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 II		
Programa:	Sistemas Computacionales	**Carácter:**	Obligatoria
Clave:	IEC982100	**Tipo:**	Curso
Nivel:	Avanzada		
Horas:	64 Totales **Teoría:** 60%		**Práctica:** 40%

II. Ubicación

Antecedentes:
Seguridad de la Información I

Clave
Pendiente asignación

Consecuente:
N/A

III. Antecedentes

Conocimientos: Tiene los fundamentos de la seguridad de la información. Tiene 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 y mecanismos de defensa, análisis de riesgo, recuperación y seguridad de la información.

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 y aplicar mecanismos de seguridad basados en criptografía y esteganografía. Se incluyen conocimientos sobre

protocolos de seguridad para información que utiliza como medio de transmisión Internet y se analizan diferentes aplicaciones para comprender la necesidad de la implementación de dichos protocolos y mecanismos de seguridad. Además se introduce al alumno en el campo de la auditoria de sistemas de información, así como en los procesos de análisis forense informático.

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 prevenir o mitigar problemas de seguridad en la información de importancia para una empresa. En forma particular es capaz de lo siguiente:

- Entender detalladamente los servicios de seguridad y sus objetivos.
- Comprender los diferentes mecanismos criptográficos, así como diseñar esquemas de seguridad para diversas aplicaciones.
- Conocer las diferentes técnicas de esteganografía para la protección de la información.
- Describir los diferentes protocolos de seguridad para aplicaciones basadas en un entorno web
- Identificar los retos de seguridad para diferentes aplicaciones.
- Comprender los procesos de auditoría para sistemas de información.
- Explicar que es el análisis forense informático
- Identificar situaciones donde el análisis forense es necesario

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. Servicios de seguridad 2 sesiones (4 horas)	**Tema 1** a. Confidencialidad b. Integridad c. Disponibilidad d. Autenticación, confiabilidad de la fuente e. No repudio	• Investigación documental • Ejemplos de casos que muestren los diferentes servicios de seguridad
2. Criptografía aplicada 8 sesiones (16 horas)	**Tema 2** a. Historia de criptografía b. Criptografía clásica c. Fundamentos de criptografía moderna d. Algoritmos de clave privada e. Algoritmos de clave pública f. Firma digital	• Investigación documental de la historia de la criptografía • Presentación de esquemas de criptografía clásica por parte de alumnos • Presentación de temas de criptografía moderna • Diseño y/o desarrollo de aplicación criptográfica
3. Esteganografía 3 sesiones (6 horas)	**Tema 3** a. Fundamentos b. Técnicas de watermarking c. Técnicas de fingerprinting	• Investigación bibliográfica de temas • Diseño y/o desarrollo de aplicación
4. Seguridad en Internet 4 sesiones (8 horas)	**Tema 4** a. SSL/TLS b. IPSec c. SSH d. Infraestructura de clave pública e. Redes privadas virtuales	• Investigación bibliográfica de temas • Presentación de temas por parte de alumnos • Implementación de SSL/TLS • Implementación de red privada virtual
5. Aplicaciones seguras 4 sesiones (8 horas)	**Tema 5** a. Comercio electrónico b. Banca electrónica c. Sistemas de voto electrónico	• Análisis de seguridad de las diferentes aplicaciones

	d. Casino online	
6. Auditoría de sistemas de información 5 sesiones (10 horas)	**Tema 6** a. Introducción a la auditoría de los sistemas de información b. Aspectos generales de la auditoría de los sistemas de información c. Metodologías de control interno y auditoría Informática d. El informe de auditoría e. Tecnología del auditor informático	• Investigación documental • Presentación de temas por parte de alumnos • Aplicación de metodología en caso práctico • Elaboración de informe
7. Análisis forense 6 sesiones (12 horas)	**Tema 7** a. Sistemas legales b. Análisis forense informático y su relación con otras disciplinas forenses c. Reglas de la evidencia d. Búsqueda e incautación e. Evidencia digital f. Análisis de medios digitales g. Preparación de informe forense h. Herramientas de análisis	• Aplicación del proceso de análisis forense en casos prácticos • Presentación de informe

VIII. Metodología y estrategias didácticas

Metodología Institucional:

a) Elaboración de ensayos, monografías e investigaciones (según el nivel) 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	20%
Tema 3	10%
Tema 4	15%
Tema 5	15%
Tema 6	15%
Tema 7	15%
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.
- Stallings, William, “Cryptography and network security: principles and practice”. 2010. 5ª edición. Editorial Prentice Hall. ISBN 0136097049.
- Schneier, Bruce. “Applied cryptography: protocols, algorithms, and source code in C” 2ª edición. 1996. Editorial Wiley. ISBN 0471128457.

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