Marco de Ciberseguridad Cuánto-Resistente para Protección de Datos Ambientales en la Amazonía usando IA

CONVOCATORIA COLOMBIA INTELIGENTE: CIENCIA Y TECNOLOGÍAS CUÁNTICAS E INTELIGENCIA ARTIFICIAL PARA LOS TERRITORIOS | Convocatoria 966

COTECMAR - December 2025

Tabla de Contenido

1. Generalidades del Proyecto

Título: Marco de Ciberseguridad Cuánto-Resistente para Protección de Datos Ambientales en la Amazonía usando IA

Convocatoria: CONVOCATORIA COLOMBIA INTELIGENTE: CIENCIA Y TECNOLOGÍAS CUÁNTICAS E INTELIGENCIA ARTIFICIAL PARA LOS TERRITORIOS | Convocatoria 966

Entidad/Persona: COTECMAR

Línea Temática: Colombia Inteligente, Ciencia Cuántica, Tecnologías Cuánticas, Inteligencia Artificial, Territorios, CTeI, Soluciones Disruptivas, Convocatoria 966

- **Descripción:** Los ecosistemas amazónicos generan datos ambientales críticos vulnerables a amenazas cibernéticas, incluidas las futuras provenientes de computadores cuánticos. Este proyecto desarrolla un marco de seguridad con IA para monitoreo y detección de anomalías, integrando esquemas de criptografía post-cuántica (PQC). Se pilotará en una comunidad amazónica para validar la protección de datos de biodiversidad y deforestación, buscando establecer un estándar avanzado de ciberseguridad para la gestión sostenible de recursos.

- **Palabras Clave:** Criptografía Post-Cuántica, Inteligencia Artificial, Seguridad de Datos, Amazonía Colombiana, Gestión Ambiental, Tecnologías Cuánticas

2. Resumen Ejecutivo

La protección de datos ambientales críticos en la Amazonía enfrenta una vulnerabilidad creciente frente a ciberamenazas actuales y futuras, especialmente con la inminente llegada de la computación cuántica, lo cual se agrava por la limitada infraestructura en regiones remotas. Este proyecto propone una solución innovadora: el desarrollo y validación de un marco integral de ciberseguridad cuánto-resistente, impulsado por Inteligencia Artificial, diseñado para salvaguardar esta información vital. Nuestra visión es cerrar las brechas tecnológicas existentes y asegurar la integridad de los datos esenciales para la gestión sostenible de los ecosistemas amazónicos.

Para lograrlo, nuestro plan se articula en torno a objetivos claros: primero, diseñar e implementar módulos avanzados de criptografía post-cuántica (PQC) e Inteligencia Artificial (IA) para la detección de anomalías y monitoreo en tiempo real. Seguidamente, desplegaremos un prototipo funcional de este marco en un entorno piloto real dentro de una comunidad amazónica. Finalmente, evaluaremos su efectividad y generaremos recomendaciones para su escalamiento y adopción ética. La ejecución se realizará mediante una metodología híbrida Ágil e Iterativa, complementada con las fases de validación del Modelo en V, garantizando flexibilidad y rigor en cada etapa.

Los resultados de este proyecto son transformadores. Entregaremos módulos PQC e IA validados y un prototipo funcional de ciberseguridad desplegado en la Amazonía, junto con un informe de evaluación y un

protocolo de adopción ética y sostenible. El impacto esperado es multifacético: posicionaremos a Colombia como líder en IA y ciberseguridad cuántica, impulsaremos la bioeconomía regional y generaremos nuevas oportunidades de negocio. Socialmente, empoderaremos a las comunidades locales con tecnología de punta y desarrollaremos talento especializado, mientras que ambientalmente, fortaleceremos la capacidad de monitoreo y gestión sostenible del ecosistema amazónico.

En síntesis, este proyecto no solo resguarda el patrimonio ambiental de la Amazonía frente a las amenazas cibernéticas del futuro, sino que también sienta las bases para un desarrollo regional resiliente, tecnológicamente avanzado y socialmente inclusivo.

3. Planteamiento del Problema y Justificación

La era digital ha transformado la interacción con el mundo, generando volúmenes masivos de datos cuya protección es una prioridad crítica, especialmente para la información ambiental sensible vital para la gestión sostenible de ecosistemas como la Amazonía. Sin embargo, este contexto se ve amenazado por un panorama de ciberseguridad en constante evolución, donde la inminente llegada de computadores cuánticos representa un desafío significativo para los esquemas criptográficos actuales, exacerbado por la limitada infraestructura de ciberseguridad robusta en regiones remotas. La vulnerabilidad intrínseca de los datos ambientales críticos en la Amazonía a las amenazas cibernéticas actuales y futuras es, por tanto, una preocupación apremiante que pone en riesgo la integridad de la biodiversidad y los esfuerzos de conservación.

