Fecha Aprobación:
15/03/2013

UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACION

ESCUELA DE INGENIERIA DE SISTEMAS

CARRERA DE INGENIERIA DE SISTEMAS Y TELEMATICA

Sílabo

1. Datos generales

Materia: TELECOMUNICACIONES III
Código: FAD0200
Créditos: 4
Nivel: 6
Paralelo: 6A-IST
Eje de formación: PROFESIONAL
Periodo lectivo: PERIODO MAR/2013 - JUL/2013
Total de horas: 64
Profesor: CRESPO MARTÍNEZ PAÚL ESTEBAN
Correo electrónico: ecrespo@uazuay.edu.ec
Prerrequisitos:
FAD0184 SISTEMAS OPERATIVOS I

2. Descripción y objetivos de la materia

La seguridad de la información es hoy el elemento fundamental que va de la mano con la tecnología. Debido al cambiante entorno tecnológico, todos los días se descubren nuevas vulnerabilidades que son explotadas por atacantes, conocidos como hackers, que se tienen como objetivo el robo de la información para su posterior comercialización y/o divulgación. Esta asignatura permitirá conocer los fundamentos y normas que permite aplicar la seguridad de la información en el negocio y las redes telemáticas modernas. La materia sigue una versión simplificada del estándar internacional ISO 27001.

Se pretende cubrir la materia desde los dos puntos de vista de un Hacker Ético: Las 5 etapas de un ataque y la formas de defenderse al mismo (parte operativa), y la gestión de la seguridad de la información (parte administrativa). Dentro de la parte operativa, se aprenderán las técnicas de ataque y contramedidas para las etapas de reconocimiento, escaneo, obtención de acceso, mantener el acceso y la eliminación de pistas. Se aprenderá a utilizar herramientas que nos permita lograr el objetivo de ataque pero también como defenderse ante los mismos. Desde el punto de vista administrativo, se conocerá de manera general la Norma ISO 27001 y la norma Magerit, para el levantamiento, gestión y control de los activos de la información mediante las políticas de seguridad.

La materia reviste una importancia fundamental para el aprovechamiento de las nuevas tecnologías de seguridad de la información, constituyendo actualmente un elemento primordial en la gestión de la información de las empresas. Se integra con las materias de telemática, programación, sistemas de información, auditoria, entre otras.

3. Contenidos

01. Principios básicos de la seguridad informática

01.01. Principios de la seguridad informática (1 horas)

01.02. Importancia de la seguridad (1 horas)

01.03. Tretas, vulnerabilidades y ataques (1 horas)

01.04. Elementos de seguridad. El Triángulo de la Seguridad, Funcionalidad y facilidad de uso (1 horas)

01.05. Revisión macro de la ISO 27001 (2 horas)

01.06. Políticas, planes y procedimientos de seguridad (2 horas)

01.07. Elementos de las políticas de seguridad (1 horas)

01.08. La importancia del factor humano en la seguridad (1 horas)

01.09. Clasificación y control de los activos de información (1 horas)

01.10. Controles de acceso (1 horas)

01.11. Adquisición, desarrollo y mantenimiento de sistemas (1 horas)

01.12. Gestión de incidentes de seguridad (1 horas)

01.13. Gestión de la continuidad del negocio (1 horas)

01.14. Ejercicios sobre el capitulo ¿ Políticas, planes y procedimientos (3 horas)

02. El Ethical Hacker

02.01. Hackers Éticos (1 horas)

02.02. Fases de un ataque (1 horas)

02.03. ¿En qué consiste el hackeo y la búsqueda de vulnerabilidades? (2 horas)

03. Problemas de seguridad en las redes y sistemas informáticos

03.01. Vulnerabilidades de los sistemas informáticos y las amenazas a la seguridad informática (2 horas)

03.02. Virus informáticos y otros códigos dañinos (1 horas)

03.03. Ciberterrorismo y espionaje en las redes de ordenadores (2 horas)

03.04. Respuesta a incidentes de seguridad y planes para la continuidad del negocio (1 horas)

04. Identificación de usuarios y sistemas biométricos

04.01. Autenticación, autorización y registro de usuarios (1 horas)

04.02.3. Herramientas para footprinting (1 horas)

04.02. El Footprinting

04.02.1. Metodologías para obtener información (1 horas)

04.02.2. Encontrando URL¿s de empresas e información de personas. (1 horas)

04.03. Herramientas de información DNS (1 horas)

04.04. Localización de un rango de red (1 horas)

04.05. e-Mail Spiders (1 horas)

04.06. Herramientas para localizar las actividades de red (1 horas)

04.07. Motores de Meta Búsqueda (1 horas)

04.08. Falsificando sitios web usando la técnica Man-In-The-Middle (1 horas)

04.09. Sistemas biométricos (2 horas)

05. Escaneo

05.01. Objetivos y metodología del escaneo (1 horas)

05.02. Navegación anónima (1 horas)

05.03. Herramientas para el escaneo (1 horas)

05.04. Ejercicios sobre escaneo (1 horas)

06. Enumeración

06.01. Introducción a la enumeración definida (1 horas)

06.02. Técnicas de enumeración (2 horas)

06.03. Procedimiento de enumeración (1 horas)

06.04. Ejercicios sobre enumeración (2 horas)

07. Hackeando el sistema

07.01. Rompiendo Passwords (1 horas)

07.02. Herramientas para romper passwords (1 horas)

07.03. KeyLoggers y Spyware (1 horas)

07.04. Ejercicios sobre Hackeo (1 horas)

08. Fundamentos y aplicaciones de la criptografía

08.01. Fundamentos de criptografía y estenografía (1 horas)

08.02. Firma electrónica y protocolos criptográficos (1 horas)

09. Aspectos técnicos de la seguridad en las redes de computadoras

09.01. Herramientas para la seguridad en redes de computadoras (1 horas)

09.02. Seguridad en sistemas operativos, redes privadas virtuales y redes inalámbricas (1 horas)

10. Seguridad en el uso de los servicios de Internet

10.01. La navegación segura en el World Wide Web y la utilización segura del correo electrónico. (1 horas)

11. Aspectos legales de la seguridad informática

12.2. Buscando evidencias (1 horas)

11.01. Protección de la propiedad intelectual y la lucha contra la piratería digital (1 horas)

12. Análisis forense

12.1. Introducción al análisis forense (1 horas)

12.3. Ejercicios de análisis forense (2 horas)

4. Sistema de Evaluación

Resultado de aprendizaje de la carrera relacionados con la materia

Resultado de aprendizaje de la materia	*Evidencias*
af. Diseña, implementa, analiza y gestiona sistemas de seguridad de la Información aplicando estandares internacionales.	
- Aprender a diferenciar los principios básicos en los que se fundamenta la seguridad de la información.	*- Lecciones escritas*
- Conocer el marco legal empresarial, leyes nacionales e internacionales que protege a la propiedad intelectual y a los datos.	*- Control de lectura*
- Conocer las diferentes etapas de un hackeo y sus mecanismos de defensa	*- Documento de ejercicios y tareas resueltas fuera del aula* *- Documento de ejercicios y tareas resueltas dentro del aula* *- Prácticas de laboratorio* *- Diaporamas (diapositivas, presentaciones, ppt, prezi, etc.).* *- Sustentaciones*
- Conocer las normas internacionales (ISO 27001 y Magerit) que sugieren prácticas y modelos para inventariar, planificar gestionar y controlar los activos de la información de una empresa.	*- Sustentaciones* *- Diaporamas (diapositivas, presentaciones, ppt, prezi, etc.).* *- Lecciones escritas*
as. Diseña y proyecta una arquitectura de redes en diversas áreas de servicio.	
- Aplicar los conocimientos adquiridos para la gestión de los activos de la información.	*- Lecciones escritas*
- Aprende a reconocer, instalar, administrar y documentar mecanismos y herramientas utilizadas en seguridad de la información, aplicando principios éticos	*- Sustentaciones* *- Diaporamas (diapositivas, presentaciones, ppt, prezi, etc.).* *- Lecciones escritas*

Desglose de Evaluación

Evidencia	Descripción Evidencia	Contenidos Sílabo Evaluar	Aporte	Calificación	Fch.Aproximada

Metodología

.

Criterios de Evaluación

¿ Los trabajos copiados textualmente de internet u otras fuentes sin haberlas citado serán consideradas como plagio y calificadas automáticamente con cero. ¿ Los documentos deben ser coherentes y mantener una adecuada redacción, ortografía y citas bibliográficas. ¿ Las presentaciones con diapositivas son simplemente una guía de apoyo al expositor. Deben ser lo más claras y visuales posibles, debido a que el marketing es un factor predominante en el emprendimiento. Diapositivas cargadas con texto tendrán un valor de cero puntos. ¿ La exposición de los trabajos exige mucha preparación a los participantes de la misma. Se tomará en cuenta la seguridad y claridad de explicación, el lenguaje corporal, el conocimiento sobre el tema, la apariencia física del expositor. ¿ En todas las pruebas y lecciones escritas se calificará procedimiento de resolución y resultados obtenidos, considerando coherencia y certeza en la aplicación de razonamientos y teorías. Además de la resolución de casos y ejercicios, todas las evaluaciones incluirán preguntas de razonamiento e interpretación de información.

5. Textos y otras referencias

Libros

BIBLIOGRAFÍA BASE

- CANO, Jeimy.(2011). Computación forense: descubriendo los rastros informáticos. México: Alfaomega. Biblioteca Hernán Malo. UDA-BG 68939.
- EC-Council.(2009). Ethical Hacking and Countermeasures: Attack Phases (Ec-Council Press Series: Certified Ethical Hacke. USA: EC-Council Press Series. Provista por el profesor.
- EC-Council.(2009). Computer Forensics: Hard Disk and Operating Systems. USA: EC-Council Press Series. Provista por el profesor.
- EC-Council.(2009). Ethical Hacking and Countermeasures: Threats and Defense. USA: EC-Council Press Series. Provista por el profesor.
- GOMEZ, Alvaro.(2011). Enciclopedia de la Seguridad Informática. México: Alfa Omega. Biblioteca Hernán Malo. UDA-BG 68935.

Web

BIBLIOGRAFÍA BASE

- HUIDROBO MOYA José, ROLDAN MARTINEZ David. Obtenido de Comunicaciones en redes WLAN: http://books.google.com.
- ICA (Instituto para la Conectividad en las Americas). Obtenido de Un puente entre la tecnología y la sociedad: http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/Telecentros%20Puente%20entre%20Tecnologia%20y%.
- JIMENEZ Jose Alfredo. Obtenido de Evaluación: Seguridad de un Sistema de Información.: http://site.ebrary.com/lib/uasuaysp/docDetail.action?docID=10316459&p00=seguridad+de+la+informaci%C3.
- ICA (Instituto para la Conectividad en las Americas). Obtenido de Mapa de conectividad de internet: http://www.uazuay.edu.ec/bibliotecas/conectividad/mapa_conectividad/mapagene.html.
- Sociedad de la información del Brasil. Obtenido de I Libro Verde de la Sociedad de la Información en Brasil: http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/Programa%20Sociedade%20da%20Informacao%20no%20.
- MOLINA MATEOS Jose Maria. Obtenido de Seguridad de la Información Criptología: http://site.ebrary.com/lib/uasuaysp/docDetail.action?docID=10018530&p00=seguridad+de+la+informaci%C3.
- Ramos Álvarez, Benjamin. Obtenido de Avances en criptologia y seguridad de la información: http://site.ebrary.com/lib/uasuaysp/docDetail.action?docID=10149820&p00=seguridad+de+la+informaci%C3.
- UIT (Union internacional de Telecomunicaciones). Obtenido de Manual de indicadores de telecomunicaciones: http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/MANUAL%20DE%20INDICADORES%20DE%20TELECOMUNICAC.

Software

BIBLIOGRAFÍA BASE

- Backtrack Linux Org.. BackTrack. 5. Laboratorio.
- Hiren. Hiren Boot CD. 15.3. Provista por el profesor.

Docente

Director Junta

Fecha Aprobación: **15/03/2013**

APROBADO