| INFORMACIÓN ESPACIO ACADÉMICO | | | | | | |
|---|---|---|---|---|---|---|
| **Nombre de asignatura** | **INTELIGENCIA ARTIFICAL Y SEGURIDAD DE LA INFORMACIÓN** | | | | | |
| **Código** | 11504002 - Electiva IV | | | | | |
| **Definición de asignatura** | ***Obligatorio*** | | ***Básico*** | | ***Complementario*** | |
| | ***Electivo*** | ***X*** | ***Intrínseco*** | ***X*** | ***Extrínseco*** | |
| **Número de créditos** | *3* | *Horas* | 4 | *Semanas* | *16* | |
| **Distribución créditos** | *HTD* | *64* | *HTC* | *32* | *HTA* | 48 |
| | ***Horas de trabajo cooperativo*** | | | | | |
| **Metodología** | • Metodología Pedagógica y Didáctica<br>• Modelo virtual con la plataforma de aprendizaje Interactiva Moodle<br>• Foros en la plataforma virtual<br>• Lecturas (artículos, fragmentos de libros)<br>• Trabajo colaborativo mediante la herramienta Moodle.<br>• Se debe procurar incentivar el trabajo de grupo más que el trabajo individual. (Se recomienda trabajar en grupos de cuatro a cinco estudiantes). | | | | | |

| PROGRAMACIÓN DEL CONTENIDO |
|---|
| **CONOCIMIENTOS PREVIOS** |
| • Tecnologías de la Información (TI)<br>• Estadística Básica<br>• Introducción a la seguridad informática |
| **DESCRIPCIÓN DEL CURSO** |
| En la era digital actual, donde la seguridad de los datos es crucial, la Inteligencia Artificial (IA) se ha convertido en una herramienta esencial para enfrentar los desafíos emergentes en Seguridad Informática. Este curso está diseñado para profesionales de la seguridad y desarrolladores de software que buscan integrar técnicas avanzadas de IA en sus estrategias de seguridad. A lo largo de cuatro unidades, los participantes explorarán cómo la IA puede mejorar la detección de amenazas, la automatización de la respuesta a incidentes, y la seguridad en aplicaciones web y móviles.<br>Desde los fundamentos de la seguridad informática junto con una introducción a la Inteligencia Artificial hasta la aplicación práctica de técnicas de aprendizaje automático y Deep Learning en entornos reales, este curso ofrece una combinación de teoría y práctica.<br>Los participantes aprenderán como desarrollar, probar y desplegar modelos de IA que puedan prevenir, detectar y responder a amenazas de seguridad.<br>Este curso también enfatiza la importancia de la ética y la privacidad en el uso de IA para la seguridad, preparando a los participantes para tomar decisiones informadas y responsables en su práctica profesional. Al final del curso, los estudiantes serán capaces de diseñar e implementar sistemas de seguridad informática potenciados por IA, con una sólida comprensión de sus principios operativos, capacidades y limitaciones. |

**ÁREAS DE CONOCIMIENTO**

En el desarrollo de la asignatura se cubrirán los siguientes temas:

- Aprendizaje automático
- Seguridad Informática

**COMPETENCIAS EN FORMACIÓN**

Al final de la asignatura el estudiante podrá contar con las siguientes competencias:

- Dominio de técnicas y herramientas para recolectar y preparar datos de seguridad, como registros de tráfico de red, logs de sistemas y reportes de incidentes, asegurando la calidad y la integridad de los datos.
- Utilizar herramientas y técnicas para limpiar y transformar datos de seguridad, eliminando inconsistencias y preparando los conjuntos de datos para análisis y modelado.
- Perfeccionar el uso de técnicas estadísticas que son cruciales para el análisis de datos en seguridad informática, como la detección de anomalías y la predicción de incidentes.
- Adquirir un conocimiento avanzado en modelos y algoritmos específicos para la seguridad informática, incluyendo clasificadores, redes neuronales, y técnicas de aprendizaje no supervisado.

