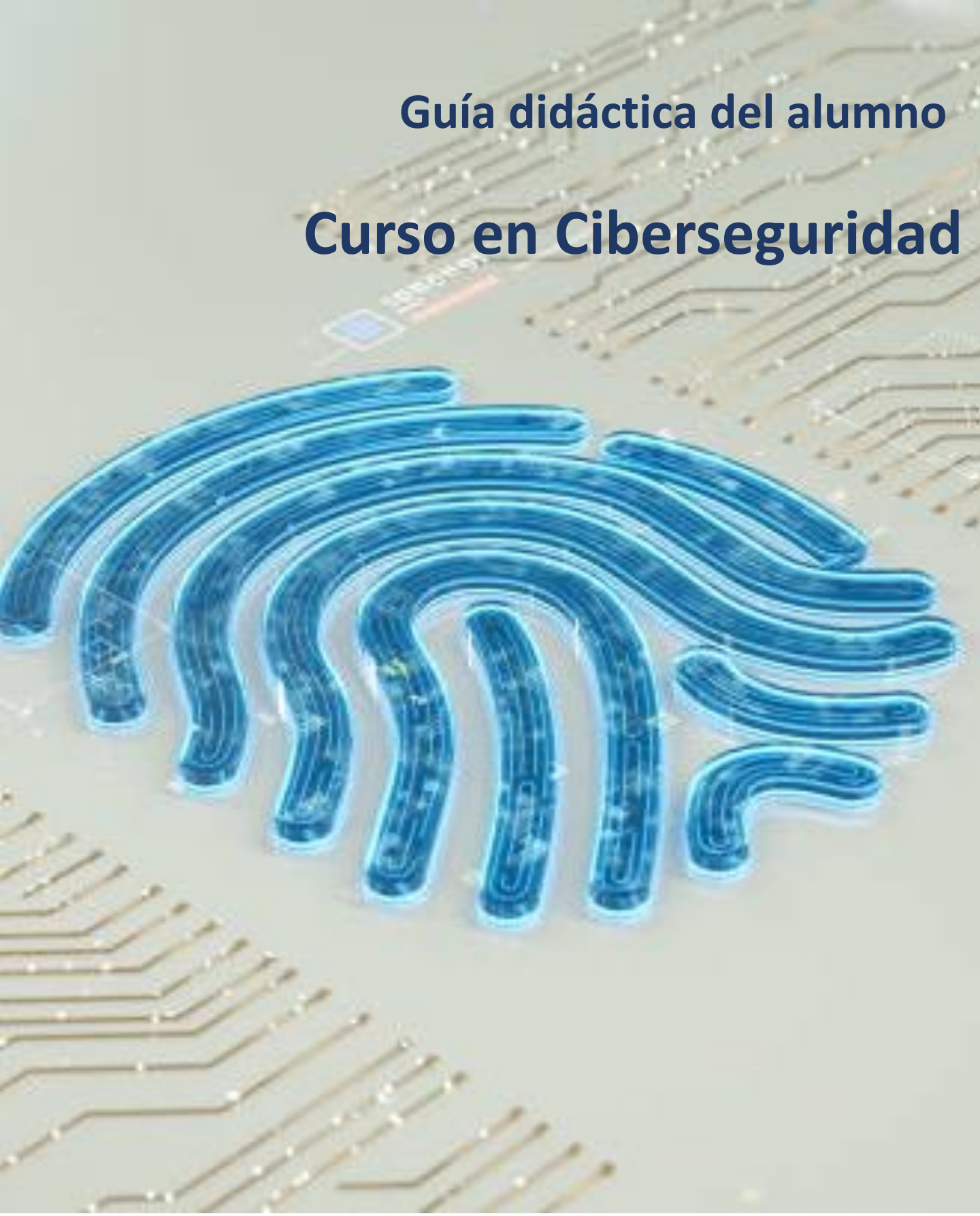
Guía didáctica del alumno

Curso en Ciberseguridad



economía, innovación y empleo | MADRID

BeJob

ÍNDICE

INTRODUCCIÓN

El perfil del profesional de la ciberseguridad es uno de los más buscados por las empresas. Conocer las amenazas y las vulnerabilidades o fallos de seguridad en los sistemas y adelantarse a los ciberataques es fundamental.

La protección de la infraestructura tecnológica y los sistemas de las empresas es fundamental y son la clave para su desarrollo.

Existen gran cantidad de amenazas por ello, las organizaciones están invirtiendo recursos para crear departamentos sólidos en las compañías que garanticen su seguridad digital gracias a los perfiles de ciberseguridad.

