UNIVERSIDAD INTERAMERICANA DE PUERTO RICO
RECINTO METROPOLITANO
FACULTAD DE CIENCIAS Y TECNOLOGÍA
PROGRAMA GRADUADO
SEGURIDAD Y GARANTIA DE INFORMACIÓN

PRONTUARIO

I. INFORMACIÓN GENERAL

Título del Curso	:	Seguridad en Redes de Voz sobre Internet(VoIP)
Código y Número	:	INSE 5400
Créditos	:	3
Término Académico	:	
Profesor(a)	:	
Horas de Oficina	:	
Teléfono de la Oficina	:	787-250-1912 Ext 2230
Correo Electrónico	:	

II. DESCRIPCIÓN

Análisis de los fundamentos relacionados con la utilización del protocolo de Internet (IP) para la realización de llamadas de voz, correos electrónicos, mensajes instantáneos y páginas Web a través de computadoras o teléfonos celulares. Examen de las tecnologías que componen el VoIP que transmiten voz y otros datos multimedios a través de la Web. Evaluaciones de las amenazas, los riesgos y la seguridad de las tecnologías de VoIP. Requiere horas adicionales en un laboratorio abierto virtual.

III. OBJETIVOS

Se espera que al finalizar el curso, el estudiante pueda:

1. Explicar el concepto de VoIP y su utilización.
2. Distinguir entre los diferentes aspectos de seguridad que contiene VoIP
3. Poder explicar el proceso de implementación de VoIP en una red.
4. Mencionar los diferentes protocolos dentro de VoIP.
5. Poder explicar algunos aspectos de problemas técnicos que pueden surgir en VoIP.

IV. CONTENIDO DEL CURSO

A. Introduction to VoIP

1. What is VoIP?
2. Why use IP for Voice?
3. VoIP-Convergence of Technologies
4. Basic VoIP Architecture

5. Need of a Layered Architecture
6. VoIP Layers
7. TCP/IP Overview
    a. Functions of TCP/IP Layers
8. VoIP Layers Vs. TCP/IP Layers
9. Public Switched Telephone Networking(PSTN)
10. Circuit Switching Vs. Packet Switching
11. Basic VoIP Features
12. Benefits of VoIP
13. Building The ROI Model
14. Disadvantages of VoIP
15. Future of VoIP
16. Growth in VoIP Subscribers

B. Analog to Digital Conversions

1. Source:
    a. A to D Conversion
    b. Types of ADC's
    c. Sigma Delta ADC
    d. Successive Approximation ADC
    e. Pipelined ADC
    f. Flash ADC
    g. Comparison of ADC's
    h. Working of ADC's
    i. Voice Compression
    j. Encryption
    k. Headers
2. Destination
    a. Sequencing
    b. Decryption
    c. Decompression
    d. Digital to Analog Conversion

C. Traditional Voice Telephony Principles

1. Analog Signaling
2. Types of Analog Signaling
    a. Earth & Magnet (E&M) Signaling
    b. Loop-Start

c. Ground-Start
d. Dial-Pulse Signaling
e. Dual Tone Multi-Frequency Signaling

3. Analog Systems
4. Analog Network Components
5. Cabling
6. Basic Telephone System Operation
7. Plain Old Telephone Service (POTS)
8. Direct Inward Dialing (DID)
9. Digital Subscriber Line (DSL)
10. Digital Loop Carrier (DLC)
11. Passive Optical Network (PON)
12. Dial Plans
13. Four-Wire Circuit
14. Time Division Multiplexing (TDM)
15. Call Control Signaling
16. Signaling System 7 (SS7)
    a. Signaling Points
    b. Signaling Links
    c. SS7 Protocol Stack

D. VoIP Devices and Cisco Components

1. Basic VoIP Equipments
2. VoIP Network Components
    a. Analog Telephone Adaptor (ATA)
    b. Media Gateway
    c. Features of Media Gateway
    d. Media Gateway Controller
    e. Signaling Gateway
    f. Call Manager
    g. VoIP Switches
    h. IP Phones
    i. Private Branch eXchange (PBX)
    j. PSTN Gateway
    k. Session Controller
    l. Modems
    m. VoIP Router
    n. Cisco's VoIP Components

o. Types of VoIP Ports
p. Foreign Exchange Station (FXS)
q. Foreign Exchange Office (FXO)
r. Earth & Magnet (E&M) Interface
s. VNM/VIC
t. VNM Models: NM-1V
u. VNM Models: NM-2V
v. VNM Models: NM-HDV High-Density VNM
w. VIC Models: VIC-2E/M
x. VIC-2FXS
y. VIC-2FXO
z. VWIC-2MFT-T1
aa. Two-Port ISDN BRI Card
bb. Four-Port Analog DID/FXS VICs

