Campus de la UNA
SAN LORENZO-PARAGUAY

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

RESOLUCIÓN Nº 0179/2026

POR LA CUAL SE APRUEBA Y SE HABILITA EL CURSO DE CIBERSEGURIDAD AVANZADA DEL ÁREA DE CIBERSEGURIDAD, PARA ABRIL 2026

03 de marzo de 2026

VISTO Y CONSIDERANDO: El Memorando DGCITIC/007/2026, del Director, Lic. Juan Fernando Duré, de la Dirección de Gestión del Centro de Innovación en TIC de la FP-UNA, en el cual solicita la aprobación y la habilitación del Curso de Ciberseguridad Avanzada del Área de Ciberseguridad, para abril 2026, presentado por el Prof. Lic. Chrystian David Ruiz Diaz Centurión.

Que la propuesta cubre una introducción fundamental al mundo de la ciberseguridad y la seguridad de redes, orientado a estudiantes que deseen iniciarse en la protección de sistemas y datos digitales. A lo largo del curso, se proporciona una visión clara de los principios esenciales de la ciberseguridad, abordando desde los tipos de amenazas y ataques más comunes hasta las estrategias básicas para mitigar riesgos en entornos digitales.

El curso está estructurado en base a 40 horas (8 semanas de duración) a ser desarrolladas en la modalidad virtual. La fecha de inicio:**06/04/2026**, la fecha de finalización: **30/05/2026**

Se estima dar apertura con una convocatoria de 10 (diez) matriculados como mínimo y 50 matriculados como máximo

El Estatuto de la Universidad Nacional de Asunción.

POR TANTO: en uso de sus facultades y atribuciones legales,

LA DECANA DE LA FACULTAD POLITÉCNICA
RESUELVE:

Art. 1º Aprobar el Programa del Curso de Ciberseguridad Avanzada del Área de Ciberseguridad, para abril 2026, detallado en el ANEXO de la presente Resolución.

Art. 2º Habilitar el Curso de Ciberseguridad Avanzada del Área de Ciberseguridad, para abril 2026, ofrecido por la FP-UNA.

Art. 3° Comunicar, copiar y archivar.

Prof. Abg. Joel Arsenio Benítez Santacruz
Secretario de la Facultad

Prof. Ing. Silvia Teresa Leiva León, MSc.
Decana

Campus de la UNA
SAN LORENZO-PARAGUAY

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

ANEXO RESOLUCIÓN Nº 0179/2026

Universidad Nacional de Asunción

Facultad Politécnica

Centro de Innovación en TIC

Proyecto Curso de corta duración

Título: Curso de Ciberseguridad Avanzada del Área de Ciberseguridad

Modalidad: *Virtual*

Docente
Prof. Lic. Chrystian David Ruiz Diaz Centurión

Sede Central, San Lorenzo

Marzo, 2026

ANEXO RESOLUCIÓN Nº 0179/2026

Ciberseguridad Avanzada

1	Título	*Ciberseguridad avanzada*
2	Código	-
3	Año propuesto	*2025*
4	Semestre propuesto	*Primero*
5	Departamento	*Centro de Innovación TIC (FP-UNA)*
6	Año Objetivo/Carrera	*Avanzado / Diplomado de Ciberseguridad*
7	Formato de clase (tipo)	*Clases interactivas, sesiones prácticas, laboratorios, etc.*

Horario y Lugar

1	Días	*Martes*
2	Horario	*de 19:00 a 21:30hs*
3	Ubicación	*Online - Síncronas*
4	Días	*Jueves*
5	Horario	*de 19:00 a 21:30hs*
6	Ubicación	*Online - Asíncronas*

Información del instructor/a

1	Nombre	*Prof. Lic. Chrystian David Ruiz Diaz Centurión*
2	Oficina (si aplica)	-
3	Contacto (correo)	*Chrystiandavid2000@pol.una.py*
4	Contacto (teléfono)	*(0982) 508.890*

□ Horario de oficina
Estoy disponible para contactar en cualquier momento por WhatsApp o correo electrónico. Las llamadas pueden coordinarse previamente según disponibilidad.

