Cartas Descriptivas

Datos de identificación				
Unidad Académica	**Facultad de Ciencias Administrativas y Sociales (Ensenada).** **Facultad de Ciencias Administrativas (Mexicali).** **Facultad de Contaduría y Administración (Tijuana).**			
Programa	**Maestría en Gestión de Tecnologías de la Información y la Comunicación**			
Nombre de la asignatura	**Seguridad en Ambiente de Redes**			
Tipo de Asignatura	**Optativa**			
Clave (Posgrado e Investigación)	**4062**			
Horas teoría	**2**	Horas laboratorio	**0**	Créditos Totales
Horas taller	**2**	Horas prácticas de campo	**0**	**6**

Perfil de egreso del programa
El egresado de la Maestría en Gestión de Tecnologías de la Información y la Comunicación tendrá la capacidad de planear, organizar, desarrollar, dirigir, controlar, proponer e implementar proyectos tecnológicos innovadores, en las organizaciones, generando soluciones que contribuyan a la competitividad de las mismas, mediante la aplicación de metodologías y técnicas vanguardistas en el ámbito de las TIC dentro de un marco social ético, responsable y sostenible.

Definiciones generales de la asignatura	
Aportación de esta materia al perfil de egreso del estudiante.	Planear, organizar, configurar e implementar planear, diseñar, implantar sistemas de seguridad en cómputo eficientes dentro de las organizaciones, atendiendo las características de los tipos de acceso, servicios de red brindados para la apertura del sistema de comunicaciones de la organización dentro de un entorno de red mundial, identificando las características y el funcionamiento de los mecanismos de seguridad dentro de un sistema operativo y de aplicaciones (sistemas) independientes. Generando así soluciones que contribuyan a la competitividad de las mismas, mediante la aplicación de metodologías y técnicas vanguardistas en el ámbito de las TIC
Descripción de la orientación de la asignatura en coherencia con el perfil de egreso.	Equilibrar los conocimientos y desarrollar las capacidades requeridas para hacer una adecuada planeación de los mecanismos y del sistema de seguridad que empleen tecnología actual y acorde a la infraestructura de red, los cuales puedan garantizar la integridad de la información electrónica de la organización y que regulen los accesos al sistema de red local, de tal manera que no vea interrumpida la actividad de la empresa por fallos en la seguridad del sistema de red.
Cobertura de la asignatura.	Trata los conceptos y elementos fundamentales de la seguridad en un sistema de comunicaciones, poniendo énfasis en la definición de estrategias de seguridad, construcción y mantenimiento de mecanismos de seguridad, así como el uso de herramientas de software para vigilar el desempeño de las barreras de seguridad durante la operación del sistema de red.

Profundidad de la asignatura.	Conocer las características y el funcionamiento de los mecanismos de seguridad dentro de un sistema operativo y de aplicaciones (sistemas) independientes. Configurar los servidores y mecanismos de seguridad necesarios atendiendo las características de los tipos de acceso, servicios de red brindados, y la apertura del sistema de comunicaciones de la organización dentro de un entorno de red mundial.		
Temario			
Unidad	**Objetivo**	**Tema**	**Producto a evaluar (evidencia de aprendizaje)**
I. Estrategias de seguridad.	Proponer las estrategias de seguridad sobre los medios físicos de un sistema de comunicaciones, realizando un análisis a conciencia de todos los componentes físicos involucrados y sus vulnerabilidades, con el fin de prevenir fallas que afecten el desempeño de las diferentes áreas operativas de la organización.	1.1. Instalaciones. 1.2. Equipos. 1.3. Cableado.	Reporte de investigación de campo sobre las medidas de seguridad en los medios físicos de un sistema de comunicaciones en operación. Diseño de sistema de seguridad en los medios físicos de un caso plateado sobre un sistema de comunicación para su puesta en marcha.
II. Elementos y técnicas que apoyan a la seguridad de la transferencia de información.	Identificar los elementos y técnicas que apoyan a la seguridad de la transferencia de información y accesos al sistema de red, a partir de un estudio y análisis a conciencia de la bibliografía y casos reales, de tal manera que adquiera un acervo cognitivo suficiente para planear, diseñar, implantar y administrar en forma responsable un sistema de seguridad eficiente que garantice la operatividad del sistema de comunicaciones.	2.1. Antecedentes de seguridad. 2.2. Algoritmos y criptografía. 2.3. Estrategias de seguridad: Ipsec, firewall, redes privadas virtuales, seguridad inalámbrica. 2.4. Protocolos de autentificación: basada en clave, centro de distribución, criptografía.	Examen escrito. Reporte escrito de la identificación de los elementos de seguridad identificados en un sistema de red en operación.