E. Configuring VoIP

1. Prerequisites for VoIP Configuration
2. Voice Port Cabling and Configuration
   a) Port Numbering: 1700 Series
   b) Port Numbering: Cisco 1760
   c) Port Numbering: 2600 and 3600 Series
   d) Port Numbering: MC3810 Series
   e) Port Numbering: 7200 Series
   f) Port Numbering: AS5300 Series
   g) Port Numbering: AS5x00 Series
3. Configuring Voice Ports
4. Configuring FXO or FXS Voice Ports
5. Configuring E&M Ports
6. Configuring to adjust Parameters of E&M Ports
7. Configuring DID Ports
8. Connection Command
9. Configuring Delay
   a) Fine-Tuning FXS/FXO Ports
   b) Fine-Tuning E&M Ports
   c) Fine-Tuning DID Ports
   d) Configuring POTS Dial Peers
   e) Configuring Dial-Peer For VoIP
   f) Configuring Dial-Peer For VoFR

g) Configuring Dial-Peer For VoATM

10. Configuring Trunking
    a) Supervisory Disconnect
    b) Configuring a Supervisory Disconnect Voice Class
    c) Configuring ISDN BRI Voice Ports
    d) Configuring ISDN PRI Voice Ports
    e) Configuring ISDN PRI Voice Ports with Q.931
    f) Configuring QSIG
    g) Configuring T-CCS
11. Configuring H.323 Gateways
12. Configuring H.323 Gatekeepers
    a) H.323 ID Addresses
    b) Zone Prefixes
    c) Gatekeeper Zone Prefix
    d) Technology Prefixes
    e) IP Precedence
    f) RTP Priority
    g) Traffic Shaping
13. Configuring cRTP
    a) Enable cRTP on a Serial Interface
    b) Enable cRTP with Frame Relay Encapsulation
    c) Change the Number Of Header Compression Connections
    d) Displaying Statistics
    e) Configuring Custom Queuing
    f) Enabling Custom Queuing
    g) Applying Configuration to an Interface
    h) Enabling Priority Queuing: Priority-List Command
    i) Enabling Priority Queuing: Set Up Configuration
    j) Configuring the Queue Limits
14. Applying Priority List to an Interface
    a) Verifying Priority Queuing: Show Interface Command
    b) Verifying Priority Queuing: Show Queuing Priority Command
15. Enabling Weighted Fair queuing
    a) Verifying Weighted Fair Queuing: Show Interface Command
    b) Verifying Weighted Fair Queuing: Show Queuing Command
16. Configuring Class-Based Weighted Fair Queuing (CBWFQ)
    a) Defining Class Maps

b) Creating Policies
c) Attaching Policies to Interfaces
d) Verifying CBWFQ: Show-Policy-Map Command
e) Verifying CBWFQ: Show-Policy-Map Interface Command
f) Configuring Packet Classification
g) IP Precedence
h) Verifying IP Precedence
i) Policy Routing
j) Verifying Policy Routing

17. Configuring RSVP
    a) Verifying RSVP
18. Call Admission Control (CAC)
    a) Verifying Call Admission Control
    b) Configuring Priority Queuing with WFQ
    c) Verifying Priority Queuing with WFQ
19. Configuring Traffic Shaping
    a) Verifying Traffic Shaping
20. Configuring Congestion Avoidance with WRED
    a) Verifying WRED
21. Configuring Link fragmentation and Interleaving
    a) Verifying Link fragmentation and Interleaving
22. Configuring a Single-Router VoIP Network
    a) Reviewing the Design
    b) Configuring the Router: Step by Step
    c) Testing and Verification

F. Implementation and Applications of VoIP

1. VoIP Implementation Types
    a. Phone to Phone Connection
    b. Analog Telephone Adaptor (ATA) Setup
    c. Phone to Phone Connection Using Gateway
    d. Phone to Phone Connection Using Router
    e. Computer to Computer Connection
    f. Phone to Computer and Vice-Versa
2. IP-Enabled PBX (Private Branch Exchange) Method
3. IP Centric LAN Method
4. Satellite VoIP
5. Software Support for VoIP