IDENTIFICACIÓN DEL CURSO

Modalidad: Online

Dedicación: el curso tiene una duración de 480 horas divididas en lo siguiente:

- 100h de curso online y trabajo individual
- 100h de master class online y trabajo en grupo
- 124h de tutoría y resoluciones individuales de preguntas
- 100h de ejercicios individuales
- 56h de proyecto final

Duración: 6 meses

Fechas: Del 15 de marzo al 24 octubre 2022

OBJETIVOS

GENERALES

- Aplicar las últimas técnicas para la detección y prevención de riesgos y amenazas.
- Reconocer la normativa española y europea sobre protección de datos y sistemas de información.
- Analizar riesgos legales relacionados con la seguridad en todo tipo de sistemas.
- Aplicar los principales estándares y buenas prácticas de auditoría de la seguridad.
- Aplicar correctamente las principales técnicas de análisis forense y elaborar informes periciales.
- Valorar los diferentes algoritmos y técnicas criptográficas y los mecanismos de protección asociados a ellas.
- Analizar las vulnerabilidades en sistemas concretos y tomar decisiones proactivas y reactivas frente a posibles fallos y brechas de ciberseguridad.

ESPECÍFICOS

- Dotar a los asistentes de las habilidades prácticas necesarias para aplicar la teoría aprendida. Familiarizar a los alumnos con las herramientas que encontrarán en el entorno profesional.
- Comprender el funcionamiento a bajo nivel de las redes TCP/IP, como medio imprescindible para la existencia de incidentes de ciberseguridad.
- Adquirir una visión horizontal del mundo de la Ciberseguridad y de los empleos relacionados.

PROGRAMA

1. **Conceptos básicos**
   - 1.1. Conceptos y comandos básicos de sistemas
   - 1.2. Instalación y administración de sistemas operativos
   - 1.3. Configuraciones básicas
   - 1.4. Arquitectura de redes
2. **Introducción al hacking ético**
   - 2.1 Introducción al hacking ético profesional
   - 2.2. La necesidad del hacking ético
   - 2.3. Terminología básica
   - 2.4. Hacking ético vs. escaneo de vulnerabilidades
   - 2.5. Fases del hacking ético
   - 2.6. Marcos de hacking ético
   - 2.7. Distribuciones para hacking ético
3. **Análisis de objetivos y recolección de información**
   - 3.1. Reconocimiento (RECON)
   - 3.2. Habilidades necesarias
   - 3.3. Inteligencia de fuente abierta
   - 3.4. Métodos de OSINT
   - 3.5. Búsqueda OSINT del objetivo
   - 3.6. Herramientas
4. **Análisis de objetivos y recolección de información pasiva**
   - 4.1. Reconocimiento (RECON)
   - 4.2. Inteligencia de fuentes abiertas
   - 4.3. Métodos OSINT
   - 4.4. Búsqueda OSINt del objetivo
   - 4.5. Introducción al Fingerprinting
   - 4.6. Fingerprinting externo
   - 4.7. Fingerprinting interno
5. **Análisis de objetivos y recolección de información activa**
   - 5.1. Introducción al escaneo (Scanning)
   - 5.2. Comandos básicos y otras utilidades
   - 5.3. Escaneo de puertos y servicios
   - 5.4. Escaneo web
6. **Explotación de sistemas**
   - 6.1. Introducción a la explotación
   - 6.2. Habilidades necesarias
   - 6.3. Herramientas y frameworks
7. **Post-Explotación de sistemas**
   - 7.1. Introducción a la postexplotación
   - 7.2. Habilidades necesarias
   - 7.3. Precondiciones y reglas a cumplir
   - 7.4. Técnicas básicas de análisis
   - 7.5. Herramientas disponibles
8. **Introducción al hacking web**
   - 8.1. Habilidades necesarias
   - 8.2. Introducción al proyecto OWASP
   - 8.3. Vulnerabilidades web
   - 8.4. Aplicaciones web vulnerables por diseño
   - 8.5. Herramientas disponibles
9. **Generación de informes**
   - 9.1. Nociones básicas
   - 9.2. Tipos de informes y uso de plantillas
   - 9.3. Control de cambios
   - 9.4. Herramientas para generación de informes
10. **Introducción a la seguridad defensiva**
    - 10.1. Introducción a los sistemas de monitorización
    - 10.2. Defensa perimetral con firewalls
    - 10.3. Defensa perimetral con sistemas de detección de intrusos
    - 10.4. Defensa perimetral con sistemas de registro
    - 10.5. Defensas en las estaciones de trabajo
11. **Normativa general de protección de datos: el RGPD y LOPDPgdd**

CONTENIDOS CLASES SÍNCRONAS

1. El negocio del cibercrimen.

1.1. Estudio de una campaña de ransomware.
1.2. Las cifras de negocio del cibercrimen.
1.3. Principales técnicas de ataque.
1.4 La ingeniería social como factor común.
1.5 Taller: Laboratorio phishing con Kali Linux y SET

2. Virtualización de escritorio.

2.1. Concepto de virtualización.
2.2. Virtualización con VirtualBox.
2.3. Taller I: Creación de máquinas para desarrollo del curso. Creación de instantáneas.