Como la literatura especializada indica (Reyes Rosado, 2018; Eras Chancay, 2023), la protección de datos exige soluciones avanzadas, impulsando el desarrollo de la Criptografía Post-Cuántica (PQC) y la aplicación de la Inteligencia Artificial (IA) en ciberseguridad. A pesar de los avances significativos en PQC y IA de forma individual (NIST Post-Quantum Cryptography Standardization, n.d.; Saarinen, 2020; Li et al., 2024), la Sección 4.4 del marco teórico resalta una brecha fundamental: la escasez de marcos de ciberseguridad que combinen explícitamente PQC e IA, diseñados y validados para la protección de datos ambientales críticos en entornos con infraestructura limitada y condiciones desafiantes, como la Amazonía. Las consideraciones sobre el consumo de recursos de los algoritmos PQC en dispositivos de borde (Señor Sánchez, n.d.) y la necesidad de modelos de IA eficientes para la detección de anomalías en tiempo real son retos críticos que las soluciones actuales no abordan de manera integrada.

Este proyecto surge como la respuesta directa y necesaria para cerrar esta brecha tecnológica y de conocimiento. Mediante el desarrollo de un marco integral de ciberseguridad cuánto-resistente, impulsado por Inteligencia Artificial, se proporcionará una solución innovadora y adaptada para la protección de datos ambientales críticos en la Amazonía. La integración de esquemas de criptografía post-cuántica y modelos de IA para el monitoreo en tiempo real y la detección de anomalías abordará directamente las limitaciones de los enfoques actuales, ofreciendo una defensa robusta contra las amenazas cibernéticas presentes y futuras, incluyendo los ataques cuánticos.

La relevancia estratégica de este proyecto es innegable, dada la urgencia de proteger la información vital para la gestión sostenible de los ecosistemas amazónicos. Contribuye directamente al cierre de brechas tecnológicas a nivel territorial, empoderando a las comunidades locales con herramientas avanzadas para la

toma de decisiones ambientales. Al establecer un estándar avanzado de ciberseguridad adaptado a las necesidades de la Amazonía, este proyecto no solo salvaguarda datos cruciales sobre biodiversidad y deforestación, sino que también fomenta el desarrollo de capacidades locales y posiciona a la región a la vanguardia de la ciberseguridad ambiental cuántico-resistente, asegurando la integridad de la información para futuras generaciones.

4. Marco Teórico y Estado del Arte

4.1. Introducción al Dominio

La era digital ha transformado la forma en que interactuamos con el mundo, generando volúmenes masivos de datos. En este contexto, la protección de la información se ha vuelto una prioridad crítica, especialmente para datos sensibles como los ambientales, vitales para la gestión sostenible de ecosistemas como la Amazonía. Sin embargo, el panorama de amenazas cibernéticas evoluciona constantemente, y la inminente llegada de una prioridad crítica, especialmente para datos sensibles como los ambientales, vitales para la gestión sostenible de ecosistemas como la Amazonía. Sin embargo, el panorama de amenazas cibernéticas evoluciona constantemente, y la inminente llegada de computadores cuánticos representa un desafío significativo para los esquemas criptográficos actuales (Reyes Rosado, 2018). Esta realidad ha impulsado el desarrollo de la Criptografía Post-Cuántica (PQC), una rama de la criptografía que busca diseñar algoritmos resistentes a los ataques de computadores cuánticos.

Paralelamente, la Inteligencia Artificial (IA) ha emergido como una herramienta poderosa en el ámbito de la ciberseguridad, ofreciendo capacidades avanzadas para la detección de anomalías, el análisis de comportamiento y la automatización de respuestas ante amenazas (Eras Chancay, 2023). La capacidad de la IA para procesar grandes conjuntos de datos e identificar patrones complejos la convierte en un aliado invaluable para fortalecer las defensas cibernéticas. La convergencia de PQC e IA es, por tanto, fundamental para construir marcos de ciberseguridad robustos y adaptativos, capaces de salvaguardar datos críticos frente a un espectro amplio y en constante evolución de amenazas.