6. Applications of VoIP
    a. What is Skype?
    b. System Requirements
    c. Getting Started with Skype
    d. Skype is Safe
    e. Features of Skype
7. Skype for Windows
8. Skype for Mac OSX
9. Skype for LINUX
10. Skype for Business
11. Skype Web Toolbar
12. Skype Email Toolbar
13. Skype Office Toolbar
14. Skype for Mobile

G. Quality of Service (QoS) of VoIP

1. Introduction to QoS
2. Quality of Experience (QoE) Vs. QoS
3. QoE for VoIP
4. Why is QoS needed in IP Transmission?
5. Why is QoS needed for VoIP Networks?
6. Factors Affecting Quality of Voice in VoIP
7. QoS Monitoring
    a. Passive Monitoring
    b. Active Monitoring
8. QoS Protocols
    a. RTP
    b. RTCP
    c. RSVP
9. Multiprotocol Label Switching (MPLS)
10. Integrated Services (IntServ)
11. Differentiated Services (DiffServ)
12. IntServ Vs. DiffServ

H. H.323 Standards

1. VoIP Standards
2. What is the need for VoIP Protocols?
3. Introduction to H.323

a. Network Components of H.323
b. Components of H.323
c. H.323 Protocols Suite
d. H.323 Protocol Stack
e. Control and Signaling in H.323
f. H.323 Advantages
g. Network Address Translation (NAT)
h. H.323 and NAT

4. H.225
   a. H.225/Q.931 Call Signaling
   b. Q.931 Call Signaling Messages
   c. H.225/Q.931 Signaling
   d. H.225 Registration, Admission, Status (RAS)
   e. H.225/Q.931 RAS
   f. Key RAS Messages
   g. H.225 Protocol Structure
   h. H.225 Security Considerations
   i. H.235: Security and Encryption for H.323
   j. H.245 Call Control Messages
   k. H.245 Call Control
   l. H.245 Security Mechanism
5. H.261 (Video Stream for Transport Using the Real-Time Transport)
6. H.263 (Bitstream in the Real-Time Transport Protocol)
7. DVB (Digital Video Broadcasting)
8. H.450.1
9. H.450.2
10. H.450.3
11. H.450.4
12. H.450.5
13. H.450.6
14. H.450.7
15. H.450.8
16. T.38
17. T.120
18. T.121
19. T.122
20. T.124

21. T.125
22. T.126
23. T.127

I. SIP and Supporting Protocols

1. Session Initiation Protocol (SIP)
    a. Components of SIP
    b. SIP Messages
    c. Headers for SIP Entities
    d. SIP Functions
    e. SIP: Supported Protocols
    f. Understanding SIP's Architecture
    g. Registering with a SIP Registrar
    h. Requests through Proxy Servers
    i. Requests through Redirect Servers
    j. Peer to Peer Architecture
    k. Instant Messaging and SIMPLE
    l. SIP security
    m. H.323 Vs. SIP
2. Session Description Protocol (SDP)
    a. SDP Specifications
    b. Security Issues
3. Real-Time Transport Protocol (RTP)
4. Real-Time Transport Control Protocol (RTCP)
5. Real-Time Transport Streaming Protocol (RTSP)
6. Simple Gateway Control Protocol (SGCP)
7. Session Announcement Protocol (SAP)
8. Skinny Client Control Protocol (SCCP)
9. Security Implications for Skinny
10. Dynamic Host Configuration Protocol (DHCP)
11. Trivial File Transfer Protocol (TFTP)
12. Hyper Text Transfer Protocol (HTTP)
13. Skype Protocol
14. Inter-Asterisk Exchange (IAX)
15. Simple Network Management Protocol (SNMP)

J. Megaco Protocol

1. Media Gateway Control Protocol (MGCP)

2. History of Megaco (H.248)
3. Media Gateway Reference Architecture
4. MGCP Connections
5. Per-Call Requirements
6. Megaco Vs. MGCP
7. Megaco Protocol Design
8. Megaco Commands
9. Megaco Messaging Sequence
10. Megaco Packages
11. Megaco IP Phone Media Gateway
12. Role of Call Processing Language
13. Call Processing Language Characteristics
14. Protocol Security

