UAX Universidad Alfonso X el Sabio

TFM - MU Online en Ciberseguridad

2024-2025

Nombre y apellidos	Título	Tutor	Resumen
Luis Ernesto Almeida Zambrano	Automatización del Hardening de Servidores Rocky Linux mediante Ansible y Generación Automática de Documentación con LLM	Gonzalo Martínez Ginesta	El presente trabajo presenta una solución para la automatización del hardening de servidores Rocky Linux, dada su similitud con Red Hat Enterprise Linux (RHEL), mediante el uso de Ansible para implementar configuraciones de seguridad eficientes y escalables. Se desarrolla un flujo de trabajo para la generación automática de documentación, empleando frameworks como Astro o Docusaurus, apoyado en modelos de lenguaje (LLM) locales, facilitando la creación y mantenimiento de la documentación, optimizando así la gestión de la seguridad y la documentación en entornos Rocky Linux.
Tomás Ambabi Turrión	Detección de ataques basada en aprendizaje automático	Juan José Sánchez Peña	El trabajo propuesto se centra en el desarrollo de un sistema de detección de ataques en ciberseguridad utilizando técnicas de aprendizaje automático. El desafío principal consiste en identificar patrones de comportamiento anómalos o maliciosos en sistemas informáticos y redes, con el objetivo de detectar de manera eficiente ataques como intrusiones, denegaciones de servicio (DoS), explotación de vulnerabilidades y malware.
Santiago Arias López	Desarrollo de un Banco de Pruebas Virtualizado para el Pentesting de Dispositivos OT	Ana Vázquez Meco	Diseñar, implementar y validar un banco de pruebas simulado/virtualizado para dispositivos OT, que permita realizar pruebas de pentesting con el fin de identificar vulnerabilidades y ejecutar con éxito dos o más ciberataques en un entorno controlado.

Ignacio Artímez Ayuela	Herramienta de automatización de la fase de enumeración sigilosa y reporting en escenarios militares	Alejandro Corletti Estrada	El presente Trabajo Fin de Máster tiene como propósito diseñar y desarrollar una herramienta que permita automatizar la fase de enumeración de sistemas y servicios en entornos militares o de alta seguridad, garantizando la máxima discreción y reduciendo la huella de actividad detectada. Para ello, se analizarán las técnicas de enumeración más relevantes y se adaptarán los métodos de pentesting existentes, priorizando la minimización de alertas que pudieran desencadenar acciones defensivas en el entorno objetivo. Además, se incluirá un módulo de reporting que genere informes detallados y adaptados a las necesidades específicas de las organizaciones militares o gubernamentales, teniendo en cuenta los protocolos de confidencialidad y la gestión de información sensible.
Vicente Ayarza Ocejo	Ciberseguridad personal: cyberbullying, grooming y redes sociales	Juan Manuel Matalobos Veiga	Este trabajo se centra en dos amenazas principales: el cyberbullying y el grooming, analizando cómo las redes sociales facilitan estos ataques y qué vulnerabilidades permiten su propagación. Se investigarán las tácticas utilizadas por los agresores, los mecanismos de protección disponibles y las limitaciones actuales en las plataformas digitales. Además, se explorará el papel de la inteligencia artificial y las herramientas de ciberseguridad en la detección y prevención de estos riesgos, con el objetivo de desarrollar un marco de buenas prácticas para mejorar la seguridad y concienciación de los usuarios.

Chiara Boccaletti	Detección de ataques basados en aprendizaje automático	Juan José Sánchez Peña	Este Trabajo Fin de Máster se enfoca en la implementación de un sistema de detección de intrusiones (IDS) basado en aprendizaje profundo (deep learning) para identificar ataques cibernéticos en redes informáticas. Con el aumento de los ciberataques, la necesidad de mejorar los mecanismos de defensa en redes es crucial. El objetivo es diseñar un sistema que aprenda de los datos generados por las interacciones en una red, identificando patrones de ataques conocidos y adaptándose a nuevos comportamientos maliciosos. Se propone la creación de un modelo que optimice la precisión y reduzca la tasa de falsos positivos y negativos mediante técnicas avanzadas de aprendizaje profundo. Para ello, se utilizarán arquitecturas como Redes Neuronales Artificiales (ANN), LSTM y CNN en combinación con algoritmos de machine learning. El sistema será evaluado utilizando diversos escenarios y datasets, con el fin de detectar intrusiones de manera más eficiente y adaptativa. Este enfoque de deep learning tiene como objetivo ofrecer una solución robusta para la protección de redes modernas, mejorando la capacidad de respuesta ante amenazas. Además, se compararán los resultados con sistemas tradicionales de detección de intrusiones, proporcionando una base para futuras mejoras.
Álex Carrillo Delgado	Fuzzy para código Java	Ana Vázquez Meco	Desarrollar un prototipo de una herramienta automatizada de fuzzing para código Java que identifique vulnerabilidades de seguridad y errores en aplicaciones escritas en este lenguaje. La herramienta se centrará en explorar entradas y rutas no documentadas dentro del software, buscando provocar fallos o comportamientos inesperados en aplicaciones Java mediante técnicas de generación de entradas aleatorias y adaptativas.