4.2. Revisión de la Literatura (Literature Review)

La investigación en criptografía post-cuántica ha sido impulsada significativamente por el proceso de estandarización del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. (NIST Post-Quantum Cryptography Standardization, n.d.). Este proceso ha evaluado diversos candidatos algorítmicos resistentes a ataques cuánticos, con el objetivo de seleccionar estándares globales. Saarinen (2020) analizó los requisitos energéticos de los candidatos a estándares PQC en sistemas móviles, subrayando los desafíos de implementación en entornos con recursos limitados, un aspecto crucial para el despliegue en la Amazonía. Recientemente, el NIST ha avanzado en la estandarización, seleccionando algoritmos como HQC para contrarrestar amenazas cuánticas (NIST advances post-quantum cryptography standardization, n.d.). Sowa et al. (2024) también destacaron la urgencia de la adopción de PQC y la necesidad de identificar vías de migración, dada la amenaza que representan los futuros ordenadores cuánticos para los datos cifrados actualmente.

En el campo de la inteligencia artificial aplicada a la ciberseguridad, la literatura reciente resalta su papel transformador. Eras Chancay (2023) proporciona una visión general de cómo la IA ha mejorado la detección de amenazas y la automatización de respuestas, al tiempo que introduce nuevos desafíos, como la creación de ataques más sofisticados por parte de los adversarios. La detección de anomalías, un pilar de la ciberseguridad, ha visto avances significativos con la IA. Li et al. (2024) exploraron el uso de Grandes Modelos de Lenguaje (LLMs) para la detección de anomalías en datos tabulares, demostrando su potencial como detectores de anomalías a nivel de lotes. De manera similar, King et al. (2025) investigaron el aprendizaje contextual para la detección de anomalías en datos tabulares a gran escala, un desafío persistente en dominios como la ciberseguridad y las finanzas. La IA también se aplica directamente a la protección contra amenazas específicas, como el phishing, donde León Naranjo et al. (2025) analizaron el impacto de la IA en la detección y prevención de este delito cibernético.

La integración de IA y PQC en marcos de ciberseguridad es un área emergente. Calle-Méndez y Barriga-Andrade (2025) realizaron una revisión sistemática sobre las amenazas de seguridad asociadas con la integración de IA en sistemas de información, destacando la necesidad de criptografía avanzada y detección de anomalías para mitigar riesgos. Estos autores enfatizan cómo la automatización y la complejidad de la IA amplifican el panorama de riesgos, afectando la integridad, confidencialidad y disponibilidad de los sistemas. Damiano (n.d.) en su análisis sobre la adopción de PQC e IA en ciberseguridad, subraya cómo la combinación de estas tecnologías puede crear un marco seguro capaz de proteger contra una amplia gama de amenazas cibernéticas.

4.3. Tecnologías y Enfoques Actuales (State of the Art)

El estado del arte en ciberseguridad cuánto-resistente y protección de datos ambientales se caracteriza por la evolución rápida en dos frentes principales: la criptografía post-cuántica y la aplicación de la inteligencia artificial.

En **Criptografía Post-Cuántica (PQC)**, el enfoque dominante se centra en el desarrollo y la estandarización de algoritmos que son seguros contra ataques de computadoras cuánticas. El proceso del NIST ha sido fundamental, seleccionando algoritmos basados en retículos, códigos, hash y polinomios multivariados. Ejemplos incluyen los algoritmos CRYSTALS-Dilithium y CRYSTALS-Kyber. La implementación de estos algoritmos en entornos con recursos limitados, como los dispositivos IoT en la Amazonía, es una consideración clave, como lo abordó Señor Sánchez (n.d.) en su tesis doctoral, demostrando la viabilidad de NTRU en plataformas de IoT con optimizaciones. La tendencia es hacia la adopción gradual de estos nuevos estándares en infraestructuras críticas.

En cuanto a la **Inteligencia Artificial para Ciberseguridad**, las tecnologías actuales aprovechan el aprendizaje automático (Machine Learning) y el aprendizaje profundo (Deep Learning) para tareas como la detección de intrusiones, el análisis de malware, la identificación de patrones de comportamiento anómalos y la respuesta automatizada a incidentes. Los sistemas basados en IA pueden aprender de grandes volúmenes de datos de red y de comportamiento de usuarios para identificar desviaciones que podrían indicar un ataque. Tendencias recientes incluyen el uso de LLMs para la detección de anomalías en datos complejos, como los tabulares (Li et al., 2024; King et al., 2025), y el desarrollo de defensas adaptativas impulsadas por IA contra amenazas como el phishing (Meguro & Chong, 2025). La IA también se utiliza para mejorar la gestión de riesgos cibernéticos en entornos complejos como las ciudades inteligentes y el IoT (Tito Chura, 2023).

