



Vicerrectoría Académica
Dirección Curricular y de Docencia
Formato para la Elaboración de Microdiseños de Cursos

1 Identificación del Curso			
1.1 Código	1.2 Nombre del Curso	1.3 Pre-Requisito	1.4 Co-Requisito
OPT_0006	Administración y seguridad en redes	TELEMÁTICA	
1.5 No. Créditos	1.6 HAD	1.7 HTI	1.8 HAD:HTI
4		8	1:2
1.9 Horas presenciales aula clase	1.10 Horas presenciales laboratorio/Salida campo	1.11 Horas Virtuales	1.12 Total Horas HAD
4		Espacios	4
Obligatorio <input type="checkbox"/>	Optativo <input checked="" type="checkbox"/>	Libre <input type="checkbox"/>	
Teórico <input type="checkbox"/>	Practico <input type="checkbox"/>	Teórico/Practico <input checked="" type="checkbox"/>	
1.13 Unidad Académica responsable del Curso			
Ingeniería Electrónica			
1.14 Área de Formación			
Ingeniería Aplicada			
1.15 Componente			No aplica <input type="checkbox"/>
Telecomunicaciones			

2 Justificación del Curso
<p>Hay una necesidad apremiante de medidas para garantizar la privacidad, integridad y disponibilidad de la información. Los ataques son cada vez más frecuentes y comunes en sus diferentes formas: espionaje, negación de servicios, suplantación, modificación de flujos de información, virus, etc.</p> <p>Las personas encargadas de administrar las redes informáticas en las organizaciones deben tratar con interfaces de servicios desprotegidos y redes inseguras en ambientes donde los atacantes poseen un alto conocimiento sobre los protocolos de red y los algoritmos utilizados para disponer de la información a través de la red.</p>

3 Competencias por Desarrollar
3.1 Competencias Genéricas
<ul style="list-style-type: none"> • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Habilidades en el uso de las tecnologías de la información y de la comunicación • Capacidad de investigación • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para actuar en nuevas situaciones • Capacidad creativa • Capacidad para identificar, plantear y resolver problemas • Capacidad para tomar decisiones • Capacidad de trabajo en equipo

Formato para la Elaboración de Microdiseños de Cursos

3.2 Competencias Específicas

- **Declarativo o Conceptual**
Capacidad de reconocer los riesgos presentes en las redes actuales
- **Procedimental**
Implementar las técnicas adecuadas que permitan asegurar las redes de datos actuales
- **Esquemático**
Justificar procedimientos y resultados, para el diseño de sistemas de red seguro
- **Estratégico**
Proponer alternativas de solución para problemas novedosos acorde a las tecnologías actuales

4 Resultados de Aprendizaje del Curso

Identifica los diferentes Componentes, servidores y tecnologías que se implementan en las redes actuales, configurándolos de forma adecuada para prestar servicios sobre redes seguras a los usuarios finales y evitar intrusiones no deseadas.

Reconoce herramientas, procesos y leyes de seguridad informática para mantener a salvo la información de las amenazas actuales a nivel lógico y físico.

5 Programación del Curso

Unidad Temática	Semana	Contenido de Aprendizaje	Evidencias	Actividades Aprendizaje	HAD		HTI		Total Horas
					Aula Clase	Espacio Virtual	Trabajo dirigido	Trabajo Independiente	
Introducción a la administración de redes	1, 2, 3, 4 y 5	1.1 Componentes de una red 1.2 Direccionamiento IP 1.3 Configuración de dispositivos 1.4 Redes de área local virtuales 1.5 Servidores (HTTP, SMTP, DNS)	Taller sobre la implementación de servidores y evaluación	Diagnóstico inicial Revisión de material bibliográfico simulaciones de entornos de redes	20			40	60
Introducción a la seguridad en redes	6, 7, 8, 9 y 10	2.1 Conceptos básicos de seguridad en redes 2.2 Tipos de ataques 2.3 Deep Web 2.4 Virtualización de sistemas y herramientas de hacking ético 2.5 Políticas de seguridad 2.6 Aspectos legales 2.7 Seguridad física y lógica	Informe de practica de	Revisión bibliográfica Laboratorio de hacking ético	20			40	60
Criptografía	11 y 12	3.1 Algoritmos simétricos y asimétricos 3.2 firmas digitales 3.3 Seguridad en las transacciones electrónicas 3.4 Estándares de certificación y autoridades de certificación	Taller de Criptografía	Revisión bibliográfica Desarrollo de problemas	8			16	24
Firewalls	13 y 14	4.1 Tecnologías 4.2 Proxys 4.3 Listas de control de acceso 4.4 Protocolo NAT – PAT 4.5 Manejo de puertos	Informe de practica de	Revisión bibliográfica Simulaciones de entornos de red	8			16	24
Redes privadas virtuales	14 y 15	5.1 introducción a las VPN 5.2 Usos de las VPN 5.3 Protocolos para implementación 5.4 Requerimientos para la implementación	Informe de practica de y evaluación	Revisión bibliográfica Desarrollo de problemas Simulaciones de entornos	8			16	24

