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

INSTRUCTIVO para el correcto llenado del formato SIP-30

- El formato SIP-30 es un formato digital el cual puede ser completado con un procesador de texto y guardarse como archivo PDF para su envío.
- Adicionalmente será necesario anexar la solicitud firmada por el director de la Unidad Académica respectiva y el acuerdo de Colegio donde se avaló su registro; tenga listos los archivos al momento de ingresar su solicitud en el formulario en línea.
- El enlace de atención única para esta y otras gestiones es: https://forms.office.com/r/c8DLS6VBv1 (copie y pegue en un navegador web si el enlace no funciona)

- Tome en cuenta los criterios establecidos en el Reglamento de Estudios de Posgrado (REP 2017) para el llenado de este formato, a continuación se presentan algunas definiciones útiles:
  - *Número de semanas por semestre del programa:* Es el número de semanas lectivas efectivas al semestre, indicadas en el acuerdo de creación del programa académico o en alguna actualización posterior del programa. En caso de haber tenido una actualización en este sentido, la misma deberá haber sido presentada y avalada en reunión del Colegio de Profesores de la Unidad Académica, además de haber sido aprobada por la SIP. El rango de semanas lectivas al semestre es mínimo 15 y máximo 18.
  - *Tipo de horas:* Las unidades de aprendizaje, en cuanto a las horas asignadas, están clasificadas como: Teóricas, Prácticas y Teórico-prácticas. Estas denominaciones son excluyentes, es decir, las unidades de aprendizaje solo pueden ser de un solo tipo, no pueden tener horas combinadas.
  - *Número de horas – semana:* Es el número de horas asignadas para ser impartida la Unidad de Aprendizaje a la semana.
  - *Total de horas al semestre:* Es el número de horas totales a impartir de la Unidad de Aprendizaje al semestre. Se calcula multiplicando Número de semanas por número de horas-semana.
  - *Créditos* (Reglamento de Estudios de Posgrado 2017): FÓRMULA DE CÁLCULO: 16 hrs. = 1 crédito (horas totales / 16), no deben asignarse fracciones, los créditos deben redondearse a número entero.

- Para el registro de unidades de aprendizaje de modalidad no escolarizada o mixta incluya adicionalmente los campos marcados con el color azul
- En todos los campos existen comentarios en forma de 🗨 globo que sirven de ayuda para el requisitado correspondiente, en caso de duda solicite apoyo del asesor didáctico de la UTEyCV de su Unidad Académica.

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:	Centro de Investigación en Computación								
Programa académico:	Maestría en Ciencias de la Computación								
		Doctorado				Orientación profesional			
	x	Maestría			x	Orientado a la investigación			
		Especialidad				Con la industria			
						Especialidad médica			
	Sesión de colegio donde se propuso:	7ª. Ordinaria			Fecha de propuesta:	13/07/2022			
Nombre de unidad de aprendizaje:	**Análisis de Datos para la Ciberseguridad**								
	Clave de la unidad de aprendizaje:				Créditos:	5	*REP 2017*		
	Semanas del semestre	18	Horas a la semana:	4	Horas totales:	72			
Tipo de unidad de aprendizaje:	Obligatoria:		Optativa:		Observaciones:				
	Semestre:	2							
	Teórica (%):	60	Práctica (%)	40	Teórico-prácticas (%):	100			
Área del conocimiento:	Ingeniería y Ciencias Fisicomatemáticas	X	Ciencias Sociales y Administrativas		Ciencias Medico Biológicas		Interdisciplinario		
Modalidad no escolarizada:	No escolarizada		En Nombre de la Plataforma:						
	Mixta		Presencial (%):		En plataforma (%):				
Horas establecidas en el programa de estudios:	Presenciales (si procede) (horas x semana)				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
● Principales fuentes de información y sus formatos para el análisis de aspectos de seguridad. ● Planteamiento de procesos de extracción, selección y análisis de datos orientados a la ciberseguridad ● Principales algoritmos de análisis de datos y su aplicación para el análisis y detección de amenazas cibernéticas. ● Evaluación de resultados mediante métricas y parámetros propios de la disciplina. ● Programación para el análisis de datos empleando el lenguaje de programación Python.	● Selección de fuentes de datos para la ciberseguridad ● Uso de técnicas para la extracción de datos ● Uso de técnicas para el tratamiento de datos ● Selección de algoritmos de análisis de datos ● Interpretación de resultados dentro del contexto del análisis de la ciberseguridad ● Análisis de resultados desde la perspectiva de ciberseguridad ● Habilidades avanzadas en programación con lenguaje Python ● Presentación de resultados de análisis de datos para aplicaciones de ciberseguridad.	● Apertura para contrastar opiniones y resultados fundamentados en procesos estructurados de análisis. ● Objetividad para la selección de fuentes, algoritmos y técnicas de procesamiento de datos relativos al área de la ciberseguridad ● Honestidad en la evaluación de resultados mediante el empleo de métricas pertinentes. ● Integridad en la recopilación, manejo, distribución, resguardo y procesamiento de datos.

Resolución que aborda la propuesta con su enfoque disciplinar

La alta disponibilidad de dispositivos que capturan, almacenan, procesan y transportan datos digitales, ya sea a través del Internet u otras redes de comunicación masiva como la telefonía y las señales de radio, presenta un reto de gran dimensión para los análisis de ciberseguridad; tanto por la gran variedad de datos como por la cantidad inmensa de los mismos. De esta manera, en este curso se busca dotar a los alumnos con el conocimiento básico para el tratamiento y análisis de datos dentro del contexto de la ciberseguridad, diferenciándose de un curso de ciencia de datos principalmente en el enfoque que busca permitir al participante conocer a mayor detalle los tipos de documentos o registros más comunes (archivos log, tráfico de red, archivos de código de malware, etc.) empleados para el análisis de ciberseguridad, junto con las técnicas más empleadas en herramientas y controles ciberseguridad. Así, al término del curso, el alumno será capaz de valorar de manera objetiva el uso de distintos algoritmos de análisis de datos, lo que será fundamental para el desarrollo de su proyecto de tesis, ya sea mediante el uso de los algoritmos o como base teórica para el análisis de propuestas de otros autores dentro del estado del arte. Adicionalmente, a través del análisis de casos de uso se espera fortalecer la práctica tanto en el desarrollo de programas orientados al análisis de datos como a mecanismos o actividades orientadas a fortalecer la seguridad de los sistemas dentro de su práctica profesional.

Formato para registro de Unidades de aprendizaje 2021

II. Proximidad formativa

Áreas multi, inter y transdisciplinarias	Líneas de Generación y Aplicación de Conocimiento	Sectores sociales
● Ciberseguridad ● Análisis de redes ● Análisis y prueba de software ● Ciencia de Datos ● OSINT	● Ciencia y tecnología de la Información ● Inteligencia Artificial y Cómputo Científico	● Industrial ● Doméstico ● Banca y Comercio ● Infraestructura Crítica ● Seguridad Nacional

Estrategia de asociación:
El uso de casos de estudio busca facilitar la asociación de los conocimientos adquiridos con procesos o sistemas reales, facilitando también la aplicación de los conocimientos a los trabajos de tesis y a la discusión de los resultados, permitiendo a los alumnos un acercamiento a la realidad de la industria y otros sectores que requieren servicios de ciberseguridad soportados en el análisis de datos.

III Metodología de enseñanza – aprendizaje

Descripción

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

Formato para registro de Unidades de aprendizaje 2021

IV. Descripción de la participación esperada en el estudiante

Receptiva	Resolutiva	Autónoma	Estratégica

Formato para registro de Unidades de aprendizaje 2021

Contenido temático

1. El análisis de datos en el Dominio de la Ciberseguridad 1.1 Análisis de anomalías en ciberseguridad 1.2 Análisis de paquetes de red 1.3 Análisis estático y dinámico de malware 1.4 Honeypots y análisis de datos 1.5 OSINT	8 horas
2. Fundamentos del análisis de datos 2.1 Tipos de Datos 2.1.1 Datos estructurados y Datos no estructurados 2.1.2 Datos estáticos y datos dinámicos 2.1.3 Archivos, logs y paquetes de red 2.1.4 Tipos de base de datos de ciberseguridad 2.1.5 Obtención de los datos de ciberseguridad 2.1.6 Calidad de los datos de ciberseguridad 2.2 Métodos y Técnicas de preparación de los datos 2.2.1 Inferencia Estadística 2.2.2 Análisis exploratorio de datos 2.2.3 Extracción de características	20 horas
3. Técnicas y métodos de aprendizaje máquina 3.1 Modelos de aprendizaje no supervisado 3.1.1 Clustering 3.2 Modelos de aprendizaje supervisado 3.2.1 Modelos Lineales Generalizados 3.2.2 Vecinos más Cercanos 3.2.3 Árboles de Decisión	32 horas

Formato para registro de Unidades de aprendizaje 2021

3.2.4 Bosques Aleatorios 3.2.5 Máquinas de Vectores de Soporte 3.2.6 Naïve Baye 3.3 Métricas de Evaluación 3.4 Métodos de Ensamble 3.5 Redes neuronales 3.6 Aprendizaje profundo	
4. Casos de Estudio 5.1 Análisis de Malware 5.2 Análisis de patrones anómalos en redes de comunicación 5.3 Detección de fraude	12 horas

Formato para registro de Unidades de aprendizaje 2021

V. Secuencia programática

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

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

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	

Formato para registro de Unidades de aprendizaje 2021

	Realidad aumentada	
	Otro…	

VII. Referencias

Conferencias magistrales

1. Applied Data Science and Machine Learning for Cybersecurity SANS Tactical Detection Summit 2018. https://youtu.be/m2AgYbbXz8k
2. Artificial Intelligence: A Silver Bullet in Cyber Security? CPX 360 Keynote. https://youtu.be/ggje-L0ViFM
3. Malware analysis Part 1. https://youtu.be/d4d8VRsk4-0
4. Machine Learning for Cybersecurity. https://youtu.be/cpCKhhV1wQU

Notas complementarias

Notas y presentaciones de clase

Documentales / electrónicas

5. Mongeau, S. y Hajdasinski, A. Cybersecurity Data Science, Best Practices in an Emerging Profession. Springer 2021
6. Alla, S. y Adari, S.K. Beginning anomaly detection using python-based deep learning. Apress 2019
7. Saxe, J. y Sanders, Hillary. Malware Data Science: Attack Detection and Attribution. No starch press 2018
8. SANS. SEC595: Applied Data Science and Machine Learning for Cybersecurity Professional. https://www.sans.org/cyber-security-courses/applied-data-science-machine-learning/
9. INCIBE. Minería de Datos, Big Data y Seguridad. https://www.incibe.es/protege-tu-empresa/blog/mineria-datos-big-data-seguridad

Formato para registro de Unidades de aprendizaje 2021

10. Sarker, I.H., et al. Cybersecuroty data science: an overview from machine learning perspective. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00318-5

VIII. Créditos y responsivas

Responsabilidad		Nombre completo	Clave de nombramiento /No. de empleado
	Coordinador (Autor)	Dr. Abraham Rodríguez Mota	2000593
	Participante (Coautor)		
	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

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

Por la Dirección de Posgrado	Por la Dirección para la Educación Virtual
Nombre_____	Nombre_____
FIRMA_____	FIRMA_____
SELLO DE VALIDACIÓN	