UNIVERSIDAD DEL SAGRADO CORAZÓN
DECANATO ASOCIADO DE ESTUDIOS GRADUADOS

PRONTUARIO

TÍTULO:	**Auditoría de redes y telecomunicaciones**
CODIFICACIÓN:	**GSI 751 (o ASI 751 o AUD 721)**
PRERREQUISITO:	**GSI 611 o GSI 511**
CRÉDITOS:	**Tres (3) créditos, tres (3) horas semanales, una sesión**

DESCRIPCIÓN

Estudio de los conceptos básicos de las redes. Los estudiantes conocen los componentes fundamentales de las redes y aprenden el proceso de planificación y evaluación de una red. Se da énfasis a la seguridad física, los controles técnicos, los controles de acceso y la vulnerabilidad de la red, entre otros. Se examina el proceso para llevar a cabo una auditoría de: los componentes de la red, tanto local como amplia, los aspectos de seguridad de la red y se examinan las herramientas disponibles para el análisis y auditoría de una red tanto desde la perspectiva del auditor de sistemas de información, el gerente de recursos informáticos o el oficial de seguridad. El participante aplica los conceptos del curso en ejercicios, investigaciones y proyectos de aplicación práctica.

JUSTIFICACIÓN

El comunicar, recopilar y distribuir información es una actividad vital en los negocios de hoy día. Con los avances en las telecomunicaciones y la tecnología de las computadoras, muchos negocios han implantado los sistemas de redes para distribuir y compartir la información entre clientes, empleados, proveedores y gerentes. Ante estos avances tecnológicos positivos para las empresas, también han surgido riesgos reales, por lo cual, las organizaciones tienen que asegurarse de que los recursos informáticos en la red estén disponibles, mantienen su integridad y están en un lugar seguro. Sin la seguridad, cualquier intruso, interno o externo, puede tener acceso a los recursos de información de la organización, impedir su acceso, cambiarlos, borrarlos o dañarlos. Este curso está dirigido a conocer cómo auditar la infraestructura de redes y telecomunicaciones de la organización para identificar las vulnerabilidades y los riesgos potenciales a los cuales está expuesta la red y a formular las recomendaciones para evitar estos y los posibles controles que deben establecerse.

OBJETIVOS

Al finalizar el curso, los estudiantes estarán capacitados para:

1. Distinguir los componentes básicos de una red de telecomunicaciones.
2. Definir las etapas de una auditoría
3. Planificar una auditoría y definir su alcance.
4. Reconocer los tipos de riesgos y analizar las implicaciones que tienen para las organizaciones.
5. Evaluar las herramientas e identificar los peritos que se deben incorporar al proceso de auditoría de redes.
6. Auditar los componentes físicos de la red.
7. Llevar a cabo algunos procesos de auditoría.
8. Redactar informes de auditoría de redes y telecomunicaciones

CONTENIDO

I. Tecnología de redes:
   A. Introducción:
      1. Definición
      2. Costos y beneficios
      3. Componentes físicos
      4. Programado (SW)
      5. Tipos de redes
      6. Otras consideraciones
   B. Topologías y estructuras:
      1. Estructura de una red
      2. Topologías
      3. Diagramación estructural
      4. Otras consideraciones
   C. Equipos y medios de conexión:
      1. Estructurales
      2. Servidores
      3. Medios de conexión
   D. Arquitectura de la red:
      1. Consideraciones generales
      2. Arquitecturas:
         a. “Ethernet”
         b. “Token Ring”
         c. “ARCnet”

d. “AppleTalk”
e. “FDDI”

E. Servicios:
1. Archivos compartidos
2. Impresión
3. Bancos de datos
4. Mensajería
5. Aplicaciones

F. Sistemas operativos de redes:
1. Cliente servidor
2. “Windows”
3. “Unix/Linux”
4. “Novell”
5. “Apple”

G. Modelo OSI:
1. Definición
2. Niveles:
a. Físico
b. Enlace de datos
c. Red
d. Transportación
e. Sesión
f. Presentación
g. Aplicación
3. Protocolos:
a. TCP/IP (“Transmission control protocol”):
1) TCP (“Transmission Control Protocol”):
2) IP (“Internet protocol”)
3) FTP (“File transfer protocol”)
4) HTTP (“HyperText Transfer Protocol”)
5) UDP (“User Datagram Protocol”)
6) DHCP (“Dynamic Host Configuration Protocol”)
7) DNS (“Domain Name System”)
8) HTTPS (“Secure Hypertext Transfer Protocol”)
9) SMTP (“Simple Mail Transfer Protocol”)
10) POP3 (“Post Office Protocol”)
11) ICMP (“Internet Control Message Protocol”)
12) SLIP (“Serial Line Internet Protocol”)
13) PPP (“Point-to Point Protocol”)
b. IPX/SPX (“Internetwork/sequenced packet exchange”)
4. Direccionamiento:
a. Clases de direcciones
b. Notación
c. “Masking”

H. Mecanismos de protección de las redes:
1. Riesgos y amenazas:

a. Inherentes a la tecnología
b. Naturales
c. Accidentales
d. Intencionales
e. Negligencia

