



## 1. Datos Generales de la asignatura

<b>Nombre de la asignatura:</b>	Análisis de malware
<b>Clave de la asignatura:</b>	CBD-2404
<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:

- 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 con metodologías, normas y estándares de excelencia.
- Implementa soluciones metodológicas y controles de seguridad en el ciclo de vida del desarrollo de software que permitan la reducción de vulnerabilidades y la inclusión de mejores prácticas de seguridad, con una perspectiva de responsabilidad social.

La asignatura está diseñada para proporcionar al ingeniero en ciberseguridad las habilidades y competencias necesarias para identificar, analizar y mitigar amenazas de malware de manera efectiva.

A su vez integra técnicas, métodos y herramientas de análisis de malware que permiten al ingeniero identificar, analizar y comprender el comportamiento de programas maliciosos (malware) para asegurar la integridad, confidencialidad y disponibilidad de los sistemas informáticos.

La importancia del análisis de malware radica en la comprensión del funcionamiento, técnicas de evasión y métodos de análisis para desarrollar estrategias de defensa. El análisis de malware permite detectar y neutralizar malware antes de que causen daños significativos a los sistemas.

Esta asignatura aporta al perfil de egreso del ingeniero en ciberseguridad al prepararlos para:

- Evalúa riesgos de seguridad y vulnerabilidad.
- Establece políticas de seguridad informática.
- Gestiona incidentes y eventos de seguridad de informática.
- Gestiona planes y proyectos de seguridad de la información.
- Aplica procedimientos y técnicas de auditoría informática.

Esta asignatura se relaciona con otras asignaturas del plan de estudios, como: fundamentos de ciberseguridad, sistemas operativos, redes de computadoras, criptografía y fundamentos de seguridad en sistemas operativos.

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



Las competencias específicas se manifiestan en la capacidad para comprender el comportamiento de las amenazas de malware, aplicar metodologías y hacer uso de herramientas para análisis estático, dinámico y avanzado de muestras de malware.

### **Intención didáctica**

El temario presentado se organiza en cuatro temas que abarcan contenidos teórico-prácticos que se abordan de manera estructurada y progresiva.

En el primer tema ofrecerá una visión completa de la evolución del malware, su anatomía, las motivaciones detrás de su creación y las tendencias actuales en ciberseguridad.

Posteriormente, en el segundo tema, se profundizará en el proceso de análisis estático de malware y se abordarán las técnicas de análisis de firmas, hashes, strings, desensamblado.

El tercer tema se centrará en el análisis dinámico de malware, incluyendo técnicas como sandboxing, emulación de entornos, análisis de tráfico de red entre otras.

Finalmente, el cuarto tema presentará técnicas avanzadas como la evasión, ingeniería inversa, análisis de protocolos y el machine learning.

El enfoque de la asignatura deberá ser teórico y práctico, combinando la comprensión conceptual del malware con el desarrollo de habilidades prácticas para identificar, analizar y mitigar amenazas. Se enfatizará la aplicación de metodologías y herramientas específicas de análisis de malware para fortalecer la capacidad de los estudiantes para detectar las distintas amenazas de malware.

Se propone el uso de organizadores gráficos para sintetizar la información y fomentar la capacidad de abstracción y síntesis. Además, se recomienda el análisis de casos de estudio y la realización de prácticas que promuevan la identificación, planteamiento y resolución de problemas como actividades destacadas para el desarrollo de competencias genéricas. Entre las competencias genéricas que se desarrollarán se incluyen habilidades de análisis crítico, resolución de problemas, comunicación efectiva, trabajo en equipo y toma de decisiones.

El docente deberá desempeñar un rol de facilitador y orientador, promoviendo la participación de los estudiantes en actividades prácticas, debates y análisis de casos reales para fortalecer su aprendizaje experimental y la aplicación de conocimientos. Además, se espera que el docente fomente un ambiente de aprendizaje colaborativo y estimule el desarrollo de competencias técnicas y blandas en los estudiantes.



