Ciberseguridad y agentes de la amenaza
Máster en Ciberdelincuencia

UNIVERSIDAD
NEBRIJA

GUÍA DOCENTE

Asignatura: Ciberseguridad y agentes de la amenaza

Titulación: Master en Ciberdelincuencia

Carácter: Obligatoria

Idioma: Castellano

Modalidad: presencial, semipresencial y a distancia

Créditos: 6

Curso: 1º

Semestre: 1º

Profesores/Equipo Docente: Dr. D. Fernando Davara Rodríguez/ Dr. D. Adrian Nicolas Marchal González/Dr. D. Cesar Augusto Giner Alegria/Dra. Dª Andrea Marica/ Dra. Dª Susana Raquel De Sousa Ferreira

1. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

1.1. Competencias

COMPETENCIAS GENERALES

CG1.- El alumno debe adquirir aquellos conocimientos sobre recursos humanos que le permitan trabajar en un equipo de ciberdelincuencia.
CG3.- El alumno debe dominar las técnicas de lucha contra la ciberdelincuencia suficientes en el ámbito de la ciberdelincuencia que le permitan obtener y analizar información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto.
CG4.- El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia
CG8.- El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.
CG9.- El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.

COMPETENCIAS ESPECIFICAS
CE4- Ser capaz de aplicar las propiedades biométricas al área de seguridad informática y de las comunicaciones.
CE6 – Ser capaz de programar y analizar tareas en diversos lenguajes de programación en el área de seguridad informática y de las comunicaciones.
CE7 – Ser capaz de utilizar las herramientas científico técnicas para evaluar analizar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.
CE10 – Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.
CE11 – Ser capaz de utilizar con destreza las principales herramientas de detección y clasificación de malware y de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad.

1.2. Resultados de aprendizaje

Que los estudiantes hayan demostrado:

- Sabrá detectar, en un tiempo fijado, un elevado porcentaje de las vulnerabilidades de un sistema en red dado.
- Explicar al menos una manera de introducirse en un sistema cuyas vulnerabilidades han sido detectadas.
- Justificar mediante informes razonados las vulnerabilidades encontradas y el procedimiento detallado que se seguiría para la intrusión.
- Explicar otras técnicas de ataque a un sistema que no sea susceptible de intrusión directa.
- Conocer el tipo de información y los mecanismos de defensa desplegados en un sistema, explicar el impacto de distintas amenazas e intrusiones y en especial de las fugas de información.

2. CONTENIDOS

2.1. Requisitos previos

Ninguno.

2.2. Descripción de los contenidos

La asignatura de Ciberseguridad y agentes de la amenaza identifica los problemas relacionados con la gestión de sistemas informáticos de seguridad, Estructura y organización de modelos Organizativos de un centro de operaciones de ciberseguridad y diseño de planes de auditoría y Planes de seguridad, Normas ISO/IEC. Serie 27XXX, implantación de SGSI, grado de implantación de las normativas de seguridad, Planes de Continuidad. ISO/IEC 22301 y 71599, diseño de planes de seguridad proactivos, desarrollo de políticas de seguridad, despliegue de políticas de seguridad, Metodologías de Respuesta a Incidentes. CSIRTs, seguimiento de políticas de seguridad, autenticación, control de accesos, pruebas de conocimiento nulo y en general la Formación y Concienciación de los procesos y procedimientos para el Análisis de Vulnerabilidades y el estudio de los fallos de seguridad, gestión de memoria, mecanismos de protección de memoria, espacio de usuario y de sistema, Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, exploits locales, exploits remotos, alteraciones básicas, explotaciones de memoria, shellcodes, Estándares. UNE/ISO 31000 y 27005, Laboratorios de Evaluación. Acreditación, escalada de privilegios, integer overflow, manejo de las Metodologías y Herramientas, Magerit/Pilar, buffer overflow, heap overflow, Mitigación de Riesgos y Selección de Controles, inyección de código, protección de ejecutables y perfiles de protección

El Módulo consta de cuatro temas:

I. Introducción al concepto de ciberseguridad.

II. Estrategia Nacional de Ciberseguridad y ENS

III. Evolución del cibercrimen, especialización delincuencial y nuevos delitos

IV. Riesgos y amenazas del cibercrimen

En el Tema I se hace una introducción a los principales conceptos del ciberespacio y la ciberseguridad, sus características, objetivos y funciones y una introducción a la ecuación del riesgo con sus diversos componentes, vulnerabilidades y amenazas, finalizando con una descripción de los principales agentes que se identifican actualmente en este espacio cibernético (hackers, ciberactivistas, cibercriminales, ciberterroristas y Estados)

El Tema II se dedica a una revisión del estado del arte de la ciberseguridad mediante un repaso de las principales estrategias nacionales y conjuntas de ciberseguridad con especial énfasis en la Estrategia Española finalizando con la presentación del denominado Esquema Nacional de Seguridad (ENS)

En el Tema III se expone una diferenciación entre incidentes, eventos y ataques así como una breve presentación de uno de los activos a proteger de los ciberataques, las denominadas infraestructuras críticas, para posteriormente presentar una tipología de los diferentes delitos cibernéticos y la evolución del cibercrimen caracterizada por los nuevos delitos recogidos en la reforma del Código Penal.

Finalmente el Tema IV está dedicado a los modernos riesgos y amenazas en particular el denominado CaaS, o crimen como servicio, los mercados digitales de servicios ocultos (underground) los sistemas de anonimización y los vectores de ataque con especial énfasis en las APT (amenazas persistentes avanzadas)

Al finalizar el estudio de estos cuatro temas el alumno dispondrá de información suficiente para poder comprender los aspectos principales de la ciberseguridad, sus riesgos, amenazas y vulnerabilidades, sus actores y la evolución de la ofensa y la defensa caracterizados ambos por los modernos vectores de ataque y los nuevos delitos cibernéticos.

2.3. Contenido detallado

Presentación de la asignatura.

Tema I.-Introducción al concepto de ciberseguridad.

Tema II.- Estrategia Nacional de Ciberseguridad y ENS

Tema III.-Evolución del cibercrimen, especialización delincuencial y nuevos delitos

Tema IV.- Riesgos y amenazas del cibercrimen

Sesiones presenciales Módulo 1

Tutorías Módulo 1

Autoevaluación Módulo 1

2.4. Actividades Dirigidas

AF1: Clase magistral y fundamentos teóricos: consiste básicamente en la explicación general por parte del profesor responsable y/o sus auxiliares del marco teórico conceptual de cada módulo o materia del Máster, así como también todas aquellas orientaciones conceptuales que deben ser tenidas en cuenta por el estudiante para la consecución de un correcto aprendizaje conforme a lo planificado.
En el Campus Virtual se almacenarán los materiales y lecturas correspondientes. Se incluye como parte esencial de esta enseñanza personalizada, característica de nuestro modelo educativo, la plena disponibilidad del profesor responsable y de los profesores auxiliares que en

su caso se empleen para resolver cuestiones puntuales o prestar el asesoramiento académico necesario a través de las clásicas tutorías, tanto individuales como grupales, a solicitud de los estudiantes que lo precisen, si bien en el caso de la modalidad a distancia, las mismas se harán a través del correo electrónico, foros, teleconferencias y videoconferencias, medios todos ellos presentes en nuestra plataforma electrónica como se describe en el apartado correspondiente de esta memoria.

AF2: Explicación técnica para la resolución de casos relacionados con las asignaturas o materias: se trata aquí de una explicación general aplicada al caso en la que el profesor responsable y/o sus auxiliares centran las cuestiones objeto de estudio, discusión, debate o conflicto, orientando la aplicación en la práctica de los conocimientos teóricos con los que el alumno cuenta, bien básicos por su formación previa en el Grado, bien avanzados por su profundización en el postgrado.

