www.uneweb.edu.ve

DIPLOMADO EN

CIBERSEGURIDAD

DESDE CERO HASTA AVANZADO

12 MÓDULOS · 240 HORAS ACADÉMICAS · TEÓRICO-PRÁCTICO

12 Módulos	240 Horas Académicas	60 Prácticas	Desde Cero

Programa de Formación Especializada en Ciberseguridad

Kali Linux · Wireshark · Burp Suite · Wazuh · Volatility · AWS · Docker · IA

Descripción General del Diplomado

Este Diplomado en Ciberseguridad ha sido diseñado para llevar al participante desde los conceptos fundamentales hasta las técnicas más avanzadas del sector. Con una estructura progresiva de 12 módulos y 240 horas académicas totales, cada etapa construye sobre la anterior, cubriendo pentesting, blue team, forense digital, cloud, IoT/SCADA, Inteligencia Artificial aplicada a la seguridad, y gobierno-riesgo-cumplimiento (GRC), garantizando una formación sólida, práctica y alineada con los estándares internacionales de la industria (NIST, OWASP, MITRE ATT&CK, ISO 27001).

Modalidad	**Teórico-Práctica (50% teoría / 50% práctica)**
Duración total	**240 horas académicas distribuidas en 12 módulos**
Prácticas	**5 ejercicios prácticos por módulo (60 prácticas totales)**
Nivel de entrada	**No se requieren conocimientos previos (Nivel 1)**
Certificación	**Diplomado con acreditación de horas**
Herramientas	**Kali Linux, Wireshark, Burp Suite, Wazuh, Volatility, AWS, Docker, IA**

Estructura Curricular

Niv.	Título del Nivel	Horas	Prácticas
1	Fundamentos de la Ciberseguridad	20 h	5
2	Seguridad en Sistemas Operativos y Redes	20 h	5
3	Análisis de Vulnerabilidades y Pentesting Básico	20 h	5
4	Respuesta a Incidentes y Seguridad Ofensiva	20 h	5
5	Pentesting de Aplicaciones Web Avanzado	20 h	5
6	Operaciones de Seguridad y Caza de Amenazas (Blue Team)	20 h	5
7	Análisis Forense Digital Avanzado	20 h	5
8	Seguridad en la Nube (Cloud) y Contenedores	20 h	5
9	Seguridad en IoT, SCADA e Infraestructuras Críticas	20 h	5
10	Inteligencia Artificial Aplicada a la Ciberseguridad	20 h	5
11	Gobierno, Riesgo, Cumplimiento (GRC) y Privacidad	20 h	5
12	Proyecto Final Integrador de Ciberseguridad	20 h	5
	TOTAL DEL DIPLOMADO	**240 h**	**60**

NIVEL 1

20 Horas Académicas | 5 Prácticas

Fundamentos de la Ciberseguridad

Objetivo: Establecer una comprensión sólida de los conceptos clave de ciberseguridad, amenazas comunes y buenas prácticas de protección personal y organizacional.

Módulo 1.1 — Fundamentos y Amenazas (10h)

- Tríada CIA: Confidencialidad, Integridad y Disponibilidad
- Historia, evolución y panorama actual de amenazas globales
- Legislación básica: GDPR, LOPD, ENS
- Malware, phishing/spear-phishing/vishing e ingeniería social
- Ataques a contraseñas y Denegación de Servicio (DoS/DDoS)

Módulo 1.2 — Protección y Seguridad Digital (10h)

- Gestión de contraseñas y autenticación multifactor (MFA/2FA)
- Navegación segura, antivirus, EDR y firewalls personales
- Copias de seguridad (estrategia 3-2-1) y gestión de parches
- Privacidad en redes sociales y seguridad de correo (SPF, DKIM, DMARC)
- OSINT personal y elaboración de un plan de seguridad documentado

PRÁCTICAS DEL NIVEL

P1 Auditoría de seguridad personal: contraseñas, cuentas y dispositivos propios
P2 Instalación y configuración de un gestor de contraseñas (Bitwarden/KeePass)
P3 Simulación de ataque de phishing con GoPhish y análisis de resultados
P4 Configuración de MFA en cuentas Google, Microsoft y correo corporativo
P5 Creación de un plan de seguridad personal documentado

NIVEL 2

20 Horas Académicas | 5 Prácticas

Seguridad en Sistemas Operativos y Redes

Objetivo: Dominar los conceptos técnicos de seguridad en sistemas operativos Windows/Linux y redes TCP/IP, incluyendo hardening, firewalls y detección de intrusiones.

