1. Datos Generales de la asignatura

Nombre de la asignatura:	Sistemas de Gestión de la Seguridad Informática
Clave de la asignatura:	SDI-1805
SATCA[1]:	(2 - 3 - 5)
Carrera:	Ingeniería en Tecnologías de la Información y Comunicaciones Ingeniería en Sistemas Computacionales

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 agosto 2018.	Dr. Anastacio Antolino Hernández Dr. Heberto Ferreira IC. Juan Jesús Ruiz lagunas MC. Juan Carlos Olivares Rojas Dr. Juan Manuel García García	Diseño Curricular basado en Competencias del Módulo de Seguridad de la Información.

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	Introducción	1.1 Objetivos de la seguridad informática. 1.2 Definiciones: amenaza, vulnerabilidad, riesgo, controles. 1.3 ISMS. 1.4 Implementación Norma ISO-27001
2	Análisis de riesgos (AR)	2.1 Análisis de riesgos, fases 2.2 Metodologías para el AR 2.3 Aplicación del AR. 2.4 Estándares del AR
3	Política de Seguridad Informática (PSI)	3.1 Objetivos de una PSI 3.2 Diseño de una PSI

		3.3 Casos de estudio 3.4 Implementación de una PSI
4	Planes de contingencia (PC)	4.1 Objetivos de los PC. 4.2 Diseño de un PC. 4.3 Análisis de un PC 4.4 Implementación de un PC
5	Introducción al análisis forense (AF)	5.1 Proceso de investigación en cómputo forense 5.2 Técnicas de obtención y duplicación de datos 5.3 Técnicas de recuperación de datos. 5.4 Análisis de evidencias y presentación 5.5 Certificaciones

7. Actividades de aprendizaje de los temas

Tema 1: Introducción	
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. Conocerá la norma iso-27001
Tema 2: Análisis 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.
Tema 3: Política de Seguridad Informática	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá el procedimiento para la implementación de las políticas de seguridad informática derivada del análisis de riesgos. Genéricas: - Implementará una política de seguridad informática a nivel lógico dentro de la organización.	1. Implementar el manual de políticas 2. Analizar los riesgos en los componentes de red 3. Implementar l política con esquemas de seguridad

Tema 4: 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. Elaborar el plan de contingencia basado en el análisis de riesgos 2. Implementar el manual de procedimientos, para poder hacer frente a una situación de desastre, tanto en forma lógica como física de la red.
Tema 5: Introducción al análisis forense	
Competencias	Actividades de aprendizaje
Específica(s): - Podrá llevar a cabo una investigación en computo forense. - Conocerá técnicas para la recuperación de datos. Genéricas: - Sera capaz de llevar a cabo un análisis forense en equipo de cómputo, para recuperar datos o conocer la forma de ataque recibida.	1- Llevar a cabo hacking ético para vulnerar servidores. 2- Realizar análisis forense de dichos ataques.

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

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

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

[3] Página dedicada a la seguridad desarrollada por Universidad Nacional Autónoma de México. http://www.seguridad.unam.mx.

[4] Cert Coordination Center, Trabajo sobre el análisis de información en Unix, http://www.cert.org/tech_tips/win-UNIX-system_compromise.html.

[5] Trabajo dedicado a la investigación forense en sistemas informáticos. http://www.loquefaltaba.com/documentacion/forense/.

[6] Trabajo sobre cómo hacer una auditoria informática, http://www.auditoria.com.mx/.

[7] Una colección de herramientas de un investigador forense. Utilidades escritas por Dan y Wietse, http://www.fish.com/tct/.

[8] Scarfone K., Mell P., (2017) Guide to Intrusion Detection and Prevention

Systems (IDPS), NIST. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[9] 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.

[10] 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

[11] Página principal de la metodología iso27000.es, http://www.iso27000.es