CARTA DESCRIPTIVA (FORMATO MODELO EDUCATIVO UACJ VISIÓN 2020)

I. Identificadores de la asignatura

Instituto:	IIT	**Modalidad:**	Presencial
Departamento:	Ingeniería Eléctrica y Computación	**Créditos:**	8
Materia:	Seguridad en Redes		
Programa:	Ingeniería en Sistemas Digitales y Comunicaciones	**Carácter:**	Electiva
Clave:	IEC 231300	**Tipo:**	Curso
Nivel:	Avanzado		
Horas:	64 Totales **Teoría:** 80%		**Práctica:** 20%

II. Ubicación

Antecedentes:
Redes de Computadoras II

Clave
IEC 340296

Consecuente:
N/A

III. Antecedentes

Conocimientos: Conocimientos avanzados de redes de computadoras e informática básica. Conocimientos avanzados del diseño y configuración de redes en equipo de conmutación, enrutamiento y acceso a la WAN. Nociones generales de seguridad en redes de comunicaciones.

Habilidades: Pensamiento analítico, facilidad para el razonamiento. Manejo e Instalación de componentes de hardware de una computadora y aplicación de algoritmos.

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

El objetivo de este curso es desarrollar un entendimiento detallado de los principios de

seguridad de red, así como las herramientas y configuraciones disponibles. El alumno conocerá las consecuencias de ataques, comprenderá las vulnerabilidades de sistemas de información. El alumno aplicará técnicas y prácticas recomendadas en la prevención de ataques y el buen funcionamiento de éstos sistemas.

V. Compromisos formativos

Intelectual: El alumno podrá describir las amenazas de seguridad que enfrentan las infraestructuras de red modernas y administrará políticas de seguridad efectivas. Conocerá los fundamentos de la seguridad en redes de computadoras y comprenderá los diferentes algoritmos y técnicas de encriptación.
El estudiante reconocerá los diferentes ataques de seguridad y las vulnerabilidades de los sistemas de información.

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: El estudiante incorpora a su formación los conocimientos necesarios para proveer seguridad a una infraestructura de red en todos sus niveles prevenir ataques mediante herramientas y métodos preestablecidos o desarrollados por el mismo, así como el restablecimiento de sistemas ante la presencia de ataques de seguridad..

VI. Condiciones de operación

Espacio:	Aula Tradicional		
Laboratorio:	Redes	Mobiliario:	Mesa y sillas
Población:	20 - 25		
Material de uso frecuente:	A) Proyector B) Cañón y computadora portátil		
Condiciones especiales:	No aplica		

VII. Contenidos y tiempos estimados		
Temas	Contenidos	Actividades
Tema 1: Amenazas de Seguridad en Redes Modernas 2 sesiones (4 hrs.)	Encuadre del curso. Principios Fundamentales de Seguridad en Redes Virus, Gusanos y Troyanos Tipos de Ataques	Presentación del programa, políticas del curso y evaluación. Inscripción a las plataformas de apoyo (Aula Virtual, Cisco Networking Academy). Ensayo (individual) que describa el impacto que ha tenido la tecnología e Internet en la vida del estudiante. Lectura autodirigida (alumno) previa a la exposición (docente) del tema de tipos de ataques a las redes de datos. Describir la evolución en la seguridad de la red, los controladores para proveer seguridad, las organizaciones dedicadas a preservarla, los ámbitos que abarca, las políticas de seguridad, virus, gusanos y troyanos y la forma de mitigar estos ataques; clasificación y descripción de los ataques a la red y formas para mitigarlos. Cuestionario de conceptos.
Tema 2: Seguridad en Dispositivos de Redes **4 sesiones (8 hrs.)**	Seguridad en acceso a Dispositivos Manejo de privilegios administrativos Administración y monitoreo de dispositivos de red	Lectura autodirigida (alumno) previa a la exposición (docente) de los temas de la seguridad en los diferentes tipos de dispositivos de red. Cuestionario de conceptos. Asegurar la instalación física y el acceso administrativo a dispositivos de red, gestión y presentación de informes de syslog, SNMP, SSH y NTP, revisar las configuraciones por defecto de los dispositivos y corregir vulnerabilidades. Práctica de configuración de protección de acceso a los dispositivos de red.
Tema 3: Authentication, Authorization and Accounting (AAA) **4 sesiones (8 hrs.)**	Características de AAA AAA local AAA utilizando servidores	Lectura autodirigida (alumno) previa a la exposición (docente) del tema de direccionamiento IP. Práctica de configuración de AAA local Practica de configuración de AAA con servidor

		NOTA: las prácticas se desarrollan en software de simulación.
Tema 4: Firewall **4 sesiones (8 hrs.)**	Listas de Control de Acceso Firewall Políticas basada en zonas	Lectura autodirigida (alumno) previa a la exposición (docente) de los temas de capa de enlace de datos y física. Cuestionario de conceptos. Describir ACL numeradas y con nombre, estándar y extendidas, configuración de dispositivos, describir y configurar ACL reflexivas, dinámicas, basadas en tiempo y como utilizarlas para mitigar ataques; describir los principales tipos de firewall y políticas de firewalls basadas en zonas. Práctica de configuración de listas de control de acceso.
Tema 5: Prevención de Intrusos **4 sesiones (8 hrs.)**	Tecnologías de sistemas de prevención de intrusos Firmas Implementación de IPS	Lectura autodirigida (alumno) previa a la exposición (docente) de los temas de prevención de intrusos. Describir la tecnología detrás de los sistemas IDS e IPS de Cisco, configurar y verificar el funcionamiento de estos sistemas por línea de comando y por interfaz gráfica. Práctica de configuración por línea de comandos. Práctica de configuración por interfaz gráfica.
Tema 6: Protección de LAN **5 sesiones (10 hrs.)**	Seguridad en puntos finales de la red. Seguridad de capa 2. Seguridad en redes inalámbricas, VoIP y SAN	Lectura autodirigida (alumno) previa a la exposición (docente) de los temas de protección de LAN Describir la forma de proteger puntos finales de la red con NAC, y CSA, describir los ataques de capa 2 y la manera de mitigarlos, configuración de seguridad de capa 2 en dispositivos y consideraciones de seguridad en redes inalámbricas, VoIP y SAN. Práctica de configuración de seguridad en dispositivos de red.
Tema 7: Sistemas Criptograficos **3 sesiones (6 hrs.)**	Servicios criptográficos. Integridad y Autenticidad. Confidencialidad. Criptografía de llaves públicas.	Exposición por parte del docente de los temas de Sistemas Criptográficos Exposición de temas por equipos. Cuestionario de conceptos.
Tema 8: Redes Privadas	VPN. GRE VPN.	Lectura autodirigida (alumno) previa a la exposición (docente) del tema de

Virtuales (VPN) **4 sesiones (8 hrs.)**	IPsec VPN. VPN de acceso remoto	redes inalámbricas. Describir la finalidad y los tipos de VPN y donde utilizarlos en la red, generación de túneles GRE VPN, conceptos básicos y configuración de IPSec VPN sitio a sitio; describir y configurar VPN de acceso remoto. Práctica de implementación de acceso remoto. Práctica de implementación de VPN Site-to-Site
Tema 9: Administración de una red segura **2 sesiones (4 hrs.)**	Principios para el diseño de redes seguras Operaciones de seguridad. Pruebas de seguridad en la red. Planes de continuidad y recuperación. Políticas de seguridad	Lectura autodirigida (alumno) previa a la exposición (docente) del tema de redes inalámbricas. Describir las consideraciones para el diseño de redes seguras, identificación de amenazas y análisis, gestión y evasión de riesgos; describir seguridad en transacciones, técnicas de pruebas de seguridad; describir la importancia de la disponibilidad de la red y la recuperación ante desastres; describir el concepto de ciclo de vida y cómo influye en la seguridad y disponibilidad de la red; describir el propósito y la función de una política de seguridad de red. Práctica de integración de aptitudes. Segundo examen parcial.

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:

1. aproximación empírica a la realidad
2. búsqueda, organización y recuperación de información
3. comunicación horizontal
4. descubrimiento
5. ejecución-ejercitación
6. elección, decisión
7. evaluación
8. experimentación

9. extrapolación y transferencia
10. internalización
11. investigación
12. meta cognitivas
13. planeación, previsión y anticipación
14. problematización
15. proceso de pensamiento lógico y crítico
16. procesos de pensamiento creativo divergente y lateral
17. procesamiento, apropiación-construcción
18. significación generalización
19. 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:

Contenido del Curso

Tema 1	5%
Tema 2	5%
Tema 3	10%
Tema 4	10%
Tema 5	5%
Tema 6	20%
Tema 7	15%
Tema 8	20%
Tema 9	10%
Total	100 %

X. Bibliografía

1. William Stallings, "***Cryptography and Network Security"***, Third Edition or Fourth Edition, Prentice Hall.Cisco Networking Academy, "First Year Companion Guide", 2nd Edition, Cisco Press, ISBN 1-58713-025-4

2. Kaufman, Perlman, "***Network Security"***, Private Communication in a Public World, Speciner, 2nd edition.

X. Perfil deseable del docente
Ingeniero en Sistemas Digitales y Comunicaciones o equivalente, con 2 años de experiencia en la industria. Certificación Cisco CCNA Security. Maestría, preferente Doctorado en áreas afines a Ciencias de la Computación y/o Tecnologías de Información.

XI. Institucionalización
Responsable del Departamento: Mtro. Jesús Armando Gándara Coordinador/a del Programa: Mtro. David García Chaparro Fecha de elaboración: Agosto 2013 Elaboró: Ing. Alejandro Barraza / Mtra. Alejandra Mendoza Fecha de rediseño: Rediseño: