PROGRAMA ANALÍTICO DE ASIGNATURA

1. IDENTIFICACION DE LA MATERIA

NOMBRE DE LA ASIGNATURA	: Seguridad en Redes y Transmisión de Datos
PRE-REQUISITOS	: INF423 ECO449 ELT384 RDS421 RDS429
SIGLA Y CODIGO	: RDS 519
NIVEL	: 9no Semestre
HORAS	: 4 HT 2 HP
CREDITOS	: 5
PROGRAMA VIGENTE	
REVISADO EN	

2. JUSTIFICACION

El aumento en la implantación de cada vez más y más sistemas informáticos y redes de telecomunicaciones en las diferentes organizaciones, ha dado lugar a diversas técnicas de ataque de las vulnerabilidades de nuestros sistemas y redes, para aprovechamiento malicioso de nuestros recursos. Por lo tanto surge la imperiosa necesidad para el profesional en redes y telecomunicaciones del conocimiento de técnicas de seguridad en su área. En está asignatura se perseguirá que el estudiante pueda:

- Desarrollar la capacidad de aplicar de control en redes.
- Afianzar Habilidades y destrezas mediante la resolución de problemas y determinar los problemas en una red.
- Implementar y analizara Herramientas de apoyo en redes.
- Obtener la capacidad de abstracción para explicar en forma procedimental, un proceso de análisis de la red.

3. OBJETIVOS DE LA ASIGNATURA

3.1. OBJETIVO GENERAL

Desarrollar Técnicas para resguardar los sistemas de redes, aplicando los conceptos teóricos de TCP/IP.

3.2. OBJETIVOS ESPECIFICOS

- Describir e interpretar los conceptos de Amenazas, vulnerabilidad y riesgos en forma oral y escrita.
- Desarrollar el proceso de la detección de riesgos de seguridad, mediante un análisis FODA en forma de exposición y escrita.
- Aplicar Técnicas y Tecnologías para prevenir, detectar y mitigar riesgos de seguridad.
- Describir e interpretar los mecanismos para seguridad física y lógica de la información.
- Describir e interpretar el funcionamiento de las principales técnicas para garantizar la confidencialidad, integridad, y disponibilidad de la información.

4. CONTENIDO MINIMO

Introducción al análisis de riesgo.

Seguridad Física y Lógica.

Seguridad en Redes y Telecomunicaciones.

5. UNIDADES DEL PROGRAMA ANALITICO

Unidad I. Introducción a la gestión de riesgo

Tiempo: 4 semanas.

Objetivo: Analizar los objetivos de la Unidad de Sistemas con respecto a los objetivos del negocio.

Desarrollar el proceso de Análisis de Riesgo de seguridad de la información de forma practica.

Contenido:

- Seguridad Informática y de Información.
    * Gestión de las Unidades de Sistemas.
    * Gestión del Negocio de la Empresa.
    * Integración unidad de sistemas y negocio.
- Identificación de Amenazas, Vulnerabilidades y Riesgos.
    * Proceso de Identificación.
    * Proceso de Selección y Clasificación.
- Valoración, priorización y gestión de riesgos.
    * Proceso de Ponderación de Riesgos.
    * Priorización de Riesgos a niveles aceptables
    * Reportes de Cambios en los riesgos a la administración

Unidad II. Seguridad Física y Lógica

Tiempo: 4 semanas.

Objetivo: Conocer formas y mecanismos mediante los cuales se garantizan un nivel aceptables de seguridad. Física y Lógica.

Contenido:

- Seguridad Física de los Datos e Información.
    * Entorno de protección de la Información.
    * Tecnologías y Herramientas de Seguridad.
    * Mecanismos de Confidencia, Confianza y Garantía.
    * Servicio de Administración y Protección de la información.
- Seguridad Lógica de los Datos e Información.
    * Sistemas de Respaldos.
    * Sistemas de Cifrados.
    * Funciones Digesto.

Unidad III. Seguridad en Redes y Telecomunicaciones

Tiempo: 6 semanas.

Objetivo: Detallar los principios fundamentales de la seguridad en Redes y Telecomunicaciones.

Contenido:

- Modelo OSI.

* Descripción y funcionamiento.
* Comunicación entre capas.

- TCP/IP.
  * Pila de TCP/IP.
  * Relación entre OSI y TCP/IP.
- Estándares de Calidad en Seguridad.
  * ISO 17799.
  * BS7799.
  * ISO 27000.
- Ataques y Defensa.
  * Clasificación de los Ataques.
  * Tipificación de los Ataques.
  * Clasificación de las Defensas.
  * Tipificación de la Defensas.
  * Implementación de Herramientas.

6. METODOLOGIA

Para el cumplimiento de los contenidos analíticos se han determinado los siguientes métodos educativos:

a) Clases Magistrales, en el cual el profesor guiará los conceptos escenciales de los temas dictados.

b) Trabajo de investigación, para profundizar sobre alguna herramienta de seguridad vista en clases.

c) Proyecto Final, será el desarrollo de una aplicación práctica por parte de los estudiantes, sobre los contenidos teóricos vistos en la materia.

Los medios de enseñanza utilizados son: Computador, Reproductor Multimedia, Herramientas de Software, Pizarra Acrílica y Marcadores de agua.

7. CRONOGRAMA DE ACTIVIDADADES

SEMANA / ACTIVIDADES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Presentación																		
Unidad I																		
Unidad II																		
Primer Parcial Teórico																		
Primer Parcial Práctico																		
Unidad III																		
Segundo Parcial Teórico																		
Segundo Parcial Práctico																		
Presentación Investigación																		
Examen Final																		
Proyecto Final																		
Examen Recuperatorio																		

8. SISTEMA DE EVALUACION

El sistema de evaluación permitirá asignar un valor "Cuantitativo-Cualitativo" a los conocimientos de los estudiantes. Se tomarán dos evaluaciones parciales, una a mitad de semestre y otra casi al finalizar el mismo, también se tomará un examen final de todo lo avanzado a la terminación del semestre, y se darán dos trabajos: un trabajo práctico de investigación sobre alguna herramienta vista en clase y un proyecto final de la materia para que estudiante desarrolle una aplicación práctica sobre los contenidos vistos en clases. Cada ponderación de estos elementos está detallado a continuación:

a) Ponderación Parciales	40%	
Primera Evaluación	20%	Unidades I y II
Segunda Evaluación	20%	Unidades III
a) Ponderación Final	30%	Unidades I, II y III
c) Ponderación Trabajos	30%	Unidades I, II y III
Trabajo de Investigación	10 %	
Proyecto Final	20 %	

9. BIBLIOGRAFIA

Normas:
- AS/NZS 4360
- ISO 17799
- COBIT
- ISO/IEC 15408

Libros:
- Manual de Seguridad en Redes; Equipo de Seguridad en Redes; Subsecretaría de Tecnologías Informática, Secretaría de la Fundación Pública; Diciembre de 1998.
- Aspectos Avanzados de Seguridad en Redes; Jordi Herrera Joancomartí, Joaquín García Alfaro, Xavier Perramón Tornill; Grupo de Software Libre, Universitat Oberta de Catalunya; Barcelona-España, Julio de 2004.
- Seguridad Por Niveles; Alejandro Corletti Estrada; DarFE Learning Consulting S.L.; Madrid-España, Septiembre de 2011.
- Hacking Ético; Carlos Tori; Rosario-Argentina, Mayo de 2008.
- CCSP EXAM GUIDE, Robert E. Larson.