



## 1. Datos Generales de la asignatura

<b>Nombre de la asignatura:</b>	Administración de sistemas operativos
<b>Clave de la asignatura:</b>	CBD-2402
<b>SATCA<sup>1</sup>:</b>	2-3-5
<b>Carrera:</b>	Ingeniería en Ciberseguridad.

## 2. Presentación

### Caracterización de la asignatura

Esta asignatura aporta el perfil del ingeniero en ciberseguridad las siguientes habilidades:

- Utiliza sistemas operativos, lenguajes de programación, redes y entornos tecnológicos para integrar soluciones de seguridad con responsabilidad e inclusión social en las organizaciones.
- Dirige el monitoreo, análisis y control de la información utilizando herramientas y marcos de referencia, con perspectiva ética, de respeto por la persona y de responsabilidad social.
- Evalúa riesgos de seguridad y vulnerabilidad en aplicaciones o instalaciones de tecnologías de la información con apoyo de herramientas de vanguardia automatizadas de acuerdo a metodologías, normas y estándares de excelencia.
- Diseña políticas de seguridad informática para establecer controles de seguridad pertinentes atendiendo los principios de no discriminación, Inclusión y equidad social.
- Gestiona incidentes y eventos de seguridad de informática para reducir la afectación negativa de la seguridad de la información y dar continuidad a las operaciones de la organización, atendiendo los principios de no discriminación, Inclusión y equidad social.
- Gestiona planes y proyectos de seguridad de la información de acuerdo con las necesidades del negocio, considerando riesgos y contingencias, promoviendo el cumplimiento de los principios de no discriminación, inclusión, equidad social, políticas, normas y acuerdos de nivel de servicio.

Esta asignatura desempeña un papel fundamental para el plan de estudios de esta ingeniería porque el estudiante aplica en detalle, funciones de seguridad en un sistema operativo cliente; así como, valora el trabajo de mantener seguro un sistema operativo.

El sistema operativo es la plataforma base por la que las aplicaciones pueden ejecutarse en las computadoras. Por este motivo, es necesario que el estudiante aplique a detalle la implementación de seguridad en un sistema operativo para entender su funcionamiento y administrarlo de una mejor manera.

<sup>1</sup> Sistema de Asignación y Transferencia de Créditos Académicos



### Intención didáctica

El conjunto de conocimientos organizados en esta asignatura se encuentra divididos en cuatro temas, mismos que pretenden guiar a los estudiantes en la comprensión de los fundamentos de la administración segura de sistemas operativos.

En primer tema se encuentran los contenidos básicos: los comandos fundamentales asociados a la administración de un sistema operativo.

En segundo tema se aplican los conceptos que tienen que ver con la administración de cuentas, de usuarios para mejorar la seguridad de procesos, proponiendo al estudiante la configuración de políticas de grupo para el mejoramiento de la seguridad y que permita el aprovechamiento de las capacidades de seguridad del sistema operativo como recurso fundamental que requiere ser administrado por el ingeniero en ciberseguridad.

La introducción a la administración de seguridad de la información se presenta en el tercer tema, siendo éste un punto débil y que resulta muy importante su administración correcta, por lo que se requiere de mejores estrategias de gestión para poder atender las peticiones de los usuarios de sistemas administrados.

El cuarto tema ofrece a los estudiantes un análisis de la filosofía de diseño con el que trabajan actualmente los diseñadores de sistemas de protección para permitir el control de tráfico de red; además se proporcionan los conocimientos de seguridad indispensables que emplea el sistema operativo en la protección orientada a los procesos, memoria y archivos, así como control de usuarios y permisos de acceso a diferentes recursos.

### 3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México del 4 al 6 de marzo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Propuesta sintética de la carrera de Ingeniería en Ciberseguridad.



Tecnológico Nacional de México del 22 al 26 de abril del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas.  Representante de Ciencias Básica de los Institutos de: Celaya, Morelia CENIDET y CIIDET.	Diseño y/o desarrollo curricular de la carrera de Ingeniería en Ciberseguridad
Tecnológico Nacional de México del 27 al 31 de mayo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Jiquilpan, Mérida, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Consolidación curricular de la carrera de Ingeniería en Ciberseguridad.