La **integración de PQC e IA** representa la frontera de la ciberseguridad. Los enfoques actuales buscan crear sistemas híbridos que combinan la robustez criptográfica de PQC con las capacidades predictivas y adaptativas de la IA. Aunque aún incipiente, esta integración se visualiza como un marco de ciberseguridad más resiliente, capaz de anticipar y mitigar tanto las amenazas clásicas como las cuánticas. Los marcos emergentes proponen utilizar la IA para optimizar el rendimiento de los algoritmos PQC, gestionar claves de manera segura y detectar ataques que podrían explotar debilidades en cualquier capa del sistema.

4.4. Brechas de Conocimiento y Oportunidades (Knowledge Gaps & Opportunities)

A pesar de los avances significativos en criptografía post-cuántica y la aplicación de la inteligencia artificial en ciberseguridad, existen brechas notables en la integración y aplicación de estas tecnologías en contextos específicos. Una limitación fundamental es la escasez de marcos de ciberseguridad que combinen explícitamente PQC e IA, diseñados y validados para la protección de datos ambientales críticos. La mayoría de la investigación se centra en la PQC como una solución criptográfica independiente o en la IA para la ciberseguridad en dominios más generales, sin una convergencia profunda que aborde las particularidades de los datos ambientales sensibles y los entornos remotos.

Además, la implementación práctica de estas soluciones en regiones con infraestructura limitada y condiciones desafiantes, como la Amazonía, presenta retos únicos que no han sido suficientemente explorados. Las consideraciones sobre el consumo de recursos de los algoritmos PQC en dispositivos de borde (Saarinen, 2020; Señor Sánchez, n.d.) y la necesidad de modelos de IA eficientes para la detección de anomalías en tiempo real son críticas y requieren investigación aplicada. El proyecto propuesto aborda directamente estas brechas al desarrollar un marco de ciberseguridad cuánto-resistente con IA específicamente para la protección de datos ambientales en la Amazonía, validando su eficacia en un entorno real y sentando las bases para un estándar avanzado de ciberseguridad adaptado a las necesidades de la gestión sostenible de recursos.

5. Objetivos

Objetivo General

Desarrollar y validar un marco integral de ciberseguridad cuánto-resistente, impulsado por Inteligencia Artificial, para la protección de datos ambientales críticos en la Amazonía, contribuyendo al desarrollo regional y al cierre de brechas tecnológicas en la gestión sostenible de los ecosistemas.

Objetivos Específicos

1. **Objetivo:** Diseñar e implementar módulos de criptografía post-cuántica (PQC) e Inteligencia Artificial (IA) para la protección de datos ambientales.

    - **Específico (S):** Desarrollo de componentes técnicos clave del marco (algoritmos PQC para cifrado/firmas, modelos de IA para detección de anomalías y monitoreo).

- **Medible (M):** Métricas: 1) Integrar y validar al menos 2 algoritmos PQC del NIST con una latencia de cifrado/descifrado no superior al 20% de los algoritmos clásicos equivalentes. 2) Desarrollar y entrenar un modelo de IA para la detección de anomalías en flujos de datos ambientales, logrando una precisión (accuracy) y F1-score superior al 90% en conjuntos de datos de prueba específicos.

- **Alcanzable (A):** Basado en el estado del arte de PQC e IA (Sección 4.3 Tecnologías y Enfoques Actuales) y la experticia del equipo (TALENTO).

- **Relevante (R):** Establece la base tecnológica del proyecto para enfrentar amenazas cuánticas y mejorar la resiliencia cibernética.

- **Plazo (T):** Cronograma: Completado para el mes 12 del proyecto.

2. **Objetivo:** Implementar y desplegar un prototipo funcional del marco de ciberseguridad en un entorno piloto real de una comunidad amazónica.

- **Específico (S):** Instalación, configuración y puesta en marcha del marco desarrollado, incluyendo la infraestructura de hardware y software necesaria en un contexto territorial específico.

- **Medible (M):** Métricas: 1) Desplegar un prototipo funcional del sistema en una comunidad amazónica específica, logrando una cobertura del 80% de los puntos de recolección de datos ambientales definidos. 2) Mantener una disponibilidad operativa del sistema del 95% durante el período de pilotaje inicial de tres meses. 3) Asegurar la protección criptográfica del 100% de los datos ambientales transmitidos por el prototipo durante el piloto, conforme a los algoritmos PQC integrados.

