



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			
	Sesión de colegio donde se propuso:		Reunión Ordinaria #				Fecha de propuesta:		dd-mm-yyyy	
Nombre de unidad de aprendizaje:	Cybersecurity for Artificial Intelligence and Data Science									
	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 - 3							
	Teórica (%):		30		Práctica (%):		40		Teórico-prácticas (%): 30	
Área del conocimiento:	Ingeniería y Ciencias Fisicomatemáticas		X		Ciencias Sociales y Administrativas				Ciencias Médico Biológicas	
									Interdisciplinario	



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

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):	



Formato para registro de Unidades de aprendizaje 2021

I. Aprendizajes que el estudiante deberá demostrar al finalizar

Conocimientos	Habilidades y destrezas	Actitudes y valores
• Fundamentos de ciberseguridad aplicada a IA y CD. • Herramientas tecnológicas para implementar servicios de ciberseguridad.	• 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.	• 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

• Seguridad de la información • Matemáticas para análisis • Modelado e inferencia • Aprendizaje de máquina • Reconocimiento de patrones	• 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
Solución de problemas y preguntas Desarrollo de proyectos Exámenes	Tareas Proyectos Exámenes	50% 30% 20%



Formato para registro de Unidades de aprendizaje 2021

IV. Descripción de la participación esperada en el estudiante

Receptiva	Resolutiva	Autónoma	Estratégica

Contenido temático

1. Introduction to Cybersecurity for Artificial Intelligence (AI) and Data Science (DS) (8 hours)
 - a. Fundamental Concepts of Cybersecurity
 - b. Cybersecurity Scope
 - c. Cybersecurity services
 - d. Cybersecurity risks in AI and DS
2. Secure data management (10 hours)
 - a. Data life cycle
 - b. Data encryption
 - c. Data access control
 - d. Data minimization
 - e. Secure data visualization
 - f. Secure data distribution
3. Adversarial Attacks and Mitigation (10 hours)
 - a. Data poisoning attack
 - b. Evasion or exploratory attack
 - c. Extraction attack



Formato para registro de Unidades de aprendizaje 2021

- d. Inversion attack
- e. Generative Adversarial Networks
- f. Defense through anomaly detection
- g. Defense through robust evidence
- 4. Safe practices for development of AI and DS systems (12 hours)
 - a. Threat model and design review
 - b. Static analysis
 - c. Security testing and code review
 - d. Security assessment and secure configurations
 - e. Risk assessment
- 5. Security in Big Data (12 hours)
 - a. Non-transactional data security
 - b. Secure storage of data and transaction logs
 - c. Real-time security and compliance monitoring
 - d. Preservation of data privacy
 - e. Granular access control
- 6. Privacy and ethics (10 hours)
 - a. Privacy regulations
 - b. Bias, fair trial and legal support of cybersecurity
 - c. Responsible use of AI and DS
 - d. Evolution of ethics in AI and DS
 - e. Challenges in definition and in practice
- 7. Trends (10 hours)
 - a. The impact of quantum computing
 - b. Cryptography for AI and DS
 - c. Data security in the Cloud
 - d. Secure data processing
 - e. Machine learning and privacy preservation
 - f. Limitations and future directions



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):	
			Referencias (s):	
Evidencia(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	
Big Data	
Machine Learning	
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 responsabilidades

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

Por la División de Operación y Promoción al Posgrado de la SIP

Nombre _____

FIRMA _____

REVISIÓN DE LA PLANEACIÓN DIDÁCTICA (VIABILIDAD)

Por la Subdirección de Diseño y Desarrollo de la DEV

Nombre _____

FIRMA _____

VERIFICACIÓN PARA SU PUESTA EN OPERACIÓN

Por la Dirección de Posgrado

Nombre _____

FIRMA _____

SELLO DE VALIDACIÓN

REVISIÓN TÉCNICO-PEDAGÓGICA PARA LA MODALIDAD

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

--	--