1.- DATOS DE LA ASIGNATURA

Nombre de la asignatura:	**Protección de Sistemas Operativos**
Carrera:	**Ingeniería en Sistemas Computacionales**
Clave de la asignatura:	**SIF-1604**
(Créditos) SATCA:	**3-2-5**

2.- PRESENTACIÓN

Caracterización de la asignatura.

Esta asignatura desempeña un papel fundamental en el plan de estudio de estas ingenierías porque a través de ella el estudiante conoce los conceptos básicos de seguridad de las funciones de los sistemas operativos, así como aspectos generales de la construcción de sistemas operativos.

Los sistemas operativos son la plataforma base a través de la cual los usuarios pueden manipular las computadoras y el software puede funcionar. Por este motivo, es necesario que el estudiante conozca las normas de seguridad en sistemas operativos a detalle para entender su seguridad informática y realizar software de sistemas de una manera segura y estable.

Intención didáctica.

El conjunto de conocimientos organizados en esta asignatura se encuentran divididos en cinco unidades temáticas, mismas que pretenden guiar a los estudiantes en la comprensión de los fundamentos teóricos sobre la seguridad en los sistemas operativos y lo orientan capacitándolo para planificar, analizar y diseñar soluciones de módulos que forman parte de la estructura de un sistema operativo, así como diseñar sistemas operativos para diferentes plataformas de aplicación.

En la primera unidad se encuentran los contenidos básicos: los conceptos fundamentales y Terminologías asociadas al sistema operativo.

En la segunda unidad se establece la filosofía de seguridad en sistemas operativos, las normas de seguridad en los sistemas operativos, los niveles de seguridad y políticas, para mejorar la capacidad de procesamiento de los programas de los usuarios, proponiendo al estudiante la creación y mejoramiento de un algoritmo que permita la seguridad como recurso fundamental que requiere ser administrado por el sistema operativo, ya que estos se desarrollan más rápidamente que los programas para aprovechar su capacidad.

La introducción al aprendizaje para los niveles de seguridad y la práctica cotidiana, se presenta en la tercera unidad.

La cuarta unidad orienta a los estudiantes a proponer estrategias para dar seguridad a un sistema operativo que permita que los usuarios puedan acceder de forma segura.

La quinta unidad se proporciona los conocimientos de seguridad indispensables para la protección de los archivos de los usuarios, así como técnicas de protección de acceso a los Sistemas cómputo.

3.- COMPETENCIAS A DESARROLLAR

Competencias Específicas	**Competencias genéricas**
Proporcionar al egresado los conocimientos básicos de seguridad para el desarrollo de proyectos de tecnología de información y la visión de los aspectos que influyen en la seguridad informática.	**Competencias instrumentales** • Capacidad de análisis y síntesis • Conocimientos básicos de la carrera • Comunicación oral y escrita • Conocimiento de una segunda lengua • Conocimiento generales básicos del lenguaje ensamblador. • Habilidad para buscar y analizar información proveniente de fuentes diversa. • Habilidad lógica para solucionar problemas • Habilidades del manejo de la Computadora **Competencias interpersonales** • Capacidad crítica y autocrítica. • Trabajo en equipo interdisciplinario. • Habilidades interpersonales. **Competencias sistémicas** • Habilidades de investigación • Capacidad de aplicar los conocimientos en la práctica. • Capacidad de aprender • Capacidad de generar nuevas ideas (creatividad) • Habilidad para trabajar en forma autónoma • Capacidad para diseñar y gestionar proyectos • Estándares de calidad aplicados a los lenguajes de programación • Búsqueda del logro

4.- HISTORIA DEL PROGRAMA

Lugar y Fecha	Participantes	Evento
Instituto Tecnológico de Tláhuac, México D.F. 18 de Mayo de 2012 Instituto Tecnológico de Tláhuac, CDMX. 11 de Abril de 2016.	Academia de Sistemas y Computación	Revisión y actualización de contenidos temáticos del programa de estudios para esta especialidad.

5.- OBJETIVO(S) GENERAL(ES) DEL CURSO (competencias específicas a desarrollar).

La protección de los sistemas operativos es fundamental en las organizaciones de cualquier índole, por tal motivo en este curso el alumno conocerá, explicará y aplicará las diferentes filosofías de seguridad en sistemas operativos, así como las líneas generales para dar seguridad al mismo además de los pasos para instalar un sistema seguro.

6.- COMPETENCIAS PREVIAS

- Conocer, analizar e interpretar la filosofía de diseño de los sistemas operativos actuales y proponer aplicaciones para el manejo de los recursos del sistema.
- Conocer los conceptos fundamentales de los modelos de arquitecturas de cómputo.
- Conocer y analizar los bloques que conforman un sistema de cómputo.
- Elegir componentes y ensamblar equipos de cómputo.
- Identificar las diferencias de los sistemas de memoria compartida y los sistemas de memoria distribuida.

