UDS	PLANEACION LICENCIATURA EJECUTIVA	SAC-FOR-35

Licenciatura: INGENIERIA EN SISTEMAS COMPUTACIONALES
Modalidad: EJECUTIVA
Materia: SEGURIDAD EN LA INFORMACION
Cuatrimestre: 9°.
Clave: PE-ISC902
Horas: 2

OBJETIVO:	Esta asignatura 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
1	**ENCUADRE**	**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. 1.5.-Técnicas de aseguramiento del sistema.
2	1.6.- Criptografía clásica: Un primer acercamiento. 1.6.1.- En la antigüedad. 1.6.2.- Cifradores del siglo XIX. 1.6.3.- Criptosistemas clásicos. 1.6.4.- Máquinas de cifrar (siglo XX) y estadística del lenguaje.	**UNIDAD II** **CERTIFICADOS Y FIRMAS DIGITALES** 2.1.- Distribución de claves. 2.2.- Certificación.
3	2.3.- Componentes de una PKI. 2.4.- Arquitecturas PKI. 2.5.- Políticas y prácticas de certificación.	2.6.- Gestión de una PKI. 2.7.- Estándares y protocolos de certificación. 2.8.- Ejemplo de un protocolo de seguridad: HTTPS. 2.9.- SSL, TSL, SSH. 2.10.- Prueba con un generador de certificados gratuito, libre y en línea.
4	**UNIDAD III** **SEGURIDAD EN REDES** 3.1.- Aspectos de seguridad en las comunicaciones. 3.2.- Debilidades de los protocolos TCP/IP. 3.2.1.- Transmisión de paquetes y promiscuidad. 3.2.2.- Redes locales (VLAN) y amplias (VPN).	3.2.3.- Domicilios IP. 3.2.4.- Vigilancia de paquetes. 3.3.- Estándares para la seguridad en redes. 3.4.- Vulnerabilidad de los protocolos inalámbricos WEP, WPA, WPA2.
5	**UNIDAD IV** **VIGILANCIA DE LOS SISTEMAS DE INFORMACIÓN** 4.1.- Definición de vigilancia. 4.2.- Anatomía de un ataque. 4.2.1.- Identificación de objetivos. 4.2.2.- Reconocimiento inicial. 4.2.3.- Técnicas de recopilación de información y análisis forense. 4.3.- Escaneos. 4.3.1.- Identificación y ataques a puertos TCP/UDP.	4.3.2.- Identificación y ataques a servicios. 4.4.- Identificación de vulnerabilidades. 4.4.1.- Técnicas manuales. 4.4.2.- Técnicas automáticas. 4.5.- Actividades de infiltración. 4.5.1.- Sistema operativo. 4.5.2.- Aplicaciones.
6	4.5.3.- Bases de datos. 4.6.- Consolidación. 4.7.- Defensa perimetral. 4.7.1.- Creación de una DMZ. 4.7.2.- Antivirus. 4.7.3.- Nat. 4.7.4.- Proxy.	**RETROALIMENTACION DE CONTENIDO**
7	**EXAMEN FINAL**	

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. Exposiciones

CRITERIOS, PROCEDIMIENTOS DE EVALUACION Y ACREDITACION.	
Trabajos Escritos	10%
Actividades Aulicas	20%
Trabajos en Plataforma Educativa	20%
Examen	50%
Total	100%
Escala de calificación	7- 10
Minima aprobatoria	7
Minima aprobatoria	7