3. El sistema operativo Windows.

3.1. Organización del sistema.
3.2. Sistema de ficheros y ubicaciones importantes.
3.3. La línea de comandos y powershell
3.4. Concepto de servicio.
3.5. Administración básica del sistema.
3.6. Taller I: Puesta en práctica en un sistema Windows.

4. El sistema operativo Linux.

4.1. Organización del sistema.
4.2. Sistema de ficheros y ubicaciones importantes.
4.3. Shell del sistema.
4.4. Concepto de servicio.
4.5. Administración básica del sistema.
4.6. Taller I: Puesta en práctica en un sistema Linux.

5. Trabajando con redes.

5.1. La pila de protocolos TCP/IP
5.2. Dispositivos de red. Switches, routers y firewalls.
5.3 Concepto de firewall de capa 3 y capa 4.
5.4. Taller I: Implementación de una red con servicios de DHCP y DNS en el simulador Cisco Packet Tracer
5.5. Taller II: Implementación de un firewall en una red típica de empresa en el simulador Cisco Packet Tracer.
5.6. Taller III: Simulación de ataques DHCP rogue y suplantación de IP en el simulador Cisco Packet Tracer.

6. Análisis de riesgos.

6.1. Importancia y metodologías.
6.2. Conceptos de activo, amenaza, incidente de seguridad, impacto, frecuencia y riesgo.
6.3. La metodología Magerit y herramienta Pilar.
6.4. Taller I: Caso práctico de análisis de riesgos cualitativo.

7. Hacking Ético. Enumeración de servicios.

7.1. Metodología y fases en la auditoría de Hacking Ético.
7.2. La enumeración en la metodología de hacking.
7.3. Herramientas. Nmap.
7.4. Escaneos básicos y avanzados con nmap.
7.5. Ejecución de scripts con nmap.
7.6. Fases de explotación y postexplotación.
7.7. Taller I: Reto tipo CTF. Obtén información de un host. Puertos, versiones y vulnerabilidades.

8. Hacking Ético. Análisis de vulnerabilidades.

8.1. Concepto de vulnerabilidad, exploit y payload.
8.2. Fuentes de información. Mitre. CVE's, CWE's y CAPEC. Otras fuentes de información.
8.3. Análisis automatizado de vulnerabilidades.
8.4. Taller I: Análisis de vulnerabilidades con Nessus.

9. Hacking Ético. Explotación de vulnerabilidades.

9.1. Explotación manual y automática.
9.2. Fuentes de información.
9.3. Taller I: Explotación de vulnerabilidades con Metasploit.

10. Protección de redes I.

10.1. Segmentación de redes. VLAN's
10.2. Arquitectura básica de una infraestructura de red segura.
10.3. Taller I: Creación de VLAN's con Cisco Packet Tracer.

11. Protección de redes II.

11.1. Dispositivos de protección de redes: Firewall (NGF), IDS, UTM.
11.2. Demo de NGF.
11.3. Taller I: Implantación de IDS con Snort.

12. Entornos WEB I.

12.1. Arquitecturas más habituales en entornos web. 12.2. Tecnologías y lenguajes.
12.3. Debilidades más comunes. OWASP Top 10.
12.4. Taller I: Explotación de vulnerabilidades web básicas.

13. Entornos WEB II.

13.1. Arquitecturas más habituales en entornos web.
13.2. Tecnologías y lenguajes.
13.3. Laboratorios online para la práctica en entornos WEB. OWASP y otros.
13.4. Taller I: Explotación de vulnerabilidades con Kali Linux y Burpsuite.
13.5. Taller II: Análisis de vulnerabilidades con Arachni.

14. Análisis forense.

14.1. Introducción a la forensia digital.
14.2. Toma de evidencias en sistemas apagados.
14.3. Toma de evidencias en sistemas encendidos.
14.4. Taller I: Adquisición para triage en máquina Linux.
14.5. Taller II: Adquisición para triage en máquina Windows.
14.6. Taller III: Análisis de un caso práctico.

CALENDARIO

Las 100 horas de master class y trabajo en grupo se impartirán de forma síncrona, distribuidas en dos sesiones semanales.

Las clases se estructurarán alrededor del siguiente calendario:

2022	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D
marzo		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31										
abril					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30									
mayo							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
junio			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30										
julio					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
agosto	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31										
septiembre				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30									

Cada másterclass en los días marcados, tendrán 2 horas de duración en jornada de tarde. El horario será de martes y jueves desde las 16:00 hasta las 18:00, excepto los días 22/03, 24/03, 29/03, 31/03 y 05/04 que será en horario de 10:00 hasta las 12:00

METODOLOGÍA

El desarrollo del programa del curso requiere del papel activo de los y las participantes como protagonistas del proceso de aprendizaje.

