EL 65C SEGURIDAD EN TELECOMUNICACIONES

08 U.D.

REQUISITOS: EL 55A Sistemas de Telecomunicaciones DH: (3-2-3)
EL 54B Sistemas para el procesamiento de la Información

CARACTER: Electivo de la carrera de Ingeniería Civil Electricista.

OBJETIVOS:

General:

Comprender y aplicar los conceptos de seguridad que se aplican a las redes de telecomunicaciones y a la empresa en general

Específicos:

- Aplicar técnicas de control de acceso a los sistemas
- Conocer como funcionan elementos que permiten mejorar la seguridad en una red de datos
- Entender y manejar redes privadas virtuales
- Conocer metodologías y herramientas de hacking legalmente permitido.
- Entender como se administra la seguridad en la empresa
- Aplicar protocolos y dispositivos de seguridad para hacer negocios utilizando redes públicas (e-business)

CONTENIDOS: Horas de Clases

1. Introducción Importancia de la seguridad en la empresa 1,0

1.1. Tendencias y estadísticas
1.2. Certificaciones y estándares en Seguridad
1.3. Objetivos del curso

2. Control de acceso a los sistemas 2,0

2.1. Identificación, autenticación, autorización y accounting
2.2. Matriz de acceso, listas de acceso
2.3. Protocolos de control de acceso

3. Dispositivos de seguridad en red 2,0

3.1 Firewall
3.2 Intrusion Detection Systems
3.3 Honeypots
3.4 Uso de routers y switches para mejorar la seguridad

4. Criptografía 2,0

4.1 Repaso de teoría de números y de la información

4.2 Criptografía simétrica y asimétrica
4.3 Ejemplos de algoritmos y técnicas de cifrado.

5. Redes Privadas Virtuales (VPNs) 1,0

5.1 Tipos de VPN
5.2 Tecnologías de VPNs: MPLS, L2TP, IPSec
5.3 Detalles de IPSec

.

6. Seguridad en e-business 2,0

6.1 Entorno requerido: PKI
6.2 Negocios entre empresas y usuarios (B2B, B2C)
6.3 Seguridad en la WEB: SSL, SET
6.4 Marco legal

7. Cómo administrar la seguridad en la empresa 1,0

7.1 Ciclo de la seguridad
7.2 Conceptos básicos (triada CIA)
7.3 Amenaza, Costo, Vulnerabilidad, Riesgo
7.4 Análisis Cualitativo y Cuantitativo
7.5 Políticas y procedimientos
7.6 Mantención de la seguridad

8. Seguridad en redes Inalámbricas 1,0

8.1 Introducción a redes Wireless
8.2 Arquitecturas y protocolos para mejorar la seguridad

9. Seguridad en telefonía IP 1,0

9.1 Introducción a la telefonía IP
9.2 Autenticación de usuarios
9.3 Uso de IPSec

ACTIVIDADES:

Clases expositivas y actividades practicas (auxiliares)
Controles y tareas

EVALUACION:

La nota final se calcula de la siguiente forma:

$$NF = 0.4\,NT + 0.6\,NC$$

NT : Nota Tares
NC : Nota de Control

BIBLIOGRAFIA:

1. CISSP Certification, All in One, Shon Harris, McGraw-Hill/Osborne 2002.

2. Network Security, Private Communication in a public world (2nd Edition), Charlie Kaufman, Radia Perlman, Mike Speciner, Prentice Hall 2002.

3. Maximun Linux Security (2nd Edition), John Ray, Anonymous, Sams 2001.

4. The CISSP Prep Guide: Gold Edition, Ronald L. Krutz, Russell Dean Vines, John Wiley & Sons 2002.

5. Computer Networks, Fourth Edition, Andrew S. Tanenbaum, Prentice Hall PTR 2002.

6. CISSP Examination Textbooks, Volume 2: Practice, S. Rao Vallabhaneni & Devi Vallabhaneni, SRV Professional Publications, 2002

Links:

http://www.sans.org
http://www.nsa.gov
http://www.cert.org
http://computer.org/security
https://www.isc2.org/cgi-bin/index.cgi
http://packetstorm.linuxsecurity.com
http://www.kriptoplis.com
http://www.hispasec.com
http://www.icsa.com
http://www.nist.gov
http://www.cccure.org
http://www.isaca.org
http://www.coso.org
http://www.cisecurity.org

RESUMEN DE CONTENIDOS:

Introducción. Control de acceso a los sistemas. Dispositivos de seguridad en red. Criptografia. Redes Privadas Virtuales (VPNs). Aplicaciones seguras en Internet. Inseguridad en la red. Seguridad en e-business. Cómo administrar la seguridad en la empresa. Seguridad en redes Inalámbricas. Seguridad en telefonía IP.