## 1. DATOS INFORMATIVOS

| | |
|---|---|
| **DOMINIO:** | |
| **CARRERA: Ingeniería en Ciberseguridad y Gestión de Tecnologías de la Información** | |
| **Asignatura/Módulo: Programación I** | **Procesamiento de Lenguaje Natural** |
| **Paralelo:** | **N° horas** |
| **Plan de estudios:** | H. aprendizaje en contacto con el docente: 32 |
| **Prerrequisitos:** | |
| **Periodo académico:** | H. aprendizaje autónomo: 72<br>H. aprendizaje práctico-experimental: 16 |
| **Docenteo o Co-Docente 1:** | **Grado académico y título profesional:** |
| Rafael Melgarejo Heredia | PhD in WebScience,<br>Ingeniero en Sistemas Informáticos y de Computación |
| **Breve reseña de la actividad académica y/o profesional:** | |
| Rafael Melgarejo es docente e investigador de la Pontificia Universidad Católica del Ecuador (PUCE). Su trabajo se centra en áreas como la interdisciplinariedad, ciencias de la web y del internet, y la inteligencia artificial.<br><br>Consultor y perito informático por +20 años (1992-2013) | |
| **dicación de horario de atención al estudiante:** | |
| **Tutoría presencial: lunes 11:00 a 13:00** | **Teléfono: 02 2991700 ext 2009** |
| **Tutoría virtual: martes y miércoles 18:00 a** | **Correo electrónico: rmelgarejo@puce.edu.ec** |

## 2. DESCRIPCIÓN DE LA ASIGNATURA

La asignatura Procesamiento de Lenguaje Natural (PLN) introduce los fundamentos teóricos, metodológicos y prácticos del análisis computacional del lenguaje humano, con especial énfasis en su aplicación a problemas propios del ámbito de la seguridad de la información. El curso presenta el PLN como un campo interdisciplinar que articula conceptos de lingüística computacional, inteligencia artificial y aprendizaje automático, orientados a la detección, análisis y mitigación de riesgos en entornos digitales.
El curso está diseñado para adquirir una comprensión sólida de los conceptos fundamentales del PLN, incluyendo la representación del texto, los modelos estadísticos y neuronales, y las arquitecturas modernas basadas en deep learning. Sobre esta base, se diseñarán e implementarán sistemas de PLN capaces de realizar tareas como clasificación de texto, análisis de sentimiento y generación de lenguaje natural, aplicadas a casos de uso relevantes para la ciberseguridad, tales como detección de phishing, análisis de amenazas, monitoreo de comunicaciones digitales y análisis automatizado de incidentes.
El curso introduce la evaluación de sistemas de PLN mediante métricas y técnicas de precisión y eficacia, promoviendo el análisis crítico del desempeño, la robustez y las limitaciones de los modelos en contextos de seguridad. De este modo, la asignatura contribuye a la formación de profesionales en ciberseguridad con capacidades para diseñar, evaluar y utilizar soluciones basadas en lenguaje natural como herramientas estratégicas para la protección de sistemas y datos.

## 3. DESCRIPCIÓN DE COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

| COMPETENCIAS TRANSVERSALES | COMPETENCIAS DISCIPLINARES DEL DOMINIO | RESULTADOS DE APRENDIZAJE DE LA CARRERA | RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA |
|---|---|---|---|
| | | Seleccionar herramientas y tecnologías adecuadas para el desarrollo y despliegue de sistemas de software, considerando factores como la usabilidad, escalabilidad, seguridad y rendimiento | Comprender los conceptos fundamentales del procesamiento de lenguaje natural para analizar información textual proveniente de incidentes de ciberseguridad, a través de técnicas de recolección, limpieza y análisis exploratorio de datos no estructurados. |
| | | Aplicar técnicas de inteligencia artificial y aprendizaje automático para la resolución de problemas complejos en diferentes áreas de la computación, como el procesamiento de lenguaje natural, la visión artificial | Diseñar sistemas de procesamiento de lenguaje natural para detectar y clasificar amenazas presentes en comunicaciones digitales, a través de la construcción de modelos de clasificación de texto, análisis semántico e identificación de |
| | | Evaluar críticamente la efectividad y limitaciones de las soluciones tecnológicas actuales y emergentes en diferentes áreas de la computación. | Evaluar sistemas de procesamiento de lenguaje natural para apoyar la toma de decisiones en ciberseguridad, a través de técnicas y métricas de precisión, eficacia, explicabilidad e impacto ético de los modelos. |