Módulo 2.1 — Hardening y Redes (10h)

- Hardening de Windows (GPO) y Linux (permisos, SELinux/AppArmor)
- Auditoría de logs (Event Viewer, journalctl, syslog)
- Modelos OSI/TCP-IP y protocolos vulnerables (DNS, HTTP, FTP, Telnet)
- Firewalls, ACLs, segmentación de red (VLAN/DMZ) y VPN
- Reducción de superficie de ataque: deshabilitar servicios innecesarios

Módulo 2.2 — Detección de Intrusiones y Seguridad Web (10h)

- Sistemas IDS vs IPS: Snort y Suricata
- Análisis de tráfico de red con Wireshark
- OWASP Top 10: inyección SQL, XSS y CSRF
- Configuración segura de servidores web (Apache, Nginx)
- HTTPS y certificados SSL/TLS con Let's Encrypt

PRÁCTICAS DEL NIVEL

P1 Hardening de una máquina Windows Server: aplicación de CIS Benchmark
P2 Hardening de un servidor Linux Ubuntu/Debian con checklist documentada
P3 Captura y análisis de tráfico de red con Wireshark en entorno de laboratorio
P4 Configuración de reglas Suricata/Snort para detectar escaneos y ataques
P5 Configuración de servidor web seguro con HTTPS y cabeceras de seguridad

NIVEL 3

20 Horas Académicas | 5 Prácticas

Análisis de Vulnerabilidades y Pentesting Básico

Objetivo: Introducir las metodologías de análisis de vulnerabilidades y pruebas de penetración éticas, desarrollando habilidades prácticas con herramientas estándar del sector.

Módulo 3.1 — Análisis de Vulnerabilidades y Reconocimiento (10h)

- Tipos de vulnerabilidades y metodologías (OSSTMM, PTES, OWASP Testing Guide)
- Herramientas de escaneo (Nessus, OpenVAS) y sistema CVSS
- Definición de alcance y reglas de enfrentamiento (RoE)
- Reconocimiento pasivo (OSINT: theHarvester, Maltego, Shodan) y activo (Nmap)
- Introducción a Metasploit Framework: módulos y meterpreter

Módulo 3.2 — Kali Linux e Informes de Pentesting (10h)

- Entorno Kali Linux y comandos de terminal para pentesting
- Enumeración de servicios (gobuster, enum4linux, nikto)
- Ataques a contraseñas (Hydra, Medusa, John the Ripper, Hashcat)
- Plataformas de práctica: HackTheBox, TryHackMe, DVWA
- Estructura de un informe de pentesting y clasificación de riesgos (CVSS, DREAD, STRIDE)

PRÁCTICAS DEL NIVEL

P1 Escaneo completo con OpenVAS/Nessus sobre una red de laboratorio virtualizada
P2 Reconocimiento OSINT sobre un objetivo ficticio: recopilación de información pública
P3 Explotación de vulnerabilidades en máquina Metasploitable con Metasploit Framework
P4 Resolución guiada de una máquina fácil en TryHackMe (formato CTF)
P5 Redacción de informe completo de pentesting con hallazgos y recomendaciones

NIVEL 4

20 Horas Académicas | 5 Prácticas

Respuesta a Incidentes y Seguridad Ofensiva

Objetivo: Preparar al estudiante para gestionar incidentes de seguridad reales y comprender las técnicas avanzadas de seguridad ofensiva, análisis forense y tendencias emergentes.

Módulo 4.1 — Respuesta a Incidentes (10h)

- Tipos de incidentes: malware, phishing, DDoS, ransomware, APT
- Ciclo de vida NIST: preparación, detección, contención, erradicación, recuperación
- Roles del equipo CSIRT/CERT y responsabilidades
- Herramientas SIEM (Splunk, Wazuh) y técnicas de triage
- Comunicación con equipos externos, clientes y autoridades

Módulo 4.2 — Seguridad Ofensiva y Forense Básico (10h)

- Marco MITRE ATT&CK y técnicas de evasión de defensas
- Movimiento lateral (PsExec, Pass-the-Hash) y post-explotación
- Principios forenses: adquisición, preservación y cadena de custodia
- Análisis con Autopsy y FTK Imager
- Tendencias: seguridad en la nube, IA aplicada e IoT

PRÁCTICAS DEL NIVEL

P1 Simulación de respuesta a un incidente de ransomware: contención y recuperación
P2 Ejercicio Red vs Blue: ataque con Metasploit y defensa con Wazuh
P3 Adquisición y análisis forense de imagen de disco con Autopsy
P4 Análisis de un sample de malware en entorno sandbox (Any.run/Cuckoo)
P5 Creación de un playbook de respuesta a incidentes para una empresa ficticia

NIVEL 5

20 Horas Académicas | 5 Prácticas

Pentesting de Aplicaciones Web Avanzado

Objetivo: Especializar al estudiante en pruebas de penetración contra aplicaciones web modernas, dominando el OWASP Top 10 y herramientas profesionales como Burp Suite.