María Carvajal Cortés	Diseño e implementación de un pipeline DevSecOps con herramientas de código abierto	Iván García Cobo	Este trabajo tiene como objetivo diseñar e implementar un pipeline DevSecOps utilizando herramientas de código abierto, asegurando la seguridad en todas las etapas del desarrollo y despliegue de aplicaciones. El principal desafío radica en automatizar las pruebas de seguridad sin afectar la velocidad ni la eficiencia del proceso de entrega continua. Para ello, se integrarán herramientas de análisis de código estático (SAST), escaneo de dependencias (SCA) y pruebas dinámicas de seguridad (DAST), entre otras.
Gary Alfredo Cedano Morla	Cultura de ciberseguridad en niños y adolescentes de república dominicana: Retos y estrategias de formación	Verónica Juliana Caicedo Buitrago	Este trabajo tiene como objetivo analizar el estado de la educación en ciberseguridad en menores, identificar los principales desafíos en su formación y proponer estrategias adaptadas al contexto dominicano. Se utilizará una metodología mixta, combinando un análisis documental y encuestas a docentes y padres. Los resultados esperados incluyen un conjunto de recomendaciones y estrategias de concienciación en ciberseguridad para menores, con el fin de fomentar una cultura digital segura en el país.
Alison Marcela Coba Bonilla	Implementación del NIST Cybersecurity Framework (NIST CSF) para la compañía EBICS S.A.	Alba Martínez Gómez	El principal problema que actualmente tiene la empresa radica en el tratamiento de los datos personales que maneja del cliente final, por lo tanto, la implementación del NIST Cybersecurity Framework (NIST CSF) en EBICS S.A. tiene como propósito establecer un enfoque sólido de ciberseguridad que garantice la protección de los datos sensibles de los clientes y la continuidad de los servicios críticos, como la instalación de servicios de internet y telefonía.
Óscar Galante Herrero	V2X: Vehicle to X - Vehículos autónomos	Alejandro Corletti Estrada	Este trabajo analizará los riesgos de seguridad en la comunicación V2X, evaluando los estándares de protección existentes y proponiendo soluciones para fortalecer la seguridad en redes vehiculares. Se utilizarán herramientas de simulación para modelar posibles ataques y evaluar su impacto. Además, se analizará la normativa vigente en materia de ciberseguridad en automoción (ISO 21434, ETSI, NHTSA).

