



FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN ESCUELA INGENIERIA DE SISTEMAS Y TELEMATICA

1. Datos

Materia: TELECOMUNICACIONES III
Código: FAD0200
Paralelo: A
Periodo : Marzo-2020 a Agosto-2020
Profesor: CRESPO MARTINEZ PAUL ESTEBAN
Correo electrónico: ecrespo@uazuay.edu.ec
Prerrequisitos:

Código: FAD0184 Materia: SISTEMAS OPERATIVOS I

Nivel: 6

Distribución de horas.

| Docencia | Práctico | Autónomo:null | | Total horas | Créditos |
|----------|----------|----------------------|----------|-------------|----------|
| | | Sistemas de tutorías | Autónomo | | |
| 4 | | | | 4 | 4 |

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, auditoría, entre otras.

3. Contenidos

| | |
|-----|--|
| 1 | Principios básicos de la seguridad informática |
| 1.1 | Principios de la seguridad informática (1 horas) |
| 1.2 | Importancia de la seguridad (1 horas) |
| 1.3 | Tretas, vulnerabilidades y ataques (1 horas) |
| 1.4 | Elementos de seguridad. El Triángulo de la Seguridad, Funcionalidad y facilidad de uso (1 horas) |
| 1.5 | Revisión macro de la ISO 27001 (2 horas) |
| 1.6 | Políticas, planes y procedimientos de seguridad (2 horas) |
| 1.7 | Elementos de las políticas de seguridad (1 horas) |
| 1.8 | La importancia del factor humano en la seguridad (1 horas) |
| 1.9 | Clasificación y control de los activos de información (1 horas) |

| | |
|----------|---|
| 1.10 | Controles de acceso (1 horas) |
| 1.11 | Adquisición, desarrollo y mantenimiento de sistemas (1 horas) |
| 1.12 | Gestión de incidentes de seguridad (1 horas) |
| 1.13 | Gestión de la continuidad del negocio (1 horas) |
| 1.14 | Ejercicios sobre el capítulo ¿ Políticas, planes y procedimientos (3 horas) |
| 2 | El Ethical Hacker |
| 2.1 | Hackers Éticos (1 horas) |
| 2.2 | Fases de un ataque (1 horas) |
| 2.3 | ¿En qué consiste el hackeo y la búsqueda de vulnerabilidades? (2 horas) |
| 3 | Problemas de seguridad en las redes y sistemas informáticos |
| 3.1 | Vulnerabilidades de los sistemas informáticos y las amenazas a la seguridad informática (2 horas) |
| 3.2 | Virus informáticos y otros códigos dañinos (1 horas) |
| 3.3 | Ciberterrorismo y espionaje en las redes de ordenadores (2 horas) |
| 3.4 | Respuesta a incidentes de seguridad y planes para la continuidad del negocio (1 horas) |
| 4 | Identificación de usuarios y sistemas biométricos |
| 4.1 | Autenticación, autorización y registro de usuarios (1 horas) |
| 4.2 | El Footprinting (0 horas) |
| 4.2.1 | Metodologías para obtener información (1 horas) |
| 4.2.2 | Encontrando URL's de empresas e información de personas. (1 horas) |
| 4.2.3 | Herramientas para footprinting (1 horas) |
| 4.3 | Herramientas de información DNS (1 horas) |
| 4.4 | Localización de un rango de red (1 horas) |
| 4.5 | e-Mail Spiders (1 horas) |
| 4.6 | Herramientas para localizar las actividades de red (1 horas) |
| 4.7 | Motores de Meta Búsqueda (1 horas) |
| 4.8 | Falsificando sitios web usando la técnica Man-In-The-Middle (1 horas) |
| 4.9 | Sistemas biométricos (2 horas) |
| 5 | Escaneo |
| 5.1 | Objetivos y metodología del escaneo (1 horas) |
| 5.2 | Navegación anónima (1 horas) |
| 5.3 | Herramientas para el escaneo (1 horas) |
| 5.4 | Ejercicios sobre escaneo (1 horas) |
| 6 | Enumeración |
| 6.1 | Introducción a la enumeración definida (1 horas) |
| 6.2 | Técnicas de enumeración (2 horas) |
| 6.3 | Procedimiento de enumeración (1 horas) |
| 6.4 | Ejercicios sobre enumeración (2 horas) |
| 7 | Hackeando el sistema |
| 7.1 | Rompiendo Passwords (1 horas) |
| 7.1.1 | Herramientas para romper passwords (1 horas) |
| 7.2 | KeyLoggers y Spyware (1 horas) |
| 7.3 | Ejercicios sobre Hackeo (1 horas) |
| 8 | Fundamentos y aplicaciones de la criptografía |
| 8.1 | Fundamentos de criptografía y estenografía (1 horas) |
| 8.2 | Firma electrónica y protocolos criptográficos (1 horas) |
| 9 | Aspectos técnicos de la seguridad en las redes de computadoras |
| 9.1 | Herramientas para la seguridad en redes de computadoras (1 horas) |
| 9.2 | Seguridad en sistemas operativos, redes privadas virtuales y redes inalámbricas (1 horas) |

| | |
|------|---|
| 10 | Seguridad en el uso de los servicios de Internet |
| 10.1 | La navegación segura en el World Wide Web y la utilización segura del correo electrónico. (1 horas) |
| 11 | Aspectos legales de la seguridad informática |
| 11.1 | 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) |
| 12.2 | Buscando evidencias (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 estándares internacionales.

