Ibagué, de

Señores

COMITÉ DE INVESTIGACION

PROGRAMA DE INGENIERÍA DE SISTEMAS

UNIVERSIDAD COOPERATIVA DE COLOMBIA

Ciudad

Asunto: Solicitud Modalidad de grado en …………...

Cordial saludo:

Respetados integrantes del comité, siendo estudiante de 7 semestre de la facultad de Ingeniería de Sistemas, solicito la revisión del proyecto de grado titulado: **Implementación y despliegue web de un sistema de detección de anomalías para entornos IoT mediante la metodología MLOps** en la modalidad de **Proyecto de Investigación** De acuerdo a lo estipulado en el reglamento de la institución, dicho trabajo está clasificado dentro de la línea **Seguridad Informática y Sistemas Inteligentes**, y conforme a lo descrito en el capítulo 2 del acuerdo 219 del 27 de octubre de 2014, se consideran los recursos necesarios para su elaboración.

De antemano muchos agradecimientos por su valiosa colaboración.

Atentamente,



Nombre Andrés Felipe Yule

CC.1007248953

|  |
| --- |
| 1. **INTRODUCCIÓN** |

Este proyecto de grado tiene como objetivo implementar una plataforma web que permita el despliegue de algoritmos de detección de anomalías en sistemas de intrusión para entornos IoT, apoyándonos en la metodología MLOps para facilitar la integración y gestión continua de modelos. La detección de intrusiones en entornos IoT es crítica debido a su vulnerabilidad y la necesidad de proteger dispositivos conectados. Esto conlleva a que los sistemas de seguridad en IoT deban mejorar su precisión, velocidad y eficiencia en la detección de posibles amenazas, a la vez que optimizan el consumo de recursos.

|  |
| --- |
| 1. **DESCRIPCIÓN PROBLEMA** |

El crecimiento de los dispositivos IoT ha impulsado nuevas oportunidades de conectividad y funcionalidad, pero también ha incrementado los riesgos de intrusión en sistemas que muchas veces carecen de protección adecuada. Estos ataques afectan no solo la seguridad de los datos, sino también la funcionalidad y confiabilidad de los dispositivos involucrados. Actualmente, las soluciones para la detección de intrusiones en IoT se ven limitadas por la falta de recursos computacionales en los dispositivos y la necesidad de integrar modelos de aprendizaje que se adapten continuamente.

**Pregunta problema**: ¿Cómo implementar un sistema web de detección de intrusiones en IoT, que aproveche algoritmos de machine learning mediante la metodología MLOps para asegurar su actualización, escalabilidad y eficiencia?

|  |
| --- |
| 1. **JUSTIFICACIÓN** |

Este trabajo de grado es relevante dado el aumento de dispositivos IoT y la vulnerabilidad que estos sistemas presentan. Una implementación basada en MLOps aporta a la seguridad de la infraestructura IoT, garantizando que los modelos de detección de intrusiones se actualicen continuamente, lo cual beneficia tanto a investigadores y desarrolladores de seguridad en IoT como a las empresas y usuarios que los implementan. Organizaciones como el IEEE y la IETF han señalado la importancia de establecer protocolos de seguridad para IoT debido a las amenazas cibernéticas que afectan el desarrollo de esta tecnología OBJETIVOS

|  |
| --- |
| 1. **OBJETIVOS** |

Conservemos en los objetivos la estructura: Que se va a hacer, como se va a hacer y para que en todos los objetivos.

* 1. Objetivo General

Desarrollar una plataforma web para el despliegue de algoritmos de detección de anomalías en sistemas de intrusión para entornos IoT, aplicando principios de MLOps para facilitar la implementación continua y optimizar el monitoreo, escalabilidad y gestión del sistema.

