1. Datos Generales de la asignatura

Nombre de la asignatura:	Introducción a la Seguridad de la Información
Clave de la asignatura:	
SATCA[1]:	2 - 3 - 5
Carrera:	Ingeniería en Sistemas Computacionales Ingeniería en Tecnologías de la Información y Comunicaciones

2. Presentación

Caracterización de la asignatura
La administración de la información, servicios y/o aplicaciones en los hosts de red, no sólo implica el mantenerlos a punto para el uso diario. La información y 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 amenazas, y su implementación así como conocer elementos básicos para la seguridad

[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, 14 de agosto de 2018.	Dr. Heberto Ferreira Medina Dr. Anastacio Antolino Hernandez Ing. Juan Jesús Ruiz lagunas Dr. Juan Manuel García García M.C. Cristhian Torres Millarez M.C. Abel Alberto Pintor Estrada M.C. Juan Carlos Olivares Rojas	Diseño Curricular basado en Competencias del Módulo.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Conoce las 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 Conceptos y objetivos de la seguridad informática. 1.2 Diferencia entre amenaza, vulnerabilidad, riesgo y controles. 1.3 Norma y certificaciones.

2	Algoritmos de cifrado	2.1 Introducción y definición de criptografía 2.2 Criptografía simétrica 2.3 Criptografía asimétrica 2.4 Algoritmos de verificación 2.4.1MD5 2.4.2 SHA1
3	Control de acceso	3.1 Normas y políticas para el control de acceso 3.2 Control de acceso lógico, roles y fases 3.3 Control de acceso físico, dispositivos 3.4 Tendencias
4	Infraestructura de llave pública	4.1 Objetivos del PKI y certificados digitales 4.2 Sistemas operativo y servicios 4.3 Infraestructura física de red 4.4 Políticas de conexión 4.5 Nuevas tecnologías VPN y Blockchain

7. Actividades de aprendizaje de los temas

Tema 1. Introducción	
Competencias	Actividades de aprendizaje
Específica(s): - Conoce y aplica los conceptos y objetivos de la seguridad informática. - Conoce los conceptos e identifica las diferencias entre amenaza, vulnerabilidad y riesgo. - Conoce la norma iso 27001. Genéricas: - Conocerá los conceptos fundamentales de la seguridad informática y los estándares de la misma.	1. Documentarse en todos los conceptos de seguridad informática, aclarando las diferencias entre algunos conceptos. 2. Investigará y conocerá la norma iso-27001
Tema 2. Algoritmos de Cifrado	
Competencias	Actividades de aprendizaje
Específica(s): - Conoce los algoritmos de cifrado de llave privada. - Conoce los algoritmos de cifrado de llave pública. - Conoce los algoritmos de verificación Genéricas: - Conocer los algoritmos más utilizados en el cifrado de información, para poder enviar información segura en medios no confiables.	1. Investigar los algoritmos más utilizados en llave privada 2. Investigar los algoritmos más utilizados en llave pública 3. Investigar los algoritmos más utilizados en verificación de datos 4. Implementar los algoritmos en una aplicación de cómputo.
Tema 3. Control de Acceso	
Competencias	Actividades de aprendizaje

Específica(s): - Conoce las normas y políticas para el control de acceso de usuarios - Conoce el control de acceso lógico - Conoce el control de acceso físico de personal - Conoce los dispositivos biométricos de control de acceso. Genéricas: - Conocer y analizar las técnicas, métodos y políticas utilizadas para el control de acceso. Así como las herramientas y dispositivos de hardware utilizadas para apoyar las medidas	1. Investigar y diseñar políticas de seguridad para un entorno controlado. 2. Documentar los controles de acceso lógico existentes 3. Documentar las características de los controles físicos de acceso y control 4. Investigar, documentar y describir las características de los dispositivos biométricos
Tema 4. Infraestructura de llave pública	
Competencias	Actividades de aprendizaje
Específica(s): - Conoce los objetivos de la infraestructura de llave pública - Conoce las políticas y disposiciones de acceso remoto - Conoce las aplicaciones que permiten conexiones remotas de manera segura Genéricas: - Conocer e implementar un PKI en las TICs para ofrecer mayor seguridad en las comunicaciones.	1. Investigar e implementar políticas de seguridad, para conexiones remotas. 2. Investigar e implementar sistemas de conexiones remotas seguras 3. Documentar el uso de encadenamiento de bloques para garantizar la verificación de datos 4. Investigar y documentar el uso de certificados digitales

8. Práctica(s)

- Implementar VPN en un sistema de cómputo.
- Diseñar e implementar el uso de blockchain en una aplicación distribuida
- Implementar y generar certificados digitales para un archivo digital

9. Proyecto de asignatura

Que el alumno, sea capaz de realizar e implementar un PKI en un sistema de TICs, para ayudar a aumentar la seguridad en la transferencia de información en un ambiente no seguro

10. Evaluación por competencias

- En un laboratorio de especialidad, preferentemente con Linux Distro Red Hat, configurar los servicios de VPN, blockchain, certificados digitales.
- Elaborar pruebas de conexión remotas seguras entre clientes - servidores.
- Generar documentos digitales, con firma y certificado digital.

11. Fuentes de información

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

[2] B.CALKINS. “Solaris 10 System Administration”, SUN microsystem, 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