| | |
|---|--|
| -Aprender a diferenciar los principios básicos en los que se fundamenta la seguridad de la información. | -Foros, debates, chats y otros -Prácticas de laboratorio -Trabajos prácticos - productos |
| -Conocer el marco legal empresarial, leyes nacionales e internacionales que protege a la propiedad intelectual y a los datos. | -Foros, debates, chats y otros -Prácticas de laboratorio -Trabajos prácticos - productos |
| -Conocer las diferentes etapas de un hackeo y sus mecanismos de defensa | -Foros, debates, chats y otros -Prácticas de laboratorio -Trabajos prácticos - productos |
| -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. | -Foros, debates, chats y otros -Prácticas de laboratorio -Trabajos prácticos - productos |

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. | -Foros, debates, chats y otros -Prácticas de laboratorio -Trabajos prácticos - productos |
| -Aprende a reconocer, instalar, administrar y documentar mecanismos y herramientas utilizadas en seguridad de la información, aplicando principios éticos | -Foros, debates, chats y otros -Prácticas de laboratorio -Trabajos prácticos - productos |

Desglose de evaluación

| Evidencia | Descripción | Contenidos sílabo a evaluar | Aporte | Calificación | Semana |
|--------------------------------|--|---|--------|--------------|-----------------------------------|
| Trabajos prácticos - productos | Informe de práctica de gestión de activos de información | Principios básicos de la seguridad informática | APORTE | 4 | Semana: 2 (08/04/20 al 13/04/20) |
| Foros, debates, chats y otros | Metodologías y normas de gestión de riesgo informático | El Ethical Hacker, Principios básicos de la seguridad informática | APORTE | 2 | Semana: 3 (15/04/20 al 20/04/20) |
| Prácticas de laboratorio | Práctica de laboratorio. Reconocimiento | Problemas de seguridad en las redes y sistemas informáticos | APORTE | 4 | Semana: 4 (22/04/20 al 27/04/20) |
| Prácticas de laboratorio | Práctica de laboratorio. Enumeración (footprinting y fingerprinting) | Enumeración, Escaneo | APORTE | 4 | Semana: 6 (06/05/20 al 11/05/20) |
| Prácticas de laboratorio | Práctica de laboratorio. Bombas lógicas, xpoits | Fundamentos y aplicaciones de la criptografía, Hackeando el sistema | APORTE | 6 | Semana: 8 (20/05/20 al 25/05/20) |
| Foros, debates, chats y otros | Trabajo de investigación: Cifrado y técnicas de ocultamiento | Hackeando el sistema | APORTE | 3 | Semana: 9 (27/05/20 al 29/05/20) |
| Prácticas de laboratorio | Práctica de laboratorio: ocultamiento y cifrado | Fundamentos y aplicaciones de la criptografía, Hackeando el sistema | APORTE | 2 | Semana: 10 (03/06/20 al 08/06/20) |

| Evidencia | Descripción | Contenidos sílabo a evaluar | Aporte | Calificación | Semana |
|--------------------------------|--|--|------------|--------------|--|
| Prácticas de laboratorio | prácticas de laboratorio. Seguridad Wifi, protocolos, forense. | Análisis forense, Aspectos legales de la seguridad informática, Aspectos técnicos de la seguridad en las redes de computadoras, Fundamentos y aplicaciones de la criptografía, Seguridad en el uso de los servicios de Internet | APORTE | 5 | Semana: 14 (01/07/20 al 06/07/20) |
| Trabajos prácticos - productos | Examen. Acometimiento y protección de información | Análisis forense, Aspectos legales de la seguridad informática, Aspectos técnicos de la seguridad en las redes de computadoras, El Ethical Hacker, Enumeración, Escaneo, Fundamentos y aplicaciones de la criptografía, Hackeando el sistema, Identificación de usuarios y sistemas biométricos, Principios básicos de la seguridad informática, Problemas de seguridad en las redes y sistemas informáticos, Seguridad en el uso de los servicios de Internet | EXAMEN | 20 | Semana: 17-18 (21-07-2020 al 03-08-2020) |
| Trabajos prácticos - productos | Acometimiento y aseguramiento de información | Análisis forense, Aspectos legales de la seguridad informática, Aspectos técnicos de la seguridad en las redes de computadoras, El Ethical Hacker, Enumeración, Escaneo, Fundamentos y aplicaciones de la criptografía, Hackeando el sistema, Identificación de usuarios y sistemas biométricos, Principios básicos de la seguridad informática, Problemas de seguridad en las redes y sistemas informáticos, Seguridad en el uso de los servicios de Internet | SUPLETORIO | 20 | Semana: 19 (al) |

Metodología

La metodología de evaluación será realizada mediante

- Informes de prácticas de laboratorio
- Pruebas y debate en clase sobre experiencias adquiridas en la investigación de conceptos en trabajos científicos, casos empresariales, y en las prácticas desarrolladas.
- Trabajos de investigación individuales a manera de fortalecer los conceptos impartidos en clase, los mismos que también serán evaluados al momento de realizar las prácticas de laboratorio.
- Exposición sobre temas investigados

Criterios de Evaluación

- Los trabajos copiados textualmente de internet u otras fuentes sin haberlas citado serán consideradas como plagio y calificadas automáticamente con cero puntos y reportadas a las autoridades universitarias.
 - 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. 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.
 - Los informes de laboratorio son presentados en formato IEEE
- No se aceptarán trabajos fuera del plazo establecido. Solamente se aceptan trabajos en el campus virtual.

5. Referencias

Bibliografía base

Libros

| Autor | Editorial | Título | Año | ISBN |
|---------------|-------------------|--|------|------------|
| GOMEZ, ALVARO | Alfaomega - Ra-Ma | ENCICLOPEDIA DE LA SEGURIDAD INFORMÁTICA | 2011 | 9701512669 |

| Autor | Editorial | Título | Año | ISBN |
|---------------------------------|-------------------------|---|------|-------------------|
| CANO, JEIMY | Alfaomega | COMPUTACIÓN FORENSE: DESCUBRIENDO LOS RASTROS INFORMÁTICOS | 2011 | NO INDICA |
| EC-COUNCIL | EC-Council Press Series | COMPUTER FORENSICS: HARD DISK AND OPERATING SYSTEMS | 2009 | NO INDICA |
| EC-COUNCIL | EC-Council Press Series | ETHICAL HACKING AND COUNTERMEASURES: THREATS AND DEFENSE | 2009 | NO INDICA |
| EC-COUNCIL | EC-Council Press Series | ETHICAL HACKING AND COUNTERMEASURES: ATTACK PHASES (EC-COUNCIL PRESS SERIES: CERTIFIED ETHICAL HACKER) | 2009 | NO INDICA |
| Kevin Mitnick; William Simón | Alfa Omega | El arte de la intrusión | 2007 | 978-970-15-1260-9 |

Web

| Autor | Título | Url |
|--|---|---|
| Jimenez Jose Alfredo | Evaluación: Seguridad De Un Sistema De Información. | http://site.ebrary.com/lib/uasuaysp/docDetail.action?docID=10316459&p00=seguridad+de+la+informaci%C3 |
| Ramos Álvarez, Benjamin | Avances En Criptología Y Seguridad De La Información | http://site.ebrary.com/lib/uasuaysp/docDetail.action?docID=10149820&p00=seguridad+de+la+informaci%C3 |
| Molina Mateos Jose Maria | Seguridad De La Información Criptología | http://site.ebrary.com/lib/uasuaysp/docDetail.action?docID=10018530&p00=seguridad+de+la+informaci%C3 |
| Sociedad De La Información Del Brasil | L Libro Verde De La Sociedad De La Información En Brasil | http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/Programa%20Sociedade%20da% |
| Ica (Instituto Para La Conectividad En Las | Mapa De Conectividad De Internet | http://www.uazuay.edu.ec/bibliotecas/conectividad/mapa_conectividad/mapagene.html |
| Uif (Union Internacional De Telecomunicaciones) | Manual De Indicadores De Telecomunicaciones | http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/MANUAL%20DE%20 |
| Ica (Instituto Para La Conectividad En Las | Un Puente Entre La Tecnología Y La Sociedad | http://www.uazuay.edu.ec/bibliotecas/conectividad/pdf/Telecentros%20Puente%20entre%20 |
| Huidrobo Moya José, Roldan Martínez David | Comunicaciones En Redes Wlan | http://books.google.com |

Software

| Autor | Título | Url | Versión |
|----------------------|---------------|--------------------------|---------|
| Backtrack Linux Org. | Backtrack | Laboratorio | 5 |
| Hiren | Hiren Boot Cd | Provista por el profesor | 15.3 |

Bibliografía de apoyo

Libros

Web

Software

Docente

Director/Junta

Fecha aprobación: **02/03/2020**

Estado: **Aprobado**