K. Resource Reservation Protocol

1. Resource Reservation Protocol (RSVP)
2. RSVP Setup
3. RSVP Message Structure
4. RSVP Message
5. RSVP Message Types
6. RSVP Object Fields
7. RSVP Object Classes
8. RSVP Operation
9. RSVP Data Payload
10. RSVP Quality of Service
11. RSVP Session Start-up
12. RSVP Reservation Style
13. RSVP Tunneling
14. RSVP Traffic Control Module
15. Security Implications

L. Wireless VoIP

1. Voice Over WLAN (VoWLAN)
    a. VoWLAN Call Routing
    b. Characteristics of VoWLAN
    c. Limitations of VoWLAN
2. Wireless VoIP
    a. Wireless VoIP Deployment

b. Advantages of Wireless VoIP
c. Limitations of Wireless VoIP
d. Standards and Protocols

3. Unlicensed Mobile Access (UMA)
4. Wireless VoIP Gateway: AH1038
5. Wireless VoIP Gateway: D-Link DVG-G1402S
6. Wireless VoIP Gateway: Motorola HH1620 DSL
7. Wireless IP Phone
8. Wireless VoIP Phone: EZLoop
9. Wireless VoIP Phone: P-2000W_V2
10. Wireless VoIP Phone: Shenzhen WP10W-S
11. Challenges to Build Successful Wireless VoIP Product
12. Attacks on Wireless VoIP

M. Encryption Techniques for VoIP

1. Encryption
   a. Why VoIP needs Encryption?
   b. VoIP Encryption
   c. How to Encrypt VoIP?
   d. Pros & Cons of VoIP Encryption
   e. Voice and Data Encryption Device (V/DED)
   f. Speech Encryption
   g. Media Encryption
   h. Wireless Encryption
2. IPSec and Role of IPSec in VoIP
   a. Transport Mode
   b. Tunnel Mode
3. Solutions to VoIPSec Issues
   a. IETF Encryption Solutions for VoIP
   b. Suites from the IETF
   c. S/MIME: Message Authentication
   d. Transport Layer Security (TLS)
   e. TLS: Key Exchange and Signaling Packet Security
   f. Secure Real-Time Transport Protocol (SRTP)
4. SRTP: Voice/ Video Packet Security

N. Troubleshooting VoIP Network

1. Issues of Network Slow Down

2. Troubleshooting Packet Loss
3. Troubleshooting Jitter
4. Troubleshooting Packetization Delay
5. Troubleshooting Bandwidth Problems
6. Troubleshooting Echo
7. Troubleshooting Voice Quality on Voice Ports
8. Troubleshooting Two-stage Dialing Failures
9. Troubleshooting Socket Failures
10. Troubleshooting Speech Recognition
11. Troubleshooting Cabling
12. Troubleshooting Private Branch Exchange (PBX) Problems
13. Troubleshooting Central Office (CO) Problems
14. Troubleshooting Trunk Signaling
15. Troubleshooting Gateways and Gatekeepers
16. Troubleshooting Dial Peers
17. Troubleshooting Serial Interfaces
18. Troubleshooting Frame Relay
19. Troubleshooting FXS and FXO Voice Ports
20. Troubleshooting E&M Voice Ports
21. Troubleshooting Dial Plans
22. Basic VoIP Issues and Solutions
23. Troubleshooting RSVP
24. Troubleshooting MGCP
25. Troubleshooting RTP
26. Troubleshooting RTSP

O. VoIP Testing and Tools

1. Test Strategy
2. VoIP Network Component Testing
    a. Gateway Testing
    b. Gatekeeper Testing
    c. IVR Testing
    d. Billing and Prepaid Testing
    e. NMS Testing
    f. VoIP Test Suite
3. MediaPro: VoIP and Video Analyzer
4. 323Sim: H.323 Simulator
5. Vulnerability Assessment

6. Penetration and Vulnerability Testing
7. VoIP Security Tools
8. VoIP Sniffing Tools
    a. Auth Tool
    b. VoIPong
    c. Vomit
    d. PSIPDump
    e. Netdude
    f. Oreka
    g. Wireshark
    h. Web Interface for SIP Trace (WIST)
    i. RTP Break
9. VoIP Scanning and Enumeration Tools
    a. SNScan
    b. Netcat
    c. Smap
    d. SIPScan
    e. SIPcrack
    f. VoIPaudit
    g. iWAR
    h. SiVUS
    i. SCTPscan
10. VoIP Packet Creation and Flooding Tools
    a. Sipsak
    b. SIPp
    c. SIPNess Messenger
    d. SIP Bomber
    e. Spitter
    f. Sip Send Fun
    g. Scapy
11. VoIP Fuzzing Tools
    a. Ohrwurm
    b. Fuzzy Packet
    c. SIP Forum Test Framework (SFTF)
    d. Asteroid
    e. SIP-Proxy
12. VoIP Signaling Manipulation Tools

a. RTP Tools
b. Tcpdump
c. Windump
d. Ethereal (Wireshark)
e. Softperfect Network Sniffer
f. Http Sniffer
g. Ether Detect Packet Sniffer
h. Iris Network Traffic Analyzer
i. SmartSniff
j. NetResident Tool

13. VoIP Troubleshooting Tools
    a. P.862
    b. P.563
    c. RTCP-RFC3550
    d. RTCP XR-RFC3611
    e. Packet Statistics
    f. Test Tools
    g. Traceroute
    h. VQmon
14. Other VoIP Tools

P. Threats to VoIP Communication Network

1. VoIP is Prone to Numerous Threats
2. VoIP Vulnerabilities
    a. Denial of Service (DOS)
    b. DoS Attack Scenarios
    c. Eavesdropping
    d. Packet Spoofing and Masquerading
    e. Replay Attack
    f. Call Redirection and Hijacking
    g. ARP Spoofing
    h. ARP Spoofing Attack Scenarios
    i. Service Interception
    j. H.323-Specific Attacks
    k. SIP Security Vulnerabilities

Q. VoIP Security

1. Why VoIP Security?

2. Constituents of VoIP Security
3. VoIP Myths and Realities
4. Securing VoIP with DoS Attacks
5. Securing against Replay Attack
6. Securing ARP Caches against ARP Manipulation
7. Securing H.235 Protocol
8. Transport Layer Security (TLS)
9. Skype Protocol Security
10. IAX Protocol Security
11. Security Implications for TFTP
12. Security Implications for HTTP
13. Security Implications for DHCP
14. Security Policies and Processes
15. Physical Security
    a. Human Safeguard Recommendations
    b. Environmental Safeguard Recommendations
16. Network Intrusion Detection Systems
17. Host-Based Intrusion Detection Systems
18. Guidelines for Securing VoIP Network
19. Best-Practice Approaches for Minimizing common VoIP Network Risks

R. Logical Segregation of Network Traffic

1. Logical Separation of Data
2. Converged Network
3. Virtual LANs (VLANs)
    a. VLAN Security
    b. VLANs and Softphones
4. QoS and Traffic Shaping
5. NAT and IP Addressing
    a. How does NAT Work?
    b. NAT: Modes of Operation
    c. NAT and Encryption
6. Authentication Header (AH)
    a. AH: Transport and Tunnel Modes
7. Encapsulation Security Payload (ESP)
    a. ESP Header: Transport Mode and Tunnel Mode
8. Firewalls
    a. Deep packet Inspection (DPI)

b. Shallow packet Inspection
c. Stateful Inspection
d. Medium-Depth Packet Inspection

9. VoIP-Aware Firewalls Issues
   a. H.323 Firewalls Issues
   b. SIP Firewalls Issues
   c. Bypassing Firewalls and NAT
   d. Methods for Enabling SIP
10. Access Control Lists

S. Hardware and Software VoIP Vendors

1. Alcatel
2. Global Crossing
3. Avaya
4. Whaleback
5. Nortel
6. Norstar VoIP Gateway
7. Polycom
8. Packet8
9. Vonexus
10. Infotel
11. Net 4 India
12. Dialexia
13. NGT
14. Qwest
15. Pingtel
16. Cisco
17. 3Com
18. Vocalocity
19. Motorola
20. Nokia

T. Regulatory Compliance of VoIP

1. Regulatory Compliance
   a. Sarbanes-Oxley Act (SOX)
   b. Management Assessment of Internal Controls
   c. SOX Compliance and Enforcement
   d. Gramm-Leach-Bliley Act (GLBA)

e. Privacy Rule -Protection of Nonpublic Personal Information

f. Risk Management Guidelines for VoIP Systems

g. Development and Implementation of Information Security

h. Health Insurance Portability and Accountability Act (HIPAA)

i. Security Standards for the Protection of PHI

j. Safeguards Standard for the Protection of PHI

k. Types of Safeguards

1) Administrative safeguards

2) Physical safeguards

3) Technical safeguards

l. Communication Assistance for Law Enforcement ACT (CALEA)

m. Assistance Capability Requirements

n. Cooperation of Equipment Manufacturers and Providers of Telecommunications Support Services

o. Technical Requirements and Standards

p. Steps to Resolve CALEA

q. Enhanced 911 and Related Regulations

r. E911 Regulatory Basics

s. European Union (EU) Regulatory Framework

t. EU Regulatory Basics

U. VoIP Hacking

1. Types of VoIP Hacking

2. Stages of VoIP Hacking:

   a. Foot printing

   b. Scanning

   c. Enumeration

3. Footprinting

   a. Information Sources

   b. Unearthing Information

   c. Organizational Structure and Corporate Locations

   d. Help Desk

   e. Job Listings

   f. Phone Numbers and Extensions

g. VoIP Vendors

h. Resumes

i. WHOIS and DNS Analysis

j. Steps to Perform Footprinting

4. Scanning

a. Objectives of Scanning

b. Host/Device Discovery

c. ICMP Ping Sweeps

d. ARP Pings

e. TCP Ping Scans

f. SNMP Sweeps

g. Port Scanning and Service Discovery

h. TCP SYN Scan

i. UDP Scan

j. Host/Device Identification

5. What is Enumeration?

a. Steps to Perform Enumeration

b. Banner Grabbing with Netcat

c. SIP User/Extension Enumeration

d. REGISTER Username Enumeration

e. INVITE Username Enumeration

f. OPTIONS Username Enumeration

g. Automated OPTIONS Scanning with sipsak

h. Automated REGISTER, INVITE and OPTIONS Scanning with SIPSCAN against SIP server

i. Automated OPTIONS Scanning Using SIPSCAN against SIP Phones

j. Enumerating TFTP Servers

k. SNMP Enumeration

l. Enumerating VxWorks VoIP Devices

6. Steps to Exploit the Network

a. DoS & DDoS Attacks

b. Flooding Attacks

c. DNS Cache Poisoning

d. Sniffing TFTP Configuration File Transfers

e. Performing Number Harvesting and Call Pattern Tracking

f. Call Eavesdropping

g. Interception through VoIP Signaling Manipulation

h. Man-In-The-Middle (MITM) Attack

i. Application-Level Interception Techniques

j. How to Insert Rogue Application?

k. SIP Rogue Application

l. Listening to/Recording Calls

m. Replacing/Mixing Audio

n. Dropping Calls with a Rogue SIP Proxy

o. Randomly Redirect Calls with a Rogue SIP Proxy

p. Additional Attacks with a Rogue SIP Proxy

q. What is Fuzzing?

r. Why Fuzzing?

s. Commercial VoIP Fuzzing tools

t. Signaling and Media Manipulation

u. Registration Removal with erase_registrations Tool

v. Registration Addition with add_registrations Tool

w. VoIP Phishing

7. Covering Tracks

V. ACTIVIDADES

1. Lecturas
2. Discusiones electrónicas (Foros)
3. Búsqueda bibliográfica
4. Ejercicios prácticos
5. Correo electrónico

VI. EVALUACIÓN

	Puntuación	% Nota Final
1. Foros y Asignaciones	100	25
2. Prueba Cortas	100	25
3. Laboratorios	100	25
4. Examen Final	100	25
Total	400	100

VII. NOTAS ESPECIALES

1. Recuerde que cualquier tarea del curso debe cumplir con el Reglamento General de Estudiantes de Estudiante, Capítulo V, Artículo 1, Sección B.2 que establece "El plagio, la falta de honradez, el fraude, la manipulación o falsificación de datos y cualquier otro comportamiento inapropiado relacionado con la labor académica son contrarios a los principios y normas institucionales y están sujetos a sanciones disciplinarias."

2. Todo estudiante que requiera servicios auxiliares o asistencia especial deberá solicitar los mismos al inicio del curso o tan pronto como adquiera conocimiento de que los necesita, mediante el registro correspondiente en la oficina del Consejero Profesional José Rodríguez, Coordinador de Servicios a los estudiantes con Impedimentos, ubicada en el Programa de Orientación Universitaria.

