1. Datos Generales de la asignatura

Nombre de la asignatura:	Administración de la Seguridad Informática.
Clave de la asignatura:	SED-1705
SATCA[1]:	(2 - 3 - 5)
Carrera:	Ingeniería en Tecnologías de la Información y Comunicaciones Ingeniería en Sistemas Computacionales Ingeniería Informática

2. Presentación

Caracterización de la asignatura
La administración de servicios de red no solo implica el mantenerlos a punto para el uso diario. Los servicios, como cualquier sistema de cómputo que descansa en una infraestructura, están propensos a sufrir los embates de usuarios malintencionados o administradores de sistemas ingenuos. Es por esto que es de vital importancia proveer al estudiante del área de sistemas y computación, del conocimiento, habilidades, destrezas y herramientas para planificar y prevenir todos los posibles riesgos elaborando los procedimientos y políticas para la atención requerida
Intención didáctica
El alumno conocerá elementos para llevar a cabo un análisis de riesgos y su implementación asi como conocer elementos básicos para el análisis forense de sistemas

[1] Sistema de Asignación y Transferencia de Créditos Académicos

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Morelia, 1 de julio de 2015.	Juan Manuel García García Anastacio Antolino Hernandez Heberto Ferreira Juan Jesús Ruiz lagunas	Diseño Curricular basado en Competencias del Módulo.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
El alumno conocerá metodologías de análisis de riesgos, elaboración de procedimientos y políticas de seguridad, la norma ISO 27001 y análisis forense de un sistema de computo

5. Competencias previas

- Seleccionar, clasificar y analizar información.
- Observar el escenario problema e identificar oportunidades de desarrollo de proyectos generando ideas innovadoras de la aplicación de la investigación en su área profesional.

6. Temario

No.	Temas	Subtemas
1	INTRODUCCION	1. OBJETIVOS DE LA SEGURIDAD INFORMATICA. 2. DEFINICIONES: AMENAZA, VULNERABILIDAD, RIESGO, CONTROLES. 3. ISMS: SISTEMA DE ADMINISTRACION DE LA SEGURIDAD INFORMATICA. 4. NORMA ISO-27001
2	ANALISIS DE RIESGOS	1. OBJETIVOS DEL ANALISIS DE RIESGOS. FASES DEL A.R. 2. METODOLOGIAS DE ANALISIS DE RIESGOS. CUALITATIVAS VS. CUANTITATIVAS. 3. DESARROLLO DE UN ANALISIS DE RIEGOS. 4. REPORTE DE ANALISIS DE RIESGOS.

		5. MAGERIT 3.0
3	POLITICA DE SEGURIDAD INFORMATICA	1. OBJETIVOS DE POLITICA DE S.I. 2. DISEÑO DE UNA POLITICA DE S.I. 3. CASOS DE ESTUDIO. 4. DESARROLLO DE UNA POLITICA DE SEGURIDAD
4	PLANES DE CONTINGENCIA	1. OBJETIVOS DE LOS PLANES DE CONTINGENCIA. 2. DISEÑO DE UN PLAN DE CONTINGENCIA. 3. EJERCICIOS DE CONTINGENCIA. DE TABLE-TOP AL SIMULACRO MOFA. 4. DESARROLLO DE UN PLAN DE CONTINGENCIA
5	INTRODUCCION AL ANALISIS FORENSE	1. PROCESO DE INVESTIGACION EN COMPUTO FORENSE 2. TECNICA DE OBTENCION Y DUPLICACION DE DATOS. 3. TECNICAS DE RECUPERACION DE DATOS. 4. ANALISIS DE EVIDENCIAS Y PRESENTACION 5. CERTIFICACION

7. Actividades de aprendizaje de los temas

Nombre de tema INTRODUCCION	
Competencias	Actividades de aprendizaje
Específica(s): - Conocera los conceptos de seguridad informática - Conocera la norma iso 27001 Genéricas: - Conocera los conceptos de seguridad informática y los estándares enfocados al mismo	1. Documentarse en todos los conceptos de seguridad informática, aclarando las diferencias entre algunos conceptos. 2. Conocera la norma iso-27001
Nombre de tema ANALISIS DE RIESGOS	
Competencias	Actividades de aprendizaje
Específica(s): - Conocer la metodología FRAP, para llevarla a cabo en un análisis de riesgos. - Liderazgo para llevar a cabo dicho procedimiento. Genéricas: - Llevar a cabo la metodología para llevar a cabo el proceso del análisis de riesgos y su implementación.	1. Llevar a cabo la reunión pre-frap 2. Llevar a cabo la reunión frap 3. Llevar a cabo la documentación de dicho análisis y la elaboración de los manuales de políticas y procedimientos derivados de dichas reuniones.
Nombre de tema POLITICA DE SEGURIDAD INFORMATICA	
Competencias	Actividades de aprendizaje
Específica(s):	1. Implementar el manual de políticas, derivado del análisis