AF3: Tutoría: se trata en este caso de la explicación personalizada o en grupos mucho más reducidos tendente a asegurar la adquisición de conocimientos y competencias concretas, la resolución de dudas teóricas o prácticas, la orientación de los enfoques y el seguimiento de los procedimientos empleados por los estudiantes en la asignatura.
Tutorías a distancia:

- Los foros académicos de cada asignatura, en el Campus Virtual, moderados por el profesor, con participación de todos los alumnos, donde se pueden consultar y poner en común dudas de los alumnos y respuestas por parte del profesor, amén de efectuar discusiones sobre los temas de trabajo en cada asignatura.
- El correo electrónico individual o colectivo entre estudiantes y profesor, para aclaraciones, orientaciones y presentación de trabajos, dudas o sugerencias para el mejor aprendizaje.
- La tutoría telefónica o por teleconferencia, tanto individual como en su caso en grupo, en el horario prefijado para cada módulo.
- La tutoría telepresencial por videoconferencia utilizando herramientas tipo SKYPE o ILLUMINATE, implementadas en la Universidad e integradas en las herramientas informáticas de las que dispone el profesorado, que permiten la visualización directa entre profesor y estudiante, la visualización de documentos y la retransmisión de eventos, conferencias, presentaciones y/o sesiones magistrales con intervención bilateral de estudiantes y profesores o invitados.
- Obviamente, el alumno que lo desee y pueda desplazarse, podrá concertar además una tutoría presencial con el profesor correspondiente en el Campus de la Universidad Nebrija o en el lugar que se determine para ello.

Debe considerarse además que siendo un programa fundamentalmente práctico, a través de los medios telemáticos citados, es perfectamente posible la adquisición de las competencias, habilidades y conocimientos mediante la discusión de aspectos específicos de determinados casos prácticos en los foros, en los que los alumnos debaten sobre los mismos, entre sí y/o con el profesor, así como aquellos temas relacionados que el profesor crea conveniente plantear para que el alumno pueda adquirir y asimilar el itinerario formativo propuesto. Y desde luego también dichos medios hacen posible la exposición, individual o en grupo, tanto escrita como oral, de los casos y prácticas mencionados que, tras su evaluación, serán puestos en común con la correspondiente explicación de los pormenores, para asegurar con certeza la plena comprensión por parte de los estudiantes.

AF4: Trabajo individual del estudiante: el trabajo individual es aquella actividad que han de elaborar los alumnos y que han de entregar al término de cada uno de las asignaturas. Los alumnos tendrán que hacer asimismo trabajos breves individuales por indicación del profesor

que imparte La asignatura o parte de la misma, basados en casos. Ello implica la adquisición de habilidades y competencias adicionales.

Cabe destacar que los trabajos y casos objeto del esfuerzo individual para el aprendizaje variarán igualmente año tras año y versarán sobre los contenidos de la materia y su aplicación a problemas y ejemplos relacionados con la asignatura. Algunos de ellos se expondrán oralmente a lo largo del curso por parte de los alumnos y muchos de dichos trabajos requerirán el manejo de programas informáticos que estarán disponibles tanto en los ordenadores de la Universidad como a distancia (bases de datos jurídicas o programas de gestión de despachos, por citar un ejemplo). Además, la red Internet cuenta ya con numerosas aplicaciones y materiales disponibles gratuitamente, no sólo en la sede virtual de la Universidad, sino también en otras fuentes accesibles al público. Igualmente, otros esfuerzos personales y colectivos de los estudiantes requerirán un trabajo de investigación sobre los contenidos de la materia o similares y aplicaciones prácticas y teóricas de toda clase, acudiendo para ello a las fuentes disponibles en Red.

Para facilitar el estudio y la realización de los trabajos escritos, el alumno puede acceder, sin horario predeterminado, a los recursos electrónicos de la biblioteca con todos los programas informáticos que cada asignatura precise y que estarán a su disposición en acceso libre.

Debe tenerse pues en cuenta que desde el principio del curso se encontrarán a disposición del estudiante todos los elementos de material didáctico asociados y necesarios a cada uno de Las asignaturas del Programa de este Máster, garantizando con ello la adquisición de los conocimientos, habilidades y competencias descritas en el programa formativo, que podemos resumir en los siguientes:

1.- Contenidos teórico-prácticos del Máster, tales como notas técnicas y el programa del mismo, que incluyen bibliografía complementaria de consulta y enlaces web de interés.

2.- Resumen escrito o apuntes sobre los conceptos principales.

3.- Test de autoevaluación. El alumno podrá repetirlos y ver la puntuación obtenida cuantas veces desee, por más que debe quedar claro que el contenido y resultados de dichos test de autoevaluación no forman parte de la evaluación de la asignatura, aunque si del itinerario formativo.

4.- Prueba de conocimientos. De mayor extensión que los test y que tampoco forman parte de la evaluación de la asignatura, aunque si del itinerario formativo.

5.- Presentación resumen en *Power Point* de cada una de las partes de Las asignaturas o materias.

6.- Colecciones de problemas y ejercicios que el alumno debe realizar y entregar al profesor por vía telemática y que este corregirá y evaluará.

AF5: Trabajo en grupo del estudiante: el trabajo en grupo es aquella actividad que han de elaborar los alumnos y que han de entregar al término de cada uno de las asignaturas. Los alumnos tendrán que hacer asimismo trabajos breves por indicación del profesor que imparte La asignatura o parte de la misma, basados en casos. Ello implica la adquisición de habilidades y competencias adicionales.

Cabe destacar que los trabajos y casos objeto del esfuerzo para el aprendizaje variarán igualmente año tras año y versarán sobre los contenidos de la materia y su aplicación a problemas y ejemplos relacionados con la asignatura. Algunos de ellos se expondrán oralmente a lo largo del curso por parte de los alumnos y muchos de dichos trabajos requerirán el manejo de programas informáticos que estarán disponibles tanto en los ordenadores de la Universidad como a distancia (bases de datos jurídicas o programas de gestión de despachos, por citar un ejemplo). Además, la red Internet cuenta ya con numerosas aplicaciones y materiales disponibles gratuitamente, no sólo en la sede virtual de la Universidad, sino también en otras fuentes accesibles al público. Igualmente, otros esfuerzos colectivos de los estudiantes requerirán un trabajo de investigación sobre los contenidos de la materia o similares y aplicaciones prácticas y teóricas de toda clase, acudiendo para ello a las fuentes disponibles en Red.

AF6: Puesta en común de resultados y procedimientos: se trata en este caso de la actividad de puesta en común de los avances efectuados por cada estudiante o equipo, bien por grupos de varios equipos, bien con carácter general para todo el grupo de alumnos que constituya una clase.
AF7: Evaluación: Pruebas finales presenciales ordinaria y extraordinaria. Autoevaluación de los resultados obtenidos.

Actividades formativas:

Modalidad Presencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	100%
AF2	10	100%
AF3	10	25%
AF4	45	0%
AF5	38	0%
AF6	10	100%
AF7	2	100%

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	53	0%
AF5	30	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	63	0%
AF5	20	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad presencial: MD1; MD2; MD3; MD4
Modalidad semipresencial: MD1; MD2; MD3; MD4
Modalidad a distancia: MD1; MD2; MD3; MD4

3. SISTEMA DE EVALUACIÓN

3.1. Sistema de calificaciones

Los resultados obtenidos por el alumno en las asignaturas se calificarán en función de la siguiente escala numérica de 0 a 10, con expresión de un decimal, a la que podrá añadirse su correspondiente calificación cualitativa:

a. 0-4,9: Suspenso (SS).
b. 5,0-6,9: Aprobado (AP).
c. 7,0-8,9: Notable (NT).
d. 9,0-10: Sobresaliente (SB).