Dinamización mediante gamificación

De forma general, la dinamización se consigue mediante la presentación de prácticas en forma de "retos", formato muy usado en el mundo de ciberseguridad, también llamados ejercicios de "Capture the Flag" o "CTF's".

Dependiendo del contenido impartido, usaremos CTF's de elaboración propia, de organismos públicos creados con finalidad didáctica, como ATENEA del CCN-CERT o bien de plataformas privadas como TryHackMe.

La resolución de los retos se propondrá de forma individual o grupal de un máximo de tres alumnos, obteniendo puntos los tres primeros alumnos o grupos (todos los alumnos) que lo solventen, 10, 8 y 5 puntos respectivamente.

Los puntos se pueden utilizar a lo largo del curso para:

- Comprar pistas para la resolución de retos — 4 puntos.
- Elegir compañeros para CTF — 2 puntos.
- Realizar propuestas de CTF's o contenidos relacionados — 2 puntos.

El resto de puntos se sumarán en forma de décimas a la nota final del alumno con un máximo de 2 puntos.

EVALUACIÓN Y SEGUIMIENTO

Para la evaluación y seguimiento del alumnado, la plataforma provee dos tipos de mecanismos distintos:

- Sistemas de control internos del Aula Virtual.
- Herramientas de evaluación del alumnado.

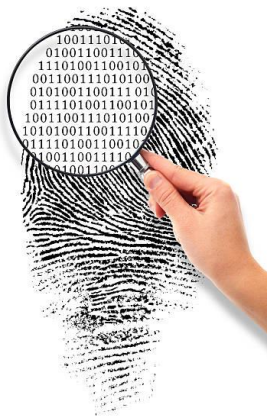
Criterios de evaluación

Sera obligatorio para considerar apto al participante:

- 75% asistencia de las clases (Justificación del resto de ausencias)
- 100 % visualización de las clases online (videos y documentación del curso online)
- Realización de los test obligatorios al finalizar cada temario
- Entrega de los ejercicios individuales al finalizar cada temario
- Entrega del del proyecto final

La nota final será resultado de todas las notas obtenidas en los test, ejercicios individuales y proyectos final repartiendo el peso de la misma en:

- 30 % ejercicios tipos test
- 30% ejercicios individuales
- 40% Proyecto final



TUTORÍAS

La misión del tutor es ayudar al alumno en su proceso de aprendizaje, resolviendo posibles dudas de contenidos, proponiendo temas relevantes para el debate conjunto, e impulsando la adecuada cumplimentación de los requisitos necesarios para poder superar el curso de manera satisfactoria.

Para una mayor fluidez en la comunicación tutor-alumno se han establecido los siguientes medios de comunicación:

Foros:

- Para cada una de las unidades didácticas, el tutor abrirá un foro donde resolver las dudas relativas al tema trabajado.
- Asimismo, los alumnos pueden iniciar hilos en estos foros.

Mensajería interna: los alumnos pueden comunicarse con su tutor de manera individual a través de la mensajería interna de la plataforma.

RECURSOS TÉCNICOS NECESARIOS

Todo el software utilizado es opensource y/o código libre, y está disponible para su uso de forma gratuita.

Es necesario que el alumno disponga de un ordenador con capacidad para virtualizar, mínimo 8 GB Ram y 150 GB de disco.

Los alumnos deberán disponer de una conexión a Internet con conectividad lo más abierta posible, pudiendo en caso contrario verse limitada alguna práctica.

MÓDULO DE EMPLEABILIDAD

HABILIDADES TRANSVERSALES PARA LA EMPLEABILIDAD:

"El 85% del éxito laboral proviene de tener habilidades personales bien desarrolladas" (Univ. Harvard)

Calendario y temática de las sesiones:

	TEMÁTICA DE LA SESIÓN	FECHAS
1	Adaptación y Flexibilidad en un mundo VICA	4 mayo
2	Inteligencia emocional en el entorno laboral I	11 mayo
3	Inteligencia emocional en el entorno laboral II	13 mayo
4	Comunicación en el entorno laboral	18 mayo
5	Psicobiología de las relaciones laborales	23 mayo
6	Liderazgo y Autoliderazgo I	27 mayo
7	Liderazgo y Autoliderazgo II	1 junio
8	Autoestima y mentalidad	8 junio
9	Creatividad	15 junio
10	CV, carta de presentación y entrevista de trabajo	17 junio

La sesiones incluyen conocimientos teóricos y herramientas prácticas que se abordarán individualmente o agrupados en "salas virtuales" diferentes.

Los contenidos de las sesiones pueden ser adaptados a necesidades específicas (afines a la temática de este módulo) expresadas por el alumnado.