UNIVERSIDAD DEL VALLE DE MÉXICO

PROGRAMA DE ESTUDIO DE LICENCIATURA

PRAXIS MES XXI

NOMBRE DE LA ASIGNATURA: CENTROS DE OPERACIÓN EN REDES Y SEGURIDAD

FECHA DE ELABORACIÓN: ENERO 2005

ÁREA DEL PLAN DE ESTUDIOS: AS ( ) AC ( ) APOBL ( ) APOPT (X)
ASIGNATURA INTEGRADORA ( )

CLAVE: 532814

ASIGNATURA ANTECEDENTE: NINGUNA
CLAVE NOMBRE

HORAS DE APRENDIZAJE A LA SEMANA		
CON DOCENTE	INDEPENDIENTES	TOTAL
3	3	6

CRÉDITOS: 5.6

TOTAL DE HORAS – CLASE POR ASIGNATURA: 90

OBJETIVO GENERAL

El estudiante analizará los diferentes centros de operación desde sus conceptos de seguridad, comunicaciones y justificación para poder planear, ejecutar y desarrollar implementaciones de dirección en sistemas de información.

ÍNDICE DE UNIDADES

1.-Auditoria de Sistemas de Comunicación.
2.- Evaluación de Empresas de Contratación de Servicios Externos.
3.-NOC (Network Operation Center)
4.-SOC (Security Operation Center)

NÚMERO Y NOMBRE DE LA UNIDAD: **HORAS: 5**

1. Auditoria de Sistemas de Comunicación

OBJETIVO DE LA UNIDAD:

El estudiante aplicará los conceptos básicos de comunicación de redes para realizar una auditoria de los sistemas que ínter operan con los centros de operación

TEMAS Y SUBTEMAS	ESTRATEGIAS DE INSTRUCCIÓN *	EXPERIENCIAS DE APRENDIZAJE	
		Con Docente	**Independientes****
1.- Conceptos 1.1 Elementos de un Sistema de Comunicación 1.1.1 MODEM 1.1.2 Interfaces 1.1.3 Medios de comunicación 1.1.4 Comunicación de Datos 1.1.5 Señales y ruido 1.1.6 Medios de comunicación 2.- Aspectos de Redes. 2.1 Internet 2.1.1. Routers 2.1.2 Multiplexores 2.1.3 Canales de comunicación (E0, E1, T0, T1) 2.1.4 Líneas Dedicadas 2.1.5 Enlaces Ultima Milla 2.1.6 **Proveedores y Costos** 3.- Redes 3.1 Dispositivos: NIC, HUB, Routers 3.2 Redes LAN 3.3 Redes WAN 3.4 Topologías. 3.5 Tecnologías 3.6 Protocolos 3.7 **Eficiencia de la Red**	Trabajo de Investigación Exposiciones Participación en Discusiones Exposición por parte de los estudiantes (Estrategia Interpersonal).	Exposición del Tema Investigación de los temas Elaboración de Ficha de Trabajo Exposición de Alumnos	Visita Exposiciones relacionadas con la materia : EXPOCOMM Investigación en Internet Investigación de Campo

ESCENARIOS	ESTRATEGIAS DE EVALUACIÓN	RECURSOS DIDÁCTICOS Y/ O SOFTWARE
• Aula. • Centro.	Trabajo de Investigación Exposiciones Participación en Discusiones	**Herrmientas de Análisis de Redes y Auditoría, encase, SolarWinds**

NÚMERO Y NOMBRE DE LA UNIDAD: 2.- Evaluación de Empresas de Contratación de Servicios Externos	**HORAS: 10**
OBJETIVO DE LA UNIDAD: El estudiante analizará a las empresas de contratación de servicios externos que ofrecen servicios de Administración de red y Seguridad.	

TEMAS Y SUBTEMAS	**ESTRATEGIAS DE INSTRUCCIÓN ***	**EXPERIENCIAS DE APRENDIZAJE**	
		Con Docente	**Independientes****
2 Generalidades 2.1 Concepto 2.2 Orígenes 2.3 Tendencias de seguridad 3 Requerimientos de inversión en seguridad 3.1 Hardware 3.2 Servidores Multipropósito 3.3 Appliance especializados 3.4 Software 3.4.1 Firewalls 3.4.2 Sistemas de Detección de Intrusos 3.4.3 Recolectores de eventos y generadores de alarmas y reportes. 3.4.4 Antivirus 3.4.5 Servidores de Autenticación 3.4.6 Consola de gestión centralizada 4 La opción del outsourcing 4.1 Cuando debe elegirse 4.2 La elección del proveedor	Exposición del profesor (Estrategia de Recepción). Exposición por parte de los estudiantes (Estrategia Interpersonal). Discusión en el grupo (Estrategia de Proceso de Grupo).	Exposición del Tema Investigación de los temas Elaboración de Ficha de Trabajo Exposición de Alumnos	Visita Exposiciones relacionadas con la materia : EXPOCOMM Creación de foros en Internet Investigación en Internet Investigación de Campo