La mención de «Matrícula de Honor» se otorgará a alumnos que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en la materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

3.2. Criterios de evaluación

Código	Sistema de Evaluación	Descripción
SE1	Desempeño del Trabajo individual	Desempeño del Trabajo individual en resolución de ejercicios o casos
SE2	Desempeño del Trabajos grupales	Desempeño del Trabajo grupal en resolución de ejercicios o casos
SE3	Prueba final presencial	Prueba final individual presencial

Modalidad Presencial:

Convocatoria Ordinaria

Sistema de Evaluación	**Ponderación mínima %**	**Ponderación máxima %**
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	**Ponderación mínima %**	**Ponderación máxima %**
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial
Convocatoria Ordinaria

Sistema de Evaluación	**Ponderación mínima %**	**Ponderación máxima %**
SE1	25	25
SE2	25	25

SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:
Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

3.3. Restricciones

Calificación mínima

Para poder hacer media con las ponderaciones anteriores es necesario obtener al menos una calificación de 5 en la prueba final.

Asistencia

El alumno que, injustificadamente, deje de asistir a más de un 25% de las clases presenciales podrá verse privado del derecho a examinarse en la convocatoria ordinaria.

Normas de escritura

Se prestará especial atención en los trabajos, prácticas y proyectos escritos, así como en los exámenes tanto a la presentación como al contenido, cuidando los aspectos gramaticales y ortográficos. El no cumplimiento de los mínimos aceptables puede ocasionar que se resten puntos en dicho trabajo.

3.4. Advertencia sobre plagio

La Universidad Antonio de Nebrija no tolerará en ningún caso el plagio o copia. Se considerará plagio la reproducción de párrafos a partir de textos de auditoría distinta a la del estudiante (Internet, libros, artículos, trabajos de compañeros…), cuando no se cite la fuente original de la que provienen. El uso de las citas no puede ser indiscriminado. El plagio es un delito.

En caso de detectarse este tipo de prácticas, se considerará Falta Grave y se podrá aplicar la sanción prevista en el Reglamento del Alumno.

4. BIBLIOGRAFÍA

Bibliografía básica

Davara, F., Las TIC y las amenazas a la seguridad nacional; Ciberseguridad, 2013, en Monografías 833. Nuevas Amenazas a la Seguridad Nacional.

Davara, F.; Riesgos vs amenazas: ¿de qué se trata realmente?; El Blog de Fernando Davara; 2015

España; Estrategia de ciberseguridad nacional. 2013.

España; Esquema Nacional de Seguridad (Real Decreto 3/2010 y RD 951/2015)

España; Ley 8/2011, de 28 de abril, por la que se establecen Medidas para la PIC

España; Ley Orgánica 1/2015

Unión Europea; Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

Bibliografía recomendada

Añadida en los cuatro temas

5. DATOS DEL PROFESOR

Nombre y Apellidos	Fernando Davara Rodríguez
Titulación académica	Doctor en Ingeniería Informática
Correo electrónico	fdavara@nebrija.es
Localización	Campus de Princesa. Sala de Profesores
Tutoría	Contactar con el profesor previa petición de hora por e-mail

Nombre y Apellidos	Adrian Nicolas Marchal Gonzalez
Titulación académica	Licenciado en Criminología/Doctor en Derecho
Correo electrónico	amarchal@nebrija.es
Localización	Campus de Princesa. Sala de Profesores
Tutoría	Contactar con el profesor previa petición de hora por e-mail

Nombre y Apellidos	Cesar Augusto Giner Alegria
Titulación académica	Licenciado en Criminología/Doctor en Derecho
Correo electrónico	cginer@nebrija.es
Localización	Campus de Princesa. Sala de Profesores
Tutoría	Contactar con el profesor previa petición de hora por e-mail

Nombre y Apellidos	Andreea Marica
Titulación académica	Doctor en Derecho
Correo electrónico	amarica@nebrija.es
Localización	Campus de Princesa. Sala de Profesores

Tutoría	Contactar con el profesor previa petición de hora por e-mail

Nombre y Apellidos	Susana Raquel de Sousa Ferreira
Titulación académica	Doctora en Seguridad Internacional
Correo electrónico	ssousa@nebrija.es
Localización	Campus de Princesa. Sala de Profesores
Tutoría	Contactar con el profesor previa petición de hora por e-mail