UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
PLAN DE ESTUDIOS DE LA LICENCIATURA EN INFORMÁTICA
Sistema Escolarizado: Modalidad Presencial
Programa de estudios de la asignatura

Seguridad en redes

Clave	**Semestre**	**Créditos**	**Campo de conocimiento:** Informática	
0386	**8°**	**8**	**Eje de formación:** Profesionalización	
Modalidad	**Curso (X) Taller ( ) Lab ( )** **Seminario ( ) Otros ( )**		**Tipo**	**T (X) P ( ) T/P ( )**
Carácter	**Obligatorio ( ) Optativo (X)** **Obligatorio E ( ) Optativo E ( )**		**Horas**	
Duración (Número de semanas)	16		**Semana**	**Semestre**
			Teóricas: 4	**Teóricas:** 64
			Prácticas: 0	**Prácticas:** 0
			Total 4	**Total** 64

Seriación	
Ninguna ( )	
Obligatoria ( )	
Asignatura antecedente	
Asignatura subsecuente	
Indicativa (X)	
Asignatura antecedente	Telecomunicaciones I Telecomunicaciones II Seguridad informática
Asignatura subsecuente	Ninguna

Objetivo general:
Al finalizar el curso, el alumnado aplicará las técnicas y herramientas que permitan la implementación de la seguridad lógica y física de red.

Objetivos particulares

Al finalizar el curso, el alumnado:

1. Adquirirá los conceptos básicos de seguridad en redes que le permitan identificar las principales amenazas y ataques de seguridad.
2. Distinguirá los principales componentes físicos de seguridad para implementarlos en el diseño de redes.
3. Distinguirá los principales mecanismos de autenticación, autorización y auditoria para la gestión del control de acceso en una red.
4. Identificará los protocolos y aplicaciones para detectar códigos maliciosos, actividades inesperadas y usos inapropiados en la red.
5. Describirá las técnicas y herramientas de seguridad que le permitan detectar vulnerabilidades e intrusiones.
6. Indicará los protocolos, aplicaciones y herramientas con los que puede contar para garantizar la seguridad de los servicios en las redes.
7. Definirá las herramientas y políticas de seguridad necesarias para gestionar la seguridad de una red.

Índice temático

Unidad	Tema	Horas Semestre	
		Teóricas	**Prácticas**
1	Fundamentos de seguridad en redes	12	0
2	Seguridad física	8	0
3	Control de acceso	8	0
4	Seguridad en la comunicación	8	0
5	Detección de vulnerabilidades e intrusiones	12	0
6	Seguridad en los servicios	8	0
7	Gestión de seguridad	8	0
	Total	64	

Estrategias didácticas

- Exposición audiovisual
- Exposición oral
- Ejercicios dentro de la clase
- Trabajos de investigación
- Lecturas obligatorias
- Desarrollos de proyecto
- Estudio de casos
- Uso de TI
- Herramientas de escaneo de redes
- Simuladores de redes

Evaluación del aprendizaje
° Exámenes parciales ° Exámenes finales ° Trabajos escritos ° Tareas fuera del aula ° Participación en clase ° Proyecto de aplicación

Perfil profesiográfico del docente	
Título o grado	Licenciatura en Informática o equivalente, preferentemente con estudios de posgrado con orientación a las tecnologías de la información y las organizaciones.
Experiencia docente	Mínima deseable de 2 años impartiendo clases en nivel media superior y/o superior.
Otras características	Experiencia Profesional mínima de 3 años en área de conocimiento. Para profesoras/es de nuevo ingreso: Haber aprobado el "Curso Fundamental para profesores de Nuevo Ingreso (Didáctica Básica)" que imparte la Facultad de Contaduría y Administración, así como cubrir satisfactoriamente los requisitos impuestos por el departamento de selección y reclutamiento de la Facultad de Contaduría y Administración. Para profesoras/es que ya imparten clases en la Facultad: Haber participado recientemente en cursos de actualización docente y de actualización disciplinar con un mínimo de 20 horas. Compartir, respetar y fomentar los valores fundamentales que orientan a la Universidad Nacional Autónoma de México.

Bibliografía básica
° Arianello, E. (2013). *Redes Cisco: Guía de estudio para la certificación CCNA Security*. México: Alfaomega ° Dordoigne, J. (2020). *Redes Informáticas: Nociones fundamentales (8ª ed.).* Barcelona: Ediciones ENI. ° Díaz, G., Alzórriz, I., Sancristóbal, E., y Castro, M. (2014). *Procesos y herramientas para la seguridad de redes.* España: Universidad Nacional de Educación a Distancia. ° Gómez, A. (2014). *Sistemas seguros de acceso y transmisión de datos.* Madrid: RA-MA. ° Katz, M. (2013). *Redes y seguridad.* Argentina; México: Alfaomega. ° Kizza, J. (2017). Guide to Computer Network Security (4a ed.). E.U.: Springer International Publishing AG. ° McMillan, T. (2018). *CCNA Security Study Guide Exam 210-260*. E.U.: Sybex ° Terán, D. (2018). *Administración y seguridad en redes de computadoras*. México: Alfaomega. ° Whitman M. (2012). *Principles of Information Security* (4ª ed.) E.U.: Cengage Learning
Mesografía (referencias electrónicas)
° Institute of Electrical and Electronics Engineers (2021). *IEEE Wireless Communications. IEEE Xplore.* Recuperado de: https://ieeexplore-ieee-org.pbidi.unam.mx:2443/xpl/issues?punumber=7742&isnumber=9363021

Bibliografía complementaria

- Das, R. y De Guise, P. (2019). *Protecting Information Assets and IT Infrastructure in the Cloud.* Florida, E. U.: Auerbach Publications.
- Kapfer, P. (2018). *Internal Hacking y contramedidas en entorno Windows: pirateo interno, medidas de protección, desarrollo de herramientas* (2ª ed.). Barcelona, España: Ediciones ENI.
- Le, D., Kumar, R., Mishra, B. K., Khari, M., y Chatterjee, J. M. (Eds.) *Cyber security in parallel and distributed computing: concepts, techniques, applications and case studies.* Massachusetts, E. U.: Wiley.
- Ramos, A., Barbero, C. A., Grijalba, J., Ochoa, Á., López, S. y Lazo, C. G. (2015). *Hacking práctico en internet y redes de ordenadores. España*: Ra-Ma.
- Sánchez, G. (2018). *Seguridad cibernética: hackeo ético y programación defensiva.* México: Alfaomega.
- Wang, L. Jajodia, S. y Singhal A. (2017). *Network security metrics.* New York: Springer.