Gonzalo García Campos	Integración de OAuth2 y OpenID en arquitecturas cloud seguras	Juan José Sánchez Peña	El estudio abordará el funcionamiento de OAuth2 como framework de autorización y cómo OIDC extiende sus capacidades para la autenticación. Se explorarán distintos flujos de autenticación y autorización, su aplicación en ecosistemas de aplicaciones distribuidas y las mejores prácticas para mitigar vulnerabilidades de ataques.
Alejandro Gil Naranjo	Diseño e implementación de un sistema de respuesta a incidentes.	Juan José Sánchez Peña	El objetivo es diseñar e implementar un sistema de respuesta a incidentes (SRI) en ciberseguridad utilizando herramientas open-source. Se analizará distintas plataformas como TheHive, Wazuh y MISP, seleccionando la más adecuada para un entorno de prueba. A través de un caso práctico, se configurará el sistema, se simularán incidentes de seguridad y se evaluará su efectividad.
Raúl Gonzalo Martín	Desarrollo e implementación de un Honeypot para detección de ataques e inteligencia de amenazas	Alejandro Corletti Estrada	Este Trabajo Fin de Master tiene como objetivo el desarrollo e implementación de un sistema honeypot orientado a la detección de ataques y recopilación sobre posibles amenazas dentro de las redes informáticas. Desarrollo de sistema para simular vulnerabilidades y atraer a los atacantes, para de este modo poder analizar y recopilar las técnicas, herramientas y comportamientos de los atacantes.
Nieves Gutiérrez García de Veas	CIBERSEGURIDAD EN ENTORNOS OT: RETOS Y SOLUCIONES EN INFRAESTRUCTURAS CRITICAS EN LA INDUSTRIA ALIMENTARIA	Ana Vázquez Meco	Este trabajo aborda los principales retos de ciberseguridad en infraestructuras críticas dentro de la industria alimentaria, analizando vulnerabilidades, amenazas y soluciones específicas para proteger los sistemas industriales. Se estudiará la implementación de herramientas como Claroty, TXOne Networks y Splunk para fortalecer la seguridad en entornos OT, con un enfoque en la detección de amenazas, segmentación de redes y respuesta ante incidentes.

Urides Loweski Casimiro	Diseño e Implementación Parcial de un Sistema de Ciberseguridad para MIPYMES: Fase inicial	Jorge Calvo Martín	El presente trabajo tiene como objetivo el diseño e implementación parcial de un sistema de ciberseguridad enfocado en las MIPYMES (Micro, Pequeñas y Medianas Empresas). Se identificará y abordará un conjunto de amenazas y vulnerabilidades comunes en este tipo de organizaciones, las cuales carecen de los recursos y capacidades de grandes empresas para afrontar ciberamenazas. El trabajo se centrará en la implementación de medidas de seguridad básicas, junto con una evaluación del impacto que tienen en la protección de activos críticos, incluyendo redes, datos y sistemas. A través de este proyecto, se pretende ofrecer un enfoque accesible y eficiente para mejorar la seguridad cibernética de las MIPYMES, con el fin de garantizar su continuidad operativa frente a ataques cibernéticos.
Antonio Mira Otero	Auditoría de ciberseguridad para el cumplimiento de la directiva NIS2 en hospitales	Alba Martínez Gómez	El presente Trabajo Fin de Máster tiene como objetivo proponer un enfoque metodológico para auditar el cumplimiento de la normativa europea NIS2 en el sector salud, centrándose en hospitales de tamaño mediano. También se realizará un caso práctico sobre un hospital de tamaño medio que haya adoptado la directiva NIS2, a través del enfoque metodológico propuesto, con el fin de comprobar la eficacia de éste. Se espera que la metodología propuesta contribuya a optimizar la seguridad de los sistemas de información en el sector salud, garantizando el cumplimiento normativo y la protección de datos sensibles.
Andrea Montoya Capote	Implementación de una herramienta automática para la realización de hacking éticos.	Juan José Sánchez Peña	El objetivo de este proyecto es desarrollar una herramienta automática para la realización de hacking éticos por personas con escasos o nulos conocimientos en ciberseguridad.
Marta Moral García	Optimización de la Gestión del Parque Tecnológico en Grandes Empresas mediante Tanium: Seguridad, Unificación y Cumplimiento Normativo	Verónica Juliana Caicedo Buitrago	El trabajo analiza los riesgos de una gestión descentralizada y la necesidad de una solución integral como Tanium, relacionándolo con la gobernanza de la ciberseguridad, la seguridad en la cadena de suministro y el control de acceso a la información. Además, se evaluó su papel en el cumplimiento de normativas como ISO 27001, NIST, ENS y GDPR, fortaleciendo la arquitectura de seguridad empresarial y la protección de activos digitales.

