INF-315: Planificación y Seguridad de los Sistemas Informáticos

Identificación

Asignatura:	Planificación y Seguridad de los Sistemas Informáticos
Sigla:	INF–315
Area Curricular:	Ciencias de la Computación y Lógica Fuzzy
Modalidad:	Semestral
Nivel Semestral:	Sexto o Séptimo Semestre, Ciclo de Orientación
Horas Teóricas:	4 por semana en dos sesiones
Horas Prácticas:	4 por semana
Horas Laboratorio:	2 por semana
Pre–Requisitos Formales:	MAT–132
Carreras destinatarias:	Matemática y Area de Ciencia y Tecnología

Objetivos

Familiarizar a los alumnos con los problemas de seguridad en redes y las soluciones a los mismos basadas en criptografía y protocolos criptográficos, con especial atención a la sacurización de protocolos de Internet.

Competencias

Comprende la importancia de la seguridad de los sistemas informáticos frente a la vulnerabilidad que está expuesta todo sistema que está integrada a una red.

Contenido Mínimo

Criptografía. Servicios de seguridad electrónica. Seguridad en sistemas no conectados. Seguridad en redes TCP/IP. Protocolos seguros sobre TCP/IP.

Programa Sintético

1. *Criptografía.1.1* Introducción *1.2* Primitivas criptográficas *1.3* Criptografía simétrica (de clave secreta) *1.4* Criptografía asimétrica (de clave pública) *1.5* Funciones hash
2. *Servicios de seguridad electrónica.2.1* Confidencialidad *2.2* Autenticación *2.3* No repudio *2.4* Firma digital *2.5* Infraestructuras de clave pública *2.6* Autoridades de certificación y TTPs *2.7* Protocolos criptográficos
3. *Seguridad en sistemas no conectados.3.1* Autenticación *3.2* Gestión de claves *3.3* Intrusiones y su taxonomía *3.4* Servicios de seguridad de sistemas operativos
4. *Seguridad en redes TCP/IP.4.1* Conceptos de TCP/IP: direcciones, puertos, routing *4.2* Protocolos de Internet *4.3* Securización de protocolos: filtrado y tunelización. *4.4* Protocolos seguros sobre TCP/IP *4.5* Correo electrónico: S/MIME/ PEM, PGP *4.6* Seguridad Web: SSL/TLS y comercio electrónico seguro *4.7* Telnet seguro: SSH, túneles y port forwarding *4.8* IPsec, Kerberos y otros productos afines.

Métodos y Medios Didácticos

Clases teóricas. Prácticas de laboratorio. Resolución de ejercicios y problemas. Lecturas, presentación y discusión de artículos científicos.

Auxiliatura de docencia

Como materia de servicio de la Carrera de Informática, esta materia no tiene auxiliar de docencia. Los trabajos prácticos realizados en la materia son monitoriados por el mismo docente.

Criterios de Evaluación

La evaluación de la asignatura consiste en pruebas escritas u orales, donde se valora la aplicación adecuada de *conceptos*, *teoremas* y *métodos* en la *demostración* o *resolución* de problemas planteados; y, en la calificación de prácticas o trabajos de laboratorios cuyo informe debe estar escrito en un *lenguaje matemático* adecuado con rigor lógico. Se valora de forma adicional la *creatividad* y la *simplicidad* en la presentación de sus resultados.

Cronograma de Avance

Semana	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Capítulos	1				2				3				4				5			

Bibliografía

[1] Daniel J. Barret and Richard E. Silverman. SSH, The secure Shell: The definitive Guide.

[2] O?Reilly & Associates, Inc. 2001, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubi, Firewalls and Internet Security: Repelling the Wily acker, Addison-Wesley, reading, MA, USA, Second Edition, 2003.