RdAs de la carrera

1. Aplicar los principios de programación para el diseño e implementación de soluciones de software eficientes y escalables, cumpliendo con los estándares de calidad y seguridad.
2. Implementar algoritmos y estructuras de datos para la resolución de problemas de complejidad media y alta en distintas áreas de la computación.
3. Seleccionar herramientas y tecnologías adecuadas para el desarrollo y despliegue de sistemas de software, considerando factores como la usabilidad, escalabilidad, seguridad y rendimiento.
4. Aplicar técnicas de inteligencia artificial y aprendizaje automático para la resolución de problemas complejos en diferentes áreas de la computación, como el procesamiento de lenguaje natural, la visión artificial y la robótica.
5. Evaluar críticamente la efectividad y limitaciones de las soluciones tecnológicas actuales y emergentes en diferentes áreas de la computación.
6. Resolver problemas de seguridad en los sistemas de información y tecnologías de la información mediante técnicas de análisis, solución de problemas y a través de proyectos.
7. Diseñar soluciones de seguridad en un entorno empresarial trabajando de manera colaborativa.
8. Aplicar de manera efectiva las nuevas tendencias y tecnologías en ciberseguridad y tecnologías de la información.
9. Remediar incidentes de seguridad en los sistemas y tecnologías de la información mediante técnicas de análisis forense y respuesta a incidentes en el marco de los conceptos y principios de la ética y la responsabilidad social.
10. Implementar auditorías de sistemas de seguridad cumpliendo los estándares y políticas establecidos que minimicen los impactos negativos de los riesgos asociados con la seguridad y la gestión de TI.