7.- TEMARIO

Unidad	Temas	Subtemas
1	Introducción	1.1 Funciones de un sistema operativo 1.2 Procesos 1.3 Comunicación entre procesos 1.4 Conflictos entre procesos 1.5 Manejo de la memoria 1.6 Memoria protegida 1.7 Memoria virtual 1.8 Riesgos en el manejo de la memoria 1.9 Sistemas de archivos 1.10 Control de acceso y derechos
2	Filosofía de Seguridad en Sistemas Operativos	2.1 Normas de seguridad en sistemas operativos 2.2 Conceptos básicos del libro naranja 2.2.1 Niveles de seguridad y políticas 2.2.2 Rendición de cuentas 2.2.3 Mecanismos de seguridad 2.2.4 Protección continua 2.2.5 TCB 2.2.6 División D 2.2.7 División C 2.2.7.1 Clase C1 2.2.7.2 Clase C2: Protección por acceso controlado 2.2.8 División B: Protección obligatoria 2.2.8.1 Clase B1: Protección por seguridad etiquetada 2.2.8.2 Clase B2: Protección estructurada 2.2.8.3 Clase B3: Dominios de seguridad 2.2.9 División A: Protección verificada 2.3 El libro amarillo 2.3.1 Selección de niveles de seguridad 2.3.2 Modos de operación 2.3.3 Índice de riesgo
3	Implementación de la seguridad	3.1 Sistemas y mecanismos de protección 3.1.1 Seguridad física 3.1.1.1 Protección del hardware 3.1.1.1.1 Acceso físico 3.2 Sistemas y mecanismos de protección 3.2.2 Seguridad lógica 3.2.2.1 Identificación y Autenticación 3.2.2.2 Modalidad de Acceso

		3.2.2.3 Control de Acceso Interno 3.2.2.3.1 Contraseñas 3.2.2.3.2 Listas de Control de Acceso 3.2.2.3.3 Cifrado 3.2.2.4 Control Acceso Externo 3.2.2.4.1 Dispositivos de control de puertos 3.2.2.4.2 Firewalls 3.2.2.4.2.1 Selección de tipo de Firewall 3.2.2.4.2.2 Integración de las políticas de seguridad 3.2.2.4.2.3 Revisión y análisis del mercado 3.2.2.4.3 Proxies 3.2.2.4.4 Integridad del Sistema 3.2.2.4.5 VPN (Virtual Private Networks) 3.2.2.4.6 DMZ (Zona Desmilitarizada) 3.2.2.4.7 Herramientas de seguridad 3.3 Seguridad en Sistemas 3.3.1 Riesgos de Seguridad en Sistemas 3.3.2 Arquitectura de los Sistemas 3.3.3 Problemas Comunes de Seguridad 3.3.4 Administración de Usuarios y controles de acceso 3.3.5 Administración de Servicios 3.3.6 Monitoreo 3.3.7 Actualización de los sistemas 3.3.8 Mecanismos de Respaldo 3.4 Seguridad en Redes de Datos 3.4.1 Amenazas y Ataques a Redes 3.4.2 Elementos básicos de protección 3.4.3 Introducción a la Criptografía 3.4.4 Seguridad de la Red a nivel: 3.4.4.1 Aplicación 3.4.4.2 Transporte 3.4.4.3 Red 3.4.4.4 Enlace 3.4.5 Monitoreo 3.5 Seguridad en Redes Inalámbricas 3.5.1 Seguridad en el Access Point

		3.5.2 SSID (Service Set Identifier) 3.5.3 WEP (Wired Equivalent Privacy) 3.5.4 Filtrado de MAC Address 3.5.5 RADIUS Authentication 3.5.6 WLAN VPN 3.5.7 Seguridad sobre 802.11(x) 3.5.8 Nuevas Tecnologías de Seguridad para Redes inalámbricas
4	Líneas generales para dar seguridad a un sistema operativo	4.1 Principios básicos 4.1.1 Principio de las funciones mínimas necesarias 4.1.2 Principio del mínimo privilegio 4.2 La seguridad se inicia desde la instalación 4.3 Instalar servicios seguros cuando haya opción 4.4 Servicio de archivos seguro 4.5 Correo electrónico 4.6 Web 4.7 FTP 4.8 Acceso al Shell 4.9 Eliminar servicios que provean información interna 4.10 Instalar mecanismos adicionales de seguridad
5	Pasos para instalar un sistema seguro	5.1 Planeación 5.2 Instalación 5.3 Configuración 5.4 Revisión de puertos abiertos 5.5 Sistema seguro de contraseñas 5.6 Versiones de los programas 5.7 Protección de la cuenta del súper usuario 5.8 Protección de rutas 5.9 Acceso seguro 5.10 Derechos de acceso 5.11 Verificación del sistema 5.12 Sistemas de detección de intrusos 5.13 Endurecimiento adicional

8.-SUGERENCIAS DIDÁCTICAS (desarrollo de competencias genéricas)

- Trabajos de investigación en equipo.
- Exposición audio visual
- Ejercicios dentro de clase
- Prácticas de taller o laboratorio en equipo.
- Ejercicios fuera del aula

9.-SUGERENCIAS DE EVALUACIÓN

- Ejercicios de evaluación por unidad
- Desarrollo de prácticas
- Tareas y trabajos fuera del aula
- Participación en clases

10.-UNIDADES DE APRENDIZAJE

UNIDAD 1.- Introducción

Competencias específicas a desarrollar	Actividades de Aprendizaje
Conocer y explicar la importancia de los sistemas operativos, así como el manejo de procesos, memoria y archivos en los mismos.	El alumno definirá las funciones de los sistemas operativos y los procesos que se ejecutan en el mismo.

UNIDAD 2.- Filosofías de seguridad en sistemas operativos

Competencias específicas a desarrollar	Actividades de Aprendizaje
Analizar e identificar las diferentes filosofías de seguridad de Sistemas operativos que actualmente existen. Generará en base a estas filosofías diferentes políticas y mecanismos de seguridad para la protección de los sistemas operativos partiendo de un análisis de riesgos y de la identificación de las amenazas y vulnerabilidades más comunes al respecto.	El alumno identificara las diferentes políticas y mecanismos de seguridad que se implementan en los diferentes sistemas operativos

UNIDAD 3.- Implementación de la Seguridad Informática

Competencias específicas a desarrollar	Actividades de Aprendizaje
Explicar y aplicar los mecanismos de seguridad física y lógica	Investigar los requisitos necesarios para poder implementar mecanismos de seguridad informática de manera física y lógica.

UNIDAD 4.- Líneas generales para dar seguridad a un sistema operativo

Competencias específicas a desarrollar	Actividades de Aprendizaje
Analizar las diferentes líneas de seguridad para la protección de Sistemas operativos que garanticen la instalación de servicios seguros.	El alumno observará los diferentes niveles de privilegios y servicios internos del sistema que proveen información, el sistema seguro de archivos entre otros como mecanismos de seguridad.

UNIDAD 5.- Pasos para instalar un sistema seguro

Competencias específicas a desarrollar	Actividades de Aprendizaje
Implementar las técnicas necesarias para lograr la instalación de Sistemas operativos con un margen de seguridad óptimo.	El alumno investigará y debatirá que dispositivos físicos y lógicos necesita para poder implementar o instalar un sistema operativo con un margen de seguridad óptimo.

11. FUENTES DE INFORMACIÓN

1. STEVENS, Richard. *UNIX Network Programming.*USA. Prentice Hall, 1990.
2. STEVENS, Richard. *UNIX Network Programming, Volume I.* 3rd. Edition. USA. Addison Wesley, 2003.
3. COMER, Douglas E. *Interconectividad de Redes con TCP/IP Vol. I. Principios Básicos y Arquitectura.* 3a. Edición.México.Prentice Hall, 2000.
4. COMER, Douglas E. *Internetworking with TCP/IP Vol. III. Client Server Programming and applications.*3rd. Edition. USA. Prentice Hall, 2000.
5. MÁQUEZ GARCÍA, Francisco Manuel. *Unix Programación Avanzada.* España. Ra-ma, 1993.

12.- PRÁCTICAS PROPUESTAS

PRÁCTICA 1. RIESGOS EN EL MANEJO DE MEMORIA.

Objetivo: El alumno hará un análisis de los riesgos en el manejo de la memoria del Sistema Operativo Windows y propondrá las políticas de seguridad necesarias para disminuir dichos riesgos. Trabajarán en equipos de 4 integrantes.

PRÁCTICA 2. APLICACIÓN DEL PRINCIPIO DE LAS FUNCIONES MÍNIMAS NECESARIAS Y EL PRINCIPIO DEL MÍNIMO PRIVILEGIO PARA DAR SEGURIDAD AL SISTEMA OPERATIVO UNIX/LINUX.

Objetivo: El alumno aprovechará lo visto en clase sobre estos dos principios usados para dar seguridad a los sistemas operativos y haciendo un análisis meticuloso del Sistema Operativo Unix/Linux pondrá en práctica dichos principios con la finalidad de optimizar la seguridad de este tan importante sistema usado principalmente en grandes organizaciones.

PRÁCTICA 3. ANÁLISIS DE ATAQUES BÁSICOS SOBRE PROCESOS Y PROPUESTA DE LAS POLÍTICAS Y MECANISMOS DE SEGURIDAD PARA PREVENIRLOS.

Objetivo: El alumno hará un análisis de los ataques básicos más comunes sobre procesos del sistema operativo Windows y Linux para posteriormente elaborar una propuesta con las políticas y mecanismos de seguridad apropiados que permitan prevenir dichos ataques.

PRÁCTICA 4. PROPUESTA DE LOS PASOS PARA INSTALAR UN SISTEMA OPERATIVO "SEGURO".

Objetivo: El alumno elegirá el sistema operativo de su preferencia (Windows, Windows NT, Linux, Unix, Mac OS X) y en equipos de 4 integrantes tomando en cuenta lo visto en clase, elaborará una propuesta de los pasos para instalar de manera segura el sistema elegido. Las consideraciones a tomar en cuenta son las siguientes:

- Planeación
- Instalación
- Configuración
- Revisión de puertos abiertos
- Sistema seguro de contraseñas
- Versiones de los programas
- Protección de rutas
- Acceso seguro
- Derechos de acceso
- Verificación del sistema
- Sistemas de detección de intrusos