- Conocera el procedimiento para la implementación de las políticas de seguridad informática derivada del análisis de riesgos. Genéricas: - Implementara una política de seguridad informática a nivel lógico dentro de la organización.	de riesgos en redes virtualizadas.
Nombre de tema PLANES DE CONTINGENCIA	
Competencias	Actividades de aprendizaje
Específica(s): - Implementar las medidas y criterios requeridos para enfrentar las eventualidades tanto de manera física, como lógica. Genéricas: - Desarrollar e implementar un plan de contingencias para la organización.	1.- Implementara el manual de procedimientos, para poder hacer frente a una situación de desastre, tanto en forma lógica como física de la red.
Nombre de tema INTRODUCCION AL ANALISIS FORENSE	
Competencias	Actividades de aprendizaje
Específica(s): - Podrá llevar a cabo una investigación en computo forense. - Conocera técnicas para la recuperación de datos. Genéricas: - Sera capaz de llevar a cabo un análisis forense en equipo de computo, para recuperar datos o	1- Llevar a cabo hacking ético para vulnerar servidores. 2- Realizar análisis forense de dichos ataques.

conocer la forma de ataque recibida.	

8. Práctica(s)

Implementar servicios de red en los servidores, para ser vulnerados y analizados de manera posterior.

9. Proyecto de asignatura

Que el alumno, sea capaz de llevar a cabo etical hacking, para conocer el nivel de seguridad implementado en las redes actuales y futuras.

10. Evaluación por competencias

- En un laboratorio de especialidad, preferentemente con Linux Distro Red Hat, configurar los servicios de DNS, DHCP, FTP, WEB y CORREO.
- Elaborar los planes de respuesta a contingencia para cada uno de los servicios.
- Resguardar cada uno de los servicios.
- Recuperar cada uno de los servicios después de haber experimentado una contingencia.

11. Fuentes de información

[1] S.SHAH; W.SOYINKA. “Linux Administration”, Mac Graw Hill, 2005.

[2] B.CALKINS. “Solaris 10 System Administration”, SUNmicrosystem, 2005.

[3] H.BRELSFORD. “Windows 2000 Server” Arrayan, 2007.

[4] J.RAYA; E.RAYA. “Windows NT Server”,Ra-Ma.

[5] E.NAVARRO; V.PIATTINI. ”Auditoria Informática: Un enfoque practico”, RaMa.

[6] G.MARK “Commands, Editors, and shell Programming ”

[7] TANENBAUM A. (2003). Redes de computadoras. Prentice Hall. Cuarta ed. Mexico.

[8] Cert coordination Center, “Análisis de un sistema comprometido”,

http://www.cert.org/security-improvement/practices/p046.html

[9] Página dedicada a la seguridad desarrollada por Universidad Nacional Autónoma de México.

http://www.seguridad.unam.mx.

[10] Cert Coordination Center, Trabajo sobre el análisis de información en Unix,

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html.

[11] Trabajo dedicado a la investigación forense en sistemas informáticos.

http://www.loquefaltaba.com/documentacion/forense/.

[12] Trabajo sobre cómo hacer una auditoria informática,

http://www.auditoria.com.mx/.

[13] Una colección de herramientas de un investigador forense. Utilidades escritas por Dan y Wietse (trabaja para IBM, y el autor de postfix)

http://www.fish.com/tct/.

[14] Benson C., (s.f.), Estrategia de seguridad, Microsoft TechNet. Desde

https://www.microsoft.com/latam/technet/articulos/200011/art04/default.asp

[15] Carli F. (2003), Security Issues With DNS.

http://www.sans.org/reading room/whitepapers/dns/1069.php.

[16] Red Hat Enterprise Linux (RHEL), (2008), Deployment Guide 5.1, Red Hat Inc,

USA.

https://www.redhat.com/docs/manuals/enterprise/RHEL-5-manual/en-

US/RHEL510/Deployment Guide/index.html

[17] Scarfone K., Mell P., (2007) Guide to Intrusion Detection and Prevention

Systems (IDPS), NIST.

http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[18] Wack J., Cutler K., y Pole J. (2002), Guidelines on Firewalls and Firewall Policy,

NIST, Computer Security Division.

http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

[19] May C., Baker M., y Gabbard D., et. al., (2004), Advanced Information

Assurance Hand-book, CERT, Carnegie Mellon University, USA.

http://www.cert.org/archive/pdf/aia-handbook.pdf

[20] Ferrer J., Fernández-Sanguino J., (s.f.), El sistema operativo GNU/Linux y sus

herramientas libres en el mundo de la seguridad: estudio del estado del arte.

http://mmc.igeofcu.unam.mx/LuCAS/Presentaciones/200103hispalinux/ferrer/pdf/seguridad-y-sw-libre v1.0.pdf

[21] Herzog P. (2003), Manual de la Metodología Abierta de Testeo de Seguridad,

ISECOM, segunda ed., USA.

http://isecom.securenetltd.com/osstmm.en.2.2.pdf

[22] Miles T., Wayne J., McLarnon M., (2002), Guidelines on Securing Public Web Servers, NIST, USA.

http://csrc.nist.gov/publications/nistpubs/800-44 ver2/SP800-44v2.pdf

[23] Stoneburner G., Goguen A., Feringa A., (2001), Underlying Technical Models for Information Technology Security, NIST.

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[24] Sondeo realizado por Macias Saucedo denominado Encuesta Nacional sobre la Seguridad Informática en México 2007.

http://www.acis.org.co/fileadmin/Revista 101/ArticuloEncuestaUNIVA.pdf

[25] Página principal de la metodología iso27000.es

http://www.iso27000.es