UDS	PLANEACION LICENCIATURA EJECUTIVO	DAC-FOR-02-B
	DIRECCION ACADEMICA	

Licenciatura: INGENIERÍA EN SISTEMAS COMPUTACIONALES	**Materia:**	SEGURIDAD DE LA INFORMACIÓN	**Clave:**	PE-ISC902
Modalidad: EJECUTIVO	**Cuatrimestre:**	9	**Horas:**	4

OBJETIVO:	Desarrolla e Implementa Planes de Seguridad basado en normas y estándares internacionales para el aseguramiento de los activos de la organización y la continuidad del negocio, además de aporta al perfil del Ingeniero Informático las capacidades de aplicar conocimientos científicos y tecnológicos en la solución de problemas en el área informática con un enfoque interdisciplinario; de seleccionar y utilizar de manera óptima técnicas y herramientas computacionales actuales y emergentes; y la aplicación de normas, marcos de referencia y estándares de calidad y seguridad vigentes en el ámbito del desarrollo y gestión de tecnologías y sistemas de información.

S	CLASE 1	CLASE 2	CLASE 3	CLASE 4	PLATAFORMA EDUCATIVA
1	**UNIDAD I INTRODUCCIÓN A LA SEGURIDAD INFORMACIÓN** 1.1 El valor de la información. 1.2 Definición y tipos de seguridad información	1.3 Objetivos de la seguridad información	1.4 Posibles riesgos en la información	1.5 Técnicas de aseguramiento del sistema.	
EN CASA	**CLASE 5**	**CLASE 6**	**CLASE 7**	**CLASE 8**	
	1.6 Criptografía clásica: Un primer acercamiento	1.7 Criptografía en la antigüedad.	1.8 Cifradores del siglo XIX.	1.9 Criptosistemas clásicos.	
S	**CLASE 1**	**CLASE 2**	**CLASE 3**	**CLASE 4**	**PLATAFORMA EDUCATIVA**
2	1.10 Máquinas de cifrar (siglo XX)	1.11 Estadística del lenguaje. 1.12 Ejemplos de la estadística del lenguaje.	**UNIDAD II CERTIFICADOS Y FIRMAS DIGITALES** 2.1 Distribución de claves.	2.2 Certificación.	
EN CASA	**CLASE 5**	**CLASE 6**	**CLASE 7**	**CLASE 8**	
	2.3 Componentes de una PKI.	2.4 Arquitecturas PKI	2.5 Políticas y prácticas de certificación.	2.6 Gestión de una PKI.	
S	**CLASE 1**	**CLASE 2**	**CLASE 3**	**CLASE 4**	**PLATAFORMA EDUCATIVA**
3	2.7 Estándares y protocolos de certificación	2.8 Ejemplo de un protocolo de seguridad: HTTPS	2.9 SSL 2.10 TSL 2.11 SSHs	**UNIDAD III SEGURIDAD EN REDES** 3.1 Aspectos de seguridad en las comunicaciones 3.2 Debilidades de los protocolos TCP/IP	**MAPA CONCEPTUAL**
EN CASA	**CLASE 5**	**CLASE 6**	**CLASE 7**	**CLASE 8**	
	3.3 Transmisión de paquetes y promiscuidad.	3.4 Redes locales (VLAN) y amplias (VPN)	3.5 Domicilios IP.	3.6 Vigilancia de paquetes	