3. Uso de dispositivos electrónicos.
   Se desactivaran los teléfonos celulares y cualquier otro dispositivo electrónico que pudiese interrumpir los procesos de enseñanza y aprendizaje o alterar el ambiente conducente a la excelencia académica. Las situaciones apremiantes serán atendidas, según corresponda. Se prohíbe el manejo de dispositivos electrónicos que permitan acceder, almacenar o enviar datos durante evaluaciones o exámenes.

4. Cumplimiento con las disposiciones del Título IX
   La Ley de Educación Superior Federal, según enmendada, prohíbe el discrimen por razón de sexo en cualquier actividad académica, educativa, extracurricular, atlética o en cualquier otro programa o empleo, auspiciado o controlado por una institución de educación superior independientemente de que esta se realice dentro o fuera de los predios de la institución, si la institución recibe fondos federales.

Conforme dispone la reglamentación federal vigente, en nuestra unidad académica se ha designado un(a) Coordinador(a) Auxiliar de Titulo IX que brindará asistencia y orientación con relación a cualquier alegado incidente constitutivo de discrimen por sexo o género, acoso sexual o agresión sexual. Se puede comunicar con el Coordinador(a) Auxiliar, George Rivera, Director de Seguridad, al teléfono 787-250-1912, extensión 2147, o al correo electrónico grivera@metro.inter.edu .

El Documento Normativo titulado Normas y Procedimientos para Atender Alegadas Violaciones a las Disposiciones del Título IX es el documento que contiene las reglas institucionales para canalizar cualquier querella que se presente basada en este tipo de alegación. Este documento está disponible en el portal de la Universidad Interamericana de Puerto Rico (www.inter.edu).

VIII. RECURSOS EDUCATIVOS

Libro de texto

Recursos electrónicos:

Materiales Necesarios

- Computadora
- Servicio de Internet

IX. BIBLIOGRAFÍA

A. Libros y artículos de revistas

Pfleeger, C.P. y Pfleeger, S. L.. (2003). **Security in Computing Third Edition.** Upper Saddle River, NJ: Prentice Hall.

Code, E., Krutz, R. L., Conley, J. W. Reisman, B. Ruebush, M., y Gollman, D.. (2008). **Network Security Fundamentals**. NJ: Wiley.

Stallings, W. (2005). **Cryptography and Network Security: Principles and Practice 4rd Edition**. Upper Saddle River, NJ: Prentice Hall.

Stallings, W. (2006). **Network Security Essentials: Applications and Standards (3rd Edition)**. Upper Saddle River, NJ: Prentice Hall.

Bishop, M. (2002) **Computer Security: Art and Science**. Addison-Wesley Professional.

Brenton, C y Hunt, C. (2002). **Mastering Network Security**. Sybex

Gollmann, D. (2006) **Computer Security**. Wiley

Goldreich, O. (2004) **Foundations of Cryptography: Volume 2, Basic Applications**. Cambridge University Press

B. Referencias electrónicas:

http://www.linuxsecurity.com/ - página de Linux Security que contiene información de seguridad bajo el sistema operativo Linux.

http://www.microsoft.com/security/default.mspx - página de Microsoft que contiene información sobre seguridad (Ingles)

http://webdia.cem.itesm.mx/ac/rogomez/seguridad/index.html - página del Grupo de Interés de Seguridad Computacional del ITESM-CEM

http://www.microsoft.com/spain/technet/seguridad/recursos/glosario/default.mspx - página de Microsoft que contiene un Glosario de seguridad.

http://www.criptored.upm.es/paginas/software.htm : esta página provee acceso a programas de prácticas en criptografía y el Programa chinchon para análisis de riesgo.

http://www.mundotutoriales.com/tutoriales_seguridad_informatica-mdpal14063.htm - página de Mundo de Tutoriales que provee acceso a tutoriales de informática y seguridad.

http://www.sans.org/ - página que provee información sobre cursos y certificaciones en seguridad para diferentes sistemas operativos.

http://www.securityfocus.com_ - página que provee información sobre seguridad para diferentes sistemas operativos.

http://www.microsoft.com/spanish/msdn/latam/estudiantes/ - página de Microsoft para Estudiantes que proveen las últimas noticias sobre Microsoft Student Live y otros.