Instituto Politécnico Nacional

Secretaría Académica
Dirección de Educación Virtual

Secretaría de Investigación y Posgrado
Dirección de Posgrado

SIP-30

Formato para registro de Unidades de aprendizaje 2021

I.- Datos de identificación de la unidad de aprendizaje

Unidad académica:	Multisede (CIC, CIDETEC, ESCOM, ESFM y UPIITA)								
Programa académico:	Doctorado en Ciencia y Tecnología de Inteligencia Artificial y Ciencia de Datos								
	X	Doctorado						Orientación profesional	
		Maestría					X	Orientado a la investigación	
		Especialidad						Con la industria	
								Especialidad médica	
Nombre de unidad de aprendizaje:	Sesión de colegio donde se propuso:		Reunión Ordinaria #				Fecha de propuesta:		dd-mm-yyyy
	Artificial Intelligence and Data Science for Cybersecurity								
	Clave de la unidad de aprendizaje:		**XXXX**				Créditos:	5	*REP 2017*
	Semanas del semestre		18		Horas a la semana:	4		Horas totales:	72
Tipo de unidad de aprendizaje:	Obligatoria:			Optativa:	X		Observaciones:		
	Semestre:		1 - 4						
	Teórica (%):	30		Práctica (%)	40			Teórico-prácticas (%):	30
Área del conocimiento:	Ingeniería y Ciencias Fisicomatemáticas		X	Ciencias Sociales y Administrativas			Ciencias Medico Biológicas		Interdisciplinario
Modalidad no escolarizada:	No escolarizada			Nombre de la Plataforma:					
	Mixta			Presencial (%):	100		En plataforma (%):		
Horas establecidas en el programa de estudios:	Presenciales (si procede) (horas x semana)				4		En plataforma (horas x semana):		

Instituto Politécnico Nacional

Secretaría Académica
Dirección de Educación Virtual

Secretaría de Investigación y Posgrado
Dirección de Posgrado

SIP-30

Formato para registro de Unidades de aprendizaje 2021

I. Aprendizajes que el estudiante deberá demostrar al finalizar

Conocimientos	Habilidades y destrezas	Actitudes y valores
• Inteligencia artificial (IA) y ciencia de datos (CD) aplicados en ciberseguridad. • Herramientas tecnológicas para implementar algoritmos de IA y CD para servicios de ciberseguridad.	• Habilidad para identificar herramientas y algoritmos de IA y CD para ofrecer servicios de ciberseguridad. • Habilidad para utilizar las herramientas tecnológicas de IA y CD para diseñar e implementar servicios de ciberseguridad.	• Aprecio por la dedicación, la concentración y el esfuerzo. • Adaptación a distintos escenarios de actividad de investigación. • Participación crítica y argumentativa. • Pensamiento crítico para la solución de problemas. • Liderazgo en la propuesta de soluciones de problemas y acciones de investigación.

Resolución que aborda la propuesta con su enfoque disciplinar

El objetivo del curso de inteligencia artificial y ciencia de datos para ciberseguridad es dotar a los estudiantes con el conocimiento y las habilidades para identificar, analizar y mitigar las amenazas de seguridad utilizando enfoques basados en ciencia de datos e inteligencia artificial. Este curso también les enseñará a los estudiantes cómo construir y usar modelos de IA con fines de seguridad, tales como detección de intrusos, detección de malware y predicción de ataques. Los estudiantes aprenderán a identificar patrones en grandes conjuntos de datos y utilizarán algoritmos de aprendizaje automático para identificar y responder a amenazas de seguridad. También obtendrán una comprensión de las implicaciones éticas de la inteligencia artificial y la ciencia de datos aplicadas en el campo de la ciberseguridad.