#### 4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
<ul style="list-style-type: none"><li>Conoce, selecciona y gestiona la seguridad de un sistema operativo en plataformas cliente-servidor, para resolver problemáticas reales y aplicar procedimientos de configuración de seguridad en plataformas de software.</li></ul>

#### 5. Competencias previas

<ul style="list-style-type: none"><li>Aplica los paradigmas de diseño de sistemas operativos actuales y emergentes, para la administración de los recursos del sistema.</li></ul>
---

#### 6. Temario

No.	Temas	Subtemas
1	Administración de un sistema operativo.	1.1. Comandos básicos, aplicaciones y servicios. 1.1.1. Manejo de archivos y directorios. 1.1.2. Niveles de ejecución. 1.1.2.1. Modo usuario. 1.1.2.2. Modo administrador. 1.1.2.3. Modo recuperación. 1.1.3. Instalación de actualizaciones, aplicaciones y servicios.



2	Administración de usuarios del sistema operativo.	<ul style="list-style-type: none"><li>2.1. Administración de usuarios del sistema.<ul style="list-style-type: none"><li>2.1.1. Administración de usuarios, grupos y permisos.</li><li>2.1.2. Creación masiva de usuarios.</li><li>2.1.3. Creación de contraseñas seguras.</li><li>2.1.4. Política de simétrico de contraseñas</li><li>2.1.5. Listas de control de acceso.</li><li>2.1.6. Auditoria de eventos de seguridad.</li><li>2.1.7. Política de complejidad de contraseñas.</li><li>2.1.8. Otras políticas de contraseñas.</li><li>2.1.9. Políticas de desbloqueo de pantalla e inicio de sesión.</li></ul></li></ul>
3	Seguridad e integridad.	<ul style="list-style-type: none"><li>3.1. Seguridad e Integridad.<ul style="list-style-type: none"><li>3.1.1. Planificación de seguridad de la información.<ul style="list-style-type: none"><li>3.1.1.1. Conexión segura a una red corporativa.</li><li>3.1.1.2. Cifrado de información confidencial.</li></ul></li><li>3.1.2. Planificación y ejecución de respaldos del sistema y datos.</li><li>3.1.3. Mecanismos de Recuperación ante desastres.<ul style="list-style-type: none"><li>3.1.3.1. Clonación de discos.</li><li>3.1.3.2. Congelación Profunda y Sistemas Inmutables.</li></ul></li></ul></li></ul>
4	Seguridad y cortafuegos.	<ul style="list-style-type: none"><li>4.1. Cortafuegos y detección de intrusión.<ul style="list-style-type: none"><li>4.1.1. Firewalls basados en host.</li><li>4.1.2. Sistemas de detección de intrusos en el host.</li></ul></li><li>4.2. Concepto y objetivos de protección y seguridad.</li><li>4.3. Clasificación aplicada a la seguridad.</li><li>4.4. Funciones del sistema de protección.</li><li>4.5. Implantación de matrices de acceso.</li><li>4.6. Protección basada en el lenguaje.</li><li>4.7. Validación y amenazas al sistema.</li><li>4.8. Cifrado.</li></ul>



## 7. Actividades de aprendizaje de los temas

1. Administración de un sistema operativo	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i></p> <p>Aplica las técnicas de administración de credenciales de usuarios e identifica sus implicaciones en la gestión de seguridad de un sistema de operativo.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"><li>• Capacidad de análisis y síntesis.</li><li>• Capacidad de investigación.</li><li>• Habilidad para buscar, procesar y analizar información procedente de fuentes diversas.</li><li>• Capacidad de conocimiento de una segunda lengua.</li></ul> <p><i>Transversal(es):</i></p> <ul style="list-style-type: none"><li>• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.</li><li>• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.</li><li>• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.</li></ul>	<ul style="list-style-type: none"><li>• Investigar y exponer las diferencias y similitudes en, administración de archivos y directorios, en los sistemas operativos vigentes en la industria.</li><li>• Identificar, en equipo, los modos de arranque de dos sistemas operativos, sus funciones y características. Elaborar conclusiones por equipo y presentarlas al grupo.</li></ul>



2. Administración de usuarios del sistema operativo	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Aplica las técnicas de administración de credenciales de usuarios e identifica sus implicaciones en la gestión de seguridad de un sistema de operativo.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"><li>• Capacidad de análisis y síntesis.</li><li>• Capacidad de investigación.</li><li>• Habilidad para buscar, procesar y analizar información procedente de fuentes diversas.</li><li>• Capacidad de conocimiento de una segunda lengua.</li></ul> <p><i>Transversal(es):</i></p> <ul style="list-style-type: none"><li>• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.</li><li>• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.</li><li>• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.</li></ul>	<ul style="list-style-type: none"><li>• Investigar en diferentes plataformas la creación de grupos y usuarios.</li><li>• Investigar y aplicar Policy Groups y Mandatory Access Control.</li></ul>



3. Seguridad e integridad	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i></p> <p>Aplica las técnicas de administración de seguridad para el máximo aprovechamiento de las capacidades de las plataformas de software vigentes. Así como, las estrategias adecuadas de respaldo de información, conexión local y de forma remota.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"><li>• Capacidad de análisis y síntesis</li><li>• Capacidad de aplicar los conocimientos en la práctica</li><li>• Habilidad para buscar, procesar y analizar información procedente de fuentes diversas</li><li>• Capacidad de comunicación oral y escrita</li><li>• Capacidad de conocimiento de una segunda lengua</li></ul> <p><i>Transversal(es):</i></p> <ul style="list-style-type: none"><li>• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.</li><li>• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.</li><li>• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.</li></ul>	<ul style="list-style-type: none"><li>• Investigar las diferentes soluciones de Virtual Private Network.</li><li>• Investigar las diferentes soluciones de cifrado de discos y archivos.</li><li>• Investigar las ventajas y desventajas entre respaldo completo e instantáneas del sistema.</li><li>• Plantear un caso de recuperación de datos y credenciales de acceso, en caso de falla del hardware y analizar las diferentes soluciones propuestas.</li></ul>



4. Seguridad y cortafuegos	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Conoce y analiza los mecanismos de protección y como éstos son empleados para proteger la integridad del sistema.</p> <p><i>Genéricas:</i></p> <ul style="list-style-type: none"><li>• Capacidad de aplicar los conocimientos en la practica</li><li>• Habilidad para buscar, procesar y analizar información procedente de fuentes diversas</li><li>• Capacidad para identificar, plantear y resolver problemas</li><li>• Capacidad de conocimiento de una segunda lengua</li></ul> <p><i>Transversal(es):</i></p> <ul style="list-style-type: none"><li>• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.</li><li>• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.</li><li>• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.</li></ul>	<ul style="list-style-type: none"><li>• Documentar la clasificación de los sistemas de prevención y detección de intrusos estableciendo semejanzas y diferencias.</li><li>• Plantear un caso de configuración de cortafuegos y listas de control de acceso.</li><li>• Investigar y comentar en clase el concepto de seguridad, vulnerabilidad, protección y los mecanismos que emplean los sistemas operativos.</li><li>• Documentar las amenazas más comunes que se aplican a los sistemas operativos hoy.</li><li>• Elaborar una tabla comparativa de los diferentes tipos de seguridad y técnicas de cifrado incluyendo las ventajas y desventajas.</li></ul>





## 8. Práctica(s)

- Descargar de Internet los sistemas operativos AlmaLinux y Windows 11, instalar herramientas de software, para su instalación en una máquina virtual, en el servidor de virtualización. Y aplicar un perfil de seguridad adecuado a las necesidades del sistema.
- Configurar passphrase de acceso para usuario sin privilegios.
- Cifrado de datos con LUKS y BitLocker.
- Instalar NextCloud en AlmaLinux con SELinux en modo Enforcing.
- Configuración de segundo factor de autenticación en NextCloud.
- Configuración de un sistema de archivos WebDAV en NextCloud, usar cliente Windows y Linux.
- Configuración de un sistema sincronización de archivos, se sugiere Clientes Windows y Android.
- Configurar respaldos automáticos con Windows 11. Configurar respaldos automáticos de Servidor Web Linux. Respaldo completo de sistema clientes Windows y máquinas virtuales Linux.
- Instalar una Distribución GNU/Linux inmutable, como Fedora SilverBlue u otra, para demostrar el concepto de inmutabilidad del sistema.

## 9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance del(los) logro(s) formativo(s) de la asignatura, considerando las siguientes fases:

**Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.

**Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.

**Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de los saberes, habilidades y destrezas a desarrollar.

**Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.



## 10. Evaluación de saberes, habilidades y destrezas

- Para evaluar las actividades de aprendizaje se recomienda solicitar: mapas conceptuales, reportes de investigación, estudios de casos, exposiciones en clase, reportes de visitas, portafolio de evidencias, tablas comparativas, glosarios, entre otros.
- Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de valoración, rúbricas, entre otros, mediante la heteroevaluación, coevaluación y autoevaluación.

## 11. Fuentes de Información

1. Stallings, W. (2005). Sistemas Operativos (Quinta ed.). Pearson. Prentice-Hall.
2. Tanenbaum, A. y Escalona, R. (2009). Sistemas Operativos Modernos (3ra ed.) Madrid España. Prentice Hall.
3. Tanenbaum, A. y Woodhull, A. (2009). Sistemas Operativos: Diseño e Implementación (2da ed). México. Pearson Educación.
4. Carretero, J., De Miguel, P., García, F. y Pérez, F. (2001). Sistemas Operativos una visión aplicada. Mc. Graw Hill.
5. 5. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI.