CARTA DESCRIPTIVA (FORMATO MODELO EDUCATIVO UACJ VISIÓN 2020)

I. Identificadores de la asignatura

Instituto:	Ingeniería y Tecnología	**Modalidad:**	Presencial
Departamento:	Eléctrica y Computación	**Créditos:**	8
Materia:	Seguridad de la Información I		
Programa:	Sistemas Computacionales	**Carácter:**	Obligatoria
Clave:	IEC981500	**Tipo:**	Curso
Nivel:	Intermedio		
Horas:	64 Totales **Teoría:** 70%		**Práctica:** 30%

II. Ubicación

Antecedentes:	Clave
Sistemas Web II	IEC981400
Consecuente:	
Seguridad de la Información II	IEC982100

III. Antecedentes

Conocimientos: Tiene antecedentes de programación, conoce los fundamentos de las bases de datos y de la configuración y uso de redes de computadoras e Internet.

Habilidades: El alumno emplea su conocimiento de computación y matemáticas, analiza problemas e identifica y define los requerimientos de cómputo necesarios para la solución de éstos.

Actitudes y valores: Disposición al trabajo en equipo. Iniciativa de aprendizaje. Demostrar honestidad, responsabilidad, respeto, puntualidad. El alumno tendrá disposición a creatividad lógica, tenacidad, dedicación y constancia.

IV. Propósitos Generales

Introduce al estudiante a los conocimientos necesarios para entender, aplicar y manejar la seguridad de la información en el cómputo, las comunicaciones y los sistemas organizacionales. Se incluyen conocimientos sobre aspectos operacionales de seguridad, políticas y procedimientos, ataques, análisis de riesgo, recuperación y seguridad de la

información.

V. Compromisos formativos

Intelectual: El estudiante se autodirige en la búsqueda de información y aprendizaje de técnicas ó métodos que permitan la solución de problemas relativos a su profesión. Analiza e implementa tecnologías de información para la solución de problemas. Se comunica efectivamente tanto en forma oral como escrita en el ejercicio de su profesión, siendo capaz de adecuar el nivel y contenido técnico de la comunicación de acuerdo a las necesidades o intereses del destinatario.

Humano: Aporta esfuerzo, compromiso, integridad y honestidad a cualquier negocio, industria u organización pública o privada en donde ejerza sus servicios profesionales. Participa como un miembro productivo cuando integre equipos de trabajo.

Social: Respeta las leyes y normas establecidas por la sociedad y de manera particular aquellas relacionadas con el ejercicio de su profesión. Es cuidadoso de actuar bajo los principios éticos de su profesión. Se muestra interesado por contribuir, desde el ejercicio de su profesión, a la conservación del medio ambiente.

Profesional:

En lo general, desarrolla o elige soluciones que permitan la integración de una estructura de soporte de seguridad como base fundamental en el manejo de las TI en una empresa. En forma particular es capaz de lo siguiente:

- Conocer la historia de la Seguridad de la Información.
- Explicar la relación entre amenazas, vulnerabilidad, ataques y contramedidas, así como el proceso de gestión de riesgos.
- Entender la importancia de construir la seguridad de la información desde el diseño y construcción para asegurar su máxima efectividad.
- Comprender la relación del ciclo de vida de los sistemas con la seguridad.
- Elaborar documentos organizacionales de políticas de seguridad.
- Describir los diferentes mecanismos de autenticación como recurso de seguridad.
- Comprender los diferentes sistemas de detección y prevención de intrusos.

VI. Condiciones de operación

Espacio:	Aula tradicional		
Laboratorio:	Cómputo	Mobiliario:	mesa redonda y sillas
Población:	25 – 30		
Material de uso frecuente:	A) Cañón y computadora portátil		
Condiciones especiales:	No aplica		

VII. Contenidos y tiempos estimados

Temas	Contenidos	Actividades
1. Aspectos Fundamentales 3 sesiones (6 horas)	**Tema 1** a. Historia y terminología. b. Conciencia sobre la seguridad. c. Principios de diseño. d. Ciclo de vida de los sistemas y su seguridad.	**Tema 1** Investigación documental. Análisis de artículos. relacionados con problemas de seguridad Presentación de temas por parte de alumnos.
2. Dominios de Seguridad 4 Sesiones (8 horas)	**Tema 2** a. Interacción hombre-máquina b. Manejo de información c. Redes d. Programación e. Administración de sistemas f. Integración y arquitectura de sistemas g. Aspectos sociales y profesionales h. Sistemas web i. Planta física.	**Tema 2** Presentación de casos prácticos para cada dominio de seguridad
3. Vulnerabilidades y ataques 6 sesiones (12 horas)	**Tema 3** a. Tipos y ejemplos de vulnerabilidades • Red • Hardware (diseño, implementación, instalación, etc.) • Software (diseño, implementación, instalación, etc.) • Acceso físico b. Proceso de identificación de vulnerabilidades c. Tipos de atacantes d. Tipos y ejemplos de ataques • Ataques activos • Ataques pasivos • Ingeniería Social • Negación de servicio • Malware (virus, caballos de Troya,	**Tema 3** Investigación bibliográfica de temas Selección de casos prácticos para identificación de vulnerabilidades y ataques