- **Alcanzable (A):** Involucra la alianza con una Organización Local – Regional (DIRIGIDO_A) y contempla las salidas de campo y adecuaciones de infraestructura (PRODUCTOS y FINANCIACIÓN). TRL esperado 6.

- **Relevante (R):** Permite la validación de la tecnología en un entorno relevante y el abordaje del ENFOQUE TERRITORIAL.

- **Plazo (T):** Cronograma: Finalizado el despliegue y validación inicial para el mes 22 del proyecto.

3. **Objetivo:** Evaluar la efectividad del marco implementado y desarrollar recomendaciones para su escalamiento y adopción ética y sostenible.

- **Específico (S):** Realizar un análisis de rendimiento del sistema, su impacto en la seguridad de datos, y el nivel de apropiación por parte de los usuarios locales.

- **Medible (M):** Métricas: 1) Registrar una reducción del 98% en la detección de intrusiones no autorizadas o manipulaciones de datos durante el período de validación comparado con el monitoreo previo. 2) Documentar al menos 1 protocolo de buenas prácticas o guía de implementación para la adopción ética y sostenible del sistema, basándose en la retroalimentación de los usuarios y expertos. 3) Capacitar al menos a 30 miembros de la comunidad local y técnicos, con una tasa de satisfacción superior al 85% en las formaciones impartidas.

- **Alcanzable (A):** A través de monitoreo continuo, talleres (PRODUCTOS) y la participación activa de la alianza local. TRL esperado 7-8.

- **Relevante (R):** Contribuye al ENFOQUE DIFERENCIAL y asegura la transferibilidad de los resultados, cumpliendo con los COMPONENTES OBLIGATORIOS sobre IA ética.

- **Plazo (T):** Cronograma: Concluido el análisis y la formulación de recomendaciones para el mes 30 del proyecto.

6. Metodología Propuesta

Framework Seleccionado: Metodología Híbrida: Ágil (Iterativa) con Fases de Validación del Modelo en V.

La naturaleza de I+D del proyecto, que abarca desde el TRL 3 hasta el 8, la integración de componentes de hardware y software de tecnologías emergentes (IA y criptografía cuántica), y su implementación en un entorno complejo como la Amazonía, requiere un enfoque metodológico flexible pero riguroso. La adopción de una Metodología Híbrida, que combina la adaptabilidad y retroalimentación constante de los enfoques Ágiles (Scrum/Kanban) con la rigurosidad en la verificación y validación del Modelo en V, permitirá manejar la evolución de requisitos, asegurar la calidad en cada iteración y validar de forma exhaustiva el prototipo en entornos reales, cumpliendo con los objetivos de desarrollo tecnológico y despliegue territorial.

Fases Principales de la Metodología:

- **Fase 1: Planificación y Diseño Conceptual (Orientado al V-Model)** - Establecimiento de requisitos funcionales y no funcionales, definición de la arquitectura del sistema, selección de tecnologías clave (PQC, IA), y planificación de las primeras iteraciones de desarrollo.

- **Fase 2: Desarrollo Iterativo de Componentes (Agile Sprints)** - Implementación, pruebas unitarias y de integración de los módulos de criptografía post-cuántica y los modelos de IA en ciclos cortos y adaptativos, con retroalimentación continua para optimizar el rendimiento y la funcionalidad.

- **Fase 3: Integración y Despliegue en Entorno Relevante (V-Model Validation)** - Ensamblaje del prototipo funcional, configuración para el entorno piloto en la comunidad amazónica, despliegue en campo y realización de pruebas de sistema y aceptación en condiciones operativas reales.

- **Fase 4: Verificación, Optimización y Transferencia (V-Model & Agile Refinement)** - Evaluación exhaustiva del rendimiento del marco, análisis de la efectividad de la ciberseguridad y la detección de anomalías, optimización basada en la retroalimentación del piloto, y documentación para el escalamiento y la apropiación ética y sostenible.