Francisco Navarro Madueño	Ejecución de un pentesting en un entorno real: Técnicas y metodología para el compromiso de sistemas	Iván García Cobo	Este TFM está centrado en la realización de un pentesting en un entorno real o, en caso de no disponer de uno, en un laboratorio que simule una infraestructura empresarial. La idea es definir un alcance específico con la empresa que acepte este trabajo y, a partir de ahí, emplear las herramientas y técnicas necesarias para ejecutar un ataque controlado con el objetivo de comprometer los activos definidos dentro de dicho alcance.
David Nieto Vinuesa	Seguridad en Cloud: análisis de herramientas de seguridad en cloud gratuitas	Gonzalo Martínez Ginesta	Este proyecto tiene como objetivo realizar un análisis de diversas herramientas de seguridad en cloud gratuitas, evaluando su efectividad en la detección y mitigación de riesgos específicos en entornos cloud. Se analizará la precisión, confianza y aplicabilidad de herramientas como Google Cloud Security Scanner, Microsoft 365 Defender, Cisco Umbrella y OpenVAS. La relevancia de este estudio radica en la creciente adopción de soluciones cloud y la necesidad de contar con mecanismos de seguridad efectivos y accesibles. Se espera ofrecer una comparativa detallada que facilite la selección de herramientas adecuadas según diferentes necesidades de seguridad
Jesus Alberto Nosse Hale	Análisis de Herramientas de Seguridad en Cloud Gratuitas	Gonzalo Martínez Ginesta	El estudio se centra en evaluar los riesgos específicos que cubren, su exactitud, confiabilidad y aplicabilidad en diferentes escenarios. Mediante una metodología comparativa, se busca identificar las fortalezas y debilidades de cada herramienta, proporcionando recomendaciones para su uso efectivo en la protección de infraestructuras cloud. Los resultados esperados incluyen una guía práctica para la selección e implementación de estas herramientas, contribuyendo a la mejora de la seguridad en entornos cloud.

Kevin Ortiz Falcón	Implementación de un sistema de alerta temprana para ataques phishing con Deep Learning	Juan José Sánchez Peña	Este TFM propone el desarrollo e implementación de un sistema de alerta temprana basado en Deep Learning para detectar y mitigar ataques de phishing en tiempo real. El enfoque se centrará en el uso de redes neuronales profundas (Deep Neural Networks, DNNs), redes neuronales convolucionales (CNNs) y modelos recurrentes (RNNs/LSTMs) para analizar patrones textuales en correos electrónicos, detectar URLs maliciosas y evaluar comportamientos sospechosos de los usuarios.
David Geovanny Paltan Chacha	Evaluación de seguridad en aplicaciones FinTech mediante Penetration testing	Alejandro Corletti Estrada	A través de este trabajo de fin de Máster (TFM) es evaluar la seguridad de aplicaciones FinTech mediante pruebas de penetración controladas. Se analizan metodologías reconocidas como OWASP, NIST y PTES para identificar vulnerabilidades comunes en aplicaciones de esta industria. En un entorno controlado, se utilizan herramientas de pentesting para identificar vulnerabilidades de seguridad y sugerir mejoras. El objetivo es proporcionar una evaluación comparativa de diferentes métodos de pentesting y generar un conjunto de recomendaciones para fortalecer la seguridad de estas plataformas financieras
Juan Carlos Pérez Espinar	Aprendizaje automático para el diseño e implementación de un IDS en sistemas IoT	Alejandro Corletti Estrada	Este TFM propone, a partir de un estudio previo, una solución para un sistema detector de intrusiones (IDS) que emplee algoritmos de Machine Learning para detectar patrones que puedan ser categorizados como malignos de cara a intrusiones en sistemas IoT.
Christopher Alexander Puruncaja Muñoz	Seguridad en Cloud: análisis de herramientas de seguridad en cloud gratuitas.	Gonzalo Martínez Ginesta	Este proyecto debe ofrecer un análisis de las herramientas de seguridad en cloud, identificando los riesgos específicos que cubren, la exactitud y confianza que ofrecen estas herramientas, así como aplicabilidad. Ejemplos de herramientas son Google Cloud Security Scanner, Microsoft 365 Defender, Cisco Umbrella y OpenVAS

