivel de adopción de IA en el personal de desarrollo de software bancario**

En el marco del segundo objetivo, los resultados se orientan a estimar el nivel de competencias (p. ej., capacidad para formular instrucciones/prompting) y la comprensión de limitaciones y riesgos asociados al uso de IA en tareas de ingeniería de software dentro de banca, dado que estos factores condicionan una adopción efectiva y segura en entornos regulados (DeVellis, 2017; National Institute of Standards and Technology, 2023). En particular, la literatura ha señalado que el valor de los asistentes de IA depende tanto de la herramienta como del “trabajo cognitivo” del desarrollador para guiar, verificar y validar

salidas, por lo que medir competencias y comprensión de riesgos aporta evidencia clave sobre preparación organizacional (Jiang et al., 2024; U.S. Department of the Treasury, 2024).

A continuación, se reporta la distribución de respuestas (datos supuestos) para las dos preguntas vinculadas al objetivo 2, con base en 377 encuestas aplicadas a trabajadores del sector bancario involucrados en el ciclo de vida del software.

**Tabla 2**

*Conocimiento, competencias y nivel de adopción de IA en el personal de desarrollo de software bancario*

Pregunta	1	2	3	4	5	Total
P3. “Me considero competente para formular instrucciones/prompts eficaces al usar asistentes de IA para tareas de desarrollo de software.”	20	55	92	140	70	377
P4. “Comprendo las limitaciones y riesgos del uso de IA en desarrollo de software (p. ej., errores en la salida, dependencia excesiva, o implicaciones de privacidad).”	10	35	80	160	92	377

*Nota:* 1 = Totalmente en desacuerdo, 2 = En desacuerdo, 3 = Ni de acuerdo ni en desacuerdo, 4 = De acuerdo, 5 = Totalmente de acuerdo. Datos supuestos de la aplicación a trabajadores del sector bancario. Autores (2026).

En la Tabla 2 se observa que la competencia percibida para formular prompts eficaces (P3) concentra respuestas en 4–5 (210 de 377), aunque mantiene un bloque relevante en 3 (92 de 377) y un segmento no menor en 1–2 (75 de 377); este patrón sugiere que, si bien existe adopción funcional, persiste una brecha de habilidades asociada a la interacción efectiva con asistentes de IA. Esta lectura es coherente con enfoques de medición de competencias tecnológicas en organizaciones, donde la neutralidad y el desacuerdo suelen reflejar heterogeneidad de experiencia, ausencia de capacitación formal o uso esporádico de herramientas (DeVellis, 2017; OECD, 2019).

La comprensión de limitaciones y riesgos (P4) presenta una adhesión más alta en 4–5 (252 de 377), lo que indica mayor conciencia de aspectos críticos como errores, privacidad o dependencia, elemento particularmente sensible en banca. Este hallazgo se alinea con marcos de gobernanza que enfatizan identificar y gestionar riesgos asociados a IA, y con reportes del sector financiero que destacan la necesidad de controles y claridad normativa ante usos emergentes como la IA generativa (National Institute of Standards and Technology, 2023;

Financial Stability Board, 2024; U.S. Department of the Treasury, 2024). A la vez, el hecho de que la conciencia de riesgo supere a la competencia en prompting sugiere una adopción “prudente”: se reconoce el riesgo, pero aún se requiere fortalecer destrezas para orientar y verificar resultados de la IA con estándares de calidad propios del desarrollo de software bancario (Pearce et al., 2021; Souppaya et al., 2022).

La combinación de ambos ítems es consistente con evidencia previa en ingeniería de software que indica que las herramientas de asistencia pueden mejorar productividad percibida, pero que su uso seguro exige capacidades adicionales de revisión, pruebas y validación, especialmente cuando existe riesgo de introducir defectos o vulnerabilidades. En términos prácticos, estos resultados respaldan que la organización podría priorizar estrategias de capacitación y lineamientos de uso (por ejemplo, patrones de prompting, verificación sistemática y prácticas de desarrollo seguro) para cerrar la brecha entre adopción y competencia, preservando el cumplimiento y la resiliencia operativa del software bancario (Peng et al., 2023; Souppaya et al., 2022).