7. Plan de Ejecución y Gestión

Cronograma de Actividades

7.1. Cronograma de Actividades

Fase	Actividad / Hito Clave	Entregable Principal	Duración Estimada (Semanas)
Fase 1: Planificación y Diseño Conceptual	*Establecimiento de requisitos funcionales y no funcionales, definición de la arquitectura del sistema, selección de tecnologías clave (PQC, IA), y planificación de las primeras iteraciones de desarrollo.*		**16**
	1.1. Levantamiento y análisis de requisitos funcionales y no funcionales del sistema PQC-IA.	Documento de Requisitos del Sistema (DRS)	4
	1.2. Diseño arquitectónico del marco de ciberseguridad PQC-IA y selección de algoritmos clave.	Documento de Arquitectura del Sistema (DAS) y Selección de Algoritmos PQC/IA	6
	1.3. Estudio de viabilidad e infraestructura para el entorno piloto en la Amazonía.	Informe de Viabilidad y Requisitos de Infraestructura del Piloto	4
	1.4. Planificación detallada del proyecto y definición de sprints Agile iniciales.	Plan de Proyecto Detallado y Backlog de Sprints Inicial	2
Fase 2: Desarrollo Iterativo de Componentes	*Implementación, pruebas unitarias y de integración de los módulos de criptografía post-cuántica y los modelos de IA en ciclos cortos y adaptativos, con retroalimentación continua para optimizar el rendimiento y la funcionalidad.*		**40**
	2.1. Desarrollo e implementación de módulos de criptografía post-cuántica (PQC).	Módulos PQC implementados y pruebas unitarias	10
	2.2. Desarrollo y entrenamiento de modelos de IA para detección de anomalías y monitoreo ambiental.	Modelos de IA entrenados y validados en laboratorio	12
	2.3. Integración y pruebas del sistema PQC-IA en entorno de laboratorio.	Prototipo funcional de laboratorio del marco PQC-IA (TRL 5)	8
	2.4. Adquisición y pre-configuración de hardware y software para el despliegue piloto.	Inventario de hardware/software adquirido y pre-configurado	10
Fase 3: Integración y Despliegue en Entorno Relevante	*Ensamblaje del prototipo funcional, configuración para el entorno piloto en la comunidad amazónica, despliegue en campo y realización de pruebas de sistema y aceptación en condiciones operativas reales.*		**40**
	3.1. Adaptación y configuración del prototipo para el entorno específico de la comunidad amazónica.	Plan de Adaptación y Configuración del Prototipo para el Piloto	8
	3.2. Despliegue e instalación del prototipo del marco de ciberseguridad en la comunidad piloto.	Prototipo desplegado y operativo en la comunidad (TRL 6)	10
	3.3. Ejecución del período de pilotaje y monitoreo inicial del sistema.	Informes de Monitoreo de Disponibilidad y Protección de Datos del Piloto	12
	3.4. Capacitación a usuarios locales y personal técnico sobre el uso y mantenimiento del sistema.	Materiales de Capacitación y Listado de Participantes Capacitados	10

Fase 4: Verificación, Optimización y Transferencia	*Evaluación exhaustiva del rendimiento del marco, análisis de la efectividad de la ciberseguridad y la detección de anomalías, optimización basada en la retroalimentación del piloto, y documentación para el escalamiento y la apropiación ética y sostenible.*		**24**
	4.1. Evaluación integral de rendimiento, seguridad y usabilidad del marco implementado.	Informe de Evaluación de Rendimiento y Seguridad del Sistema	8
	4.2. Desarrollo de protocolos de buenas prácticas y guías para la adopción ética y sostenible.	Protocolo de Buenas Prácticas y Guía de Adopción Ética y Sostenible	6
	4.3. Talleres de apropiación social, divulgación de resultados y transferencia de conocimiento.	Informe de Talleres de Apropiación Social y Materiales de Divulgación	6
	4.4. Preparación de informes finales, publicaciones científicas y solicitudes de propiedad intelectual.	Informe Final del Proyecto, Artículos Científicos (borrador) y Solicitudes de PI (borrador)	4

Matriz de Riesgos

7.2. Matriz de Riesgos

#	Riesgo Potencial	Probabilidad	Impacto	Estrategia de Mitigación
1	**Rendimiento de Algoritmos PQC en Entornos Restringidos** *Relacionado con: Fase 2 (2.1, 2.3) y Fase 3 (3.1, 3.2)*	Medium	High	Realizar pruebas de rendimiento exhaustivas en emuladores y hardware de bajo costo durante la Fase 2.3. Priorizar algoritmos PQC con perfiles de rendimiento conocidos y optimizables. Desarrollar una capa de abstracción de hardware que permita intercambiar implementaciones PQC si es necesario. Considerar estrategias de cifrado híbrido si la PQC pura es demasiado costosa.
2	**Calidad y Volumen de Datos para el Entrenamiento de IA** *Relacionado con: Fase 2 (2.2) y Fase 3 (3.3)*	Medium	Medium	Establecer protocolos estrictos para la recolección de datos en la Fase 1.1 y 3.3. Implementar técnicas de aumento de datos (data augmentation) y generación sintética (si es viable y ético) para complementar conjuntos de datos escasos. Utilizar modelos de IA pre-entrenados o técnicas de transferencia de aprendizaje (transfer learning) que requieran menos datos específicos. Colaborar estrechamente con expertos ambientales para validar la calidad y relevancia de los datos.

