



Formato para registro de Unidades de aprendizaje 2021

I.- Datos de identificación de la unidad de aprendizaje

Unidad académica:	Multisede (CIC, CIDETEC, ESCOM, ESFM, UPIITA)									
Programa académico:	Maestría en Ciencia y Tecnología de Inteligencia Artificial y Ciencia de Datos									
	Doctorado				Orientación profesional					
X	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		
	Ciberseguridad para Inteligencia Artificial y Ciencia de Datos									
Tipo de unidad de aprendizaje:	Clave de la unidad de aprendizaje:		XXXX			Créditos:		5		REP 2017
	Semanas del semestre		18	Horas a la semana:		4	Horas totales:		72	
	Obligatoria:				Optativa:	X	Observaciones:			
	Semestre:	1 - 3								
	Teórica (%):	30		Práctica (%):	40		Teórico-prácticas (%):		30	
Área del conocimiento:	Ingeniería y Ciencias Fisicomatemáticas		X	Ciencias Sociales y Administrativas		Ciencias Médico Biológicas		Interdisciplinario		
	No escolarizada				Nombre de la Plataforma:					



Formato para registro de Unidades de aprendizaje 2021

Modalidad no escolarizada:	Mixta		Presencial (%):	100	En plataforma (%):	
Horas establecidas en el programa de estudios:	Presenciales (si procede) (horas x semana)			4	En plataforma (horas x semana):	



Formato para registro de Unidades de aprendizaje 2021

I. Aprendizajes que el estudiante deberá demostrar al finalizar

Conocimientos	Habilidades y destrezas	Actitudes y valores
<ul style="list-style-type: none"> Fundamentos de ciberseguridad aplicada a IA y CD. Herramientas tecnológicas para implementar servicios de ciberseguridad. 	<ul style="list-style-type: none"> Habilidad para identificar servicios de ciberseguridad requeridos en el desarrollo e implementación de soluciones de inteligencia artificial y ciencia de datos. Habilidad para utilizar las herramientas tecnológicas para diseñar e implementar servicios de ciberseguridad en soluciones de IA y CD. 	<ul style="list-style-type: none"> 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 ciberseguridad para inteligencia artificial y ciencia de datos es dotar a los estudiantes del conocimiento, las habilidades y la experiencia práctica necesaria para diseñar, implementar y mantener sistemas seguros que utilicen inteligencia artificial y ciencia de datos. Los estudiantes obtendrán una comprensión de las implicaciones éticas y legales de la inteligencia artificial y la ciencia de datos, así como los fundamentos de la criptografía, los protocolos de seguridad, la autenticación y el control de acceso. El curso también cubrirá temas como la seguridad de los datos en la nube, la seguridad de la red y las tecnologías emergentes, como la computación cuántica. Los estudiantes adquirirán las habilidades para desarrollar sistemas seguros, evaluar riesgos y crear arquitecturas seguras para aplicaciones de inteligencia artificial y ciencia de datos.

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

<ul style="list-style-type: none"> • Seguridad de la información • Matemáticas para análisis • Modelado e inferencia • Aprendizaje de máquina • Reconocimiento de patrones 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • La extracción de materias primas (primario), • La manufactura (secundario), • Los servicios (terciario).
<p>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.</p>		

III Metodología de enseñanza – aprendizaje

Descripción
<p>Enseñanza basada en el estudio de casos. Aprendizaje basado en ejercicios y proyectos</p>

Evidencias como proceso de aprendizaje	Evidencias integradoras (resultados que contribuyen al curriculum)	Ponderación
<p>Solución de problemas y preguntas Desarrollo de proyectos Exámenes</p>	<p>Tareas Proyectos Exámenes</p>	<p>50% 30% 20%</p>



Formato para registro de Unidades de aprendizaje 2021

IV. Descripción de la participación esperada en el estudiante

Receptiva	Resolutiva	Autónoma	Estratégica

Contenido temático

1. Introducción a la Ciberseguridad para Inteligencia Artificial (AI) y Ciencia de Datos (CD) (8 horas)
 - a. Conceptos Fundamentales de Ciberseguridad
 - b. Ámbito de la ciberseguridad
 - c. Servicios de la ciberseguridad
 - d. Riesgos de ciberseguridad en IA y CD
2. Manejo seguro de datos (10 horas)
 - a. Ciclo de vida de los datos
 - b. Cifrado de datos
 - c. Control de acceso a datos
 - d. Minimización de datos
 - e. Visualización segura de datos
 - f. Distribución segura de datos
3. Ataques de adversario y mitigación (10 horas)
 - a. Ataque de envenenamiento
 - b. Ataque de evasión o exploratorios