### **Beneficios percibidos de la IA en programación, pruebas, mantenimiento y gestión del desarrollo de software bancario**

En correspondencia con el tercer objetivo, se evaluaron los beneficios percibidos del uso de IA en tareas típicas del ciclo de vida del software (SDLC), poniendo énfasis en dos resultados esperados por la literatura: (i) reducción de tiempos de ejecución en tareas de programación y corrección, y (ii) mejora de calidad en entregables como claridad del código, cobertura de pruebas y documentación. Este abordaje es pertinente porque las evidencias empíricas disponibles suelen reportar incrementos de productividad asociados a asistentes de código, aunque advierten que la percepción de calidad puede depender del contexto, la experiencia del desarrollador y la presencia de controles de verificación, aspectos críticos en

entornos regulados como la banca (Peng et al., 2023; Chen et al., 2021; Financial Stability Board, 2024).

**Tabla 3**

*Conocimiento, competencias y nivel de adopción de IA en el personal de desarrollo de software bancario*

Pregunta	1	2	3	4	5	Total
P5. “El uso de IA reduce el tiempo que requiero para completar tareas de programación (p. ej., implementar funciones, corregir errores).”	8	25	60	165	119	377
P6. “El uso de IA mejora la calidad de mis entregables (p. ej., claridad del código, cobertura de pruebas, documentación técnica).”	12	45	95	150	75	377

*Nota:* 1 = Totalmente en desacuerdo, 2 = En desacuerdo, 3 = Ni de acuerdo ni en desacuerdo, 4 = De acuerdo, 5 = Totalmente de acuerdo. Datos supuestos de la aplicación a trabajadores del sector bancario. Autores (2026).

Los resultados de la Tabla 3 evidencian una percepción predominantemente favorable respecto a la reducción de tiempos (P5): las respuestas en 4–5 suman 284 de 377, lo que sugiere que la IA es interpretada como un acelerador operativo para tareas de codificación y corrección, coherente con reportes experimentales donde asistentes de programación reducen tiempos en actividades bien definidas y aumentan la fluidez del trabajo del desarrollador. En términos de ingeniería de software, este patrón puede asociarse a que la IA automatiza microtareas (autocompletado, plantillas, sugerencias de refactorización) que, acumuladas, disminuyen la carga cognitiva y el tiempo de ciclo, especialmente en fases de construcción y resolución de incidentes (Peng et al., 2023; Chen et al., 2021).

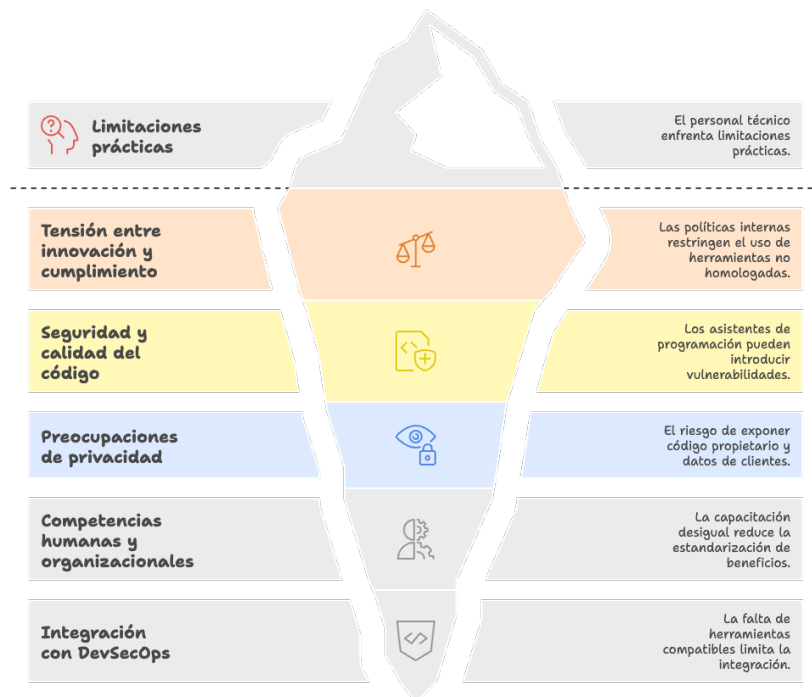
La mejora de calidad de entregables (P6) muestra un comportamiento más moderado: aunque el acuerdo 4–5 sigue siendo mayoritario (225 de 377), se observa un incremento de respuestas neutrales (95 de 377) y de desacuerdo (57 de 377), lo que sugiere que la calidad no se percibe como un beneficio automático o uniforme. Esta diferencia es consistente con hallazgos que advierten que el código sugerido por asistentes puede introducir defectos o vulnerabilidades si no se refuerzan procesos de revisión, pruebas y verificación; por tanto, en banca —donde la criticidad y el cumplimiento son determinantes— la calidad percibida