* 1. Objetivos Específicos.
* Implementar una plataforma en el framework Flask para la visualización y gestión de modelos de detección de anomalías en IoT.
* Desarrollar una arquitectura MLOps para el despliegue y actualización continua de los modelos.
* Realizar pruebas de rendimiento y seguridad en la plataforma para validar la eficacia de la detección de intrusiones en un entorno simulado de IoT.

|  |
| --- |
| 1. **MARCO REFERENCIAL** |

El presente capítulo tiene el propósito de establecer las bases conceptuales, teóricas y técnicas que sustentan el desarrollo de la plataforma web para la detección de anomalías en sistemas de intrusión en entornos IoT. Este marco referencial proporciona una visión integral sobre los aspectos fundamentales que justifican la importancia y viabilidad del proyecto.

El capítulo se organiza en dos secciones principales:

* **Marco Teórico (5.1):** Aborda los conceptos teóricos esenciales, principios y fundamentos relacionados con los sistemas de detección de intrusiones, el entorno IoT y la metodología MLOps.
* **Estado del Arte (5.2):** Presenta una revisión de los avances más recientes, investigaciones y soluciones implementadas a nivel nacional e internacional en el ámbito de detección de intrusiones en entornos IoT, con énfasis en el uso de metodologías MLOps.
  1. **MARCO TEORICO**

En esta sección se presentan los fundamentos teóricos necesarios para comprender los componentes y metodologías del proyecto.

**1. Internet de las Cosas (IoT):**  
El IoT consiste en una red de dispositivos interconectados capaces de recopilar, intercambiar y procesar datos a través de Internet. Su importancia radica en su capacidad para automatizar procesos y optimizar recursos en sectores como salud, transporte y manufactura. Sin embargo, su conectividad lo hace susceptible a vulnerabilidades y ataques [1].

**2. Sistemas de Detección de Intrusiones (IDS):**  
Los IDS monitorean actividades en redes y sistemas para identificar comportamientos anómalos o maliciosos. Se clasifican en:

* **Basados en firmas:** Detectan amenazas conocidas comparando patrones con bases de datos.
* **Basados en anomalías:** Identifican comportamientos atípicos en relación con un modelo de referencia [2].

**3. Metodología MLOps:**  
MLOps combina DevOps con el desarrollo de modelos de machine learning, permitiendo la integración y despliegue continuo de soluciones basadas en inteligencia artificial. Este enfoque asegura escalabilidad y reproducibilidad, esenciales en entornos dinámicos como el IoT [3].

**4. Detección de anomalías:**  
Identifica patrones de datos que no se ajustan al comportamiento esperado. Su aplicación en IDS permite identificar amenazas nuevas o desconocidas, siendo fundamental para mejorar la seguridad en IoT [4].

* 1. **ESTADO DEL ARTE**

En esta sección se realiza una revisión de investigaciones y desarrollos recientes sobre detección de intrusiones en IoT, con enfoque en metodologías MLOps.

**1. Avances en detección de intrusiones en IoT:**  
En los últimos años, se han desarrollado algoritmos de aprendizaje profundo, como redes neuronales recurrentes, para mejorar la precisión y reducir falsos positivos en IDS [5].

**2. Uso de MLOps en seguridad IoT:**  
Estudios recientes destacan cómo MLOps facilita el ciclo de vida de modelos en sistemas IDS, mejorando la respuesta ante amenazas mediante pipelines automatizados y actualizaciones continuas [3].

**3. Desafíos actuales:**  
Los principales retos incluyen la limitada capacidad de procesamiento de dispositivos IoT, el manejo de grandes volúmenes de datos y la necesidad de modelos ligeros que optimicen recursos computacionales [5].

|  |
| --- |
| 1. **INFORMACIÓN GENERAL** |

Seleccione con una X el trabajo de grado para el cual aplica, de acuerdo al nivel de formación:



|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Título del proyecto | | | |  | | | | | |
| Sede |  | | | |  |  |  |  | |
|  | | | |  |  |  |  | |
|  | | | |  |  |  |  | |
|  | | | |  |  |  |  | |
| Facultad: | | Ingeniería | | | | | | | |
| Programa académico: | | | Ingeniería de sistemas | | | | | |  |