**ESTRUCTURA DEL MÓDULO**

**UNIDAD 1. Fundamentos de seguridad informática e introducción a la Inteligencia Artificial (IA)**

| *OBJETIVO DE APRENDIZAJE* | *TÍTULO DE TEMA* |
|---|---|
| Desarrollar habilidades fundamentales en el uso de herramientas de Inteligencia Artificial aplicadas al análisis de datos de Seguridad Informática. | 1.1 Introducción a la Seguridad Informática. |
| | 1.2 Introducción a la Inteligencia Artificial<br>1.2.1 Machine Learning: Aprendizaje supervisado, no supervisado, por refuerzo.<br>1.2.2 Deep Learning Redes Neuronales: Convolucionales, Recurrentes, Antagonistas, de Transformación.<br>1.2.3 Inteligencia Generativa. |
| | 1.3 Herramientas y entornos de desarrollo. |
| | 1.4 Protocolos de Seguridad y Criptografía. |
| | 1.5 Primeros pasos en Machine Learning para Seguridad. |

**UNIDAD 2. Aplicación del Machine Learning (ML) a la Seguridad Informática.**

| *OBJETIVO DE APRENDIZAJE* | *TÍTULO DE TEMA* |
|---|---|
| Fortalecer competencias en técnicas estadísticas y algoritmos de Machine Learning (ML) para la identificación de patrones usados en análisis y predicción de amenazas, Defensa contra ataques automatizados y la evaluación de modelos en sistemas de Seguridad Informática. | 2.1 Análisis de Datos y Preprocesamiento. |
| | 2.2 Detección de anomalías. |
| | 2.3 Detección y Predicción de Amenazas. |
| | 2.4 Defensa automática contra ataques. |
| | 2.5 Evaluación y Validación Modelos. |

**UNIDAD 3. Automatización y Respuesta a Incidentes.**

| *OBJETIVO DE APRENDIZAJE* | *TÍTULO DE TEMA* |
|---|---|
| Desarrollar habilidades para diseñar y automatizar la respuesta a incidentes | 3.1 Introducción a la Respuesta de Incidentes. |
| | 3.2 Automatización y orquestación de la respuesta a incidentes mediante IA y ML. |

| | |
|---|---|
| utilizando algoritmos de aprendizaje automático, mejorando la eficacia de los sistemas de detección y prevención de intrusos. | 3.3. Sistema de Detección y Prevención de Intrusos (IDPS).<br>3.4 Modelos de predicción para detección y respuesta a incidentes. |
| **UNIDAD 4. Seguridad en Aplicaciones Web y Móviles.** | |
| ***OBJETIVO DE APRENDIZAJE*** | ***TÍTULO DE TEMA*** |
| Fortalecer las capacidades para implementar soluciones de Inteligencia Artificial en la seguridad de aplicaciones web y móviles, y explorar las tendencias futuras y desafíos éticos en IA y seguridad. | 4.1 Introducción a la Seguridad en Aplicaciones Web.<br>4.2 IA en Seguridad de Aplicaciones Móviles.<br>4.3 Técnicas avanzadas de protección de datos y privacidad.<br>4.4 Tópicos avanzados del uso de IA en aplicaciones para seguridad Informática.<br>4.4.1 IA Explicable.<br>4.4.2. BlockChain.<br>4.4.3 Quántica, Seguridad Informática e IA |

Tenga en cuenta las siguientes **estrategias de aprendizaje** para el planteamiento de las actividades de evaluación:

- **Estudio autónomo**: lectura y revisión de las unidades, de los recursos tales como videos, lecturas, hipervínculos, investigación, exploración en redes académicas
- **Tutoría:** revisión de clases magistrales virtuales, asistencia a tutoría virtuales presenciales, comunicación con el tutor y aclaración de dudas.
- **Autoevaluaciones:** cuestionarios de evaluación en línea
- **Prácticas:** actividades durante el desarrollo del curso de diferente índole, orientadas a proyectos, problemas, investigación, estudio de caso, entre otras
- **Trabajo final**: elaboración de una actividad que integra lo desarrollado durante el curso, la cual se debe entregar la última semana del curso.
- **Notas**: las actividades se pueden desarrollar tanto individual como grupal, según criterio del docente.