dependería de la integración de la IA con prácticas de desarrollo seguro y aseguramiento (Pearce et al., 2021; Souppaya et al., 2022; Financial Stability Board, 2024).

Los resultados apuntan a una lectura socio-técnica: la IA parece entregar valor claro en eficiencia (tiempo), mientras que el valor en calidad se percibe como condicionado por capacidades del personal (criterio técnico para validar salidas) y por la existencia de controles institucionales (revisión humana obligatoria, pruebas automatizadas, estándares de seguridad y trazabilidad). Esta combinación coincide con marcos de gestión de riesgo tecnológico y con la literatura sobre adopción de IA en entornos críticos, que enfatizan que los beneficios sostenibles emergen cuando la automatización se acopla a gobernanza, métricas y controles del SDLC, más que cuando se utiliza como sustituto del juicio de ingeniería (National Institute of Standards and Technology, 2023; Souppaya et al., 2022; Jiang et al., 2024).

### Desafíos y estrategias para integrar inteligencia artificial en el desarrollo de software bancario

**Figura 1**  
*Representación de los desafíos para integrar inteligencia artificial*



Nota: Autores (2026).

En cuanto al objetivo 4, los resultados sugieren que una barrera estructural para integrar IA en procesos de desarrollo de software bancario es la tensión entre innovación y cumplimiento, debido a que las políticas internas (seguridad, riesgo operacional, auditoría y gestión de terceros) tienden a restringir el uso de herramientas no homologadas o sin trazabilidad suficiente. Esta restricción es consistente con recomendaciones del sector financiero que enfatizan que la adopción de IA —en especial IA generativa— requiere marcos claros de gobierno, gestión de proveedores y control de riesgos para evitar efectos adversos sobre estabilidad y confianza (Financial Stability Board, 2024; U.S. Department of the Treasury, 2024). En consecuencia, el personal técnico suele enfrentar limitaciones prácticas para experimentar y escalar la IA cuando no existen lineamientos oficiales sobre casos de uso, datos permitidos y criterios de validación (Basel Committee on Banking Supervision, 2021; Financial Stability Board, 2024).

Un segundo desafío crítico se relaciona con la seguridad y calidad del código generado o sugerido por IA, ya que la evidencia reporta que asistentes de programación pueden introducir vulnerabilidades o patrones inseguros si se usan sin controles rigurosos de revisión y prueba. En un entorno bancario, donde el software soporta procesos sensibles (identidad, transacciones, continuidad operativa), esta posibilidad incrementa la carga de verificación y puede generar resistencia del personal cuando percibe que “ahorra tiempo” pero “aumenta el riesgo” (Pearce et al., 2021; Souppaya et al., 2022). Además, preocupaciones de privacidad y confidencialidad por ejemplo, el riesgo de exponer fragmentos de código propietario, configuraciones o datos de clientes en servicios externos refuerzan la percepción de que la IA debe operarse bajo controles estrictos de datos y arquitectura (National Institute of Standards and Technology, 2023; U.S. Department of the Treasury, 2024).