□ Prerrequisitos
Introducción a la Ciberseguridad a la seguridad de las redes - Seguridad de redes y en la Nube

□ Descripción del curso
Este curso de Ciberseguridad Avanzada está diseñado para profesionales que buscan elevar sus competencias más allá de los fundamentos, sumergiéndose en las tácticas, técnicas y procedimientos (TTPs - *Tactics, Techniques and Procedures*) utilizados tanto por atacantes de alto nivel (APTs - *Advanced Persistent Threat*) como por equipos de defensa de élite. El programa adopta una metodología de "Aprender haciendo" (*Learning by Doing*), centrada en simulaciones de ciberguerra y defensa activa.
El plan de estudios trasciende la teoría convencional para enfocarse en escenarios de compromiso realistas, utilizando la metodología de Aprendizaje Basado en Problemas (ABP). A través del uso de infraestructura dedicada, incluyendo servidores sqli-labs para explotación de bases de datos y plataformas CTF - *Capture The Flag* para retos gamificados de ciberseguridad, los participantes desarrollarán habilidades ofensivas (*Red Team*) y defensivas (*Blue Team*) en entornos controlados. Los contenidos están eminentemente enfocados en la práctica, proporcionando un contexto verídico sobre amenazas inminentes y situaciones del mundo real.
El curso integra profundamente las fronteras tecnológicas actuales, abordando la seguridad ofensiva en modelos de Inteligencia Artificial (*Adversarial AI*), vulnerabilidades en Internet de las Cosas (IoT) y la protección de datos mediante criptografía aplicada. Todo ello se enmarca en una rigurosa comprensión de la gestión de incidentes, forense digital avanzado y el cumplimiento de marcos legales y éticos internacionales, preparando al estudiante para la defensa proactiva y la gestión de crisis de seguridad de alto impacto.

Este curso ofrece una introducción fundamental al mundo de la ciberseguridad y la seguridad de redes, orientado a estudiantes que deseen iniciarse en la protección de sistemas y datos digitales. A lo largo del curso, se proporciona una visión clara de los principios esenciales de la ciberseguridad, abordando desde los tipos de amenazas y ataques más comunes hasta las estrategias básicas para mitigar riesgos en entornos digitales.
El plan de estudios combina teoría y práctica, permitiendo que los participantes aprendan mediante ejercicios aplicados y sesiones de laboratorio con herramientas estándar del sector. Entre los contenidos clave se incluyen: fundamentos de ciberseguridad, protocolos de seguridad, análisis de vulnerabilidades, gestión de incidentes, y buenas prácticas para proteger redes e infraestructuras tecnológicas.
El curso también incorpora temas de actualidad, como la seguridad en la nube, la protección en dispositivos del Internet de las Cosas (IoT) y el uso de inteligencia artificial en la ciberdefensa, manteniéndose alineado con las normas y tendencias del sector tecnológico.
Además del enfoque técnico, se pone énfasis en los aspectos éticos y legales que rigen la ciberseguridad, incluyendo el hacking ético, la privacidad digital y los marcos normativos nacionales e internacionales. Esto fomenta una comprensión integral del campo, destacando la importancia de la responsabilidad profesional.
Al finalizar, los estudiantes habrán adquirido las competencias básicas para identificar y prevenir amenazas cibernéticas, así como una base sólida para continuar su formación en áreas más avanzadas de la ciberseguridad.

□ Objetivo del curso
Objetivo General:

- Desarrollar en los estudiantes competencias técnicas avanzadas para ejecutar simulaciones de ataques sofisticados y diseñar estrategias de defensa resilientes en arquitecturas híbridas y modernas, utilizando laboratorios especializados para validar la capacidad de protección de activos críticos frente a amenazas emergentes.