Módulo 5.1 — Inyecciones y Autenticación (10h)

- Protocolo HTTP/S, arquitecturas modernas (APIs REST, GraphQL) y Burp Suite Pro
- Inyección SQL manual y avanzada (blind, time-based)
- XSS reflejado, almacenado y basado en DOM
- Pérdida de control de acceso (A01:2021) e IDOR
- JWT: análisis y manipulación; OAuth 2.0 y OpenID Connect

Módulo 5.2 — SSRF, APIs y Reporting (10h)

- SSRF (A10:2021) e Insecure Design (A04:2021)
- Pentesting de APIs REST: fuzzing con Postman y Burp Suite
- GraphQL: introspección, batching attacks e injection
- Business Logic Vulnerabilities: errores de lógica de negocio
- Automatización con sqlmap y reporting de vulnerabilidades web (PoC, CVSS)

PRÁCTICAS DEL NIVEL

P1 Auditoría completa de DVWA (Damn Vulnerable Web Application) documentando todos los hallazgos
P2 Explotación de SQL Injection manual y con sqlmap en laboratorio WebGoat
P3 Captura y manipulación de tokens JWT y cookies de sesión con Burp Suite
P4 Auditoría de API REST vulnerable: enumeración de endpoints y explotación de IDOR
P5 Resolución de laboratorio web en PortSwigger Web Security Academy (nivel intermedio)

NIVEL 6

20 Horas Académicas | 5 Prácticas

Operaciones de Seguridad y Caza de Amenazas (Blue Team)

Objetivo: Transitar de la respuesta reactiva a la caza proactiva de amenazas (Threat Hunting), usando SIEM, EDR y la matriz MITRE ATT&CK para detectar TTPs de atacantes.

Módulo 6.1 — SOC y Threat Hunting (10h)

- Estructura del SOC (Niveles 1, 2 y 3) y arquitectura SIEM con Wazuh
- KPIs del SOC: MTTD, MTTR y métricas de eficiencia
- Diferencia entre alertas reactivas y caza proactiva
- La Pirámide del Dolor y metodología de caza basada en hipótesis
- Fuentes de Threat Intelligence: MISP, OpenCTI, VirusTotal

Módulo 6.2 — Caza con MITRE ATT&CK y EDR (10h)

- Uso práctico de la matriz ATT&CK para generar hipótesis de caza
- Caza de Lateral Movement (PsExec, WMI) y Persistence (tareas programadas)
- Ejercicio Red vs Blue: atacante real vs defensor con logs en Wazuh
- Sysmon y detección de Living-off-the-Land Binaries (LOLBins)
- Integración SIEM + EDR: visibilidad unificada del entorno

PRÁCTICAS DEL NIVEL

P1 Despliegue y configuración completa de Wazuh SIEM con agentes Windows/Linux
P2 Creación de reglas de correlación para detectar fuerza bruta y escaneos de red
P3 Ejercicio de Threat Hunting: identificar un atacante simulado usando logs de Wazuh
P4 Análisis de campaña APT simulada usando MITRE ATT&CK Navigator
P5 Generación de informe de Threat Hunting con hipótesis, proceso y recomendaciones

NIVEL 7

20 Horas Académicas | 5 Prácticas

Análisis Forense Digital Avanzado

Objetivo: Profundizar en las técnicas de análisis forense digital, especializándose en memoria RAM, tráfico de red, dispositivos móviles y la generación de informes legalmente admisibles.