| **EVALUACIÓN** | | |
|---|---|---|
| **TIPO** | **EVALUACIÓN/ACTIVIDAD** | **PORCENTAJE** |
| Formativa | foros: Se anima a la discusión y participación de temas técnicos en un escenario real y se reflexiona sobre los cambios de la Inteligencia Artificial en el escenario de la Seguridad Informática, igual que se analiza como potenciar su uso en incidentes difundidos. | 0% |
| Evaluativa | Trabajo Colaborativo: Se anima al trabajo en grupo para analizar las mejores prácticas. | 10% |
| | laboratorios: Se desarrollan esquemas de programación en Notebook Python para entrenar, evaluar y verificar el comportamiento de modelos de aprendizaje de máquina para la Seguridad Informática. | 60% |
| | Ensayo. Se establece un (1) ensayo individual sobre las implicaciones éticas de la Inteligencia | 5% |
| | Proyecto final. Este proyecto se construirá gradualmente basado en los laboratorios planteados a lo largo de las unidades y en cada una se agregará complejidad de modo que al final será un proyecto terminado y con resultados. | 25% |
| | **Total del curso** | **100 %** |

| BIBLIOGRAFÍA | |
|---|---|
| **1** | Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons Or Opportunities. (2021). Alemania: Springer International Publishing. |
| **2** | Artificial Intelligence for Intrusion Detection Systems. (2023). Estados Unidos: CRC Press. |
| **3** | Bhattacharyya, D. K., Kalita, J. K. (2013). Network Anomaly Detection: A Machine Learning Perspective. Estados Unidos: CRC Press. |
| **4** | Chio, Clarence, and Freeman, David. Machine Learning and Security: Protecting Systems with Data and Algorithms. Estados Unidos, O'Reilly Media, 2018. |
| **5** | Chollet, F. (2021). Deep Learning with Python, Second Edition. Reino Unido: Manning. |
| **6** | Géron, A. (2020). Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems (2nd ed.). O'Reilly Media. |
| **7** | Halder, S., Ozdemir, S. (2018). Hands-On Machine Learning for Cybersecurity: Safeguard Your System by Making Your Machines Intelligent Using the Python Ecosystem. Alemania: Packt Publishing. |
| **8** | *Kim, K., Aminanto, M. E., Tanuwidjaja, H. C. (2018). Network Intrusion Detection Using Deep Learning: A Feature Learning Approach. Singapur: Springer.* |
| **9** | Ortega, J. (2018). Mastering Python for Networking and Security: Leverage Python Scripts and Libraries to Overcome Networking and Security Issues. Reino Unido: Packt Publishing. |
| **10** | Whitman, M. E., Mattord, H. J., Green, A. (2013). Principles of Incident Response and Disaster Recovery (2nd Ed). Cengage Learning. |

| ORGANIZACIÓN / TIEMPOS | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROGRAMA SINTÉTICO** | | **SEMANAS ACADÉMICAS** | | | | | | | | | | | | | | |
| | | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** |
| **1.** | **Unidad 1.** Fundamentos de Seguridad Informática e Introducción a la Inteligencia Artificial (IA) | **X** | **X** | **X** | **X** | | | | | | | | | | | | |
| **2.** | **Unidad 2.** Aplicación de Machine Learning (ML) en la Detección de Anomalías | | | | | **X** | **X** | **X** | **X** | | | | | | | | |
| **3.** | **Unidad 3.** Automatización y Respuesta a Incidentes | | | | | | | | | **X** | **X** | **X** | **X** | | | | |
| **4.** | **Unidad 4.** Seguridad en Aplicaciones Con IA | | | | | | | | | | | | | **X** | **X** | **X** | **X** |

**ELABORÓ**: Azeneth Roza Dicelis
15/11/2024