|  |
| --- |
| **Datos de estudiante** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Número de identificación: | | | | |  | | | | | |
| Escriba todos los números | | | | | | | | | | |
| Tipo: |  | | | | | | Expedida en: | |  | |
| Apellido 1: | | |  | | | Apellido 2: | | |  | |
| Nombres: | |  | | | | | | | | |
| Correo electrónico: | | | |  | | | | Teléfono: | |  |

|  |
| --- |
| **Datos Director, Codirector o Asesor** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Número de identificación: | | | |  | | |
| Escriba todos los números | | | | | | |
| Tipo: |  | | | | Expedida en: |  |
| Apellido 1: | |  | | | Apellido 2: |  |
| Nombres: | |  | | | | |
| Formación: | |  | | | | |
| Correo electrónico: | | |  | | | |

|  |
| --- |
| 1. **METODOLOGÍA** |

* 1. Metodología propuesta:

La metodología sigue un enfoque de investigación aplicada con fases definidas en el marco de MLOps para integrar el despliegue y la administración continua de modelos de machine learning en entornos IoT. La población de estudio corresponde a un entorno simulado de dispositivos IoT. Las técnicas de recolección de datos incluyen logs y métricas de rendimiento de los modelos en escenarios de prueba.Cronograma de actividades:

Acorde con las fases definidas en la metodología.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N° | ACTIVIDAD | SEMANAS | | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 0 | Revisión de la literatura xxxxxxxxxxxxx |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | |  | | --- | |  |  |  | | --- | | **Ciclo 1: Desarrollo y despliegue inicial con Streamlit** | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 | |  | | --- | |  |  |  | | --- | | Identificación de métricas y modelos | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | |  | | --- | | Diseño de interfaz inicial en Streamlit |  |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | |  | | --- | | Integración de modelos con Streamlit |  |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Implementación de CI/CD para modelos |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | |  | | --- | | Despliegue inicial con Streamlit |  |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | |  | | --- | | Implementación de captura de tráfico de red en Streamlit |  |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  |  |  | | --- | | **Ciclo 2: Ajustes y migración a Flask** | |  | |  |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 | |  |  | | --- | --- | | |  | | --- | | Monitoreo del desempeño en Streamlit | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Diseño y planificación para migrar a Flask |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | |  | | --- | | Construcción de la interfaz en Flask |  |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Integración de modelos en Flask |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | |  | | --- | | Integración de captura de tráfico en Flask |  |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 | |  | | --- | | Validación y pruebas finales en Flask |  |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | |  | | --- | | Despliegue final con Flask |  |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Presupuesto:

El proyecto no incurre en gastos adicionales, ya que se utilizarán herramientas de software de acceso gratuito y con planes sin costo, como Python, Streamlit y Flask, que son tecnologías de código abierto ampliamente utilizadas. Además, las plataformas en la nube seleccionadas ofrecen capas gratuitas que permiten el despliegue del proyecto sin necesidad de inversión en infraestructura. Estas herramientas permiten realizar el desarrollo y despliegue de la plataforma sin costos asociados, lo que optimiza el presupuesto del proyecto.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RUBROS | JUSTIFICACIÓN | FUENTES (En pesos) | | |
| CONADI \* | CONTRAPARTIDA 1\*\* | TOTAL |
| Materiales y Suministros |  |  |  |  |
| Salidas de campo[[1]](#footnote-1) |  |  |  |  |
| Bibliografía[[2]](#footnote-2) |  |  |  |  |
| TOTAL | |  |  |  |

\* El monto solicitado al fondo no debe superar:

$       Para pregrado y $       posgrado.

NOTA: Los recursos del fondo no pueden utilizarse para el pago de personal

## Resultados Esperados:

|  |  |  |  |
| --- | --- | --- | --- |
| CLASIFICACIÓN | DESCRIPCIÓN[[3]](#footnote-3) | PRODUCTO | |
| Productos de generación de nuevo Conocimiento | Son aquellos aportes significativos al estado del arte de un área de conocimiento, que han sido discutidos, validados que lleguen a ser incorporados a la discusión científica, al desarrollo de las actividades investigativas, académicas y a la práctica tecnológica | Artículos A | ☐ |
| Artículos B | ☐ |
| Libros de Investigación | ☐ |
| Capítulos en Libros de Investigación | ☐ |
| Patentes | ☐ |
| Variedad vegetal | ☐ |

|  |  |  |  |
| --- | --- | --- | --- |
| CLASIFICACIÓN | DESCRIPCIÓN[[4]](#footnote-4) | PRODUCTO | |
| Productos de apropiación social del conocimiento | La apropiación social del conocimiento se entiende como un proceso y práctica social de construcción colectiva, donde actores que pueden ser individuos, organizaciones o comunidades, se involucran en interacciones que les permiten intercambiar saberes y experiencias, donde el conocimiento circula, es discutido, puesto a prueba, usado y llevado a la cotidianidad. | Proyectos y programas de investigación con participación ciudadana | ☐ |
| Eventos de participación ciudadana | ☐ |
| Programas Pedagógicos de fomento a la investigación científica, al desarrollo y la innovación | ☐ |
| Programas o proyectos de extensión universitaria o de Responsabilidad social | ☐ |
| Redes de fomento de la Apropiación Social | ☐ |
| Proyecto de comunicación del conocimiento | ☐ |
| Generación de contenidos (documentos) | ☐ |
| Generación de contenidos (multimedia) | ☐ |
| Participación Eventos Científicos | ☐ |
| Participación Redes de Conocimiento | ☐ |
| Productos de Formación de Recursos Humanos | Se consideran los siguientes productos: la generación del espacio para asesorar y desarrollar las actividades implicadas en la realización de una tesis o trabajo de grado que otorgó el título de magister, especialista o profesional; ejecución de proyectos de I + D + i[[5]](#footnote-5) con formación y apoyo a programas de formación. | Trabajo de Grado de Maestría | ☐ |
| Trabajo de Grado Especialización | ☐ |
| Trabajo de Grado de Pregrado | ☑ |
| Proyectos I + D+ i con formación | ☐ |
| Apoyo a Programas de Formación | ☐ |

|  |
| --- |
| 1. **REFERENCIAS** |

Describa todas y cada una de las referencias utilizadas en la propuesta de TG. Deben estar en norma IEEE.

[1] M. Abeshu and N. Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169-175, Feb. 2018. Available: <https://ieeexplore.ieee.org/document/8264697>.

[2] R. Moustafa et al., "IoT Anomaly Detection Using Deep Learning: Systematic Review and Open Challenges," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5931-5942, Jul. 2020. Available: <https://ieeexplore.ieee.org/document/8990705>.

[3] P. Garcia-Teodoro et al., "A Survey of Anomaly-Based Network Intrusion Detection," *Computers & Security*, vol. 28, no. 1, pp. 18-28, Feb. 2009. doi: 10.1016/j.cose.2008.08.003.

[4] S. Rathore et al., "Recent Advances in IoT Intrusion Detection Systems: Challenges and Future Directions," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1374-1385, Jan. 2021. Available: <https://ieeexplore.ieee.org/document/9299830>.

[5] K. Hashim et al., "A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2497-2512, Mar. 2021. Available: <https://ieeexplore.ieee.org/document/9334503>.

1. Se refiere a: gastos de medios de transporte para el traslado a zonas de muestreo, ejecución de las labores de campo propias de la investigación, costos de combustible o alquiler de medios de transporte cuando se requiere [↑](#footnote-ref-1)
2. Corresponde a la adquisición de material bibliográfico, debidamente justificada y directamente relacionada con la temática del proyecto en la forma de libros y/o suscripciones a revistas científicas del tema. Una vez terminado el proyecto éste material quedara en custodia de la Universidad. [↑](#footnote-ref-2)
3. Definiciones de los tipos de productos resultados de investigación e innovación, de acuerdo con lo propuesto por Colciencias. [↑](#footnote-ref-3)
4. Definiciones de los tipos de productos resultados de investigación e innovación, de acuerdo con lo propuesto por Colciencias. [↑](#footnote-ref-4)
5. I + D + i: Investigación, Desarrollo e innovación [↑](#footnote-ref-5)