INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

PROGRAMA SINTÉTICO

UNIDAD ACADÉMICA: ESCUELA SUPERIOR DE CÓMPUTO, UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA, CAMPUS ZACATECAS	
PROGRAMA ACADÉMICO: Ingeniería en Sistemas Computacionales	
UNIDAD DE APRENDIZAJE: Computer Security	**SEMESTRE:** VI

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Implementa mecanismos de seguridad informática a partir de medidas y controles de monitorización, dispositivos de conectividad y arquitecturas de seguridad.

CONTENIDOS:

I. Seguridad ofensiva
II. Seguridad defensiva
III. Administración de la seguridad
IV. Monitorización y arquitecturas de seguridad

ORIENTACIÓN DIDÁCTICA:	**Métodos de enseñanza**		**Estrategias de aprendizaje**	
	a) Inductivo		**a) Estudio de Casos**	**X**
	b) Deductivo		**b) Aprendizaje Basado en Problemas**	
	c) Analógico		**c) Aprendizaje Orientado a Proyectos**	
	d) Heurístico	**X**		

EVALUACIÓN Y ACREDITACIÓN:				
	Diagnóstica	**X**	**Saberes Previamente Adquiridos**	**X**
	Solución de casos	**X**	**Organizadores gráficos**	
	Problemas resueltos		**Problemarios**	
	Reporte de proyectos		**Exposiciones**	
	Reportes de indagación		**Otras evidencias a evaluar:** Las que correspondan	
	Reportes de prácticas	**X**		
	Evaluación escrita	**X**		

BIBLIOGRAFÍA BÁSICA:

Autor(es)	Año	Título del documento	Editorial / ISBN
Bejtlich, R.	*2013	The Practice of Network Security Monitoring: Understanding Incident Detection and Response	Non Starch Press/ 9781593275099
Brotherston, L & Berlin, A.	2017	Defensive Security Handbook	O'Reilly Media, Inc/ 9781491960387
Bullock, J. & Parker, J.	2017	Wireshark for Security Professionals: Using Wireshark and Metasploit Framework	John Wiley & Sons/ 9781118918227
OccupyTheWeb	2018	Linux basics for hackers: getting started with networking, scripting, and security in Kali	Non Starch Press/ 978-1-59327-855-7
Oriyano, S.	2016	Penetration Testing Essentials	John Wiley & Sons/ 9781119235330

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

PROGRAMA DE ESTUDIOS

UNIDAD DE APRENDIZAJE: Computer Security **HOJA** 2 **DE** 7

UNIDAD ACADÉMICA: ESCUELA SUPERIOR DE CÓMPUTO, UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA, CAMPUS ZACATECAS		
PROGRAMA ACADÉMICO: Ingeniería en Sistemas Computacionales		
SEMESTRE: VI	**ÁREA DE FORMACIÓN:** Profesional	**MODALIDAD:** Escolarizada
TIPO DE UNIDAD DE APRENDIZAJE: Teórica-Práctica/ Obligatoria		
VIGENTE A PARTIR DE: Agosto 2022	**CRÉDITOS:**	
	TEPIC:7.5	**SATCA:** 6.3

INTENCIÓN EDUCATIVA

La unidad de aprendizaje contribuye al perfil de egreso de la Ingeniería en Sistemas Computacionales, proporcionando los conocimientos sobre la aplicación de los sistemas de seguridad necesarios para dar al equipo de seguridad la posibilidad de defenderse de forma controlada y constructiva de ataques, mitigar los riesgos, así como la capacidad de generar propuesta de soluciones y establecimiento de medidas de detección de ataques, elaborando los controles de seguridad necesarios para disminuir el riesgo de amenazas internas y externas en la organización y para la recopilación, análisis y notificación de indicaciones, para ayudar a detectar y responder a las intrusiones. Asimismo, desarrolla habilidades transversales como el pensamiento estratégico, el pensamiento creativo, el trabajo colaborativo y participativo y comunicación asertiva.

Esta unidad de aprendizaje se relaciona de manera antecedente con Redes de computadoras y Sistemas operativos; de forma lateral con Aplicaciones para comunicaciones en red; y de forma consecuente con IT Governance y Administración para servicios en red.

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Implementa mecanismos de seguridad informática a partir de medidas y controles de monitorización, dispositivos de conectividad y arquitecturas de seguridad.

TIEMPOS ASIGNADOS

HORAS TEORÍA/SEMANA: 3.0

HORAS PRÁCTICA/SEMANA: 1.5

HORAS TEORÍA/SEMESTRE: 54.0

HORAS PRÁCTICA/SEMESTRE: 27.0

HORAS APRENDIZAJE AUTÓNOMO: 24.0

HORAS TOTALES/SEMESTRE: 81.0

UNIDAD DE APRENDIZAJE REDISEÑADA POR: Academia de Sistemas Distribuidos

REVISADA POR:

M. en C. Iván Giovanny Mosso García
Subdirección Académica ESCOM/UPIIZ

APROBADA POR:
Consejo Técnico Consultivo Escolar

M. en C. Andrés Ortigoza Campos

Dr. Fernando Flores Mejía
Presidente del CTCE de ESCOM/UPIIZ

dd/mm/aaaa

APROBADO POR: Comisión de Programas Académicos del Consejo General Consultivo del IPN.

dd/mm/aaaa

AUTORIZADO Y VALIDADO POR:

Mtro. Mauricio Igor Jasso Zaranda
Director de Educación Superior

UNIDAD TEMÁTICA I Seguridad ofensiva	CONTENIDO	HORAS CON DOCENTE		HRS AA
		T	P	
UNIDAD DE COMPETENCIA Realiza procesos de emulación de escenarios de amenazas de seguridad informática, con base en pruebas de penetración.	1.1 Fundamentos para la seguridad 1.1.1. Seguridad en Linux 1.1.2. Seguridad en Windows 1.1.3. Seguridad en Red	3.0	1.0	3.0
	1.2 Pruebas de penetración en escenarios de amenazas 1.2.1 Análisis de vulnerabilidades 1.2.2 Técnicas para la intrusión 1.2.3 Ataques de suplantación de identidad 1.2.4 Técnicas para escalar privilegios 1.2.5 Persistencia 1.2.6 Elaboración de reportes	10.5	6.5	3.0
	Subtotal	13.5	7.5	6.0

UNIDAD TEMÁTICA II Seguridad defensiva	CONTENIDO	HORAS CON DOCENTE		HRS AA
		T	P	
UNIDAD DE COMPETENCIA Implementa planes de actuación con base en la monitorización de los sistemas, análisis forense y reportes ejecutivos.	2.1 Gestión de planes de actuación para amenazas y vulnerabilidades	3.0		1.0
	2.2 Operaciones y monitoreo de seguridad de los sistemas	1.5		1.5
	2.3 Respuesta a incidentes de seguridad	3.0	3.0	
	2.4 Análisis forense y de Malware	4.0	1.5	1.0
	2.5 Generación de reportes ejecutivos	2.0	1.5	1.5
	Subtotal	13.5	6.0	5.0

UNIDAD TEMÁTICA III Administración de la seguridad	**CONTENIDO**	**HORAS CON DOCENTE**		**HRS AA**
		T	**P**	
UNIDAD DE COMPETENCIA Gestiona un programa de seguridad de la información con base en la normatividad y modelos organizativos.	3.1 Estrategias, normatividad de la seguridad y planes de acción	2.0	3.0	1.5
	3.2 Manejo y administración de las vulnerabilidades	3.5	1.5	1.5
	3.3 Generación de informes y reportes de alta dirección	2.0		1.5
	3.4 Respuesta ante incidente de seguridad informática	3.0	1.5	
	3.5 Modelos organizativos de seguridad fuera de la tecnología	1.5		1.5
	Subtotal	12.0	6.0	6.0

UNIDAD TEMÁTICA IV Monitorización y arquitecturas de seguridad	**CONTENIDO**	**HORAS CON DOCENTE**		**HRS AA**
		T	**P**	
UNIDAD DE COMPETENCIA Implementa arquitecturas de seguridad informática efectivas, con base en la integración de sistemas de monitorización de seguridad de redes y dispositivos de conectividad.	4.1 Consideraciones de despliegue en la monitorización	2.5	1.0	1.0
	4.2 Monitorización para la detección y sus limitaciones	1.5		1.5
	4.3 Aplicaciones para la monitorización de redes	1.5	1.5	
	4.4 Operaciones para el proceso de seguridad en la monitorización	1.5	1.0	1.5
	4.5 Arquitecturas de seguridad y dispositivos de conectividad 4.5.1 Protección perimetral 4.5.2 Protección para la nube 4.5.3 Protección para servidores 4.5.4 Protección para aplicaciones	8.0	4.0	3.0
	Subtotal	15.0	7.5	7.0

ESTRATEGIAS DE APRENDIZAJE	**EVALUACIÓN DE LOS APRENDIZAJES**
Estrategia de aprendizaje Estudio de casos El alumno desarrollará las siguientes actividades: 1. Estudio de protocolos de seguridad 2. Exposición de temas complementarios 3. Indagación documental 4. Lluvia de ideas 5. Desarrollo de proyecto 6. Realización de prácticas	Evaluación diagnóstica. Portafolio de evidencias: 1. Fichas de trabajo de los protocolos 2. Presentación 3. Reporte de indagación documental 4. Rubrica de participación en lluvia de ideas 5. Reporte de proyecto 6. Reporte de prácticas 7. Evaluación escrita

RELACIÓN DE PRÁCTICAS			
PRÁCTICA No.	**NOMBRE DE LA PRÁCTICA**	**UNIDADES TEMÁTICAS**	**LUGAR DE REALIZACIÓN**
1	Sistema Operativo Linux: fundamentos en la seguridad informática	I	Laboratorios de Cómputo
2	Sistema Operativo Windows: controles de seguridad	I	
3	Seguridad en la red: Protocolos UDP, TCP y SCTP	I	
4	Servicios en ejecución y puertos abiertos	I	
5	Acceso inicial al sistema operativo	I	
6	Simulación de una campaña de phishing	I	
7	Búsqueda de permisos de usuario normal o de equipo	I	
8	Creación de usuarios, levantamiento y modificación de servicios	I	
9	Configuración de un honeypot	II	
10	Configuración y monitoreo de la seguridad en el sistema operativo	II	
11	Escaneo de indicadores y puntos finales	II	
12	Ingeniería inversa a un Malware	II	
13	Plan de gestión de medidas de seguridad informática	II	
14	Plan de gestión de recuperación de desastres	III	
15	Plan de seguridad fuera de la tecnología	III	
16	Configuración de un área de monitoreo	III	
17	Arquitectura de seguridad perimetral	IV	
18	Arquitectura de seguridad para la nube	IV	
		TOTAL DE HORAS	27.0

Bibliografía

Tipo	Autor(es)	Año	Título del documento	Editorial/ ISBN	Documento		
					Libro	Antología	Otros
B	Bejtlich, R	2013	The Practice of Network Security Monitoring: Understanding Incident Detection and Response	Non Starch Press/ 9781593275099	X		
B	Brotherston, L & Berlin, A.	2017	Defensive Security Handbook	O'Reilly Media, Inc/ 9781491960387	X		
C	Bullock, J. & Parker, J.	2017	Wireshark for Security Professionals: Using Wireshark and Metasploit Framework	John Wiley & Sons/ 9781118918227	X		
B	Oriyano, S	2016	Penetration Testing Essentials	John Wiley & Sons/ 9781119235330	X		
*B	Bejtlich, R	2005	El Tao de la Monitorización de la Seguridad en Redes	Prentice Hall/ 9788420546001	X		
B	OccupyTheWeb	2018	Linux basics for hackers: getting started with networking, scripting, and security in Kali	Non Starch Press/ 978-1-59327-855-7	X		

Recursos digitales

Autor, año, título y Dirección Electrónica	Texto	Simulador	Imagen	Tutorial	Video	Presentación	Diccionario	Otro
Savani, A. Y Spring, B. (2018). Try Hack Me. Recuperado el 6 de mayo de 2022, de: https://tryhackme.com/dashboard		X						
The MITRE Corporation. (2015). MITRE ATT&CK®. Recuperado el 6 de mayo de 2022, de: https://attack.mitre.org/				X				
CyberDefenders, Inc. (2021). Cyber Defenders. Recuperado el 6 de mayo de 2022, de: https://cyberdefenders.org/		X						
National Institute of Standards and Technology. (1901). Information Technology Laboratory NATIONAL VULNERABILITY DATABASE. Recuperado el 6 de mayo de 2022, de: https://nvd.nist.gov/								X

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

PERFIL DOCENTE: Ingeniería en Sistemas Computacionales, Comunicaciones, Electrónica, Informática, Sistemas o carrera a fin, con posgrado en Ciencias de la Computación o áreas a fines

EXPERIENCIA PROFESIONAL	CONOCIMIENTOS	HABILIDADES DIDÁCTICAS	ACTITUDES
Dos años en el área de seguridad informática Un año en docencia a nivel superior.	Protocolos de comunicación para Internet Comunicaciones en Redes de Computadoras Arquitecturas de comunicación seguras Seguridad en lenguajes de programación Programación de aplicaciones Idioma inglés En el Modelo Educativo Institucional	Coordinar grupos de aprendizaje Organizar equipos de aprendizaje Planificación de la enseñanza Manejo de estrategias didácticas centradas en el aprendizaje Manejo de TIC en la enseñanza y para el aprendizaje Comunicación multidireccional	Compromiso con la enseñanza Congruencia Disponibilidad al cambio Empatía Generosidad Honestidad Proactividad Respeto Responsabilidad Solidaridad Tolerancia Vocación de servicio Liderazgo

ELABORÓ **REVISÓ** **AUTORIZÓ**

M. en D. Gilberto Sánchez Quintanilla
Coordinador

M. en C. Axel Ernesto Cervantes Moreno
Coordinador

M. en C. Iván Giovanny Mosso García
Subdirección Académica ESCOM

M. en C. Andrés Ortigoza Campos
Director ESCOM

Ing. Eduardo Gutiérrez Aldana
Participante

M. en H. y P.E. Héctor Alejandro Acuña Cid
Participante

Subdirección Académica UPIIZ

Dr. Fernando Flores Mejía
Director UPIIZ