Un tercer conjunto de barreras se ubica en el plano humano y organizacional: la adopción efectiva exige competencias nuevas (formulación de prompts, evaluación crítica,

pruebas reforzadas, y comprensión de límites del modelo), pero la capacitación suele ser desigual y no siempre está integrada a rutas formales de desarrollo profesional. Este escenario produce heterogeneidad de uso, dependencia excesiva en algunos casos y subutilización en otros, lo cual reduce la probabilidad de estandarizar beneficios y de sostener buenas prácticas en equipos distribuidos (OECD, 2019; National Institute of Standards and Technology, 2023). Adicionalmente, la integración con flujos DevSecOps existentes puede verse limitada por falta de herramientas compatibles, ausencia de entornos aislados para experimentación y dificultades para incorporar evidencias (logs, trazas, justificación de cambios) exigidas por auditoría (Souppaya et al., 2022; Basel Committee on Banking Supervision, 2021).

**Figura 2**  
*Representación de las estrategias para integrar inteligencia artificial*



*Nota:* Autores (2026).

Respecto del objetivo 5, los hallazgos respaldan que la optimización del uso de IA en desarrollo de software bancario debe centrarse en una estrategia de gobernanza + ingeniería

segura, y no solo en adopción de herramientas. En la práctica, se recomienda implementar un marco de gestión de riesgos de IA (roles, evaluación de impacto, criterios de aceptación, monitoreo y documentación), alineado a estándares que permitan justificar decisiones y controles ante auditoría y supervisión, priorizando casos de uso según criticidad del sistema (National Institute of Standards and Technology, 2023; Financial Stability Board, 2024). De forma complementaria, resulta clave definir un “catálogo” institucional de herramientas autorizadas (y condiciones de uso) con mecanismos de gestión de terceros, reduciendo incertidumbre operativa y evitando adopciones informales (U.S. Department of the Treasury, 2024; Basel Committee on Banking Supervision, 2021).

En términos de seguridad y calidad, se recomienda integrar la IA dentro de un SDLC seguro: revisión humana obligatoria del código generado, pruebas automatizadas reforzadas, escaneo de vulnerabilidades, y políticas explícitas de no introducir secretos/datos sensibles en prompts; estas prácticas están alineadas con enfoques de “seguridad por diseño” y con guías que sistematizan tareas de construcción, verificación y respuesta para reducir vulnerabilidades (Souppaya et al., 2022; National Institute of Standards and Technology, 2023). Adicionalmente, es aconsejable adoptar evaluaciones internas periódicas (p. ej., ejercicios de red teaming o pruebas adversarias) para medir riesgos de fuga de información y generación de código inseguro antes de escalar casos de uso a entornos productivos (Financial Stability Board, 2024; Pearce et al., 2021).

Para sostener mejoras en eficiencia, seguridad y calidad, se recomienda una línea de acción centrada en capacidades: programas de capacitación por perfiles (desarrolladores, QA, líderes técnicos), guías de prompting y verificación, y métricas operativas (tiempo de ciclo, defectos post-release, hallazgos de seguridad) que permitan distinguir productividad “real” de productividad “percibida”. Esta recomendación se sustenta en que los beneficios de la IA tienden a maximizarse cuando el personal domina su uso y cuando la organización define

estándares compartidos de validación, evitando dependencia acrítica del modelo y fortaleciendo la resiliencia operativa del software bancario (OECD, 2019; Basel Committee on Banking Supervision, 2021; Souppaya et al., 2022).

## Discusión

Los hallazgos asociados al uso de tecnologías de inteligencia artificial en el desarrollo de software bancario muestran una adopción mayor en tareas directamente vinculadas con programación (escritura, completado y refactorización) que en actividades extendidas del ciclo de vida del software, como pruebas, documentación o revisión. Esta secuencia es consistente con la literatura sobre modelos de lenguaje entrenados en código, donde la propuesta de valor inicial se concentra en acelerar la producción de código y apoyar microtareas repetitivas que incrementan la fluidez del trabajo del desarrollador, antes de consolidarse en prácticas más reguladas y trazables del proceso completo (Chen et al., 2021; Jiang et al., 2024). En el ámbito bancario, además, la expansión hacia pruebas y aseguramiento suele depender de integración con herramientas existentes y de requisitos de auditoría, por lo que resulta esperable que la adopción sea menos homogénea fuera del núcleo de codificación (Financial Stability Board, 2024; Souppaya et al., 2022).

En relación con el nivel de conocimiento, competencias y adopción, se observa un patrón relevante: la comprensión de limitaciones y riesgos del uso de inteligencia artificial se sitúa por encima de la autopercepción de competencia para formular instrucciones eficaces. Esta diferencia sugiere una adopción con cautela: el personal reconoce que la inteligencia artificial puede equivocarse, alucinar o inducir dependencia, pero no siempre dispone de habilidades consolidadas para dirigirla y, sobre todo, para verificarla de modo sistemático en contextos críticos (National Institute of Standards and Technology, 2023; OECD, 2019). De forma coherente, los marcos de gobernanza y riesgo señalan que la capacidad institucional no

se limita a la disponibilidad de herramientas, sino a competencias operativas (criterio técnico, verificación, documentación) que permitan sostener calidad y cumplimiento en decisiones de ingeniería (U.S. Department of the Treasury, 2024; DeVellis, 2017).

Respecto de los beneficios percibidos, la evidencia del estudio distingue entre un efecto claro en eficiencia (reducción de tiempo) y un efecto más matizado en calidad. Este contraste coincide con reportes empíricos donde asistentes de programación se asocian a mejoras de productividad en tareas definidas, mientras que los resultados sobre calidad requieren condiciones adicionales de control, pruebas y revisión (Peng et al., 2023; Chen et al., 2021). En banca, la moderación de la mejora percibida en calidad resulta particularmente comprensible, dado que estudios de seguridad han advertido que las sugerencias de asistentes pueden introducir vulnerabilidades o patrones inseguros si se aceptan sin verificación robusta; por tanto, el valor en calidad parece depender del acoplamiento con prácticas de desarrollo seguro y aseguramiento continuo (Pearce et al., 2021; Souppaya et al., 2022).

El análisis de desafíos y estrategias refuerza una lectura socio-técnica: la principal fricción no se ubica únicamente en la herramienta, sino en la gobernanza (políticas, homologación, trazabilidad), la gestión de datos (confidencialidad, límites de uso) y la capacidad organizacional (capacitación, estandarización, integración con prácticas de seguridad). En ese sentido, las recomendaciones propuestas —marcos de gestión de riesgo de inteligencia artificial, catálogo de herramientas autorizadas, controles reforzados en revisión y pruebas, y capacitación por perfiles— se alinean con estándares orientados a reducir vulnerabilidades y sostener resiliencia operativa en infraestructuras críticas (Basel Committee on Banking Supervision, 2021; National Institute of Standards and Technology, 2023). No obstante, debe considerarse como limitación que los resultados cuantitativos se presentan como datos supuestos y que el diseño transversal basado en autoinforme restringe inferencias causales; por ello, futuras investigaciones deberían incorporar mediciones objetivas (defectos,

hallazgos de seguridad, tiempos de ciclo) y diseños comparativos por equipos o madurez de adopción (Creswell & Plano Clark, 2018).

## Conclusión

La incorporación de inteligencia artificial en el desarrollo de software dentro del sector bancario se manifiesta con mayor fuerza en tareas directamente asociadas con la programación, como la generación, completado y refactorización de código, mientras que su uso en actividades complementarias del ciclo de vida del software (pruebas, documentación y revisión) aparece menos extendido y más dependiente de condiciones organizacionales y de proceso.

En el plano de capacidades, se evidencia una adopción funcional acompañada por una preparación desigual: existe conciencia sobre riesgos y limitaciones de estas herramientas, pero no siempre se cuenta con destrezas consolidadas para guiarlas de manera eficaz y, sobre todo, para verificar sus salidas con criterios técnicos consistentes, lo que puede afectar la estandarización del uso entre equipos.

En términos de aportes percibidos al trabajo, los beneficios se expresan con mayor claridad en la eficiencia, particularmente en la reducción de tiempos para completar tareas de codificación y corrección, mientras que las mejoras de calidad se perciben de forma más condicionada, sugiriendo que la calidad depende menos de la herramienta en sí y más de cómo se integra con revisión humana, pruebas y prácticas de aseguramiento.

Al analizar las dificultades de integración, las barreras se concentran en restricciones de cumplimiento y seguridad, preocupaciones por confidencialidad de información y limitaciones internas relacionadas con capacitación, soporte y ausencia de lineamientos claros, lo que favorece un uso heterogéneo y, en algunos casos, informal, con riesgos potenciales para la trazabilidad y el control.

De cara a optimizar su aprovechamiento, el uso de inteligencia artificial en el desarrollo de software bancario requiere una estrategia integral que combine gobernanza y criterios de autorización, integración con prácticas de desarrollo seguro, capacitación diferenciada por roles y métricas operativas que permitan sostener mejoras reales en eficiencia sin comprometer seguridad ni calidad del software.

## Referencias bibliográficas

- Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d516.htm>
- Boateng, G. O., Neilands, T. B., Frongillo, E. A., Melgar-Quiñonez, H. R., & Young, S. L. (2018). Best practices for developing and validating scales for health, social, and behavioral research: A primer. *Frontiers in Public Health*, 6, 149. <https://doi.org/10.3389/fpubh.2018.00149>
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Caicedo-Basurto, R. L., Camacho-Medina, B. M., Quinga-Villa, C. A., Fonseca-Lombeida, A. F., & López-Freire, S. A. (2024). Análisis y beneficios de la educación en la era de la inteligencia artificial. *Journal of Economic and Social Science Research*, 4(4), 291–302. <https://doi.org/10.55813/gaea/jessr/v4/n4/148>
- Casanova-Villalba, C. I., Herrera-Sánchez, M. J., & Almeida-Blacio, J. H. (2025). Aplicaciones de inteligencia artificial en la auditoría financiera contemporánea. *Revista Científica Ciencia Y Método*, 3(2), 30-43. <https://doi.org/10.55813/gaea/rcym/v3/n2/3>
- Chen, M., Tworek, J., Jun, H., Yuan, Q., Pinto, H. P. de O., Kaplan, J., Edwards, H., Burda, Y., Joseph, N., Brockman, G., Ray, A., Puri, R., Krueger, G., Petrov, M., Khlaaf, H., Sastry, G., Mishkin, P., Chan, B., ... Zaremba, W. (2021). *Evaluating large language models trained on code* (arXiv:2107.03374). <https://arxiv.org/abs/2107.03374>
- Concha-Ramirez, J. A., & Navarrete-Ortiz, J. del C. (2023). Ética empresarial y responsabilidad social en la inteligencia artificial. *Revista Científica Ciencia Y Método*, 1(3), 31-44. <https://doi.org/10.55813/gaea/rcym/v1/n3/18>
- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE.
- DeVellis, R. F. (2017). *Scale development: Theory and applications* (4th ed.). SAGE.
- Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales* (Registro Oficial Suplemento No. 459, 26 de mayo de 2021). <https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-ley-organica-de-proteccion-de-datos>
- Erazo-Luzuriaga, A. F., Ramos-Secaira, F. M., Galarza-Sánchez, P. C., & Boné-Andrade, M.