Objetivos Específicos:

- Deconstruir la anatomía de ataques complejos (APTs) y campañas de malware "*Fileless*", utilizando inteligencia de amenazas (CTI - *Cyber Threat Intelligence*) y el marco MITRE ATT&CK para anticipar vectores de intrusión.
- Diseñar e implementar arquitecturas de seguridad basadas en el modelo "Zero Trust" y técnicas de Inspección Profunda de Paquetes (DPI), superando las limitaciones de la defensa perimetral tradicional.
- Dominar las técnicas de compromiso y aseguramiento de identidades corporativas, enfocándose en la explotación de Active Directory, protocolos Kerberos y gestión de accesos en la nube (IAM - *Identity and Access Management*).
- Ejecutar pruebas de penetración avanzadas en bases de datos y aplicaciones web utilizando servidores sqli-labs, y validar hallazgos mediante retos técnicos en la plataforma CTFd.
- Evaluar la superficie de ataque en tecnologías emergentes, identificando vulnerabilidades en sistemas de Inteligencia Artificial (LLMs), dispositivos IoT y entornos de contenedore.
- Aplicar metodologías de respuesta a incidentes y forense digital en memoria (RAM), integrando aspectos legales y éticos para la gestión efectiva de crisis de ciberseguridad.

Al finalizar con éxito este curso los estudiantes serán capaces de:

1. Analizar y perfilar técnicamente a actores de amenazas avanzadas (APTs), identificando Indicadores de Compromiso (IoCs) y aplicando contramedidas proactivas basadas en inteligencia.
2. Configurar y auditar sistemas de detección de intrusos y arquitecturas de red seguras, aplicando principios de micro-segmentación y evasión de técnicas de ocultamiento de tráfico
3. Ejecutar y mitigar ataques de identidad modernos, tales como Kerberoasting, Pass-the-Hash y escalada de privilegios en entornos de directorio activo y nube pública.
4. Realizar explotaciones técnicas de inyección SQL avanzada y vulnerabilidades web en entornos de laboratorio dedicados (sqli-labs), demostrando el impacto real de la falta de saneamiento de datos.
5. Detectar y neutralizar vectores de ataque en nuevas tecnologías, incluyendo la manipulación de modelos de IA (Prompt Injection) y la intercepción de protocolos industriales/IoT.
6. Conocer procesos de respuesta a incidentes, desde la adquisición de evidencia forense volátil hasta la toma de decisiones estratégicas y legales en escenarios de crisis simulados (War Room).

□ Política de calificación

□ Calificación absoluta □ Calificación relativa

Criterios de Evaluación:

La calificación final del curso se determinará mediante la evaluación de los siguientes componentes:

Actividad	Porcentaje
Participación y Asistencia: ❖ Asistencia regular a las sesiones. ❖ Participación activa en debates y actividades en clase.	10%

Participación en Foros: ❖ Contribuciones significativas en foros en línea y debates relacionados con los temas del curso.	10%
Trabajos Prácticos y Laboratorios: ❖ Entrega puntual y completa de ejercicios prácticos. ❖ Demostración de habilidades adquiridas en sesiones de laboratorio.	35%
Proyecto Final: ❖ Desarrollo y presentación de un proyecto integrador que aplique los conocimientos adquiridos durante el curso.	45%

□ Libros de texto y otros materiales necesarios

- J. M. STEWART Y D. KINSEY(2020), Network security, firewalls, and VPNs. Jones & Bartlett Learning.
- C. PANEK (2019), Security fundamentals. John Wiley & Sons.
- Open Worldwide Application Security Project. (s. f.). OWASP Foundation | Open Source Foundation for Application Security. Recuperado el 9 de septiembre de 2025, de https://owasp.org/
- R RADVANOVSKY, J BRODSKY (2013). SCADA/Control Systems Security. CRC Press,
- BUENDIA, J. F. (2013). Seguridad informática. España: McGraw-Hill.
- ESCRIVA, G. R. (2013). Seguridad Informática. España: Macmillan Iberia SA .
- GMV SECTORES Ciberseguridad. (18 de 03 de 0221). Obtenido de GMV SECTORES Ciberseguridad
- STEWART, J. M. (2013). Network Security, Firewalls and VPNs. Jones & Bartlett Publishers.
- VIEITES, Á. G. (2014). Gestión de Incidentes de Seguridad Informática. . RA-MA Editori

Materiales

- Acceso a internet
- Computadora
- Software para virtualización VMware (gratis)
- Kali Linux
- Herramientas de pentest (open source)

□ Tarea(s) y examen(es)

❖ Debates y participación para fomentar para el aprendizaje colaborativo y el desarrollo del pensamiento crítico.