Módulo 7.1 — Forense de Memoria y Red (10h)

- Adquisición de memoria RAM (DumpIt, WinPmem, FTK Imager)
- Volatility 3: pslist, pstree, netscan y extracción de credenciales
- Adquisición de tráfico (tcpdump, NetworkMiner) y análisis avanzado con Wireshark
- Reconstrucción de sesiones e identificación de C2 en capturas .pcap
- Detección de túneles DNS y exfiltración de datos

Módulo 7.2 — Forense Móvil y Reporting Legal (10h)

- Adquisición de evidencia Android (ADB) e iOS (backup)
- Análisis de artefactos: bases de datos SQLite de WhatsApp/Telegram
- Cadena de custodia y admisibilidad legal de evidencia digital
- Estructura de un informe forense legalmente admisible
- Herramientas de reporting: Autopsy, Magnet AXIOM, FTK

PRÁCTICAS DEL NIVEL

P1 Adquisición y análisis de volcado de memoria RAM con Volatility 3
P2 Análisis de archivo .pcap con Wireshark: identificar ataque y extraer archivo transferido
P3 Análisis forense de imagen de disco Android con Autopsy
P4 Investigación de incidente completo: desde adquisición hasta informe forense final
P5 Simulación de comparecencia pericial: presentar hallazgos ante un panel evaluador

NIVEL 8

20 Horas Académicas | 5 Prácticas

Seguridad en la Nube (Cloud) y Contenedores

Objetivo: Aplicar todos los conocimientos de pentesting, defensa y forense a los entornos modernos de nube (AWS, Azure) y contenedores (Docker, Kubernetes).

Módulo 8.1 — Fundamentos y Auditoría Cloud (10h)

- Modelo de Responsabilidad Compartida y fundamentos AWS (IAM, S3, EC2, VPC)
- Vectores de ataque cloud: credenciales IAM robadas y buckets S3 públicos
- Herramientas de auditoría AWS: Prowler, ScoutSuite
- Escalada de privilegios en AWS: técnicas y contramedidas
- Detección y respuesta en cloud: CloudTrail, GuardDuty, CloudWatch

Módulo 8.2 — Contenedores, Kubernetes y DevSecOps (10h)

- Contenedores vs VMs: aislamiento, namespaces y cgroups
- Escaneo de vulnerabilidades en imágenes Docker con Trivy
- Runtime security con Falco
- Superficie de ataque en Kubernetes (RBAC misconfiguration, kubelet API)
- Integración CI/CD segura: DevSecOps con GitHub Actions y SAST/DAST

PRÁCTICAS DEL NIVEL

P1 Auditoría de cuenta AWS con Prowler: identificar misconfiguraciones y buckets S3 expuestos
P2 Escalada de privilegios en entorno AWS de laboratorio (IAM privilege escalation path)
P3 Escaneo de vulnerabilidades en imágenes Docker con Trivy y remediación de hallazgos
P4 Configuración de Falco para detectar actividad sospechosa en contenedores en tiempo real
P5 PROYECTO: Auditoría de seguridad completa de infraestructura cloud+contenedores

NIVEL 9

20 Horas Académicas | 5 Prácticas

Seguridad en IoT, SCADA e Infraestructuras Críticas

Objetivo: Comprender y mitigar los riesgos de seguridad en dispositivos IoT, sistemas de control industrial (SCADA/ICS) e infraestructuras críticas.

Módulo 9.1 — Fundamentos de Seguridad IoT (10h)

- Arquitectura de dispositivos IoT y superficie de ataque
- Protocolos IoT: MQTT, CoAP, Zigbee y Bluetooth Low Energy
- Vulnerabilidades comunes en firmware y dispositivos embebidos
- Herramientas de análisis de firmware (Binwalk, Firmwalker)
- Segmentación de red para dispositivos IoT

Módulo 9.2 — Sistemas SCADA e Infraestructuras Críticas (10h)

- Arquitectura de sistemas de control industrial (ICS/SCADA)
- Protocolos industriales: Modbus, DNP3 y Profinet
- Amenazas específicas a infraestructuras críticas (energía, agua, manufactura)
- Normativas y marcos de referencia: IEC 62443 y NIST SP 800-82
- Estrategias de defensa en profundidad para entornos OT/IT

PRÁCTICAS DEL NIVEL

P1 Análisis de firmware de un dispositivo IoT con Binwalk
P2 Auditoría de seguridad de un protocolo IoT (MQTT/CoAP)
P3 Identificación de vulnerabilidades en un simulador SCADA/Modbus
P4 Diseño de segmentación de red para un entorno OT/IT
P5 Proyecto: evaluación de riesgos de una infraestructura crítica simulada

NIVEL 10

20 Horas Académicas | 5 Prácticas

Inteligencia Artificial Aplicada a la Ciberseguridad

Objetivo: Aplicar Inteligencia Artificial para la detección de amenazas, automatización de respuesta y análisis de seguridad.