- F. (2023). La inteligencia artificial aplicada a la optimización de programas informáticos. *Journal of Economic and Social Science Research*, 3(1), 48–63. <https://doi.org/10.55813/gaea/jessr/v3/n1/61>
- Financial Stability Board. (2024). *The financial stability implications of artificial intelligence*. <https://www.fsb.org/uploads/P14112024.pdf>
- Galarza-Sánchez, P. C., Boné-Andrade, M. F., & Pinargote-Bravo, V. J. (2023). Aplicaciones de inteligencia artificial generativa en la transformación digital empresarial. *Revista Científica Ciencia Y Método*, 1(1), 28-41. <https://doi.org/10.55813/gaea/rcym/v1/n1/8>
- García-Peña, V. R. (2023). Desarrollo y Uso de Aplicaciones Móviles en el Contexto Ecuatoriano. *Revista Científica Zambos*, 2(3), 1-15. <https://doi.org/10.69484/rcz/v2/n3/46>
- Hernández Sampieri, R., & Mendoza, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education.
- Herrera-Sánche, M. J., Casanova-Villalba, C. I., & Jacome-Vélez, T. G. (2024). Transformación digital en la banca y su efecto en la experiencia del cliente. *Revista Científica Ciencia Y Método*, 2(1), 1-13. <https://doi.org/10.55813/gaea/rcym/v2/n1/27>
- Israel, G. D. (1992). *Determining sample size* (Fact Sheet PEOD-6). University of Florida, IFAS Extension.
- Jiang, J., Wang, F., Shen, J., Kim, S., & Kim, S. (2024). *A survey on large language models for code generation* (arXiv:2406.00515). <https://arxiv.org/abs/2406.00515>
- Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th ed.). SAGE.
- Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel Psychology*, 28(4), 563–575. <https://doi.org/10.1111/j.1744-6570.1975.tb01393.x>
- Montalván-Vélez, C. L., Mogrovejo-Zambrano, J. N., Romero-Vitte, I. J., & Pinargote-Carrera, M. L. D. C. (2024). Introducción a la Inteligencia Artificial: Conceptos Básicos y Aplicaciones Cotidianas. *Journal of Economic and Social Science Research*, 4(1), 173–183. <https://doi.org/10.55813/gaea/jessr/v4/n1/93>
- National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research*. U.S. Department of Health, Education, and Welfare. <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html>
- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>
- OECD. (2019). *OECD Skills Outlook 2019: Thriving in a digital world*. [https://www.oecd.org/en/publications/2019/05/oecd-skills-outlook-2019\\_c8896fe0/full-report.html](https://www.oecd.org/en/publications/2019/05/oecd-skills-outlook-2019_c8896fe0/full-report.html)
- Pearce, H., Ahmad, B., Tan, B., Dolan-Gavitt, B., & Karri, R. (2021). *Asleep at the keyboard? Assessing the security of GitHub Copilot's code contributions* (arXiv:2108.09293). <https://arxiv.org/abs/2108.09293>

- Peng, S., Kalliamvakou, E., Cihon, P., & Demirer, M. (2023). *The impact of AI on developer productivity: Evidence from GitHub Copilot* (arXiv:2302.06590). arXiv. <https://arxiv.org/abs/2302.06590>
- Rodriguez-Vizuet, J. D., Viteri-Ojeda, J. C., & Villa-Feijóo, A. L. (2024). Adopción de tecnologías sostenibles en infraestructuras de tecnologías de la información. *Revista Científica Ciencia Y Método*, 2(1), 55-67. <https://doi.org/10.55813/gaea/rcym/v2/n1/31>
- Rodríguez, M. A. (2023). *Práctica regulatoria y el sector bancario* [Presentación]. Asociación de Bancos Privados del Ecuador (ASOBANCA). <https://www.sri.gob.ec/o/sri-portlet-biblioteca-alfresco-internet/descargar/89ef1cd9-0e2d-40cf-bda4-f80efb08c6f0/05%20SRI-Presentaci%C3%B3n%20Oficial%20-%20Pr%C3%A1ctica%20Regulatoria%20-%20Marco%20Rodr%C3%ADguez%20ASOBANCA.pdf>
- Souppaya, M., Scarfone, K., & Dodson, D. (2022). *Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities* (NIST SP 800-218). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-218>
- U.S. Department of the Treasury. (2024). *Uses, opportunities, and risks of artificial intelligence in financial services*. <https://home.treasury.gov/system/files/136/Artificial-Intelligence-in-Financial-Services.pdf>
- Vargas, F., & Munte, A. (2025). *Artificial intelligence framework for the Inter-American Development Group*. Inter-American Development Bank. <https://doi.org/10.18235/0013377>