Juan Manuel Rider Jurado	Esquemas criptográficos vulnerables a algoritmos cuánticos	Miguel Hernández Cáceres	Este Trabajo Fin de Máster plantea la simulación de este procedimiento cuántico para romper estos esquemas clásicos, aplicándolo a ejemplos concretos de estos protocolos. Se busca analizar el impacto de la computación cuántica en la seguridad de los sistemas actuales y evaluar posibles soluciones de criptografía post-cuántica.
Gabriela Mercedes Rodriguez Bonilla	Gestión de las Ciberamenazas: Servicios digitales financieros	Verónica Juliana Caicedo Buitrago	El trabajo se centrará en abordar el desafío de ciberseguridad de prevenir que un atacante altere, intercepte o se interponga en la comunicación de información crítica entre una pasarela de pago y una entidad bancaria. Este problema es de alta relevancia en un mundo digital donde los medios de pago en línea son fundamentales para el crecimiento y alcance de los negocios, especialmente en plataformas web que manejan transacciones financieras sensibles.
Juan Antonio Rodríguez Jiménez	Implementación de NIST Cybersecurity Framework (NIST CSF)	Alba Martínez Gómez	El enfoque principal será crear una guía simplificada para evaluar la implementación del NIST CSF en una entidad de tamaño mediano, realizando un análisis comparativo entre el estado "AS IS" y el estado "TO BE".
Diego Rojas Lorenzo	Seguridad en Cloud: análisis de herramientas de seguridad en cloud gratuitas.	Gonzalo Martínez Ginesta	Este trabajo se centrará en el análisis de diversas herramientas de seguridad en la nube que son gratuitas. Se identificarán los riesgos específicos que estas herramientas cubren, así como la exactitud y confianza que ofrecen. Además, se evaluará la aplicabilidad de estas herramientas en diferentes entornos empresariales. Ejemplos de herramientas a analizar incluyen Google Cloud Security Scanner, Microsoft 365 Defender, Cisco Umbrella y OpenVAS. El objetivo es proporcionar una guía práctica para empresas que buscan implementar soluciones de seguridad en la nube sin incurrir en altos costos.
Alejandro Rubio-Quintanilla Vicedo	Bastionado de una Raspberry Pi para auditoría remota	Alejandro Corletti Estrada	En este trabajo se busca configurar un dispositivo Raspberry Pi con una instalación Kali Linux para la realización de auditorías remotas de la red en la que la Raspberry se encuentre conectada.

Elena Sánchez Carvajal	Convergencia de Seguridad Gestionada y Cumplimiento Normativo: Adaptación a NIS2 y DORA	Elena Mora González	La creciente complejidad del panorama de amenazas cibernéticas y el endurecimiento de regulaciones como NIS2 y DORA han generado un desafío clave para los Proveedores de Servicios de Seguridad Gestionada (MSSP): integrar de manera efectiva la seguridad gestionada con el cumplimiento normativo. Este trabajo analiza la convergencia entre ambas áreas, explorando cómo los MSSP pueden optimizar sus servicios para garantizar la protección de infraestructuras críticas y, al mismo tiempo, cumplir con los requisitos regulatorios. El enfoque de la investigación se basa en identificar los desafíos que enfrentan los MSSP en la adaptación a estas normativas, evaluar estrategias y herramientas para su implementación eficiente y proponer un modelo de alineación entre seguridad gestionada y cumplimiento normativo. A través de este estudio, se busca contribuir a la optimización de los servicios de seguridad, mejorando su capacidad de respuesta ante amenazas y su alineación con marcos regulatorios cada vez más exigentes.
Muhammad Shahid Usman	Seguridad en Cloud: análisis de herramientas de seguridad en Cloud gratuitas.	Gonzalo Martínez Ginesta	El trabajo de fin de master se centrará en el análisis de herramientas de seguridad en la nube gratuitas, mejorando la seguridad en la protección de entornos Cloud contra amenazas comunes. Hoy en día, muchas organizaciones están migrando a la nube, la seguridad de los datos y de la infraestructura se ha convertido en un reto clave, especialmente cuando se depende de soluciones de seguridad gratuitas que no pueden ofrecer la misma cobertura que las opciones comerciales. Este estudio tiene como objetivo proporcionar una evaluación critica de las herramientas de análisis de seguridad en la nube, como Google Cloud Security scanner, Microsoft 365 Defender, Cisco Umbrela y Open VAS, analizando su capacidad para detectar vulnerabilidades, proteger contra ataques y evaluar riesgos en los entornos de Cloud.