	gusanos) e. Proceso de identificación de ataques	
4. Análisis de amenazas y gestión de riesgos 6 sesiones (12 horas)	**Tema 4** a. Modelos de análisis de amenazas y gestión de riesgos b. Identificación de amenazas c. Identificación de riesgos d. Contramedidas e. Análisis costo-beneficio f. Planes de contingencia	**Tema 4** Presentación de temas por parte de alumnos Proceso de análisis de amenazas y gestión de riesgos en casos prácticos Elaboración de documento final Elaboración de plan de contingencia
5. Diseño de políticas de seguridad 2 sesiones (4 horas)	**Tema 5** a. Objetivos b. Creación de políticas c. Mantenimiento de políticas	**Tema 5** Presentación de modelos para desarrollar políticas de seguridad Mostrar ejemplos de políticas de seguridad Desarrollo de una política de seguridad para un caso práctico
6. Mecanismos de autenticación y autorización 7 sesiones (14 horas)	**Tema 6** a. Necesidad de autenticación b. Mecanismos • De conocimiento • De posesión • Biométricos • Híbridos	**Tema 6** Presentación de temas por parte de alumnos Diseño de un mecanismo de autenticación para un caso práctico
7. **Sistemas de detección y prevención de intrusos** 4 sesiones (8 horas)	**Tema 7** (8 horas) a. Sistema operativo b. Red c. Personales	**Tema 7** Análisis de los diferentes sistemas de detección y prevención de intrusos a través de presentaciones y discusión en clase

VIII. Metodología y estrategias didácticas

Metodología Institucional:

a) Elaboración de ensayos, monografías e investigaciones consultando fuentes bibliográficas, hemerográficas y en Internet.
b) Elaboración de reportes de lectura de artículos en lengua inglesa, actuales y relevantes.

Estrategias del Modelo UACJ Visión 2020 recomendadas para el curso:

a) aproximación empírica a la realidad
b) búsqueda, organización y recuperación de información
c) comunicación horizontal
d) descubrimiento
e) ejecución-ejercitación
f) elección, decisión
g) evaluación
h) experimentación
i) extrapolación y trasferencia
j) internalización
k) investigación
l) meta cognitivas
m) planeación, previsión y anticipación
n) problematización
o) proceso de pensamiento lógico y crítico
p) procesos de pensamiento creativo divergente y lateral
q) procesamiento, apropiación-construcción
r) significación generalización
s) trabajo colaborativo

IX. Criterios de evaluación y acreditación

a) Institucionales de acreditación:

Acreditación mínima de 80% de clases programadas

Entrega oportuna de trabajos

Pago de derechos

Calificación ordinaria mínima de 7.0

Permite examen único: si

b) Evaluación del curso

Acreditación de los temas mediante los siguientes porcentajes:

Tema 1	10%
Tema 2	10%
Tema 3	10%
Tema 4	15%
Tema 5	15%
Tema 6	20%
Tema 7	20%
Total	100%

X. Bibliografía

- Maiwald, Eric. “Fundamentos de seguridad de redes”. 2ª. edición. 2005. Editorial McGraw-Hill) ISBN: 9701046242.
- Hernández Hernández, Enrique. “Auditoría en informática”. 2ª. edición. Año 2000. Editorial: CECSA. ISBN 9702400422
- Eduardo Fernández-Medina Patón, Roberto Moya Quiles y Mario Gerardo Piattini Velthuis. “Seguridad de las Tecnologías de la Información”. 2003. Editorial: AENOR. ISBN: 8481433675
- Stallings, William. “Fundamentos de seguridad en redes. Aplicaciones y estándares”. Edición 2004. Editorial Pearson Educación. ISBN 8420540021
- Mario Gerardo Piattini Velthuis, Emilio del Peso Navarro, Del Peso, Mar. “Auditoria de tecnologías y sistemas de información”. 2008. Editorial Ra-Ma. ISBN 8478978496.
- Gollman, Dieter. “Computer Security”. 2011. 3ª edición. Editorial Wiley. ISBN 0470741155.

X. Perfil deseable del docente

Maestría o doctorado en Ciencias Computacionales o Tecnologías de la Información, de

preferencia con especialidad en seguridad en sistemas de información.

Experiencia docente a nivel licenciatura.

XI. Institucionalización

Responsable del Departamento: Mtro. Armando Gandara Fernandez

Coordinador/a del Programa: Ing. Cynthia Vanessa Esquivel

Fecha de elaboración: 9 de Mayo de 2011

Elaboró: Dr. Victor Morales Rocha

Fecha de rediseño: N/A

Rediseño: N/A