❖ Cuestionarios para medir la comprensión de conceptos teóricos y prácticos

❖ Videos interactivos para evaluación y laboratorios.

❖ Prácticas de Laboratorio para que los alumnos adquieran habilidades técnicas y experimenten con herramientas y técnicas de ciberseguridad en un entorno controlado.

Trabajo Practico Final que integren y apliquen los conocimientos adquiridos a lo largo del curso en un proyecto significativo.

□ Actividades del curso

1) Clases Interactivas: Sesiones dinámicas que incorporan preguntas y respuestas en tiempo real, encuestas interactivas y discusiones abiertas para promover el pensamiento crítico y la participación activa.
2) Sesiones de Debate: Análisis y discusión de estudios de caso reales relacionados con incidentes de ciberseguridad, donde los estudiantes evalúan situaciones, identifican amenazas y proponen soluciones.
3) Prácticas de Laboratorio: Ejercicios prácticos que incluyen la configuración de sistemas seguros, análisis de vulnerabilidades, implementación de protocolos de seguridad y resolución de desafíos técnicos en entornos controlados.
4) Gamificación y Retos CTF (Capture The Flag): Implementación de dinámicas competitivas de ciberguerra mediante una plataforma CTFd propia y servidores de entrenamiento (sqli-labs). Los estudiantes validan sus habilidades resolviendo desafíos técnicos progresivos —desde la explotación de inyecciones SQL hasta el análisis forense de memoria— en un entorno de "War Games" con puntuación y ranking en tiempo real, fomentando la excelencia técnica y la capacidad de respuesta bajo presión.
5) Proyectos en Grupo: Desarrollo colaborativo de proyectos que abordan problemas específicos de ciberseguridad, incluyendo talleres de planificación, ejecución y sesiones de revisión por pares para evaluar el progreso y la calidad del trabajo.

Cronograma del curso

Semana	Tema	Tipo de clases	Materiales
1	Ciberguerra: APTs, Zero-Days y Estrategias de Ciberinteligencia	Análisis de Amenazas / CTF Challenge	CTF - KALI Linux
2	Defensa de Red, Evasión de DPI y Arquitecturas Zero Trust	Laboratorio / Análisis de Paquetes	CTF – IPS – Tcpdump - Wireshark
3	Compromiso de Identidad: Active Directory y Kerberos	Hacking Ético / Simulación	CTF - BloodHound
4	Explotación de Infraestructura Cloud y Contenedores	Auditoría / Análisis de Caso	CTF - Prowler
5	Data Exfiltration & Database Warfare (Integración sqli-labs)	Laboratorio de Hacking Web / Gestión de Datos	CTF – sqli-labs - SQLMap
6	Infraestructuras Críticas: Hacking IoT, SCADA y Redes Industriales (OT)	Laboratorio / Investigación	CTF – Mosquitto – Simulador de protocolos
7	Seguridad en Inteligencia Artificial y Adversarial AI	Laboratorio "Red Team" / Debate	CTF - Gandalf
8	Forense Digital Avanzado y Defensa de proyecto integrador Final	Evaluación Práctica	VMware

□ Contenidos del curso

Descripción Semanal Detallada – Curso: Introducción a la ciberseguridad y a la seguridad de redes
Semana 1: Ciberguerra: APTs, Zero-Days y Estrategias de Ciberinteligencia
Tipo de clase: Análisis de Amenazas / CTF Challenge
Objetivo: Deconstruir las tácticas de las Amenazas Persistentes Avanzadas (APT) y utilizar la plataforma CTF para identificar indicadores de compromiso en escenarios simulados.

Actividades de clase detalladas:

Clase 1 – Martes - Fundamentos de Ciberguerra y CTI

1. **Panorama de Amenazas Avanzadas (APTs) y Actores Estatales.**

- Descripción: Análisis técnico de la estructura de una Amenaza Persistente Avanzada. Diferenciación entre cibercrimen oportunista y operaciones patrocinadas por estados (State-Sponsored). Estudio de casos: SolarWinds y Lazarus Group.
- **Metodología**: Clase magistral con disección de reportes de inteligencia reales (Mandiant/CrowdStrike).
- **Duración**: 1 hora.

2. **Frameworks de Ciberdefensa: The Cyber Kill Chain & MITRE ATT&CK.**

- Descripción: Profundización en la matriz MITRE ATT&CK (Enterprise). Cómo mapear las TTPs (Tácticas, Técnicas y Procedimientos) de un adversario para predecir sus siguientes movimientos. Diferencia entre IoC (Indicador de Compromiso) e IoA (Indicador de Ataque).
- **Metodología**: Taller interactivo utilizando "MITRE ATT&CK Navigator" para visualizar el perfil de un atacante.
- **Duración**: 1 hora.

3. **Setup del Entorno de Inteligencia y Plataforma CTF.**

- **Descripción**: Despliegue y configuración de las herramientas de análisis. Introducción a la plataforma CTFd propia del curso, donde se registrarán los avances y "flags".
- Metodología: Laboratorio guiado de registro y configuración de acceso a los servidores del curso.
- Duración: 0.5 hora.

Funcionamiento de la clase:

Interacción: Análisis crítico de noticias recientes de brechas de seguridad para clasificarlas según la matriz MITRE.

Práctica: Verificación de acceso al servidor CTFd.

Recursos: Los accesos a la infraestructura privada (CTFd) se entregarán vía credenciales seguras. Se requerirá la instalación de:

- Máquina Virtual (Kali Linux / Windows 7-10 "Victim").
- Sysinternals Suite (para monitoreo avanzado en Windows).
- Acceso al MITRE ATT&CK Navigator (Web).

Nota Ética: Todas las técnicas de reconocimiento de amenazas se enseñan para la defensa proactiva. El uso de información de inteligencia para atribución o contraataque fuera del marco legal está prohibido.

Clase 2 - Jueves (Vectores de Ataque y Reto de Inteligencia)

4. **Vectores de Ataque Avanzados:** "*Living off the Land*" (LotL) y *Fileless Malware*.

Descripción: Demostración técnica de cómo los atacantes evaden los antivirus tradicionales utilizando herramientas nativas del sistema (PowerShell, WMI, Certutil) para ejecutar código en memoria sin tocar el disco.

Metodología: Demostración en vivo ("Live Fire Demo") de ejecución de un script ofuscado y su detección mediante Sysmon.

Duración: 1 hora.

5. **Ejercicio Práctico (CTF Challenge)**: "*The Intelligence Hunter*".

Descripción: Los estudiantes reciben un "Informe de Incidente" crudo (ficticio o sanitizado) que contiene logs, correos electrónicos y hashes. Deben actuar como analistas de CTI para extraer la inteligencia clave.

Reto: Encontrar las "Flags" ocultas en el informe (ej. la IP del C2, el nombre del malware, el CVE explotado) e ingresarlas en la plataforma CTFd.

Metodología: Trabajo individual o en parejas contra reloj en la plataforma gamificada.

Duración: 1.5 horas.

Materiales:
Framework: Matriz MITRE ATT&CK y Navigator.
Plataforma: Servidor CTFd con el reto .
Software: Sysinternals Suite (Sysmon), PowerShell ISE.
Lectura Técnica: Reporte "M-Trends" (Mandiant) o "Global Threat Report" (CrowdStrike) del año en curso.
Funcionamiento de la clase:
Interacción: Se fomentará la participación activa de los estudiantes a través de preguntas, debates y trabajos en grupo.
Práctica: Descarga e instalación de las diversas herramientas que serán utilizada en los cursos.
Recursos: Todos los materiales y herramientas necesarios estarán disponibles en la plataforma educativa, archivos grandes con sus respectivas referencias para su descarga, asegurando el acceso equitativo para todos los participantes. La primera clase se mencionará lo siguiente:

- Software para virtualización (VMware o equivalente)
- Software para pentest (Kali Linux)

Interacción: "War Room" simulado. El instructor actúa como CISO solicitando actualizaciones de inteligencia mientras los alumnos resuelven el reto en el CTFd.
Práctica: Los estudiantes aplicarán la teoría de la Clase 1 para filtrar el ruido y encontrar la amenaza real en los datos proporcionados.

Semana 2: Defensa de Red, Evasión de DPI y Arquitecturas Zero Trust
Tipo de clase: Clase interactiva/práctica
Objetivo: Entender la inspección profunda de paquetes (DPI) y detectar tráfico anómalo, validando los hallazgos mediante retos de análisis forense de red.
Actividades:

- Laboratorio práctico: Análisis de un archivo PCAP corrupto. Los estudiantes deben extraer la carga útil (payload) del atacante y la IP de origen, subiendo el hash del archivo extraído como "Flag" al CTFd.
- Análisis de evasión: Estudio de técnicas de tunelización (DNS/ICMP) para exfiltrar datos.
- Debate: Arquitecturas "Zero Trust" y micro-segmentación vs. VPN tradicional.

Materiales:

- Plataforma: Servidor CTFd (Reto de Network Forensics).
- Herramienta: Wireshark.

Guía: NIST SP 800-207 "Zero Trust Architecture".

Semana 3: Compromiso de Identidad: Active Directory y Kerberos
Tipo de clase: Hacking Ético / Simulación
Objetivo: Explotar la infraestructura de identidad, entendiendo cómo los atacantes abusan de Kerberos y las configuraciones de directorio.
Actividades:

- Demostración técnica: Uso de BloodHound para visualizar rutas de ataque ("Attack Paths") hacia el Domain Admin.
- Simulación: Ejecución conceptual de "Kerberoasting". El hash extraído (simulado) debe ser crackeado y la contraseña resultante ingresada en CTFd para validar el módulo.
- Debate: Vulnerabilidades en MFA y ataques de identidad híbrida.

Materiales:

- Libro: "Network Security, Firewalls and VPNs" (Stewart, J. M., 2013) – Capítulo 4: Firewalls y su papel en la seguridad de redes.
- Guías de laboratorio y software de simulación de redes disponibles en la plataforma educativa

- Herramientas: BloodHound CE, Rubeus (simulado).
- Plataforma: CTFd (Reto de Cracking de Hashes NTLM).

Semana 4: Explotación de Infraestructura Cloud y Contenedores
Tipo de clase: Auditoría / Análisis de Caso
Objetivo: Identificar vulnerabilidades críticas en entornos de nube pública (AWS/Azure) y contenedores, enfocándose en IAM y secretos expuestos.
Actividades:

- Laboratorio práctico: Auditoría de un entorno de contenedores. Encontrar una "Service Account Token" expuesta y usarla para validar el acceso en el CTFd.
- Análisis de caso: Brecha de Capital One y vulnerabilidades SSRF.
- Debate: Riesgos de "Infraestructura como Código" (IaC) y secretos en repositorios.

Materiales:

- Estándar: CIS Benchmarks para Kubernetes.
- Plataforma: CTFd (Reto de Cloud Security / Docker Escape conceptual).

Recurso: OWASP Cloud-Native Top 10.

