FACULTAD:	ESCUELA:	DEPARTAMENTO:	
Ingeniería.	Ingeniería Eléctrica.	Comunicaciones	
ASIGNATURA: Seguridad en Redes y Criptografía		**CÓDIGO:** 2450	**PAG.:** 1 **DE:** 5
REQUISITOS: Comunicaciones II (2427), 150 Unidades			**UNIDADES:** **4**

HORAS					
TEORÍA	**PRÁCTICA**	**TRAB. SUPERV.**	**LABORATORIO**	**SEMINARIO**	**TOTALES DE ESTUDIO**
3	1				

PROPÓSITO

En esta era de conectividad global, de Internet y de comercio electrónico, de fraudes informáticos y de teléfonos interceptados, de virus y de hackers, la seguridad se ha vuelto un asunto de vital importancia. El crecimiento explosivo en sistemas computarizados y sus interconexiones a través de las redes, ha aumentado la dependencia, tanto de las organizaciones como de los individuos, de la información almacenada y transmitida usando tales sistemas. Esto a su vez ha llevado a una mayor necesidad de resguardar la confidencialidad y la integridad de la información, de garantizar la autenticidad de los datos y de los mensajes, y de defender a los sistemas de ataques internos o provenientes de las redes. Por otro lado las técnicas de protección han madurado, llevando al desarrollo de aplicaciones fácilmente disponibles para garantizar un alto grado de seguridad.

En este curso se estudian los aspectos básicos de la seguridad informática (confidencialidad, disponibilidad, integridad y autenticidad) en lo que atañe a las computadoras y a las redes. Después de explicar la terminología pertinente, se identifican las vulnerabilidades y riesgos que podrían afectar la seguridad de un sistema. Se muestran las herramientas usadas por los hackers para penetrar en las redes, explotando las brechas de los sistemas operativos y el descuido de los usuarios. Se analizan distintas formas de ataque, tales violación de contraseñas, captura de tráfico y negación de servicio. Se hace énfasis en la importancia de desarrollar una estrategia de seguridad integral con políticas, procedimientos y planes de contingencia. Se llevan a cabo experiencias prácticas a fin de familiarizarse con las nuevas tecnologías de seguridad utilizadas en ambiente corporativo y en las transacciones electrónicas, tales claves públicas y privadas, firmas digitales, autoridades de certificación, barreras de protección, redes privadas virtuales (VPN), etc.

OBJETIVO GENERAL

Conocer y evaluar los problemas de seguridad que afectan a las organizaciones que manejan sistemas informáticos y que poseen redes privadas o están conectadas a redes públicas como Internet. Aprender cómo implantar las medidas apropiadas para defenderse de las amenazas internas y externas a través de técnicas tales como criptografía, identificación, control de acceso, autenticación, detección de intrusos y barreras de protección (firewalls).

CONTENIDO

FACULTAD:	ESCUELA:	DEPARTAMENTO:	
Ingeniería.	Ingeniería Eléctrica.	Comunicaciones	
ASIGNATURA: Seguridad en Redes y Criptografía		**CÓDIGO:** 2450	**PAG.:** 2 **DE:** 5
REQUISITOS: Comunicaciones II (2427), 150 Unidades			**UNIDADES:** **4**

HORAS					
TEORÍA	**PRÁCTICA**	**TRAB. SUPERV.**	**LABORATORIO**	**SEMINARIO**	**TOTALES DE ESTUDIO**
3	1				

A- PROGRAMA SINÓPTICO

Aspectos generales sobre seguridad. Vulnerabilidades y riesgos. Medidas de protección Defensa contra intrusos y firewalls. Sistemas criptográficos modernos. Sistemas de clave pública. Identificación y control de acceso. Control de errores. Seguridad en redes. Acceso remoto y VPN

B- PROGRAMA DETALLADO

TEMA 1. ASPECTOS GENERALES SOBRE SEGURIDAD

Introducción. Modelo para un sistema de seguridad. Ejemplos de amenazas a la seguridad. Fuentes de información sobre seguridad en Internet. Bibliografía.