III. Sistemas de detección y protección de la red.	Seleccionar los sistemas de detección y protección de la red, mediante una identificación de necesidades y valoración las tecnologías actuales, con el fin de ajustar las medidas de seguridad necesarias que garanticen la integridad en la información y un flujo y navegación confiables a través del sistema de comunicaciones,	3.1. Sistemas de detección de intrusos. 3.2. Sistemas orientados a conexión de red. 3.3. Sistemas de análisis de vulnerabilidad 3.4. Sistemas de protección a la privacidad e integridad de la información. 3.5. Configuración de servidores: Firewall, Proxy, etc.	Reporte de investigación bibliográfica sobre las características de los diferentes sistemas de protección en redes LAN, MAN y WAN, wireless. Presentación de práctica de configuración de un servidor Proxy.
IV. Herramientas de software.	Utilizar las herramientas de software que apoyen a la vigilancia de la seguridad en el sistema de comunicaciones, explotando sus características y capacidades de usabilidad y generación de reportes con información clara y oportuna; de tal manera que se detecten y resuelvan los problemas de manera rápida y confiable para mantener un adecuado desempeño del sistema de red.	4.1. Uso de Software para el monitoreo en redes. 4.2. Atención a los avisos de conflictos en el sistema de red. 4.3. Trato de las vulnerabilidades detectadas.	Reporte de investigación bibliográfica sobre el software utilizado en la actualidad para el monitoreo y seguridad de una red. Reporte de una investigación de campo sobre el uso de software especial para el monitoreo en una empresa de la localidad.
V. Mecanismos de seguridad.	Construir los mecanismos de seguridad para los accesos de nombres y uso de correo electrónico, integrando un sistema seguro que permita garantizar el identificación y localización en la red y la integridad de la información a través de la mensajería electrónica con la finalidad de garantizar un funcionamiento eficiente del entorno de red.	5.1. Seguridad en el Web: nombres, SSL, código móvil. 5.2. Seguridad en correo electrónico: PGP, PEM, SMINE.	Reporte de la configuración y activación de un mecanismo de seguridad en un sistema de servicios Web y en un sistema de correo electrónico.

VI. Medidas de seguridad.	Proponer las medidas de seguridad sobre las instalaciones físicas que hospedan al sistema de comunicaciones, realizando un análisis a conciencia de los puntos de acceso, permisos, riesgos de desastres, y todo factor que atente contra la estabilidad física, de tal manera que asegure el buen desempeño de las actividades operativas de la organización.	6.1. Puertas. 6.2. Accesos. 6.3. Equipos de Protección.	Reporte de investigación de campo sobre las medidas de seguridad en las instalaciones y edificios donde se encuentra operando un sistema de comunicaciones. Diseño y planeación de un centro de cómputo, atendiendo las medidas de seguridad en las instalaciones físicas.
Estrategias de aprendizaje utilizadas: • Desarrollo de investigaciones bibliográficas y de campo. • Tareas extra-clase. • Desarrollo del diseño y planeación de un centro de cómputo			
Métodos y estrategias de evaluación: • Examen escrito 40% • Reporte de investigación de campo y bibliográfica 20% • Tareas extra clase 20% • Diseños realizados por los estudiantes. 20%			

Bibliografía:

Básica:

- Omar Santos, Panos Kampanakis y Aaron Woland, (2016). Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. Cisco Press.
- Peter Guerra, Drew Farris, (2016). Data Security for Modern Enterprises: Data Security in the World of Cloud Computing, Big Data, Data Science, and Modern Attacks. O'Reilly Media
- Arturo Mora Rioja, (2016). Seguridad y alta disponibilidad. Editorial Círculo Rojo.
- Michael E. Whitman, Herbert J. Mattord (2014) Principles of Information Security, Cengage Learning.
- Seymour Bosworth, Michel E. Kabay, Eric Whyne, (2014). Computer Security Handbook. Wiley; 6 edition.
- Ariganello, Ernesto (2013), Redes cisco: guía de estudio para la certificación CCNA Security, Alfaomega.
- Sheila Ayelen Berta (2013). Web Hacking. Creative Andina Corp.
- Stallings, William (2014), Network security essentials: applications and standards, Pearson Education.
- Jason Andress (2014), The Basics of Information Security, Second Edition: Understanding the Fundamentals of InfoSec in Theory and Practice, Syngress.

Complementaria

- Luis R. Castellanos H. (2014). Seguridad en informática. Editorial Académica Española.
- Mark Talabis, Robert McPherson, I Miyamoto, Jason Martin (2014), Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data.
- Karina Astudillo, (2013). Hacking Etico 101: Como hackear profesionalmente en 21 dias o menos!. CreateSpace Independent Publishing Platform.
- Jamsa, Kris, (2013), Cloud computing : SaaS, PaaS, IaaS, virtualization, business models, mobile, security and more,Jones & Bartlett Learning,
- Stuttard, Dafydd (2011), The web application hacker's handbook: finding and exploiting security flaws, Wiley Pub.

Nombre y firma de quién diseñó carta descriptiva:

1. **Evelio Martínez Martínez**[1]
2. **Oscar Ricardo Osorio Cayetano**
3. **José Manuel Valencia Moreno**[1]
4. **Omar Álvarez Xochihua**[1]

[1]Cuerpo Académico de Tecnologías de Información y Visualización

Nombre y firma de quién autorizó carta descriptiva:

- **Dr. Sergio Octavio Vázquez Núñez**
  Director de la Facultad de Contaduría y Administración – Tijuana
- **Dr. Raúl González Núñez**
  Director de la Facultad de Ciencias Administrativas – Mexicali
- **Dra. Mónica Lacavex Berumen**
  Director de la Facultad de Ciencias Administrativas y Sociales – Ensenada

Nombre(s) y firma(s) de quién(es) evaluó/revisó(evaluaron/ revisaron) la carta descriptiva:

- **Dra. Margarita Ramírez Ramírez**
  Coordinadora de Posgrado de la Facultad de Contaduría y Administración-Tijuana
- **Dr. Manuel Alejandro Ibarra Cisneros**
  Coordinador de Posgrado de la Facultad de Ciencias Administrativas-Mexicali
- **Dr. Ariel Moctezuma Hernández**
  Coordinador de Posgrado de la Facultad de Ciencias Administrativas y Sociales-Ensenada