Módulo 10.1 — IA para Detección de Amenazas (10h)

- Machine Learning aplicado a la detección de anomalías
- Modelos de detección de malware basados en IA
- Análisis de comportamiento de usuarios y entidades (UEBA)
- IA generativa para simulación de ataques (red teaming asistido)
- Limitaciones y sesgos de los modelos de IA en seguridad

Módulo 10.2 — Automatización y SOAR con IA (10h)

- SOAR (Security Orchestration, Automation and Response)
- Automatización de playbooks de respuesta a incidentes con IA
- Uso de LLMs (Claude, GPT) para análisis de logs y alertas
- IA adversarial: ataques a modelos de IA y defensas
- Consideraciones éticas y de gobernanza en IA para seguridad

PRÁCTICAS DEL NIVEL

P1 Modelo de detección de anomalías con Machine Learning
P2 Análisis de comportamiento de usuarios (UEBA) sobre datos simulados
P3 Automatización de un playbook SOAR con IA
P4 Uso de un LLM para triage y resumen de alertas de seguridad
P5 Proyecto: sistema de detección de amenazas asistido por IA

NIVEL 11

20 Horas Académicas | 5 Prácticas

Gobierno, Riesgo, Cumplimiento (GRC) y Privacidad

Objetivo: Comprender los marcos de gobierno, gestión de riesgo, cumplimiento normativo y privacidad de datos aplicados a la ciberseguridad empresarial.

Módulo 11.1 — Gobierno y Gestión de Riesgo (10h)

- Marcos de gobierno de seguridad: ISO 27001, NIST CSF y COBIT
- Gestión de riesgos: identificación, análisis y tratamiento
- Políticas, procedimientos y estándares de seguridad
- Auditorías internas y externas de seguridad
- Métricas e indicadores de gestión de riesgo (KRI)

Módulo 11.2 — Cumplimiento Normativo y Privacidad (10h)

- Regulaciones de privacidad: GDPR, LOPD y leyes locales de protección de datos
- Cumplimiento sectorial: PCI-DSS, HIPAA y SOX
- Evaluaciones de impacto en la protección de datos (DPIA)
- Gestión de terceros y cadena de suministro (vendor risk management)
- Preparación para auditorías de cumplimiento

PRÁCTICAS DEL NIVEL

P1 Análisis de brechas frente a la norma ISO 27001
P2 Matriz de riesgos de seguridad para una organización
P3 Evaluación de impacto en la protección de datos (DPIA)
P4 Checklist de cumplimiento PCI-DSS para un entorno de pagos
P5 Proyecto: programa de GRC documentado para una organización

NIVEL 12

20 Horas Académicas | 5 Prácticas

Proyecto Final Integrador de Ciberseguridad

Objetivo: Integrar todos los conocimientos del diplomado en un proyecto de ciberseguridad completo, desde la evaluación hasta la remediación y el reporte ejecutivo.

Módulo 12.1 — Evaluación y Explotación (10h)

- Definición del alcance y reglas de enfrentamiento del proyecto
- Reconocimiento y análisis de vulnerabilidades del entorno objetivo
- Explotación controlada y post-explotación
- Documentación de hallazgos técnicos con evidencias
- Simulación de un incidente de seguridad real

Módulo 12.2 — Remediación, Reporte y Presentación (10h)

- Plan de remediación priorizado por riesgo
- Informe ejecutivo y técnico del proyecto
- Presentación de resultados ante un panel evaluador
- Recomendaciones de mejora continua (GRC y arquitectura)
- Lecciones aprendidas y documentación final del proyecto

PRÁCTICAS DEL NIVEL

P1 Alcance y reglas de enfrentamiento documentados
P2 Pentesting completo del entorno objetivo del proyecto
P3 Simulación de respuesta a un incidente de seguridad
P4 Informe ejecutivo y técnico del proyecto final
P5 PROYECTO FINAL: presentación de resultados ante un panel evaluador

Perfil de Egreso y Salidas Profesionales

Al completar los 12 módulos del Diplomado, el participante habrá adquirido competencias integrales que le habilitarán para desempeñarse en los principales roles de la industria de la ciberseguridad.

Rol Profesional	Niveles Requeridos
Analista de Seguridad (SOC Tier 1-2)	Módulos 1-4
Especialista en Pentesting Web	Módulos 1-5
Threat Hunter / Blue Team	Módulos 1-4, 6
Analista Forense Digital	Módulos 1-4, 7
Ingeniero de Seguridad Cloud / IoT	Módulos 1-4, 8-9
Consultor de Ciberseguridad (GRC e IA aplicada)	Módulos 1-12 (completo)

Al completar los 12 módulos del Diplomado, el participante habrá desarrollado competencias completas para analizar, proteger y auditar sistemas e infraestructuras en cualquier organización, industria o proyecto propio.