II. Proximidad formativa

Áreas multi, inter y transdisciplinarias	Líneas de Generación y Aplicación de Conocimiento	Sectores sociales

Formato para registro de Unidades de aprendizaje 2021

• Seguridad de la información • Matemáticas para análisis • Modelado e inferencia • Aprendizaje de máquina • Reconocimiento de patrones • Redes neuronales	• Aprendizaje automático • Redes neuronales y aprendizaje profundo • Minería de datos, descubrimiento de conocimiento y analítica avanzada • Procesamiento del lenguaje natural y minería de textos • Reconocimiento de patrones	• La extracción de materias primas (primario), • La manufactura (secundario), • Los servicios (terciario).
Estrategia de asociación: Esta unidad aplica los conocimientos de otras unidades del programa como: fundamentos de IA y CD, Matemáticas para IA y CD, redes neuronales, datos masivos y minería de datos, aprendizaje profundo, por mencionar algunas. Además, estos conocimientos son útiles para su trabajo de tesis que puede impactar en cualquiera de los sectores sociales, líneas y disciplinas mencionadas.		

III Metodología de enseñanza – aprendizaje

Descripción
Enseñanza basada en el estudio de casos. Aprendizaje basado en ejercicios y proyectos

Evidencias como proceso de aprendizaje	Evidencias integradoras (resultados que contribuyen al curriculum)	Ponderación

Formato para registro de Unidades de aprendizaje 2021

Solución de problemas y preguntas Desarrollo de proyectos Exámenes	Tareas Proyectos Exámenes	50% 30% 20%

IV. Descripción de la participación esperada en el estudiante

Receptiva	Resolutiva	Autónoma	Estratégica

Contenido temático

1. Introduction to Artificial Intelligence (AI) and Data Science (DS) for Cybersecurity (8 hours)
   a. Fundamental Concepts of Cybersecurity
   b. Cybersecurity for AI and CD
   c. AI and CD for Cybersecurity
   d. Malicious use of AI
   e. AI in the context of Cybersecurity
2. Exploring common types of cyber-attacks (8 hours)

Formato para registro de Unidades de aprendizaje 2021

a. Phishing
b. Malware
c. Denial of service
d. SQL injection
e. Password attack
    i. Social engineering attacks
f. Man in the middle attack
g. Internet of things attacks

3. AI for network attack detection (8 hours)
    a. Introduction
    b. Network anomaly detection techniques
    c. Classification of network attacks
    d. Botnet topology detection
    e. Machine learning (ML) algorithms for botnet detection
    f. Intrusion detection systems
4. AI Methods for Endpoint Protection (10 hours)
    a. Ransomware detection
    b. Anomaly detection
    c. Real-time behavior analysis
    d. Automated incident response
    e. Multi-factor authentication and access control
5. Detection of malware using AI techniques (12 hours)
    a. Introduction to malware analysis methodology
    b. Detection of malware with machine learning techniques
    c. Implementation of malware detection systems based on machine learning
    d. Evaluation of malware detection systems
    e. Visualization of malware trends
    f. Advanced malware detection with deep learning
    g. Implementation of malware detection systems based on neural networks
6. Fraud prevention with AI solutions (8 hours)
    a. Introduction of fraud detection algorithms
    b. Machine learning for fraud detection

Formato para registro de Unidades de aprendizaje 2021

c. Fraud detection and prevention systems
   i. Expert-led predictive models
   ii. Data-driven predictive models
d. Fraud Detection and Prevention System (FDPS)
e. Predictive analytics for credit card fraud detection

7. Generative Adversarial Networks (GAN) - Attacks and Defenses (10 hours)
   a. Introduction to GANs
   b. Python libraries and tools for GANs
   c. Network attack using model substitution
   d. Intrusion Detection System evasion via GAN
   e. Facial recognition attacks with GAN
8. Evaluation of algorithms (8 hours)
   a. Feature engineering best practices
   b. Performance evaluation of a detector with ROC
   c. How to split data into training and test sets
   d. Using cross validation in machine learning algorithms