3	**Retrasos en la Preparación del Sitio Piloto y Permisos Locales** *Relacionado con: Fase 1 (1.3) y Fase 3 (3.1, 3.2)*	High	High	Iniciar la gestión de permisos y la coordinación logística con la Organización Local – Regional desde la Fase 1.3. Establecer un equipo dedicado a la gestión de campo y relaciones comunitarias. Desarrollar un plan de contingencia para la infraestructura (ej., uso de energía solar portátil, conectividad satelital de respaldo). Realizar visitas de campo previas detalladas para una planificación más precisa.
4	**Evolución Acelerada de Amenazas Cibernéticas y Computación Cuántica** *Relacionado con: Fase 1 (1.2) y Fase 4 (4.1)*	Medium	High	

8. Resultados e Impactos Esperados

8.1. Resultados Esperados (Entregables)

- **Módulos de Criptografía Post-Cuántica (PQC) e IA Desarrollados y Validados:** Componentes de software funcionales que integran algoritmos PQC para cifrado y firmas digitales, junto con modelos de Inteligencia Artificial para la detección de anomalías y monitoreo de datos ambientales, validados en un entorno de laboratorio. (Corresponde al Objetivo Específico 1)

- **Prototipo Funcional del Marco de Ciberseguridad Desplegado en Entorno Amazónico:** Un sistema integral de ciberseguridad cuánto-resistente, operativo y configurado en una comunidad amazónica específica, protegiendo puntos de recolección de datos ambientales críticos. (Corresponde al Objetivo Específico 2)

- **Informe de Evaluación y Protocolo de Adopción Ética y Sostenible:** Un documento exhaustivo que detalla el rendimiento, la seguridad y la usabilidad del marco de ciberseguridad en el entorno piloto, incluyendo un protocolo de buenas prácticas y una guía para su escalamiento y adopción ética y sostenible, así como materiales de capacitación para usuarios locales. (Corresponde al Objetivo Específico 3)

8.2. Impactos Esperados

- **Impacto Técnico/Científico:**

El proyecto posicionará a Colombia como un referente en la investigación y desarrollo de IA y ciberseguridad cuánto-resistente, especialmente en la integración de estas tecnologías para la protección de datos ambientales sensibles. Se avanzará significativamente el estado del arte en la implementación práctica de algoritmos PQC y modelos de IA para la detección proactiva de amenazas, generando nuevo conocimiento y metodologías aplicables a otros sectores críticos. La consecución de un TRL 7-8 del marco demuestra una

madurez tecnológica lista para la transferencia y el escalamiento.

- **Impacto Económico:**

La protección robusta de datos ambientales estratégicos en la Amazonía fomentará la confianza y la inversión en iniciativas de bioeconomía y gestión sostenible de recursos. El desarrollo del marco creará potencial para la formulación de nuevos servicios y productos de ciberseguridad especializados, abriendo nichos de mercado para la empresa aliada y fortaleciendo la competitividad del sector tecnológico nacional. Además, la optimización en la gestión de datos reducirá costos asociados a la pérdida o manipulación de información crítica, mejorando la eficiencia en la toma de decisiones por parte de entes territoriales y comunidades.

- **Impacto Social:**

El proyecto contribuirá al cierre de brechas tecnológicas y al empoderamiento de comunidades amazónicas, proporcionándoles herramientas de vanguardia para la autogestión y protección de sus recursos naturales. Se generarán oportunidades significativas para el desarrollo de talento local, mediante la formación y capacitación de al menos 30 miembros de la comunidad y técnicos en IA y ciberseguridad. Esto no solo mejorará la empleabilidad calificada en la región, sino que también promoverá la inclusión social y la participación activa de las poblaciones rurales en la construcción de soluciones tecnológicas que responden a sus necesidades reales, bajo un enfoque diferencial y ético.

- **Impacto Ambiental:**

Al asegurar la integridad, confidencialidad y disponibilidad de los datos sobre biodiversidad, deforestación y clima, el marco de ciberseguridad fortalecerá directamente la capacidad de monitoreo, conservación y gestión sostenible del ecosistema amazónico. Una información ambiental más segura y confiable permitirá a las autoridades y comunidades implementar políticas de conservación más efectivas, tomar decisiones informadas para la adaptación al cambio climático y combatir actividades ilícitas. Esto reducirá la vulnerabilidad de programas de sostenibilidad e investigaciones críticas frente a la manipulación o pérdida de datos, salvaguardando el patrimonio natural de la región a largo plazo.

