1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad en Sistemas Operativos
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
El Sistema Operativo (SO) es uno de los más vulnerados, la instalación configuración y puesta a punto de un sistema seguro, es una de las tareas más importantes en la seguridad informatica. Se revisan conceptos fundamentales del endurecimineto de SO (hardening), las actividades encaminadas a las actualizaciones, el firewall, asegurar puertos de servicios, garantizar el acceso seguro, servicios de compartición de recursos seguros, uso de contenedores de virtualización seguros, passwords seguros, respaldos, uso de la encriptación, entre otras, son muy importantes.
Intención didáctica
El alumno conocerá las actividades más importantes para granatizar el uso de un sistema operativo seguro, se revisará la seguridad en sistemas Unix y Windows y los esquemas utilizados para garantizarla.

[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 agosto de 2018.	Dr. Heberto Ferreira Medina Dr. Juan Manuel García García Dr. Anastacio Antolino Hernández Ing. Juan Jesús Ruiz Lagunas M.C. Juan Carlos Olivares Rojas M.C. Cristhian Torres Millarez M.C. Abel Alberto Pintor Estrada	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 las actividades más importantes para el endurecimiento en sistemas operativos, además aplicarlas a sistemas Unix y Windows, realizará actualizaciones, configuración del firewall, asegurar puertos de servicios, garantizar el acceso seguro, servicios de compartición de recursos, uso de la virtualización, passwords, respaldos, uso de la criptografía.

5. Competencias previas

- Seleccionar, clasificar y analizar información.
- Conocimientos de SO Unix y Windows
- Conocimientos de redes y servicios
- Conocimientos de PKI
- Conocimiento de certificados digitales
- Capacidad de desarrollar un proyecto para el endurecimiento de SO aplicados a necesidades de la industria

6. Temario

No.	Temas	Subtemas
1	Introducción	1.1 Definición de Sistemas Operativos (SO) seguros 1.2 Objetivos de la seguridad

		1.3 Modelo de confianza y amenazas 1.4 Tipos de seguridad en SO 1.5 Estándares de seguridad
2	Control de acceso en SO	2.1 Protección del SO 2.2 Sistemas de protección obligatorios 2.3 Acceso seguro y criterios de evaluación 2.4 Control de acceso en Unix y Windows 2.5 Firewall
3	Seguridad en UNIX	3.1 Kernel 3.2 Sistemas de protección 3.3 Autorización 3.4 Análisis de seguridad, vulnerabilidades y amenazas 3.5 Endurecimiento
4	Seguridad en servidores Windows	4.1 Sistemas de protección 4.2 Acceso seguro 4.3 Análisis de la seguridad 4.4 Servidores de dominios 4.5 Vulnerabilidades y amenazas

7. Actividades de aprendizaje de los temas

Tema 1: Introducción	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá los conceptos de un SO seguro - Analizará los objetivos de la seguridad en un SO - Conocerá los modelos de confianza y amenazas - Investigará los tipos de SO y los estándares de seguridad Genéricas: - Conocerá los conceptos de seguridad aplicados a SO	1. Documentarse en todos los conceptos de seguridad informática en el endurecimiento de SO. 2. Conocerá estándares de seguridad en SO
Tema 2: Control de Acceso	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá métodos de protección en un SO - Estudiará el sistema de protección obligatorio - Investigará la definición de un SO seguro y los criterios de evaluación y Control de acceso seguros en los SO Unix y Windows Genéricas: - Aplicar una metodología para llevar a cabo el control de acceso seguro en SO.	1. Elabora los pasos para un control de acceso seguro 2. Aplicar el sistema de protección obligatorio 3. Realizar los pasos necesarios para un acceso seguro en sistemas Unix y Windows, uso del Firewall
Tema 3: Seguridad en Unix	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá la forma de garantizar un Kernel seguro - Conocerá los sistemas de protección y autorización en Unix - Realizará un análisis de la	1. Implementar el endurecimiento en sistemas Unix. 2. Establecer los pasos para el análisis de la seguridad en sistemas Unix 3. Verificará las posibles vulnerabilidades y amenazas de Unix

seguridad del SO - Revisará las posibles vulnerabilidades y amenazas de Unix, endurecimiento Genéricas: - Implementará el endurecimiento de SO Unix.	
Tema 4: Seguridad en Windows	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá la forma de garantizar un Kernel seguro - Conocerá los sistemas de protección y autorización en Windows - Realizará un análisis de la seguridad del SO - Revisará las posibles vulnerabilidades y amenazas de Unix, endurecimiento Genéricas: - Implementará el endurecimiento de SO Windows.	1. Implementar el endurecimiento en sistemas Windows. 2. Establecer los pasos para el análisis de la seguridad en sistemas Windows 3. Verificará las posibles vulnerabilidades y amenazas en servidores Windows

8. Práctica(s)

- Actualizaciones y parches para un Kernel seguro en Linux
- Métodos de protección y autorización en Linux
- Monitoreo y análisis de la seguridad en Linux
- Revisar métodos de detección de vulnerabilidades y amenazas Linux
- Revisar el estado del endurecimiento en Linux
- Actualizaciones y parches para un Windows seguro
- Métodos de protección y autorización en Windows
- Monitoreo y análisis de la seguridad servidores Windows
- Revisar métodos de detección de vulnerabilidades y amenazas en Windows
- Revisar el estado del endurecimiento en servidores Windows

9. Proyecto de asignatura

Que el alumno, sea capaz de llevar a cabo el endurecimiento en Sistemas Operativos Linux y en servidores Windows. Realizará un proyecto del análisis y detección de vulnerabilidades en servidores implementados en la industria Implementará esquemas de seguridad que permitan disminuir las amanezcas y vulnerabilidades detectadas

10. Evaluación por competencias

- Elaboración de prácticas y su evaluación.
- Elaborar un proyecto de endurecimiento de un servidor.
- Realizar un análisis de vulnerabilidades y amenazas.
- Aplicar esquemas de seguridad en SO para disminuir las amenazas.

11. Fuentes de información

[1] Nemeth Evi, Snyder Garth. Unix and Linux system administration. Kindle Edition, 2017.

[2] Tevault Donald. Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Kindle Edition, 2018.

[3] Barrett Daniel, Silverman Richard, Byrnes Robert. Linux Security Cookbook. O-Reilly. 2017

[4] Sivarajan Santhosh. Getting Started with Windows Server Security. Kindle Edition, 2015.

[5] Miroshnikov Andrei. Windows Security Monitoring: Scenarios and Patterns. Ed. Wiley. 2018

[6] Krause Jordan. Windows Server 2016 Security, Certificates, and Remote Access Cookbook: Recipe-based guide for security, networking and PKI in Windows Server 2016. Kindle Edition, 2018.