Semana 5: Data Exfiltration & Database Warfare
Tipo de clase: Laboratorio de Hacking Web / Gestión de Datos
Objetivo: Conocer técnicas avanzadas de inyección SQL para exfiltrar bases de datos corporativas y entender la importancia del saneamiento de inputs y cifrado.
Actividades:

- Laboratorio práctico: Despliegue de ataques contra el servidor sqli-labs.
  * Reto 1: Bypass de autenticación (Lesson 1-4).
  * Reto 2: Explotación de "Blind SQL Injection" para enumerar la base de datos sin ver errores en pantalla (Lesson 8-10).
  * Objetivo: Extraer la tabla de usuarios y subir el hash del administrador al CTFd.
- Debate: Cifrado de datos en reposo (TDE) y cómo mitiga el impacto de una inyección SQL exitosa.

Materiales:

- Infraestructura: Servidor sqli-labs propio (accesible por los alumnos).
- Herramientas: Burp Suite Community, SQLMap (opcional, se sugiere manual primero).
- Plataforma: CTFd (Flags vinculadas a las tablas de sqli-labs).

Semana 6: Infraestructuras Críticas: Hacking IoT, SCADA y Redes Industriales (OT)
Tipo de clase: Laboratorio Híbrido (OT/IoT) / Investigación
Objetivo: Evaluar la superficie de ataque en Infraestructuras Críticas (SCADA) y dispositivos conectados, explotando la falta de autenticación en protocolos industriales y vulnerabilidades en firmware.
Actividades:

- Laboratorio práctico (SCADA): Ataque al protocolo Modbus TCP.
- Análisis de Firmware (IoT): Uso de la herramienta Binwalk para realizar ingeniería inversa sobre una imagen de actualización de un dispositivo.
- Debate: La convergencia IT/OT y el mito del "Air Gap" (aislamiento físico). Análisis de cómo ataques como Stuxnet o Triton saltaron las barreras físicas.

Materiales:

- Libro: "Seguridad informática" (Buendía, J. F., 2013) – Capítulo 7: Seguridad en el desarrollo de software.
- Herramienta OWASP
- Herramientas de análisis estático y dinámico de código disponibles en el laboratorio.

Semana 7: Seguridad en Inteligencia Artificial y Adversarial AI
Tipo de clase: Laboratorio "Red Team" / Debate
Objetivo: Analizar vulnerabilidades en Modelos de Lenguaje (LLMs) y desarrollar estrategias contra la manipulación de IA.
Actividades:

- Laboratorio práctico: Ejercicio de "Prompt Injection". Lograr que un Chatbot (simulado o externo) revele una contraseña oculta en su "System Prompt" y entregarla en CTFd.
- Análisis: Detección de Deepfakes y validación de integridad.
- Debate: Automatización de ciberataques mediante IA y el futuro de la defensa.

Materiales:

- OWASP Top 10 for LLM Applications.
- Plataforma: CTFd (Reto de AI Jailbreak).
- NIST AI 100-2 "Adversarial Machine Learning".

Semana 8: Forense Digital Avanzado y CTF Final (War Room)
Tipo de clase: Evaluación Práctica / Forense
Objetivo: Ejecutar una respuesta a incidentes completa y demostrar las habilidades adquiridas mediante una competencia final de "Capture The Flag".
Actividades:

- Laboratorio práctico Forense Digital
- Defensa final del proyecto integrador

Materiales:

- Herramienta: Volatility Workbench.
- Diversas herramientas desarrolladas a lo largo del curso

Acceso a Materiales:
Todos los recursos del curso estarán centralizados en la plataforma educativa, facilitando un acceso organizado y eficiente. Los materiales disponibles incluirán:

- Lecturas Asignadas: Enlaces directos a capítulos específicos de los libros de texto requeridos, permitiendo una consulta rápida y focalizada.
- Guías Prácticas: Documentos detallados que complementan las lecciones teóricas, diseñados para reforzar y aplicar los conceptos aprendidos.
- Herramientas Recomendadas: Acceso a software y aplicaciones esenciales para las actividades prácticas del curso, con instrucciones claras para su instalación y uso.

Recursos Adicionales: Enlaces a sitios web de acceso libre, artículos académicos y otros materiales complementarios que enriquecen el aprendizaje y ofrecen perspectivas adicionales.