PROGRAMA SINÓPTICO POR COMPETENCIAS

I. DATOS DE IDENTIFICACIÓN

PROGRAMA ACADÉMICO:	Ingeniería en Sistemas Computacionales		
NOMBRE:	Seguridad en Redes		**CLAVE:**ICD-1903
TIPO DE CURSO:	Obligatorio/Opcional		
HORAS: (T.P.C.)	**TEÓRICAS:** 2	**PRÁCTICAS:** 3	**CRÉDITOS ACADÉMICOS:** 5
SEMESTRE:	Octavo(8o.)		
FECHA DE ELABORACIÓN:	Septiembre del 2018 ITESRC		
ELABORADO POR:	Academia Sistemas Computacionales		

II. COMPETENCIAS A DESARROLLAR:

Totalmente presencial o combinado con actividades a distancia (BDL). Todos los laboratorios prácticos del curso se pueden realizar en el equipo físico real.

También se debe propiciar mediante prácticas, la implementación de casos de estudio reales que ofrezcan escenarios distintos que permitan la aplicación de los conceptos para lograr que el aprendizaje sea significativo para el desarrollo de las competencias.

En el desarrollo de la materia, deberá observarse:

- Que los contenidos sean abordados en su totalidad.
- Que se cuente con la infraestructura necesaria para realizar las prácticas
- Que el laboratorio de prácticas cuente con el equipo necesario que deberá utilizarse durante el desarrollo de la asignatura.
- Que todas prácticas diseñadas por el docente sean afines a los temas del plan de estudios.
- Que los estudiantes adquieran las competencias específicas de cada tema.

Instala, configura y administra la seguridad en dispositivos de capa 2 y capa 3 para gestionar la información generada en los diversos procesos de una organización, optimizando la infraestructura de manera segura.

Desarrolla un entendimiento teórico en profundidad de los principios de seguridad de la red, así como de las herramientas y configuraciones disponibles.

Hincapié en la aplicación práctica de los conocimientos necesarios para diseñar, implementar y respaldar la seguridad de la red.

Desarrolla un pensamiento crítico y habilidades de resolución de problemas complejos, a través de las prácticas desarrolladas en los laboratorios.

Fomenta la exploración de los conceptos de seguridad de la red y permita experimentar con el comportamiento de la red y formular preguntas del tipo “¿qué pasaría sí?”, las actividades de aprendizaje basadas en simulaciones de Packet Tracer

III. CONTENIDOS:

UNIDAD I: Riesgos de seguridad en redes modernas.	
Específica(s):	**CONTENIDO:**
• Describe la evolución de la seguridad de red • Describe las políticas de seguridad de red • Comprende como mitigar los ataques de red	1.1 Principios fundamentales de la seguridad de la red 1.2 Virus, gusanos, caballos de troya 1.3 Metodologías de ataque

UNIDAD II: Dispositivos de redes seguros	
Específica(s): • *Configura la instalación física de la seguridad y el acceso administrativo en los routers cisco* • *Configura administrativa de reglas usando los niveles de privilegios* • *Implementar la administración y reporte de características de syslog, SNMP, SSH y NTP* • Examinar la configuración del router utilizando el auditor de seguridad	**CONTENIDO:** 2.1 Protegiendo el acceso al dispositivo 2.2 Asignación de roles administrativos 2.3 Monitorizando y gestionando dispositivos 2.4 Automatizando la función de seguridad

UNIDAD III: Autentificación, Autorización y Contabilidad..	
COMPETENCIA ESPECÍFICA DE LA UNIDAD: **Específica(s):** • Configura de autentificación en ruteadores • Configura de usuarios y determinar	**CONTENIDO:** 3.1 Finalidad de la AAA 3.2 Autentificación local AAA 3.3 Servidor basado en AAA 3.4 Servidor basado en AAA, autorización y contabilidad

UNIDAD IV: Implementación de tecnologías de Firewall.	
COMPETENCIA ESPECÍFICA DE LA UNIDAD: **Específica(s):** • Comprende el funcionamiento de un firewall • *Identifica los tipos de firewall y en donde se instalan* • Configura elementos básicos del firewall • Implementa y prueba funcionamiento de firewall	**CONTENIDO:** 4.1 Listas de Control de Acceso 4.2 Seguridad de las redes con firewalls 4.3 Características CBAC 4.4 Características de políticas de firewall basadas en zone 4.5 Operación ZPF

UNIDAD V: Implementación de dispositivos ASA (Adaptive Security Appliance).	
COMPETENCIA ESPECÍFICA DE LA UNIDAD: **Específica(s):** • Comprende el funcionamiento de un dispositivo ASA • Identifica los tipos de dispositivos ASA y en donde se instalan • *Configura elementos básicos del dispositivo ASA* • Implementa y prueba funcionamiento de un dispositivo ASA	**CONTENIDO:** 5.1 Definición de los dispositivos ASA 5.2 Funcionamiento 5.3 Tipos de dispositivos 5.4 Configuración

IV. FORMA DE EVALUACIÓN:

La evaluación debe ser permanente y continua. Se debe hacer una evaluación diagnóstica, formativa y sumativa. Se debe aplicar la autoevaluación, coevaluación y heteroevaluación.
Se debe generar un portafolio de evidencias, de preferencia en formato digital.
Instrumentos:
Mapa conceptual
Tablas comparativas
Examen teórico
Examen Práctico
Reportes escritos de investigación
Reporte de prácticas de laboratorio y simulador
Guía de proyecto

V. REFERENCIA BIBLIOGRÁFICA:

1. Graff, Jon C., Cryptography and E-Commerce, John Wiley & Sons, 2001
2. Goldreich, O, Modern Cryptography, Probabilistic Proofs and Pseudo-Randomness, Springer-Verlag, 2000
3. Horak,Ray, How Secure is your Connection? Nueva York:M&T books, 2000
4. Hutt,A.E.,S. Bosworth y D.B. Hoyt, eds, Computer Security Handbook, 3rd ed., Nueva York; John Wiley & Sons, 1995
5. Knudsen, Jonathan, Java Cryptography, O Reilly, 1998
6. Lai, Xuejia, On the design and Security of Block Ciphers, ETH Series in Information Processing, vol.1, 1992
7. Martin,Frederick Thomas, Top Secret Intranet: Hoe the U.S. Intelligent built intelink-The Worlds Largest, Most Secure Network, Prentice Hall,1997
8. Curso “Introduction to Cybersecurity” en Cisco Networking Academy
9. Curso “Cybersecurity Essentials” en Cisco Networking Academy