### 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>Identifica, analiza y clasifica diferentes tipos de malware utilizando técnicas de análisis estático y dinámico, aplicando metodologías de detección y técnicas avanzadas de análisis para evaluar la integridad, confidencialidad y disponibilidad de los sistemas informáticos en entornos controlados y reales.</li></ul>



## 5. Competencias previas

- Aplica conceptos fundamentales de arquitectura de computadoras para diseñar, implementar y evaluar desde una perspectiva de seguridad, los sistemas informáticos que satisfagan necesidades específicas.
- Conoce, comprende y aplica eficientemente estructuras de datos, métodos de ordenamiento y búsqueda para la optimización del rendimiento de soluciones a problemas del mundo real, garantizando la seguridad de la estructura de datos al implementar la validación y el saneamiento de estos.
- Aplica los paradigmas de diseño de los sistemas operativos actuales y emergentes, para el manejo de los recursos del sistema.

## 6. Temario

No.	Temas	Subtemas
1	Introducción al análisis de malware	1.1. Definición y tipos de malware. 1.2. Características del malware. 1.3. Historia y evolución del malware. 1.4. Anatomía de un ataque. 1.5. Motivaciones detrás del malware. 1.6. Tendencias actuales en el panorama de amenazas.
2	Métodos de análisis estático	2.1. Proceso de análisis estático de malware. 2.2. Análisis de firmas y hashes. 2.2.1. Firma digital. 2.2.2. MD5 (message digest algorithm 5). 2.2.3. SHA-1 (secure hash algorithm 1). 2.2.4. SHA-256 (secure hash algorithm 256 bits). 2.2.5. SHA-384 y SHA-512. 2.2.6. SHA-3 (secure hash algorithm 3). 2.3. Análisis de strings. 2.4. Análisis de desensamblado. 2.5. Análisis de archivos de configuración.
3	Métodos de análisis dinámico	3.1. Proceso de análisis dinámico de malware. 3.2. Sandboxing. 3.2.1. Herramientas de sandboxing. 3.3. Emulación de entornos. 3.3.1. Herramientas de virtualización. 3.4. Análisis de tráfico de red. 3.4.1. Herramientas de análisis de red. 3.5. Análisis de comportamiento. 3.6. Análisis de artefactos forenses.



4	Métodos avanzados de análisis	<p>4.1. Técnicas de evasión.</p> <p>4.1.1. Rootkits.</p> <p>4.1.2. Polymorphic malware.</p> <p>4.2. Ingeniería inversa.</p> <p>4.2.1. Análisis de Inyecciones de código.</p> <p>4.2.2. Análisis de protocolos de comunicación.</p> <p>4.3. Métodos de machine learning para el análisis de malware.</p>
---	-------------------------------	---

## 7. Actividades de aprendizaje de los temas

1. Introducción al análisis de malware.	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Analiza y comprende las amenazas de malware en el contexto actual de la ciberseguridad.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"><li>• Capacidad de análisis y síntesis.</li><li>• Capacidad de organizar y planificar.</li><li>• Habilidad para buscar y analizar información proveniente de fuentes diversas.</li><li>• Solución de problemas.</li><li>• Toma de decisiones.</li><li>• Trabajo en equipo.</li><li>• Capacidad de aplicar los conocimientos.</li><li>• Habilidades de investigación.</li><li>• Capacidad de generar nuevas ideas</li><li>• Liderazgo.</li><li>• Habilidad para trabajar en forma autónoma.</li><li>• Búsqueda del logro.</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></ul>	<ul style="list-style-type: none"><li>• Recopilar información sobre la definición y la clasificación de diferentes tipos de malware, presentar los hallazgos y discutir en plenaria.</li><li>• Elaborar una línea del tiempo sobre la evolución del malware, desde sus inicios hasta las amenazas actuales.</li><li>• Organizar un debate o mesa redonda donde se discuta el panorama de las amenazas y las respuestas de seguridad.</li><li>• Analizar casos de estudio de malwares conocidos y las motivaciones detrás de su creación.</li></ul>



<ul style="list-style-type: none"><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>	
<b>2. Métodos de análisis estático.</b>	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Aplica metodologías avanzadas y herramientas especializadas para realizar un análisis estático exhaustivo de muestras de malware.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"><li>● Capacidad de análisis y síntesis.</li><li>● Capacidad de organizar y planificar.</li><li>● Habilidad para buscar y analizar información proveniente de fuentes diversas.</li><li>● Solución de problemas.</li><li>● Toma de decisiones.</li><li>● Trabajo en equipo.</li><li>● Capacidad de aplicar los conocimientos.</li><li>● Habilidades de investigación.</li><li>● Capacidad de generar nuevas ideas</li><li>● Liderazgo.</li><li>● Habilidad para trabajar en forma autónoma.</li><li>● Búsqueda del logro.</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></ul>	<ul style="list-style-type: none"><li>● Diseñar un flujo de trabajo para realizar un análisis estático de una muestra de malware.</li><li>● Identificar las similitudes y diferencias de las firmas y hashes de una muestra de malware.</li><li>● Analizar cadenas de texto para identificar posibles indicadores de compromiso o información útil para el análisis de comportamiento.</li><li>● Examinar archivos de configuración asociados a malware para identificar configuraciones maliciosas o actividad sospechosa.</li></ul>