Formato para la Elaboración de Microdiseños de Cursos

				de red				
Total					64		128	192
Créditos Académicos					4			

6 Prácticas de campo (Laboratorios y Salida de Campo)

Unidad Temática	Fundamentación Teórica	Evidencias	Actividades Aprendizaje	Recursos	Tiempo (h)	Semana

7 Mecanismos de Evaluación del Aprendizaje

Resultado de Aprendizaje	Mediación de Evaluación	Mecanismos, Criterios y/o Rúbricas	Semana de Evaluación
Identifica los diferentes Componentes, servidores y tecnologías que se implementan en las redes actuales, configurándolos de forma adecuada para prestar servicios sobre redes seguras a los usuarios finales y evitar intrusiones no deseadas.	Aulas virtuales, software especializado, presentaciones magistrales, consultas bibliograficas	Practica de laboratorio, taller de apropiación de conocimientos y prueba escrita	Semana 5 y 15
Reconoce herramientas, procesos y leyes de seguridad informática para mantener a salvo la información de las amenazas actuales a nivel lógico y físico.	Aulas virtuales, software especializado, presentaciones magistrales, consultas bibliograficas	Practica de laboratorio, taller de apropiación de conocimientos y prueba escrita	Semana 10

8 Valoración de los Resultados de Aprendizaje

Valoración	Sobresaliente	Destacado	Satisfactorio	Básico	No Cumplimiento
Fundamentos Cualitativos					
Identifica los diferentes Componentes, servidores y tecnologías que se implementan en las redes actuales, configurándolos de forma adecuada para prestar servicios sobre redes seguras a los usuarios finales y evitar intrusiones no deseadas.	Con gran destreza Identifica los diferentes Componentes, servidores y tecnologías que se implementan en las redes actuales, configurándolos de forma adecuada para prestar servicios sobre redes seguras a los usuarios finales y evitar intrusiones no deseadas.	Identifica adecuadamente los diferentes Componentes, servidores y tecnologías que se implementan en las redes actuales para prestar servicios sobre redes seguras a los usuarios finales.	Identifica de forma satisfactoria los Componentes, servidores y tecnologías que se implementan en las redes actuales, configurándolos de forma adecuada para prestar servicios sobre redes seguras a los usuarios finales y evitar intrusiones no deseadas.	De forma aceptable Identifica los Componentes, servidores y tecnologías que se implementan en las redes actuales, configurándolos de forma adecuada para prestar servicios sobre redes seguras a los usuarios finales y evitar intrusiones no deseadas.	Demuestra dificultades para Identificar Componentes, servidores y tecnologías que se implementan en las redes actuales, configurándolos de forma adecuada para prestar servicios sobre redes seguras a los usuarios finales y evitar intrusiones no deseadas.
Utiliza herramientas, procesos y leyes de seguridad informática para mantener a salvo la	Utiliza con gran habilidad herramientas, procesos y leyes de	Utiliza de forma coherente herramientas, procesos y leyes	Utiliza de forma satisfactoria herramientas, procesos y leyes	Utiliza de forma aceptable herramientas, procesos y leyes de	Presenta dificultades para utilizar recursos y herramientas de

Formato para la Elaboración de Microdiseños de Cursos

información de las amenazas actuales a nivel lógico y físico.	seguridad informática para mantener a salvo la información de las amenazas actuales a nivel lógico y físico.	de seguridad informática para mantener a salvo la información de las amenazas actuales a nivel lógico y físico.	de seguridad informática para mantener a salvo la información de las amenazas actuales a nivel lógico y físico.	seguridad informática para mantener a salvo la información de las amenazas actuales a nivel lógico y físico.	seguridad informática para mantener a salvo la información de las amenazas actuales a nivel lógico y físico.
---	--	---	---	--	--

9 Recursos Educativos y Herramientas TIC

N	Nombre	Justificación	Contenido de Aprendizaje
	Laboratorio de Redes	Complementar conceptos, implementar, proponer, diseñar, simular sistemas de redes de datos y seguridad en sistemas de información.	Todos
	Video Beam	Proyección de material audiovisual para desarrollo de contenidos y actividades	Todos
	Brightspace	Desarrollo de aula virtual	Todos
	MS Teams	Complemento al aula virtual	Todos
	Simuladores de redes (Cisco Packet Tracer, GNS3)	Herramientas software utilizadas para la creación y simulación de entornos seguridad en redes	Todos

10 Referencias Bibliográficas

10.1 Libros y materiales impresos disponibles en la Biblioteca y Centros de Documentación de la Universidad

- [1] Network security essentials:, Stallings, William.. Boston : Pearson, 2014.
- [2] Cryptography and network security, Stallings, William. Boston: Pearson, 2014.
- [3] Redes: administración de servidores. Creative andina Corp, 2014
- [4] Herramientas para hacking ético, Editorial académica española, 2017
- [5] CCNA security Certification Guide, Cisco Networking Academy, Cisco Press, 2018.

10.2 Bases de datos de la universidad del Magdalena - eLibros.

- [6] Bases de datos de la universidad del Magdalena - eLibros.

10.3 Documentos y Sitios Web de acceso abierto a través de Internet

- [7] www.cisco.com
- [8] www.ieee.org
- [9] cve.mitre.org
- [10] www.iso.org

Director de Programa

Decano Facultad