V. Secuencia programática

No.	Tema	Objetivo de aprendizaje / competencia específica	Tiempo/Horas/Semanas
1			

Actividad(es):	No. Nombre de la actividad: Descripción de la actividad:	Tipo de interacción(es):	
		Referencias (s):	

Formato para registro de Unidades de aprendizaje 2021

Evidencia(s):	

Tipo de interacción: ID–Instrucción directa, TC–Trabajo colaborativo, AC–Análisis en campo, RP–Reflexión personal, PE–Presentación expositiva

Indicar solo el número de las *Referencias* indizadas en la sección VII de este documento.

Nota: Replique esta sección las veces que sea necesario para cubrir toda la secuencia programática

VI. Habilitadores tecnológicos

	Disposiciones	Especificaciones / descripción de efectos
	Conectividad	
	Habilidades digitales	
	Interoperabilidad	
	Datos abiertos	
	Big Data	
	Machine Learning	
	Simulación	
	Realidad aumentada	
	Otro…	

VII. Referencias

Conferencias magistrales	Notas complementarias
1. Xin, Yang, et al. "Machine learning and deep learning methods for cybersecurity. IEEE Access 6 (2018): 35365-35381.	
2. Prasad, Ramjee, et al. "Artificial intelligence and machine learning in cyber security." Cyber security: the lifeline of information and communication technology (2020): 231-247.	

Formato para registro de Unidades de aprendizaje 2021

Documentales / electrónicas

1. Parisi, Alessandro. *Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies*. Packt Publishing Ltd, 2019.
2. Clarence, Chio and Freeman, David. *Machine learning and security: Protecting systems with data and algorithms*. O'Reilly Media, Inc., 2018.
3. Saxe, Joshua, and Hillary Sanders. *Malware data science: attack detection and attribution*. No Starch Press, 2018.
4. Kamhoua, Charles A., et al., eds. *Game theory and machine learning for cyber security*. John Wiley & Sons, 2021.
5. Alla S, Adari SK. *Beginning anomaly detection using python-based deep learning*. New Jersey: Apress; 2019.

VIII. Créditos y responsivas

	Responsabilidad	Nombre completo	Clave de nombramiento /No. de empleado
	Coordinador (Autor)	Ponciano Jorge Escamilla Ambrosio	17132-ED-23

Instituto Politécnico Nacional

Secretaría Académica
Dirección de Educación Virtual

Secretaría de Investigación y Posgrado
Dirección de Posgrado

SIP-30

Formato para registro de Unidades de aprendizaje 2021

	Participante (Coautor)	Abraham Rodríguez Mota	16822-EC-2022/2000593
	Participante (Coautor)	Gina García Gallegos	16939-EF-2022
	Asesor didáctico / Diseñador Instruccional		
	Tecnólogo educativo / Comunicólogo		
	Corrector de estilo		
	Programador multimedia / Diseñador gráfico		
Otro…			

VERIFICACIÓN GENERAL DE LA PLANEACIÓN DIDÁCTICA	REVISIÓN DE LA PLANEACIÓN DIDÁCTICA (VIABILIDAD)
Por la División de Operación y Promoción al Posgrado de la SIP Nombre_____ FIRMA_____	Por la Subdirección de Diseño y Desarrollo de la DEV Nombre_____ FIRMA_____

VERIFICACIÓN PARA SU PUESTA EN OPERACIÓN	REVISIÓN TÉCNICO-PEDAGÓGICA PARA LA MODALIDAD
Por la Dirección de Posgrado Nombre_____ FIRMA_____ SELLO DE VALIDACIÓN	Por la Dirección para la Educación Virtual Nombre_____ FIRMA_____

Instituto Politécnico Nacional

Secretaría Académica
Dirección de Educación Virtual

Secretaría de Investigación y Posgrado
Dirección de Posgrado

SIP-30

Formato para registro de Unidades de aprendizaje 2021