TEMA 2. VULNERABILIDADES Y RIESGOS - 1

Medios de transmisión. Transmisión analógica y digital. Intercepción de datos e intervención telefónica. Privacidad y libre flujo de información. Accidentes y catástrofes. Terrorismo, guerra y espionaje cibernético. Fallas, congestión y errores en el software.

TEMA 3. VULNERABILIDADES Y RIESGOS - 2

Virus, caballos de Troya y bombas lógicas. Cookies y spams. Intrusos y hackers. Ataques de negación de servicio. Fraudes telefónicos y phreakers. Fraudes en telefonía móvil celular. Delitos informáticos y fraudes bancarios. Piratería de software. Piratería en audio y video.

TEMA 4. MEDIDAS DE PROTECCIÓN - 1

Planificación de la seguridad. Análisis de riesgos. Evaluación de vulnerabilidades. Políticas de seguridad. Plan de contingencia y prevención de desastres.

TEMA 5. MEDIDAS DE PROTECCIÓN - 2

Aspectos generales. Protección contra fallas eléctricas. Sistemas tolerantes a fallas. Protección contra los virus. Propiedad intelectual y protección del software. Aspectos legales y éticos. Privacidad, libertad y comercio electrónico.

TEMA 6. DEFENSA CONTRA INTRUSOS Y FIREWALLS

Sistemas de detección de intrusos (IDS). Los cortafuegos (firewalls). Los filtros de paquetes. Configuración de filtros.

TEMA 7. LA CRIPTOLOGÍA

Criptografía, criptoanálisis y esteganografía. Técnicas de cifrado. Sistema DES (Data Encryption Standard). Complejidad de los algoritmos. Generación de números aleatorios. Distribución de claves.

Fecha Emisión:	Nro. Emisión:	Período Vigente:	Ultimo Período:
Enero 2003	**3ra**	**Mayo de 1994**	

Profesor:	Jefe Dpto.:	Director:	Aprob. Cons. Escuela:	Aprob. Cons. Facul.:
Vincenzo M.	**M. Wesolowsky**	**E. Tremamunno**	**Mayo 1994**	**Mayo de 1994**

HORAS					
TEORÍA	PRÁCTICA	TRAB. SUPERV.	LABORATORIO	SEMINARIO	TOTALES DE ESTUDIO
3	1				

TEMA 8. SISTEMAS CRIPTOGRÁFICOS MODERNOS
Nuevos algoritmos de cifrado (IDEA, SAFER, CAST, Blowfish, RC2, RC4, RC5, Clipper, AES). Herramientas para la esteganografía (S-Tools, Texto, Mandelsteg, Stealth). Otros productos y aplicaciones.

TEMA 9. SISTEMAS DE CLAVE PÚBLICA
Criptografía de 2 claves. Sistema RSA (Rivest-Shamir-Adleman). Introducción a la teoría de números. Distribución de claves. Sistema DH (Diffie-Hellman). Función hash y firma digital (MD4, MD5, SHA, DSS). Certificados digitales X.509 y PKI. Correo electrónico seguro con Outlook y PGP.

TEMA 10. IDENTIFICACIÓN Y CONTROL DE ACCESO
Uso de contraseñas. Sistemas de contraseñas dinámicas y tarjetas inteligentes. Técnicas biométricas. Control de acceso a datos y autorización. Seguridad y control de acceso en Windows NT/2000 y Unix.

TEMA 11. CONTROL DE ERRORES
La integridad de la información. Los métodos de detección de errores. Estrategias de control de errores.

TEMA 12. SEGURIDAD EN REDES
Aspectos generales. El cifrado en el modelo de capas OSI. Seguridad en las capas altas (SSL, PCT, SET, S-HTTP, S/MIME).

TEMA 13. ACCESO REMOTO Y VPN
Seguridad para el acceso remoto. Redes privadas virtuales (VPN).