<ul style="list-style-type: none"><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>	
<b>3. Métodos de análisis dinámico.</b>	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Aplica metodologías avanzadas y herramientas especializadas para realizar un análisis dinámico exhaustivo de muestras de malware.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"><li>• Capacidad de análisis y síntesis.</li><li>• Capacidad de organizar y planificar.</li><li>• Habilidad para buscar y analizar información proveniente de fuentes diversas</li><li>• Solución de problemas.</li><li>• Toma de decisiones.</li><li>• Trabajo en equipo.</li><li>• Capacidad de aplicar los conocimientos.</li><li>• Habilidades de investigación.</li><li>• Capacidad de generar nuevas ideas</li><li>• Liderazgo.</li><li>• Habilidad para trabajar en forma autónoma.</li><li>• Búsqueda del logro.</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>• Diseñar un flujo de trabajo para realizar un análisis dinámico de una muestra de malware.</li><li>• Realizar una simulación practica de un entorno de sandboxing utilizando herramientas específicas.</li><li>• Identificar conexiones sospechosas, trafico cifrado y comunicaciones con servidores.</li><li>• Identificar actividades anómalas y generar alertas basadas en comportamientos sospechosos.</li><li>• Analizar artefactos forenses para comprender el impacto del malware en el sistema.</li></ul>



4. Métodos avanzados de análisis.	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Analiza y contrarresta técnicas avanzadas de evasión y manipulación de malware mediante métodos de ingeniería inversa y análisis avanzado.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"><li>• Capacidad de análisis y síntesis.</li><li>• Capacidad de organizar y planificar.</li><li>• Habilidad para buscar y analizar información proveniente de fuentes diversas.</li><li>• Solución de problemas.</li><li>• Toma de decisiones.</li><li>• Trabajo en equipo.</li><li>• Capacidad de aplicar los conocimientos.</li><li>• Habilidades de investigación.</li><li>• Capacidad de generar nuevas ideas</li><li>• Liderazgo.</li><li>• Habilidad para trabajar en forma autónoma.</li><li>• Búsqueda del logro.</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>• Recopilar información sobre diferentes técnicas de evasión utilizadas por el malware.</li><li>• Discutir en plenaria las técnicas de evasión y su efecto en la detección y análisis de amenazas.</li><li>• Identificar características clave del malware y comprender su funcionalidad.</li><li>• Analizar cómo se puede utilizar algoritmos de aprendizaje automático para identificar patrones de comportamiento malicioso.</li><li>• Diseñar técnicas de defensa contra técnicas de evasión.</li></ul>





## 8. Práctica(s)

- Analizar muestras de malware en entornos controlados, para identificar las características de cada muestra.
- Simular un ataque controlado para comprender los diferentes pasos de un ataque.
- Utilizar herramientas de análisis de Malware para comparar firmas digitales y hashes de archivos sospechosos con bases de datos conocidas de malware.
- Utilizar herramientas de desensamblado para traducir el código máquina de un malware a lenguaje ensamblador.
- Configurar una herramienta de Sandboxing en un entorno de laboratorio.
- Utilizar herramientas de captura de paquetes para analizar el tráfico de red generado por malware.
- Realizar procedimientos de análisis forense para recuperar artefactos de un sistema comprometido.
- Utilizar máquinas virtuales comprometidas con Rootkits para análisis forense.
- Utilizar herramientas de análisis estático y dinámico para analizar muestras de malware polimórfico.

## 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

Las técnicas, herramientas y/o instrumentos sugeridos que permiten obtener el producto del desarrollo de las actividades de aprendizaje: cuestionarios, portafolios, mapas conceptuales, resúmenes, infografías, estudio de casos, debates, ensayos, presentaciones, exposiciones en clase, videos, reportes de prácticas, proyecto de asignatura o integrador.

Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de valoración, guías de observación, coevaluación y autoevaluación.

## 11. Fuentes de Información

1. ¿Cuáles son los diferentes tipos de malware? (2022, May 6). Latam.kaspersky.com. <https://latam.kaspersky.com/resource-center/threats/types-of-malware>
2. ciberinseguro. (2023, May 11). Análisis de malware: técnicas avanzadas de detección y respuesta. CiberInseguro. <https://ciberinseguro.com/analisis-de-malware-tecnicas-avanzadas-de-deteccion-y-respuesta/>
3. Fernando, M. (2019). Evolución del Malware. Recuperado abril 17, 2024, de <https://eventos.ufps.edu.co/CIINATIC2019/memorias/Evoluci%C3%B3n%20del%20Malware.pdf>
4. Coronel Ayala, F. M., & López Sevilla, G. M. (2023). Mapeo del panorama actual de la ciberseguridad en la era moderna digital. RECIMUNDO, 7(2), 441-452. [https://doi.org/10.26820/recimundo/7.\(2\).jun.2023.441-452](https://doi.org/10.26820/recimundo/7.(2).jun.2023.441-452)
5. Rubiano, J. E. R. (2023). Ciberataques: análisis de Ransomware y métodos de protección [Universitat Oberta de Catalunya]. <https://openaccess.uoc.edu/bitstream/10609/148181/1/jromerorubTFM0623memoria.pdf>
6. Rubiano, J. E. R. (2023). Ciberataques: análisis de Ransomware y métodos de protección [Universitat Oberta de Catalunya]. <https://openaccess.uoc.edu/bitstream/10609/148181/1/jromerorubTFM0623memoria.pdf>
7. Páez, E. A. (2022). Análisis dinámico de Malware 2020 [Escuela Técnica Superior de Ingeniería Universidad de Sevilla]. <https://biblus.us.es/bibing/proyectos/abreproy/94086/fichero/TFG-4086+Aroca+P%C3%A1ez.pdf>
8. Javier Ros Raposo, F. (2023). Análisis de la capacidad de detección e identificación de Malware basado en tráfico de red mediante IoC [Escuela Técnica Superior de Ingeniería Universidad de Sevilla]. [https://idus.us.es/bitstream/handle/11441/143867/TFG4437\\_Ros%20Raposo.pdf?sequence=1&isAllowed=y](https://idus.us.es/bitstream/handle/11441/143867/TFG4437_Ros%20Raposo.pdf?sequence=1&isAllowed=y)
9. Rea, C. P. P. (2023). Análisis de los datos enviados por una sandbox para monitorear malware en tiempo real. Pontificia Universidad Católica de Ecuador. <https://repositorio.puce.edu.ec/server/api/core/bitstreams/b2a93d80-514f-42ee-a924-997976a5e4d4/content>
10. García, G. P. (2023). Análisis de técnicas de evasión usadas por malware para su orquestación en entornos aislados de ejecución [Universitat Politècnica de València]. <https://riunet.upv.es/handle/10251/198113>
11. Enríquez, E. G. V. (2022). Revisión de algoritmos de detección de malware ofuscados basados en machine learning. <https://revistas.ulima.edu.pe/>, 132–136.
12. Castro-Salaverry, C. R., Bravo-Huivín, E. K., & Cieza-Mostacero, S. E. (2022). Revisión Sistemática de la Literatura: Machine Learning para la Detección de Ransomware en Dispositivos Móviles. <https://www.risti.xyz/index.php/es/>, 54(11/2022), 341–353.



13. Fortinet. (2024). FCF - Introduction to the Threat Landscape 2.0 Self-Paced.  
<https://training.fortinet.com>
14. Cisco – Networking Academy. (2024). Defensa de la red.  
<https://skillsforall.com/es/course/network-defense?courseLang=es-XL>
15. Cisco. (2017). Ransomware: Defendiendo el perímetro del sector público.  
[https://www.cisco.com/c/dam/global/es\\_mx/solutions/industries/cisco\\_ransomware\\_defendiendo\\_perimetro\\_de\\_ps-10.pdf](https://www.cisco.com/c/dam/global/es_mx/solutions/industries/cisco_ransomware_defendiendo_perimetro_de_ps-10.pdf)
16. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI