CARTA DESCRIPTIVA (FORMATO MODELO EDUCATIVO UACJ VISIÓN 2020)

I. Identificadores de la asignatura

Instituto:	Ingeniería y Tecnología	**Modalidad:**	Presencial
Departamento:	Eléctrica y Computación	**Créditos:**	6
Materia:	Seguridad en Cómputo		
Programa:	Maestría en Cómputo Aplicado	**Carácter:**	Obligatoria
Clave:	MCA000514	**Tipo:**	Curso
Nivel:	Maestría		
Horas:	40 Totales **Teoría:** 70%		**Práctica:** 30%

II. Ubicación

Antecedentes: Clave

Consecuente:

III. Antecedentes

Conocimientos:

- Esquema básico de comunicaciones digitales
- Conocimientos básicos de bases de datos.
- Conocimientos básicos de ciclo de vida de desarrollo de software

Habilidades:

- Oensamiento lógico y crítico para la detección de problemas en sistemas de información
- Creatividad para proponer soluciones eficientes e innovadoras

Actitudes y valores:

- Responsabilidad con la sociedad
- Honestidad
- Respeto

IV. Propósitos Generales

El estudiante adquirirá conocimientos y habilidades relacionados con la evaluación de servicios

de seguridad, así como para proponer y elegir o desarrollar protocolos de seguridad que puedan aplicarse como parte de las soluciones de cómputo orientadas a cualquier tipo de organización.

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 protocolos de seguridad para las aplicaciones de cómputo. 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 aspectos básicos de seguridad y sus objetivos.
- Comprender los retos de seguridad en las bases de datos y aplicar los mecanismos de seguridad necesarios para cada situación particular.
- Comprender la relación del ciclo de vida de software con la seguridad requerida en cada parte del ciclo.
- Comprender los diferentes mecanismos criptográficos, así como diseñar esquemas de seguridad para diversas aplicaciones de cómputo.
- Describir los diferentes protocolos de seguridad para comunicaciones en Internet.
- Identificar los retos de seguridad para diferentes aplicaciones basadas en entorno Web.
- Comprender los riesgos de seguridad en los servicios en la nube y proponer arquitecturas para mitigarlos.

VI. Condiciones de operación

Espacio:	Aula tradicional		
Laboratorio:	Cómputo	Mobiliario:	mesa redonda y sillas
Población:	20-25		

Material de uso frecuente:

A) Cañón y computadora portátil

Condiciones especiales:	No aplica

VII. Contenidos y tiempos estimados		
Temas	**Contenidos**	**Actividades**
1. Aspectos básicos	a. Objetivos de seguridad b. Ataques y atacantes c. Administración de riesgos d. Principios de diseño	• El profesor introduce los aspectos básicos de seguridad. • El estudiante investiga los principales ataques y atacantes. • El profesor presenta diferentes metodologías de administración de riesgos y se desarrollan ejemplos en clase. • Se analizan los principios de diseño de los sistemas de cómputo y su relación con los principios de seguridad.
2. Seguridad en Bases de Datos	a. Introducción b. Bases de datos relacionales c. Control de acceso d. Seguridad en B.D. estadísticas e. Privacidad	• El profesor da una introducción a bases de datos y la importancia de mantenerlas seguras. • Se analizan las bases de datos relacionales a fin de determinar la seguridad que debe haber en el diseño. • El estudiante investiga acerca de los diversos mecanismos de control de acceso. Se realizan presentaciones en clase. • Se analiza el uso de bases de datos estadísticas y su seguridad.
3. Seguridad en Software	a. Introducción b. Caracteres y números c. Administración de	• El profesor introduce conceptos de seguridad en el desarrollo de

	memoria d. Datos y código e. Contramedidas	software. • El estudiante investiga acerca de las diversas formas de administrar la memoria y sus implicaciones. • Se presentan tipos de datos. • El estudiante presenta un tema asignado de contramedidas.
4. Criptografía	a. Introducción b. Funciones de control de integridad c. Firmas digitales d. Algoritmos de clave privada e. Algoritmos de clave pública f. Ejemplos de aplicación	• El profesor introduce los conceptos básicos de criptografía. • Se explican las diferentes formas de preservar la integridad de los datos. • El estudiante realiza un trabajo de investigación de firmas digitales y su aplicación. • El profesor introduce los conceptos de criptografia de clave privada y clave pública. • El estudiante investiga y presenta un algoritmo criptográfico.
5. Seguridad en Comunicaciones	a. Introducción b. IPSec c. SSL/TLS d. Comunicaciones móviles	• Se presenta una introducción a la seguridad en comunicaciones. • El estudiante investiga acerca de lso principales protocolos de seguridad. • El estudiante investiga acerca de los protocolos y algoritmos utilizados en comunicaciones móviles.
6. Seguridad en la Web	a. Introducción b. Sesiones autenticadas c. Seguridad en Servicios Web	• Se presentan los conceptos de seguridad en la web.

7. Seguridad de servicios en la nube	a. Fundamentos b. Amenazas y vulnerabilidades c. Arquitectura de seguridad	• El profesor introduce los fundamentos de seguridad en la nube. • Se analizan en clase las amenazas y vulnerabilidades asociadas a los servicios en la nube. • El profesor presenta los diferentes aspectos a considerar para establecer una arquitectura de seguridad.

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 8.0

Permite examen único: no

b) Evaluación del curso

- Presentaciones orales
- Ejercicios
- Examen

X. Bibliografía

- Dieter Gollman. Computer Security, tercera edición.. Ed. Wiley. ISBN: 978-0-470-74115-3
- Dafydd Stuttard y Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley. ISBN: 978-1118026472
- Ronald L. Krutz y Russell Dean Vines. Cloud Security. Ed. Wiley. ISBN: 978-0-470-58987-8

X. Perfil deseable del docente

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

Especialidad en seguridad informática.

Experiencia docente a nivel maestría.

XI. Institucionalización
Responsable del Departamento: Mtro. Armando Gándara Fernandez Coordinador/a del Programa: Fecha de elaboración: 10 de Junio de 2013 Elaboró: Víctor Morales Rocha Fecha de rediseño: N/A Rediseño: N/A