9. Referencias Bibliográficas

- Buelvas Castellar, S. J. (2020). *Algoritmos para resolver el problema de rango mínimo para matrices 3-dimensionales y su aplicación a la seguridad de criptosistemas basados en polinomios cúbicos*. [Tesis de maestría, Universidad de Cartagena].

- Calle-Méndez, J. L., & Barriga-Andrade, J. J. (2025). Amenazas de seguridad asociadas con la integración de inteligencia artificial en sistemas de información: Revisión sistemática. (Manuscrito no publicado).

- Consultora Ambiental. (2025, 24 de abril). *Ciberseguridad y Sostenibilidad: ¿cómo proteger los datos sin comprometer el planeta?*. https://consultoraambiental.mx/2025/04/24/ciberseguridad-y-sostenibilidad-como-proteger-los-datos-sin-comprometer-el-planeta/

- Damiano, G. (n.d.). *Navigating the Future: The Adoption of PQC and AI in Cybersecurity*. LinkedIn. Recuperado de https://www.linkedin.com/pulse/navigating-future-adoption-pqc-ai-cybersecurity-giuseppe-damiano-v0eqf

- DPL News. (n.d.). *Rescatar el Amazonas: tecnologías clave para proteger los pulmones del mundo*. Recuperado de https://dplnews.com/rescatar-el-amazonas-tecnologias-clave-para-proteger-los-pulmones-del-mundo/

- Eras Chancay, S. X. (2023). *Ciberseguridad en la Era de la Inteligencia Artificial*. [Tesis de grado, Universidad de Guayaquil].

- Enigma Security. (n.d.). *El Banco Interamericano de Desarrollo y Francia invertirán 324 ...*. Recuperado de https://enigmasecurity.cl/noticias-7430/

- King, S., Zhang, Z., Yu, R., Coskun, B., Ding, W., & Cui, Q. (2025). *Contextual Learning for Anomaly Detection in Tabular Data*. arXiv.

- León Naranjo, J., Oleas Morán, M. M., & Pimentel Salazar, K. Z. (2025). El papel de la inteligencia artificial en la detección del phishing: un enfoque descriptivo sobre su impacto en la ciberseguridad. (Manuscrito no publicado).

- Li, A., Zhao, Y., Qiu, C., Kloft, M., Smyth, P., Rudolph, M., & Mandt, S. (2024). *Anomaly Detection of Tabular Data Using LLMs*. arXiv.

- Meguro, R., & Chong, N. S. T. (2025). *AdaPhish: AI-Powered Adaptive Defense and Education Resource Against Deceptive Emails*. arXiv.

- NIST advances post-quantum cryptography standardization, selects HQC algorithm to counter quantum threats. (n.d.). *Industrial Cyber*. Recuperado de https://industrialcyber.co/nist/nist-advances-post-quantum-cryptography-standardization-selects-hqc-algorithm-to-counter-quantum-threats/

- NIST Post-Quantum Cryptography Standardization. (n.d.). *National Institute of Standards and Technology*. Recuperado de https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

- Reyes Rosado, Á. R. (2018). *Estado de la criptografía post-cuántica y simulaciones de algoritmos post-cuánticos*. [Tesis de maestría, Universidad de Valladolid].

- Saarinen, M.-J. O. (2020). *Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards*. arXiv.

- Sánchez Botello, M., Quimis Moreira, M. A., & Macías Arias, E. J. (2024). Tendencias de ciberseguridad en base de datos relacionales: una revisión sistemática de literatura. (Manuscrito no publicado).

- Señor Sánchez, J. (n.d.). *Analysis and Evaluation of the Impact of Post-Quantum Cryptography at the Edge of IoT*. [Tesis doctoral, Universitat Politècnica de València].

● Sowa, J., Hoang, B., Yeluru, A., Qie, S., Nikolich, A., Iyer, R., & Cao, P. (2024). *Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways*. arXiv.

● Tito Chura, V. F. (2023). CIBERSEGURIDAD Y SU RELACIÓN CON EL RIESGO CIBERNÉTICO, CIUDADES INTELIGENTES, EL INTERNET DE LAS COSAS (IOT) Y LA INTELIGENCIA ARTIFICIAL. (Manuscrito no publicado).