2. Mecanismos de protección:
a. "Firewalls"
b. Control y claves de acceso ("passwords")
c. Copias de resguardo
d. Servicios de batería ("UPS")
e. Cifrado (*encryption)*

I. Administración de las redes:
1. Administración
2. Fiscalización ("Monitoring")
3. Optimización de ejecución
4. Políticas y procedimientos
5. Consultoría ("Outsourcing")

J. Servicios de Intranet:
1. Definición
2. Ventajas y desventajas
3. Beneficios
4. Otras consideraciones

K. Conexión a Internet:
1. Administración
2. Fiscalización ("monitoring")
3. Optimización de ejecución
4. Políticas y procedimientos
5. Consultoría ("Outsourcing")

L. Redes inalámbricas:
1. Equipos
2. Tipos
3. Ventajas y desventajas
4. Riesgos
5. "Issues" de seguridad

II. Planificación y evaluación de redes:

A. Planificar:
1. Determinar necesidades
2. Planificar configuración
3. Seleccionar aplicaciones para la red
4. Estimar tamaño de la red
5. Determinar ancho de banda requerido
6. Identificar posibles consultores/proveedores
7. Documentar proceso

B. Analizar o actualizar :
1. Inventario de equipo

2. Avalúo de bitácoras
3. Inventario de servicios
4. Avalúo de seguridad

C. Adoptar plan de implantación:
1. Selección de proveedores
2. Itinerario de implantación
3. Integración de consultores
4. Métricas previo a la instalación
5. Pruebas de integración
6. Planificación de instalación (transición)
7. Adiestramiento a usuarios y técnicos
8. Métricas luego de la instalación
9. Documentación

D. Adquirir e implantar infraestructura:
1. Servicios de conexión
2. Componentes
3. Servidores

E. Administrar:
1. Responsabilidad primaria
2. Áreas que comprende
3. Equipo de trabajo
4. Programación necesaria
5. Políticas y procedimientos

F. Evaluar uso:
1. Periódica
2. Programada
3. Especial

G. Proyectar para su crecimiento

III. Seguridad y protección de redes:

A. Introducción:
1. Riesgos
2. Amenazas
3. Vulnerabilidades
4. Controles

B. Estándares aplicables
1. COBIT
2. COSO
3. ITIL
4. ISO 17799
5. Herramientas” CAAT’s

C. Ámbitos de seguridad:
1. Protección del perímetro físico:
a. Dimensiones de protección
b. Componentes de riesgo
c. Otros factores de riesgo

2. Protección del perímetro lógico:
    a. Controles técnicos:
        1) *Router*
        2) *Firewall*
        3) Zona demilitarizada (DMZ)
        4) Redes virtuales (VPN)
        5) Subredes lógicas (VLAN's)
        6) Traducción de direcciones (NAT)
        7) Encryption Digital Sign
    b. Controles de acceso
3. Análisis de vulnerabilidades:
    a. Conexión a Internet
    b. Conexión a otras entidades u organizaciones
    c. Conexiones remotas
    d. Conexión de usuarios
    e. Acceso físico
4. Tipo de ataques:
    a. Spam
    b. Virus/Worms/Trojans/Logic bombs
    c. Buffer overflow
    d. Denial of service/Distributed Denial of service
    e. Man in the middle
    f. IP Address spoofing
    g. Password /brute-force attacks
    h. Sniffing/eavesdropping
    i. Anonimous user
    j. Remote file system viewing
    k. Cross-site scripting/tracing
5. Técnicas de ataque:
    a. Social engineering
    b. Address recognissance: ARIN/Whois.net
    c. Phone number recognissance
    d. System recognissance
    e. Business recognissance
    f. Physical recognissance
    g. Uso de sistemas comprometidos
6. Vulnerabilidad de procesos
7. Herramientas disponibles:
    a. Router audit tool (RAT)
    b. Network mapping
    c. Vulnerability scanners
    d. Sniffers
    e. Intrusion detection systems
    f. Virus detection/prevention
    g. Integrity checking
    h. War dialers

i. *Policy compliance/violations*
j. CAAT's

8. Tipo de controles de acceso:
    a. Dirigidos a prevenir
    b. Dirigidos a detener
    c. Dirigidos a corregir

D. Políticas y procedimientos:
1. Proceso adopción:
    a. Contenido
    b. Áreas a reglamentar
    c. Modelo mínimo sugerido
2. Implantación:
    a. Participación
    b. Vigencia
    c. Divulgación
3. Avalúo de cumplimiento

E. Contingencia y controles de riesgo:
1. Contingencias
2. Comité de respuesta a incidentes
3. Controles de riesgo

IV. Elementos que se deben tomar en cuenta al planificar una auditoría:

A. Tipo de peritos técnicos:
1. Especialistas en *routers* (Cisco) y *switchs*
2. Especialista en seguridad
3. Programador de sistemas operativos
4. Programador en DBMS
5. Técnico de telecomunicaciones (red voz/datos)

B. Áreas a examinar:
1. Configuración de la red
2. Configuración de *Router* y *Firewall*
3. Configuración de servidores y servicios
4. Código malicioso
5. Ataques
6. Terrorismo cibernético
7. *Information warfare*

C. Herramientas disponibles:
1. UNIX/LINUX
2. Windows
3. *Toolkits*

D. Naturaleza de la auditoría:
1. Interna periódica
2. Vulnerabilidades:
    a. Servidores
    b. Servicios
    c. Controles de acceso
    d. Otras

3. Externa:
    a. Acceso
    b. Intrusión
    c. Sede virtual
    d. otras

V. Proceso de auditoría de redes:
- A. Procesos preliminares a la auditoría:
    1. Ámbito de la auditoría
    2. Expectativas
    3. Personal asignado
    4. Colaboración requerida
    5. Itinerario
- B. Técnicas de recopilación de evidencia
- C. Proceso de auditoría:
    1. Avalúo previo a la visita
    2. Determinación de procesos y sistemas críticos
    3. Examen del entorno de seguridad de sistemas
    4. Avalúo técnico
- D. Procesos luego de concluir la auditoría:
    1. Análisis de hallazgos
    2. Entrevistas y presentaciones
    3. Informe de auditoría
- E. Responsabilidad del Auditor
    1. Herramientas y estándares
    2. Descripción del ámbito del proyecto
    3. Descripción del proceso
    4. Hallazgos
    5. Clasificación de los hallazgos
    6. Recomendaciones

ESTRATEGIAS INSTRUCCIONALES

Conferencias, charlas y discusión de conceptos
Discusión de casos
Desarrollo de investigaciones
Trabajos independientes y trabajos de grupo

EVALUACIÓN

Proyecto de investigación	30%
Exámenes	30%
Paneles y discusiones en línea	10%
Proyecto final	30%
Total	100%

BIBLIOGRAFIA

Fitzgerald H. & Dennis A. (2002). Business Data Communications and Networking. New York: John Wiley & Sons, Inc. ISBN: 0-471-39100-X.

Habraken J., (2004). Absolute Beginner's Guide to Networking, Indianapolis: Que Publising, ISBN: 0-7897-2911-3.

Hioki W., (2001). Telecommunications. New Jersey: Prentice Hall. ISBN: 013020031X.

Maiwald, E. (2001). Network Security: A Beginner's Guide, Osborne: McGraw Hill.

Miles G., Rogers R., Fuller E., Hoagberg M. & DykstraT., (2004). Security Assessment, Rockland, MA: Syngress.

Panko R., (2002). Business Data Networks and Telecommunications. New York: Prentice Hall. ISBN: 0-13-035914-9.

Smith G., (1999). Network Auditing: A Control Assesment Approach, New York: John Wiley & Sons.

Tanenbaum A., (2003). Computer Networks. New Jersey: Prentice Hall. ISBN: 0-13-066102-3.

Weber, R., (1999). Information Systems Control and Audit, New Jersey: Prentice Hall.

Whitehead P., (2000). Teach Yourself Visually Networking. Ontorio: IDG Boos Worldwide, Inc. ISBN: 0-7645-3534-X.

Las bases de datos electrónicas a las cuales la Biblioteca Madre María Teresa Guevara está suscrita directamente y a través del Consorcio COBIMET, incluyen, documentos, artículos de revistas y periódicos y otros recursos de información relacionados con los temas del curso. Al utilizarlas siga los siguientes pasos:

Para **acceder desde cualquier lugar en la Universidad**

- escriba la dirección **http://biblioteca.sagrado.edu/**,
- seleccione **Biblioteca Virtual** y aparecerá la página en donde podrá acceder a las bases de datos, por disciplina o en orden alfabético.

Para **acceder fuera de la Universidad**

- escriba la dirección **http://biblioteca.sagrado.edu/**,
- seleccione **Biblioteca Virtual** y aparecerá la página en donde podrá acceder a las bases de datos, por disciplina o en orden alfabético.
- escriba el nombre del usuario y la contraseña (El nombre de usuario y la contraseña, los solicita personalmente en la Biblioteca)

INTERNET

ITAudit (2003). Auditing Physical Network Components. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5423

ITAudit (2003). First-time Network Audits. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5413

ITAudit (2003). Data Networking Basics. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5405

ITAudit (2003). Auditing Local Area Networks. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5439

ITAudit (2002). Network Management Using the ISO Model. Recuperado el 13 de diciembre de 2007 de ttp://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=353

ITAudit (2004). Understanding TCP/IP. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5484

ITAudit (2002). TCP/IP and the ISO Model. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=414

ITAudit (2003). Protecting Against Wireless Threats. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5426

ITAudit (2002). Wireless Security. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=501

ITAudit (2003). Auditing Wide Area Networks. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5450

ITAudit (1999). Introduction to Virtual Private Networks and Their Tunneling Protocols: Advantages, & Disadvantages - Part 1. Recuperado el 13 de diciembre de 2007 de http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=182

Cualquier estudiante que necesite acomodo razonable deberá solicitarlo al Decano Asociado de Asuntos Estudiantiles.

Noviembre 2007