Cristhian Torrico Castellón	Protocolos de distribución de claves cuánticas	Miguel Hernández Cáceres	Este trabajo analizará los principales protocolos de distribución de claves cuánticas, sus fundamentos teóricos y sus ventajas en comparación con los métodos tradicionales de intercambio de claves. Se abordarán diferentes esquemas de implementación y los desafíos que enfrenta esta tecnología en la actualidad.
Julia Vidal Rivas	Ciberseguridad personal: Ciberbullying, grooming y redes sociales	Juan Manuel Matalobos Veiga	Este TFM se va a centrar en la temática del ciberbullying, grooming y la utilización de las redes sociales por parte de niños y adolescentes.
Oana Maria Zaharia		Verónica Juliana Caicedo Buitrago	El objetivo principal es investigar y analizar el cumplimiento de las normativas legales en ciberseguridad dentro de las organizaciones, poniendo énfasis en las regulaciones nacionales e internacionales más relevantes. Se estudiará cómo las empresas implementan las normativas, los desafíos que enfrentan y cómo los equipos de ciberseguridad deben colaborar para garantizar el cumplimiento adecuado.

UAX

TFM – MU Online en Inteligencia Artificial

2024 - 2025

Somos
#**UAX**makers

NOMBRE ALUMNO	Título TFM	Breve Resumen	TUTOR ASIGNADO
Anas Zine Boujemaoui	Exploración de estrategias de privacidad y seguridad en aprendizaje federado descentralizado	Analizar las vulnerabilidades de privacidad y seguridad en DFL. Explorar técnicas de preservación de privacidad, como el uso de agregación con DP. Evaluar el impacto de estas técnicas en el rendimiento del modelo y su aplicabilidad a distintos escenarios DFL. Proponer mejoras a los métodos existentes o diseñar un enfoque híbrido que equilibre privacidad y rendimiento	Juan Agustín Fraile
Ane Múgica Urbina	Estrategias de defensa ante ataques engañosos en IA generativa	Los modelos de IA Generativa, como ChatGTP, Gemini o DeepSeek, han demostrado que son muy potentes en generación de texto, imágenes y contenido creativo. Pero estos modelos presentan vulnerabilidades de seguridad que pueden ser explotadas por atacantes para manipular sus respuestas y así, generar contenido dañino o sesgado, y conseguir información en el entrenamiento y backdoor attacks, los cuales pueden comprometer la integridad de los modelos. Aunque ya se ha avanzado en la investigación de los modelos generativos, no existen muchos estudios sobre la evaluación de estas amenazas y propuestas estratégicas efectivas de defensa. Con este TFM, se tratará de responder a la pregunta "¿Qué tipos de ataques engañosos afectan a los modelos generativos y cómo se pueden defender?", con el objetivo de evaluar y mejorar la seguridad en IA Generativa.	Sonia Silva Hidalgo

Belén Sánchez Pardo	Phishing Email detection	El phishing representa una de las amenazas más persistentes y peligrosas en el ámbito de la ciberseguridad, afectando tanto a usuarios individuales como a organizaciones a nivel global. Este tipo de ataque se basa en la ingeniería social para engañar a las víctimas y obtener información confidencial como credenciales de acceso, datos bancarios, etc. Los métodos tradicionales de detección han demostrado ser insuficientes ante la evolución constante de los ataques, ya que presentan limitaciones significativas como la incapacidad de identificar ataques modificados con LLMs. Por lo tanto, es crucial evaluar estos modelos tradicionales y contar con mecanismos de detección más robustos y eficientes. En este contexto, los enfoques basados en IA y aprendizaje automático han surgido como una solución prometedora, permitiendo la identificación de patrones en grandes volúmenes de datos y mejorando la capacidad de detección de ataques desconocidos. Por consiguiente, este trabajo tiene como objetivo evaluar los métodos tradicionales de	Juan Agustín Fraile

		ML con correos reformulados con LLMs y ver la efectividad de estos. Además de probar la efectividad de modelos pre-entrenados como BERT, RoBert, DeBERTA, XLNET, etc. Se analizarán también técnicas de deep learning para identificar la combinación más eficiente en términos de rendimiento y aplicabilidad en escenarios del mundo real.	
Gonzalo Martínez Ginesta	Definición de un programa de trabajo orientado a la revisión de seguridad de despliegues de servicios basados en LLM	Definir un programa de trabajo integral para la revisión de seguridad de despliegues de servicios basados en LLM, que permita identificar y mitigar vulnerabilidades de manera efectiva.	Juan Agustín Fraile
Ibon Bengoechea Cazorla	Robustez de redes neuronales frente a ataques adversariales de evasión mediante entrenamiento adversarial	El desarrollo de modelos de inteligencia artificial ha alcanzado niveles de precisión sin precedentes en tareas como clasificación de imágenes, procesamiento de lenguaje natural y detección de anomalías. Sin embargo, estos modelos son vulnerables a ataques adversariales de evasión, donde pequeñas perturbaciones imperceptibles pueden inducir errores significativos en sus predicciones. Esta vulnerabilidad representa una amenaza en aplicaciones críticas, como la seguridad informática, la conducción autónoma y la medicina, donde la manipulación de datos de entrada puede comprometer la fiabilidad del sistema. Si bien existen diversas estrategias de defensa, el entrenamiento adversarial ha demostrado ser una de las más efectivas para mejorar la robustez de los modelos frente a estos ataques. No obstante, la mayoría de los estudios se han centrado en redes	Angel Rayo

		neuronales completamente conectadas o arquitecturas básicas, dejando abierta la necesidad de analizar el impacto del entrenamiento adversarial en redes más sofisticadas, como las Redes Neuronales Convolucionales (CNN), Redes Neuronales Recurrentes (RNN) y otros modelos avanzados. Este trabajo tiene como objetivo evaluar y mejorar la resistencia de estas arquitecturas frente a ataques adversariales de evasión mediante el uso de técnicas de entrenamiento adversarial.	
Pablo Simon Sainz	Detección Facial basada en Microservicios	Desarrollo de un producto que, basado en metodologías MLOps, permita entrenar y desplegar un modelo de detección facial mediante microservicios.	Óscar Fernández Mora
Rafael Mejia	Reconocimiento de Patrones de Movimiento en Videos	El reconocimiento de patrones de movimiento en videos es un campo de investigación crucial en la visión artificial debido a sus múltiples aplicaciones prácticas. Desde sistemas de vigilancia hasta análisis deportivo y detección de comportamientos anómalos, esta tecnología tiene el potencial de transformar industrias y mejorar la seguridad pública. Sin embargo, el procesamiento eficiente de videos presenta desafíos significativos, como la alta dimensionalidad de los datos, la variabilidad en las condiciones de iluminación, ángulos de cámara y la complejidad computacional asociada con el análisis temporal.	Beatriz Magan

Ricardo David Llorente Valle	Detección y análisis de phishing en correos electrónicos mediante técnicas de Procesamiento de Lenguaje Natural e Inteligencia Artificial	El objetivo de este proyecto es desarrollar un sistema que pueda detectar y analizar correos electrónicos de phishing con la mejor precisión posible, haciendo uso de técnicas de IA y procesamiento de lenguaje natural. Se espera que la solución ayude a identificar este tipo de correos, reduciendo las probabilidades de que un usuario reciba un ataque de este tipo y de ese modo mejorando la seguridad de las organizaciones.	Sonia Silva Hidalgo

UAX

TFG – Grado en Ingeniería Informática e Ingeniería Matemática

2024 - 2025

Somos
#**UAX**makers

Alumno	Tutor	Proyecto
Eloy Sánchez Tamayo	Juan Miguel Aguayo	Análisis y explotación de ataques a Kerberos
Diego Fernández Fernández	Juan Miguel Aguayo	Investigación Forense de un Incidente de Seguridad en un Dominio Windows: Técnicas y Herramientas
David Peinado Díaz	Fernando Rodríguez Sela	Remote Administration Tool
Jorge Alejandro Cadrecha Del Rey	Juan Miguel Gil	Estudio de los Tipos Principales de Ciberataques y Esquemas de Defensa Correspondientes
Juan José Sánchez Cerdera	Fernando Rodríguez Sela	DISEÑO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD BASADO EN HERRAMIENTAS OPEN SOURCE PARA UNA EMPRESA DE TAMAÑO MEDIO
Pablo Tornero Casas	Fernando Rodríguez Sela	Impacto de la Ingeniería Social en la Ciberseguridad
Álvaro Cano Mantero	Juan Miguel Gil	Implementación de la norma ISO/IEC 27001 en la PYME SIC Restauración S.L.
Juan Ramón Rodríguez Cortegoso	Juan Miguel Gil	Honeypots en Redes Domésticas: Seguridad y Privacidad
Pelayo Huerta Mijares	Jorge Calvo Martin (UAX) Ignacio Fernández Rua (Universidad de Oviedo)	Un algoritmo de Shor de forma cuántica para potenciar las vulnerabilidades de la factorización de enteros