## 4. EVALUACIÓN DE LOGROS DE APRENDIZAJE

| | | | | | | Nivel de logro alcanzado al RdA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **PROYECTO DEL NIVEL** | **Retos** | **Resultado de aprendizaje** | **Pesos** | **Definición del criterio de evaluación del RdA** | **Ponderación criterios** | Alcanzado con excelencia (A) (45-50) | Alcanzado muy bueno (B) (40-44) | Alcanzado bueno (C) (30-39) | Pendiente de alcanzar (D) (29 y menos) | **Observaciones (Alertas para tutorías académicas)** |
| Este proyecto tiene como objetivo desarrollar progresivamente un sistema de análisis automático de texto que permita detectar, clasificar y alertar sobre amenazas de ciberseguridad a partir de fuentes textuales reales como: correos electrónicos (phishing), tickets de soporte, logs de incidentes, mensajes en foros o chats corporativos, reportes de seguridad. El proyecto se divide en 4 retos secuenciales, donde cada uno introduce conceptos clave de PLN aplicados a escenarios reales de ciberseguridad | Reto 1 (Formativo): Preparación de datos.<br>Objetivo: Comprender el lenguaje natural en contextos de ciberseguridad y preparar datos textuales para su análisis automático.<br>Entregable: Dataset limpio y documentado; informe de patrones | Comprender los conceptos fundamentales del procesamiento de lenguaje natural para analizar información textual proveniente de incidentes de ciberseguridad, a través de técnicas de recolección, limpieza y análisis exploratorio de datos no estructurados. | 33 | Criterio 1: Comprensión y análisis de los conceptos de PLN aplicados a textos de ciberseguridad | 50% | Analiza y explica con precisión los conceptos de PLN (tokenización, normalización, ruido, n-gramas, vocabulario) relacionándolos con características reales de incidentes de ciberseguridad. Distingue y compara patrones lingüísticos de phishing, malware e ingeniería social, sustentando su interpretación con evidencia del corpus. | Explica y describe adecuadamente los conceptos fundamentales del PLN y los relaciona con textos de ciberseguridad. Identifica patrones lingüísticos relevantes, aunque con análisis parcial de su impacto en la detección de amenazas. | Reconoce y parafrasea algunos conceptos del PLN, pero los vincula de forma limitada con el contexto de ciberseguridad. La identificación de patrones es general y poco diferenciada. | Enumera o menciona términos del PLN sin demostrar comprensión funcional ni relación con incidentes de ciberseguridad. No logra identificar patrones lingüísticos pertinentes. | Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico. |
| | | | | Criterio 2: Aplicación de procedimientos de recolección, limpieza y análisis exploratorio del dataset | 50% | Aplica y organiza de forma coherente un pipeline de preparación de datos: recolección, anonimización, limpieza y normalización. Justifica y documenta cada decisión técnica y genera análisis exploratorios que evidencian relaciones lingüísticas relevantes para la detección de amenazas. | Aplica los procedimientos de limpieza y análisis con criterios adecuados. Documenta el proceso, aunque con justificaciones parciales o con análisis exploratorio suficiente pero no profundo. | Ejecuta la limpieza de datos de manera mecánica, con organización limitada y escasa fundamentación técnica. El análisis exploratorio es descriptivo y poco vinculado al problema de seguridad. | No aplica adecuadamente los procedimientos de preparación de datos o los realiza con errores conceptuales. El dataset carece de documentación y el análisis es inexistente o irrelevante. | Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico. |
| | Reto 2 (Formativo): Clasificación<br>Objetivo: Construir modelos de PLN que clasifiquen textos según el tipo de amenaza.<br>Entregable: Modelo de clasificación funcional, y Reporte técnico justificando métricas desde la | Diseñar sistemas de procesamiento de lenguaje natural para detectar y clasificar amenazas presentes en comunicaciones digitales, a través de la construcción de modelos de clasificación de texto, análisis semántico e identificación de señales de ingeniería social. | 33 | Criterio 1: Diseño e implementación del modelo de clasificación de amenazas textuales | 50% | Diseña y organiza un pipeline completo de clasificación: etiquetado, vectorización y entrenamiento. Aplica técnicas adecuadas al contexto de ciberseguridad y justifica la selección del modelo mediante métricas pertinentes. El clasificador es funcional y reproducible para distintos tipos de amenazas. | Aplica y construye un modelo de clasificación operativo con etapas claramente definidas. Explica de forma adecuada las decisiones técnicas, aunque con justificación parcial de métricas o parámetros. | Ejecuta un modelo de clasificación con integración limitada de etapas. La vectorización y el entrenamiento son funcionales pero poco organizados y con escasa fundamentación técnica. | No logra construir un pipeline coherente de clasificación. Las etapas son fragmentadas o incorrectas y el modelo no responde al problema de detección de amenazas. | Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico. |
| | Reto 3 (Formativo): Análisis semántico<br>Objetivo: Detectar intenciones maliciosas más allá de palabras clave explícitas.<br>Entregable: Módulo de detección semántica, y Casos demostrativos de evasión detectada. | | | Criterio 2: Diseño del módulo de análisis semántico e identificación de intención maliciosa | 50% | Diseña el significado contextual de los mensajes para detectar intenciones maliciosas implícitas, integra evidencias de ingeniería social y anomalías lingüísticas, demostrando capacidad para identificar estrategias de evasión más allá de palabras clave. | Analiza el contenido semántico y detecta intenciones implícitas en la mayoría de los casos. Relaciona señales de ingeniería social, aunque con profundidad limitada. | Identifica algunos elementos semánticos, pero el análisis es superficial y poco diferenciado de enfoques basados en palabras clave. | No analiza el significado contextual ni logra identificar intención maliciosa. El módulo depende casi exclusivamente de coincidencias léxicas. | Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico. |
| | Reto 4 (Sumativo): Sistema integrado.<br>Objetivo: Integrar todo lo aprendido en un sistema funcional de apoyo a la toma de decisiones en ciberseguridad.<br>Entregable final: Prototipo funcional del sistema, demo y diseño | Evaluar sistemas de procesamiento de lenguaje natural para apoyar la toma de decisiones en ciberseguridad, a través de técnicas y métricas de precisión, eficacia, explicabilidad e impacto | 34 | Criterio 1: Evaluación técnica de precisión y eficacia del sistema de PLN | 50% | Evalúa el sistema integrado utilizando métricas pertinentes (precisión, recall, F1, matriz de confusión, AUC). Interpreta y justifica los resultados en función del riesgo operativo de un SOC, diferenciando el impacto de falsos positivos y falsos negativos en un contexto crítico. | Evalúa el sistema con métricas adecuadas y explica los resultados de manera correcta. Relaciona el desempeño con el contexto de ciberseguridad, aunque con análisis parcial del impacto del error. | Calcula métricas de forma descriptiva, pero interpreta de manera limitada su significado para la toma de decisiones. La validación es incompleta o poco contextualizada. | No evalúa adecuadamente el sistema o utiliza métricas incorrectas. No demuestra comprensión de la precisión y eficacia del modelo. | Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico. |
| | | | | Criterio 2: Análisis crítico, ético y de explicabilidad del sistema de alertas | 50% | Analiza críticamente el impacto del sistema considerando sesgos, privacidad y explicabilidad. Propone y defiende mecanismos de uso responsable y valora las consecuencias éticas de la automatización de alertas. | Analiza aspectos éticos y de explicabilidad del sistema y argumenta su relevancia para la ciberseguridad, aunque con profundidad moderada. | Reconoce algunos riesgos éticos, pero no los integra de forma coherente con la evaluación técnica del sistema. | No considera implicaciones éticas ni de explicabilidad en la evaluación del sistema. | Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico. |

**5. METODOLOGÍA**

La asignatura Procesamiento de Lenguaje Natural PLN sigue una metodología de aprendizaje basado en proyectos y retos combinados, lo que permite que los estudiantes aprendan de manera activa y práctica. Desde el primer día, los estudiantes comenzarán a trabajar en un proyecto transversal que se desarrollará a lo largo del curso. Este enfoque les permite aplicar los conceptos aprendidos de manera continua, integrando teoría y práctica en cada etapa del proyecto.

El curso se organiza en 4 retos: tres retos formativos que abordan los conceptos y habilidades clave del PLN programación (clasificación de texto, análisis de sentimiento y

**6. RELACIÓN RESULTADOS DE APRENDIZAJE, EXPERIENCIAS DE APRENDIZAJES Y DIMENSIÓN DEL CONOCIMIENTO**

| PROYECTO DE NIVEL | RETOS | RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA | Semanas | Experiencias / estrategias Aprendizaje en contacto con el docente | Horas | Recursos | Escenario | Experiencias / estrategias de aprendizaje práctico-experimental: | Horas | Recursos | Escenario | Experiencias / estrategias de aprendizaje autónomo | Horas | Recursos | Escenario | DIMENSIÓN DEL CONOCIMIENTO (conceptos, hecho, procedimientos o principios) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Este proyecto tiene como objetivo desarrollar progresivamente un sistema de análisis automático de texto que permita detectar, clasificar y alertar sobre amenazas de ciberseguridad a partir de fuentes textuales reales como: correos electrónicos (phishing), tickets de soporte, logs de incidentes, mensajes en foros o chats corporativos, reportes de seguridad.<br>El proyecto se divide en 4 retos secuenciales, donde cada uno introduce conceptos clave de PLN aplicados a escenarios reales de ciberseguridad | Reto 1 (Formativo): Preparación de datos.<br>Objetivo: Comprender el lenguaje natural en contextos de ciberseguridad y preparar datos textuales para su análisis automático.<br>Entregable: Dataset limpio y documentado; informe de patrones | Comprender los conceptos fundamentales del procesamiento de lenguaje natural para analizar información textual proveniente de incidentes de ciberseguridad, a través de técnicas de recolección, limpieza y análisis exploratorio de datos no estructurados. | 1 | Tutorías asincrónicas por videoconferencia. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Exploración guiada de un mini-corpus de correos de phishing y reportes de incidentes.<br>Identificación manual de elementos lingüísticos relevantes (asuntos, verbos de acción, URLs, entidades). | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. Dataset de ejemplo provisto por el docente | Entorno virtual de aprendizaje, Colab, software especializado | Lectura dirigida sobre fundamentos del PLN aplicado a seguridad.<br>Elaboración de un glosario técnico contextualizado.<br>Búsqueda de 10 ejemplos reales de textos de incidentes. | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 1. Bases del texto y del dataset en ciberseguridad<br>1.1. Naturaleza del texto no estructurado en ciberseguridad: correos, tickets, logs narrativos.<br>1.2. Conceptos básicos de PLN: token, corpus, ruido, stopwords, n-grams.<br>1.3. Características lingüísticas de amenazas: urgencia, suplantación, lenguaje persuasivo. |
| | | | 2 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Integración de textos desde distintas fuentes simuladas.<br>Revisión de anonimización de datos sensibles.<br>Documentación inicial del corpus. | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. Checklist ético | Entorno virtual de aprendizaje, Colab, software especializado | Recolección del dataset propio del equipo.<br>Redacción de la descripción técnica del corpus.<br>Identificación de tipos de amenazas presentes. | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 1. Bases del texto y del dataset en ciberseguridad<br>1.4. Fuentes de datos textuales en SOC/CSIRT.<br>1.5. Estructura del dataset: campos, metadatos y etiquetas.<br>1.6. Problemas éticos y de privacidad. |
| | | | 3 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Aplicación de scripts básicos de limpieza.<br>Comparación "texto crudo vs. limpio".<br>Registro de decisiones técnicas. | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. Notebook con código base (Python + spaCy/NLTK)<br>Dataset de prueba<br>Rúbrica de calidad del texto | Entorno virtual de aprendizaje, Colab, software especializado | Implementación de la limpieza en el dataset propio.<br>Documentación del pipeline aplicado.<br>Control de versiones del corpus. | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 2. Preparación del texto para análisis<br>2.1. Tokenización y normalización.<br>2.2. Eliminación de ruido: firmas, HTML, URLs.<br>2.3. Manejo de stopwords y lematización. |