C- PROGRAMA DE LABORATORIO

No existe laboratorio para esta asignatura

D- REQUISITOS

Haber aprobado las asignaturas:

Comunicaciones II

150 Unidades

FACULTAD: Ingeniería.	ESCUELA: Ingeniería Eléctrica.	DEPARTAMENTO: Comunicaciones	
ASIGNATURA: Seguridad en Redes y Criptografía		CÓDIGO: 2450	PAG.: 4 DE: 5
REQUISITOS: Comunicaciones II (2427), 150 Unidades			UNIDADES: 4

HORAS					
TEORÍA	PRÁCTICA	TRAB. SUPERV.	LABORATORIO	SEMINARIO	TOTALES DE ESTUDIO
3	1				

E- PROGRAMACIÓN CRONOLÓGICA

El tiempo total destinado a esta asignatura se distribuirá de la siguiente manera**:**

TEORÍA

TEMAS	HORAS
1-3	12
4-6	12
7-10	12
11-13	12
TOTALES	48

LABORATORIO

TEMA	HORAS

F- HORAS DE CONTACTO

La asignatura comprende:

48 horas de teoría.

4 horas de evaluación.

Lo que permite una distribución semanal de 4 horas de teoría

G- PLAN DE EVALUACIÓN

La calificación del alumno se obtendrá de la aplicación de los siguiente instrumentos:

TEORÍA.

Instrumento	Contenido A Evaluar	Valor Porcentual
Examen parcial (1^{ro})	Temas 1-6	30%
Examen parcial (2^{do})	Temas 7-13	30%

SUBTOTAL DE TEORÍA: 60%

FACULTAD: Ingeniería.	ESCUELA: Ingeniería Eléctrica.	DEPARTAMENTO: Comunicaciones	
ASIGNATURA: Seguridad en Redes y Criptografía		CÓDIGO: 2450	PAG.: 5 DE: 5
REQUISITOS: Comunicaciones II (2427), 150 Unidades			UNIDADES: 4

HORAS					
TEORÍA	PRÁCTICA	TRAB. SUPERV.	LABORATORIO	SEMINARIO	TOTALES DE ESTUDIO
3	1				

PRACTICAS

Instrumento	Contenido A Evaluar	Valor Porcentual
Tareas para la casa	Tema en tratamiento	40%

SUBTOTAL DE PRACTICAS: 40%

NOTA DEFINITIVA: 60% (teoría) + 40% (prácticas).

H- BIBLIOGRAFÍA

1. Chris Brenton, *Mastering Network Security*, Sybex, 1999.
2. Anonymous, *Maximum Security: A Hacker's Guide to Protecting your Internet Site and Network*, Sams Publishing, 1999.
3. *IT Security Cookbook*, Boran Consulting, 2000.
4. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1999.
5. Manuel Lucena López, *Criptografía y Seguridad en Computadores*, Universidad de Jaen, España, 1999.
6. Antonio Villalón Huerta, *Seguridad en Unix y Redes*, 2000.
7. Manuel Pons Martorell, *Criptología*, Escuela Universitaria Politécnica de Marató, España, 2000.
8. José de Jesús Angel, *Criptografía para Principiantes*, 1999.
9. Fernando Pardo Seco, *Apuntes de Criptografía*, 1999.
10. Simson Garfinkel y Gene Spafford, *Seguridad y Comercio en el Web*, McGraw-Hill, 1999.
11. William Stalling, *Cryptography and Network Security: Principles and Practice*, Second Edition, Prentice Hall, 1999.
12. Dieter Gollmann, *Computer Security*, John Wiley & Sons, 1999.

Fecha Emisión: Enero 2003	Nro. Emisión: 3ra	Período Vigente: Mayo de 1994	Ultimo Período:

Profesor: Vincenzo M.	Jefe Dpto.: M. Wesolowsky	Director: E. Tremamunno	Aprob. Cons. Escuela: Mayo 1994	Aprob. Cons. Facul.: Mayo de 1994