Formato para registro de Unidades de aprendizaje 2021

- c. Ataque de extracción
- d. Ataque de inversión
- e. Redes adversarias generativas
- f. Defensa mediante detección de anomalías
- g. Defensa mediante pruebas robustas
- 4. Prácticas seguras para desarrollo de sistemas IA y CD (12 horas)
 - a. Modelo de amenazas y revisión del diseño
 - b. Análisis estático
 - c. Pruebas de seguridad y revisión del código
 - d. Evaluación de la seguridad y configuraciones seguras
 - e. Evaluación del riesgo
- 5. Seguridad en Big Data (12 horas)
 - a. Seguridad en datos no transaccionales
 - b. Almacenamiento seguro de datos y logs de transacciones
 - c. Monitoreo de seguridad y cumplimiento en tiempo real
 - d. Preservación de la privacidad de los datos
 - e. Control de acceso granular
- 6. Privacidad y ética (10 horas)
 - a. Regulaciones de privacidad
 - b. Sesgos, juicio justo y soporte legal de la ciberseguridad
 - c. Uso responsable de la IA y CD
 - d. Evolución de la ética en la IA y CD
 - e. Retos en la definición y en la práctica
- 7. Tendencias (10 horas)
 - a. Impacto del cómputo cuántico
 - b. Criptografía para IA y CD
 - c. Seguridad de datos en la nube
 - d. Procesamiento de datos seguros
 - e. Aprendizaje de máquina preservando la privacidad
 - f. Limitaciones y direcciones futuras



Formato para registro de Unidades de aprendizaje 2021

--

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):	
Evidencia(s):			Referencias (s):	

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

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

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

VI. Habilitadores tecnológicos

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



Formato para registro de Unidades de aprendizaje 2021

VII. Referencias

Conferencias magistrales

1. How to make AI hack-proof - 3 questions. https://youtu.be/9B2jKXGUZtc
2. Cybersecurity of AI powered systems - BDVA, Big Data Value. https://youtu.be/YzKJvQ1XBh4
3. Comiter, M. Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It. Harvard Kennedy School. 2019.

Notas complementarias



Formato para registro de Unidades de aprendizaje 2021

Documentales / electrónicas

1. Gibian, D. Hacking Artificial Intelligence: A leader’s guide from deepfakes to breaking deep learning. Rowan & Littlefield Publishers. 2022
2. Thames, L. y Schaefer, D. Cybersecurity for Industry 4.0. analysis for Design and Manufacturing. Springer 2017.
3. Ijlal, T. Artificial Intelligence (AI) Governance and Cyber-Security: A beginner’s handbook on securing and governing AI systems. 2022
4. Priyadarshini, I., y Sharma, R. Editores. Artificial Intelligence and Cybersecurity: advances and Innovations. CRC Press 2022.
5. Reznik, Leon. Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work for and Against Computer Security. John Wiley & Sons, 2021.
6. Mongeau, S. y Hajdasinski, A. Cybersecurity Data Science, Best Practices in an Emerging Profession. Springer 2021
7. Alla, S. y Adari, S.K. Beginning anomaly detection using python-based deep learning. Apress 2019
8. Saxe, J. y Sanders, Hillary. Malware Data Science: Attack Detection and Attribution. No starch press 2018
9. SANS. SEC595: Applied Data Science and Machine Learning for Cybersecurity Professional. https://www.sans.org/cyber-security-courses/applied-data-science-machine-learning/
10. INCIBE. Minería de Datos, Big Data y Seguridad. https://www.incibe.es/protege-tu-empresa/blog/mineria-datos-big-data-seguridad

VIII. Créditos y responsabilas

Responsabilidad	Nombre completo	Clave de nombramiento /No. de empleado
Coordinador (Autor)	Abraham Rodríguez Mota	16822-EC-2022



Formato para registro de Unidades de aprendizaje 2021

Participante (Coautor)	Ponciano Jorge Escamilla Ambrosio	17132-ED-23
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

--	--