ESCENARIOS	**ESTRATEGIAS DE EVALUACIÓN**	**RECURSOS DIDÁCTICOS Y/ O SOFTWARE**
• Aula. • Centro.	Trabajo de Investigación Exposiciones Participación en Discusiones	Herramientas de evaluación de proveedores: licitación, concurso. Internet.

NÚMERO Y NOMBRE DE LA UNIDAD **HORAS: 15**

3.- NOC (Network Operation Center)

OBJETIVO DE LA UNIDAD:

El estudiante identificará la estructura y el funcionamiento de un NOC, para desarrollar implementaciones de dirección en el sistema.

TEMAS Y SUBTEMAS	ESTRATEGIAS DE INSTRUCCIÓN *	EXPERIENCIAS DE APRENDIZAJE	
		Con Docente	**Independientes****
3 Conceptos 3.1 Definición 3.2 Metas 3.3 Descripción de funciones 3.3.1 Atención y seguimiento de fallas 3.3.2 Monitoreo de la RED 3.3.3 Operación/Soporte 3.3.4 Ingeniería de la Red 3.3.5 Administración de software 3.3.6 Análisis/Configuración 4 Operación del NOC 4.1 Definiciones 4.2 Alcances 4.3 Estructura de Servicio, Enlaces e Infraestructura 4.4 Estructura funcional interna y actividades 4.4.1 Monitoreo 4.4.2 Tarificación 4.4.3 Generación de estadísticas 4.4.4 Administración y Configuración 4.4.5 Seguridad 4.4.6 Recepción y Seguimiento de reportes 4.4.7 Documentación y Difusión 5 Responsabilidades de Las entidades 5.1 NOC 5.2 Nodos Asociados 3.3 Proveedores 3.4 Nodos de Interconexión Internacional 3.5 Usuarios 5.3 Medios de contacto 5.3.1 Teléfono 5.3.2 Página Web 5.3.3 Correo de voz 5.3.4 Correo Electrónico 5.3.5 Paging	Exposición del profesor (Estrategia de Recepción). Exposición por parte de los estudiantes (Estrategia Interpersonal). Discusión en el grupo (Estrategia de Proceso de Grupo).	Exposición del Tema Investigación de los temas Elaboración de Ficha de Trabajo Exposición de Alumnos	Visita a sitios NOC productivos Practicas en sitio Investigación en Internet

5.3.6 Call Center 5.4 Horarios 5.5 Horario Extendido 6 Administración de Fallas 6.1 Objetivo 6.2 Sistema de Detección de fallas 6.3 Sistema de atención y seguimiento de reportes 6.4 Reporte al usuario 6.5 Número de reporte. 6.6 Procedimiento de escalamiento.			

ESCENARIOS	**ESTRATEGIAS DE EVALUACIÓN**	**RECURSOS DIDÁCTICOS Y/ O SOFTWARE**
• Aula. • Centro.	Trabajo de Investigación Exposiciones Practicas en sitio	Presentaciones en computadora. Pizarrón Bases de conocimiento de mejores prácticas.

NÚMERO Y NOMBRE DE LA UNIDAD: **HORAS: 15**

4.- SOC (Security Operation Center)

OBJETIVO DE LA UNIDAD:

El estudiante distinguirá la estructura y el funcionamiento de un SOC, para desarrollar implementaciones de dirección en el sistema.

TEMAS Y SUBTEMAS	ESTRATEGIAS DE INSTRUCCIÓN *	EXPERIENCIAS DE APRENDIZAJE	
		Con Docente	Independientes**
4 Conceptos 4.1 Definición 4.2 Macro Arquitectura 5 Módulos del SOC 5.1 Sensores (IDS) 5.2 Pollers (Tipo de evento generado) 5.3 Colección de eventos y formato 5.4 Eventos de Base de Datos 5.5 Análisis de Eventos y Reconocimiento de base 5.6 Evento de reacción. 6 Arquitectura global del SOC 6.1 Adquisición de datos 6.2 Inventario Técnico y de organización 6.3 Vulnerabilidad de la Base de Datos 6.4 Políticas de Seguridad 6.5 Evaluación de estatus 6.6 Generación, colección y almacenaje de eventos. 6.7 Análisis y reporte de datos 6.7.1 Interfaces 6.7.1.1 Consola del SOC 6.8 Reacción y escalación de procedimientos 7 Colección y almacenaje 7.1 Colección de Datos 7.2 Protocolo 7.2.1 Funciones Básicas 7.2.2 Disponibilidad y Rendimiento 7.2.3 Seguridad 7.3 Dispacher y agente de aplicación 7.4 Formato y almacenaje de datos 7.4.1 Host entry 7.4.1.1 Identificación de Host unico 7.4.1.2 Estructura de datos de entrada del host	Exposición del profesor (Estrategia de Recepción). Exposición por parte de los estudiantes (Estrategia Interpersonal). Discusión en el grupo (Estrategia de Proceso de Grupo).	Exposición del Tema Investigación de los temas Elaboración de Ficha de Trabajo Exposición de Alumnos	Visita a sitios SOC productivos Practicas en sitio Investigación en Internet

7.4.1.3 Manejador de datos y mantenimiento 7.4.2 Message 7.4.2.1 Third-party structures 8 Correlación 8.1 Descripción 8.2 Operando la correlación 8.3 Introducción a los contextos 8.4 Contextos 8.4.1 Fuentes y objetivos 8.4.2 Protocolo y puertos 8.4.2.1 Tipos de intrusión 8.4.2.2 Intrusión ID 8.4.3 Estructura de Contextos 8.4.3.1 Arquitectura funcional 8.4.3.2 Estructura de datos 8.4.4 Estatus del contexto 8.5 Análisis 8.5.1 Estructura de los módulos de análisis. 8.5.1.1 Activación de los módulos de análisis 8.5.2 Correlación avanzada 8.5.2.1 Análisis Funcional 8.5.2.2 Análisis del comportamiento			

ESCENARIOS	ESTRATEGIAS DE EVALUACIÓN	RECURSOS DIDÁCTICOS Y/ O SOFTWARE
• Aula. • Centro.	Trabajo de Investigación Exposiciones Practicas en sitio	Presentaciones en computadora. Pizarrón. Bases de Conocimiento de Mejores Prácticas

REFERENCIAS BIBLIOGRÁFICAS

BÁSICA:

1.- Redes Locales y Seguridad Digital de Aldermeshian, Hrair. Edit Anaya Multimedia. ISBN 8441515492.
2.- Manual de Outsourcing de Emilio del Peso Navarro
3.- Network Security : Private Communication in a public Word by Charlie Kaufman
4.- Setting up a Network Operations Center by Faulkner Information Service
5.- Call Center Operation:Design, operation and maintenaces by Duane Sharp
6.- Network Intrusión Detection by Charles P Pfleeger
7.- Business Data Networs and Telecommunications by Ray Panko

COMPLEMENTARIA:

1.- Redes Locales y Seguridad Digital de Aldermeshian, Hrair. Edit Anaya Multimedia. ISBN 8441515492.
2.- Manual de Outsourcing de Emilio del Peso Navarro
3.- Network Security : Private Communication in a public Word by Charlie Kaufman
4.- Setting up a Network Operations Center by Faulkner Information Service
5.- Call Center Operation: Design, operation and maintenance by Duane Sharp
6.- Network Intrusion Detection by Charles P Pfleeger
7.- Business Data Networks and Telecommunications by Ray Panko

UNIVERSIDAD DEL VALLE DE MÉXICO

PROGRAMA DE ESTUDIO DE LICENCIATURA

PRAXIS MES XXI

ASIGNATURA: CENTROS DE OPERACIÓN EN REDES Y SEGURIDAD **CLAVE:** 532814

PERFIL DOCENTE							
NIVEL DE ESCOLARIDAD	**PROFESIÓN**	**EXPERIENCIA PROFESIONAL**			**EXPERIENCIA DOCENTE**		
		ÁREA	**ACTIVIDADES**	**AÑOS**	**NIVEL EDUCATIVO**	**ASIGNATURAS**	**AÑOS Y/O SEMESTRES**
Maestría en TI	Lic en Sistemas Computacionales. Ing en Sistemas Computacionales	Seguridad Operación de un Web Hosting, Call Center o Help Desk Certificación de la Industria en Seguridad Informática	- Desarrollar Políticas de Seguridad - Conocimiento de la operación de un Web Hosting, NOC, Call Center o Help Desk.	2 a 3 años	Licenciatura o Ingeniería	Telecomunicaciones Ing de Redes	2 Años

OTROS CONOCIMIENTOS DESEABLES:

Conocimiento de Redes, Administración de Centro de Cómputo, Configuración de Firewalls y Administración de un WEB Hosting.