| | | | 4 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Generación de nubes de palabras y estadísticas.<br>Identificación de patrones de ingeniería social.<br>Discusión crítica de hallazgos. | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Herramientas de visualización<br>Plantilla de informe<br>Foro de retroalimentación | 5 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 2. Preparación del texto para análisis<br>2.4. Distribución léxica y frecuencias.<br>2.5. Principio de representación del lenguaje.<br>2.6. Relación entre patrones lingüísticos y ataques. |
| | Reto 2 (Formativo): Clasificación<br>Objetivo: Construir modelos de PLN que clasifiquen textos según el tipo de amenaza.<br>Entregable: Modelo de clasificación funcional, y Reporte técnico justificando métricas desde la perspectiva de ciberseguridad. | Diseñar sistemas de procesamiento de lenguaje natural para detectar y clasificar amenazas presentes en comunicaciones digitales, a través de la construcción de modelos de clasificación de texto, análisis semántico e identificación de señales de ingeniería social. | 5 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Revisión de un dataset previamente etiquetado<br>Análisis del desbalance de clases y su impacto<br>Discusión de criterios para definir etiquetas de riesgo | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. Notebook base con dataset de ejemplo<br>Guía de tipologías de amenazas | Entorno virtual de aprendizaje, Colab, software especializado | Definición del esquema de etiquetas del equipo<br>Etiquetado inicial de una muestra del corpus<br>Lectura guiada sobre modelos de clasificación de texto | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 3. Fundamentos de la clasificación de amenazas.<br>3.1. Aprendizaje supervisado en PLN.<br>3.2. Etiquetas y clases de amenazas. |
| | | | 6 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Construcción de vectores a partir del dataset propio<br>Comparación entre representaciones<br>Visualización de similitud entre textos | 1 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. Notebook guiado<br>Dataset del Reto 1 limpio | Entorno virtual de aprendizaje, Colab, software especializado | Implementación de vectorización definitiva<br>Documentación de decisiones técnicas<br>Preparación de datasets divididos | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. Tutorial de TF-IDF y embeddings | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 3. Funndamentos de la clasificación de amenazas.<br>3.3. Representación vectorial: BoW, TF-IDF, embeddings.<br>3.4. Desbalance de clases y riesgo en ciberseguridad. |
| | | | 7 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Entrenamiento de al menos dos modelos<br>Comparación rápida de resultados<br>Discusión sobre falsos negativos críticos | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. Notebook de entrenamiento<br>Matriz de confusión interactiva<br>Guía de interpretación de métricas | Entorno virtual de aprendizaje, Colab, software especializado | Entrenamiento final del modelo del equipo<br>Ajuste de hiperparámetros<br>Registro de experimentos | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. Scikit-learn / PyTorch | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 4. Construcción del Clasificador.<br>4.1 Vectorización TF-IDF y embeddings.<br>4.2. Conjuntos train/validation/test.<br>4.3. Algoritmos 1: Naive Bayes |
| | | | 8 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Análisis de casos donde el modelo falla<br>Ajuste de umbrales según riesgo<br>Debate técnico de consecuencias operativas | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Elaboración del entregable<br>Modelo funcional<br>Reporte técnico con justificación de métricas | 5 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 4. Construcción del Clasificador.<br>4.4. Algoritmos 2: SVM, redes simples.<br>4.5. Métricas orientadas a riesgo.<br>4.6. Sobreajuste y validación cruzada. |
| | Reto 3 (Formativo): Análisis semántico<br>Objetivo: Detectar intenciones maliciosas más allá de palabras clave explícitas.<br>Entregable: Módulo de detección semántica, y Casos demostrativos de evasión detectada. | | 9 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Comparación entre mensajes maliciosos explícitos y evasivos<br>Identificación manual de intenciones implícitas<br>Mapeo de señales discursivas de manipulación | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. Python + scikit-learn<br>Notebook guiado<br>Dataset del Reto 1 limpio | Entorno virtual de aprendizaje, Colab, software especializado | Lectura dirigida sobre análisis semántico en PLN<br>Elaboración de matriz de señales de ingeniería social<br>Selección de 20 casos problemáticos del dataset propio | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 5. Evaluación del clasificador desde ciberseguridad.<br>5.1. Interpretación de precisión, recall y F1.<br>5.2. Impacto de errores en SOC. |
| | | | 10 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Cálculo de similitud entre mensajes<br>Detección de frases sospechosas por contexto<br>Exploración de clusters semánticos | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. Notebook con embeddings<br>Herramientas de visualización<br>Dataset del Reto 2 | Entorno virtual de aprendizaje, Colab, software especializado | Implementación inicial del módulo semántico<br>Pruebas con mensajes evasivos<br>Registro de hallazgos | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 5. Evaluación del clasificador desde ciberseguridad.<br>5.3. Umbrales de alerta<br>5.4. Costo del error. |
| | | | 11 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Pruebas con textos modificados por estudiantes<br>Evaluación de robustez del módulo<br>Discusión de fallos y sesgos | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Ajuste del módulo de detección<br>Integración con el clasificador previo<br>Documentación técnica | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 6. Análisis semántico e intención maliciosa.<br>6.1. Palabras clave vs. semántica.<br>6.2. Intención comunicativa y pragmática.<br>6.3. Señales de ingeniería social. |
| | | | 12 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab | Entorno virtual de aprendizaje, Colab, software especializado | Presentación de 5 casos de evasión detectada<br>Justificación lingüística de decisiones<br>Debate sobre falsos positivos | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Elaboración del entregable final:<br>Módulo de detección semántica<br>Casos demostrativos documentados | 5 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 6. Análisis semántico e intención maliciosa.<br>6.4. Embeddings y similitud semántica.<br>6.5. Detección de anomalías lingüísticas.<br>6.6. Modelado de intención e heurísticas híbridas. |
| | Reto 4 (Sumativo): Sistema integrado.<br>Objetivo: Integrar todo lo aprendido en un sistema funcional de apoyo a la toma de decisiones en ciberseguridad, a través de técnicas y métricas de precisión, eficacia, explicabilidad e impacto ético de los modelos.<br>Entregable final: Prototipo funcional del sistema, demo y diseño | Evaluar sistemas de procesamiento de lenguaje natural para apoyar la toma de decisiones en ciberseguridad, a través de técnicas y métricas de precisión, eficacia, explicabilidad e impacto ético de los modelos. | 13 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Diseño guiado de arquitectura:<br>Modelado del flujo de datos del sistema<br>Definición de puntos de decisión y alertas<br>Discusión de requerimientos operativos | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab.<br>Diagramador (Draw.io/Whimsical) | Entorno virtual de aprendizaje, Colab, software especializado | Diseño del prototipo propio<br>Integración de módulos previos<br>Redacción inicial del documento de diseño | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 7. Validación semántica y ética.<br>7.1. Evaluación cualitativa de casos de evasión.<br>7.2. Explicabilidad del modelo. |
| | | | 14 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Medición del sistema integrado<br>Simulación de escenarios de ataque<br>Ajuste de umbrales | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Evaluación formal del prototipo<br>Análisis de resultados<br>Redacción de sección de métricas | 4 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 7. Validación semántica y ética.<br>7.3. Límites éticos del análisis semántico. |
| | | | 15 | Tutorías asincrónicas por mensajes, videos, correos electrónicos, foros, chats. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab | Entorno virtual de aprendizaje, Colab, software especializado | Análisis de casos controversiales<br>Evaluación de transparencia<br>Diseño de mensajes de alerta responsables | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Incorporación de capa explicable<br>Redacción de sección ética<br>Mejora del prototipo | 6 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 8. Integración y Comunicación de Resultados.<br>8.1. Arquitectura de sistemas de PLN en ciberseguridad.<br>8.2. Integración clasificación + semántica.<br>8.3. Métricas avanzadas: ROC, AUC. |
| | | | 16 | Tutorías sincrónicas por videoconferencia. | 2 | Dispositivos electrónicos portátiles o de escritorio.<br>Conexión a internet.<br>Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Presentación del sistema<br>Pruebas en vivo<br>Retroalimentación cruzada | 1 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado | Entregable final:<br>Prototipo funcional<br>Presentación técnica<br>Documento de diseño | 7 | Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma Educativa Google Colab. | Entorno virtual de aprendizaje, Colab, software especializado, acceso a la biblioteca virtual | 8. Integración y Comunicación de Resultados.<br>8.4. Sesgos, privacidad y explicabilidad.<br>8.5. Validación técnica final.<br>8.6. Comunicación de resultados y decisiones. |
| | | | 32 | | | | | | 16 | | | | 72 | | | |