S	CLASE 1	CLASE 2	CLASE 3	CLASE 4	PLATAFORMA EDUCATIVA
4	3.7 Estándares para la seguridad en redes.	3.8 Vulnerabilidad de los protocolos inalámbricos WEP, WPA, WPA2.	3.9 Firewall de capas inferiores	3.10 Firewall de capa de aplicación	
EN CASA	CLASE 5	CLASE 6	CLASE 7	CLASE 8	
	3.11 Firewall personal	3.12 Ventajas de un firewall	3.13 Limitaciones de un firewall	3.14 Políticas del firewall	
S	CLASE 1	CLASE 2	CLASE 3	CLASE 4	PLATAFORMA EDUCATIVA
5	3.15 Enlaces externos.	**UNIDAD IV VIGILANCIA DE LOS SISTEMAS DE INFORMACIÓN Y HACKING** 4.1 Definición de vigilancia. 4.2 Anatomía de un ataque	4.2 Anatomía de un ataque	4.3 Escaneos	
EN CASA	CLASE 5	CLASE 6	CLASE 7	CLASE 8	
	4.3 Escaneos	4.4 Identificación de vulnerabilidades	4.4 Identificación de vulnerabilidades	4.5 Actividades de infiltración.	
S	CLASE 1	CLASE 2	CLASE 3	CLASE 4	PLATAFORMA EDUCATIVA
6	4.6 Consolidación	4.7 Defensa perimetral.	4.8 Ética de hacking.	4.8 Ética de hacking.	**CUADRO SINÓPTICO**
EN CASA	CLASE 5	CLASE 6	CLASE 7	CLASE 8	
	4.9 Introducción a Kali Linux.	4.9 Introducción a Kali Linux	4.10 Penetración I 4.11 Penetración II.	4.10 Penetración I 4.11 Penetración II.	
7	CLASE 1	CLASE 2			PLATAFORMA EDUCATIVA
	EXAMEN DE MODULO				**EXAMEN FINAL EN PLATAFORMA OPCIONAL, OBLIGATORIO PARA LOS ALUMNOS EN MODALIDAD VIRTUAL**

ACTIVIDADES EN EL AULA PERMITIDAS:	1.-Conducción Docente, manejo de Esquemas, Conceptos Básicos y Referentes Teóricos (Pizarron) 2.-Estructuración de Reportes de Lectura y Fichas de Trabajo; uso de Medios Audiovisuales. (Pantalla). 3.-Realizar Lecturas de Referencias Bibliográficas Sugeridas y Adicionales para generar Lluvia de Ideas. 4.-Propiciar Actividades de Interes dentro del Proceso de Enseñanza - Aprendizaje para generar Investigaciónes. 5.-Vinculación de la Materia con Casos Prácticos y Reales que se puedan sustentar teoricamente.

ACTIVIDADES NO PERMITIDAS:	1. Examenes Orales. 2. Exposiciones como Evaluacion. 3. Improvisaciones.

SUGERENCIA BIBLIOGRAFICA				
No	**TIPO**	**TITULO**	**AUTOR**	**EDITORIAL**
1	Libro	"Seguridad Informática"	Garcia-Cerevignon A. Alegre Ramos M. (2010)	PARANINFO
2	Libro	"Firewalls and Internet Security: Repelling the Wily Hacker."	Cheswick, William R.; Bellovin, Steven M	Addison-Wesley Pub Co.
3	Libro	"Libro Electrónico de Seguridad Informática y Criptografía".	Aguirre, Jorge R	Legal M-10039-2003. Disponible en Internet en http://www.criptored.upm.es/guiateoria/gt_m001a.htm

SUGERENCIAS DE VIDEOS ACADEMICOS				
No	**TIPO**	**TITULO**	**LINK**	**AUTOR**
1	Video	Seguridad informática vs Seguridad de la información	https://youtu.be/Z2aF4UqHKkA	Instituto de Ciberseguridad
2	Video	Cultura Hacker. Conociendo al enemigo	https://youtu.be/MYBZpeq-h_M	Instituto de Ciberseguridad
3	Video	Cultura Hacker. Conociendo al enemigo	https://youtu.be/_PsB2e0U5FU	Chema Alonso

CRITERIOS, PROCEDIMIENTOS DE EVALUACION Y ACREDITACION.	
Actividades en Plataforma Educativa	40%
1er Actividad	20%
2da Actividad	20%
Examen	60%
Total	100%

Escala de calificación	7- 10
Minima aprobatoria	7

NOTA:	En la planeación los exámenes aparecen siempre en día lunes, pero dependerá de la programación de la subdireccion académica, y en esa semana se podrán hacer los cambios necesarios.