## 8. BIBLIOGRAFÍA

### a. BÁSICA / LIBROS

| Bibliografía (basarse en normas APA) | Código Biblioteca PUCESI | Nro. de ejemplares |
|---|---|---|
| Alawida, M., Mejri, S., Mehmood, A., Chikhaoui, B., & Isaac Abiodun, O. (2023). A Comprehensive Study of ChatGPT: Advancements, Limitations, and Ethical Considerations in Natural Language Processing and Cybersecurity. *Information* , *14* (8), 462. https://doi.org/10.3390/info14080462 | https://researchs.puce.elogim.com/c/26kgwn/search/details/6p5mkowrsj?limiters=FT1%3AY&q=cybersecurity+and+natural+language+processing&searchMode=boolean | On line |
| Martínez Porras, E., Ramírez Fernández, A., Solís Bastos, L. P., & Díaz González, J. A. (2025). Uso de Procesamiento de Lenguaje Natural para procesar respuestas abiertas de una encuesta de Opinión Pública. Revista Latinoamericana de Metodología de La Investigación Social: ReLMIS, Nº. 29 (Abril - Septiembre 2025), 2025 (Ejemplar Dedicado a: La Problematización Como Método En La Indagación Social), Pags. 51-67. | https://dialnet.unirioja.es/servlet/articulo?codigo=10140930# | On line |
| Petrlik Azabache, I., Rodriguez Rodriguez, C., Lezama Gonzales, P., Torres-Talaverano, L., Vásquez Hurtado, E. G., & Hinojosa Pedraza, K. I. (2025). Procesamiento de lenguaje natural y Bert para el perfilado de autores en la red social X. Revista Campus, 30(39), 147–165. https://doi.org/10.24265/campus.2025.v30n39.08 | https://researchs.puce.elogim.com/c/26kgwn/viewer/pdf/mulokqb7yf | On line |
| Agudelo Ortiz, A. M., Rodríguez Pulecio, L. S., & Bedoya Leiva, O. F. (2025). Cyberbullying detection in Spanish using natural language processing and machine learning. Investigación e Innovación En Ingenierías, 13(2), 168–183. https://doi.org/10.17081/invinno.13.2.7922 | https://researchs.puce.elogim.com/c/26kgwn/viewer/pdf/6oitwacco5 | On line |

**Elaborado por:**

Damián Nicolalde R

**Revisado y Aprobado por:**

Damián Nicolalde R
**Coordinador de la carrera**

**f) Docente**