Ciberterrorismo
Máster en Ciberdelincuencia

UNIVERSIDAD NEBRIJA

GUÍA DOCENTE

Asignatura: Ciberterrorismo

Titulación: Master en Ciberdelincuencia

Carácter: Optativa (Itinerario policial)

Idioma: Castellano

Modalidad: presencial, semipresencial y a distancia

Créditos: 6

Curso: 1º

Semestre: 2º

Profesores/Equipo Docente: Dª Maria Riesco Garcia/Dr. D. Antonio Nicolas Marchal Escalona/D. Antonio Esteban Lopez.

1. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

1.1. Competencias

COMPETENCIAS GENERALES

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
CG5.- El alumno debe ser capaz de comunicarse correctamente tanto oralmente como por escrito, utilizando la tecnología más actual, en el ámbito de la ciberseguridad y ciberdelincuencia.
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.
CG11.- Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.

COMPETENCIAS ESPECIFICAS

CE5 – Ser capaz de distinguir los diferentes agentes implicados en seguridad informática, y saber asesorarlos de forma integrada permitiendo la colaboración con otros departamentos de la entidad.
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:

- Elaborar planes de intervención policial relacionados con el entorno de seguridad informática dentro del Esquema Nacional de seguridad e infraestructuras críticas, aplicados a la Ciberterrorismo y la ciberdelincuencia.

- Saber incorporar en las aplicaciones mecanismos de seguridad que ayuden a controlar el acceso seguro a los datos que se manejan desde el software, tales como técnicas criptográficas y de control de acceso a los datos.
- Comprender y saber aplicar las técnicas y funciones de la investigación policial en los Sistemas de Información, conociendo los mecanismos de ataque por el Ciberterrorismo y la ciberdelincuencia.

2. CONTENIDOS

2.1. Requisitos previos

Ninguno en particular

2.2. Descripción de los contenidos

El uso de Internet hace posible interconectar ordenadores personales, servidores con información de empresas y organizaciones, sistemas de control de infraestructuras críticas, teléfonos móviles. Esto nos lleva a una sociedad fuertemente dependiente de las tecnologías de la información. En este escenario se han replicado también los aspectos negativos de la sociedad como representa el Ciberterrorismo. El objetivo de la asignatura es conocer los principales mecanismos de ataque a los sistemas y a la información que utilizan los ciberterroristas en la red y saber desplegar, configurar y desarrollar medidas de seguridad para defenderse contra estas amenazas. Las fuerzas y cuerpos de seguridad del estado son las encargadas de observar y responder de los operativos que formen parte de una investigación oficial contra el Ciberterrorismo. Teniendo en cuenta la gran cantidad de aspectos que puede abarcar el control llevado a cabo por los equipos de investigación las fuerzas y cuerpos de seguridad del estado, es un proceso normal que exista un equipo que se especialice en entornos o actividades que requieran conocimientos muy particulares sobre los distintos fenómenos del Ciberterrorismo. Además de lo anterior, la investigación informática por parte del sector de las fuerzas y cuerpos de seguridad del estado es una tarea fundamental como soporte técnico a procesos legales y de conformidad técnica y acreditación, debiéndose conocer sus aspectos específicos, sabiendo aplicar técnicas avanzadas de testing, validación y verificación del software, saber aplicar técnicas y métodos para asegurar la calidad y la seguridad de los sistemas informáticos. Investigar y analizar los sistemas de aplicación que se están desarrollando o que ya están implantados. Realizar auditorías de datos reales y resultados de los sistemas que se estén utilizando. Realización de auditorías de seguridad. Gobierno y Gestión de Servicios de TI, Análisis y evaluación de riesgos de seguridad, Gestión de políticas de seguridad, Esquema Nacional de seguridad e infraestructuras críticas, Ciberterrorismo y ciberdelincuencia, Mecanismos de ataque, Protección de infraestructuras TIC. Infraestructuras Críticas, Supervisión de la seguridad, Reacción en casos de ataques de Ciberterrorismo, Análisis forense y los Aspectos Éticos y Legales que deben regir en todas las actuaciones de las fuerzas y cuerpos de seguridad del estado.

El Módulo consta de cuatro temas:

I. Normativa en el ámbito del ciberterrorismo y el uso de internet con fines terroristas.

II. Ciberterrorismo y ciberoperaciones contra infraestructuras críticas.

III. Aspectos generales de las infraestructuras estratégicas y críticas, ciberespionaje, ciberterrorismo y otros conceptos.

IV. OSINT-Análisis de casos prácticos

En el Tema I se hace una introducción a la normativa en el ámbito del ciberespacio referido a la ciberseguridad, referido en primer lugar al ámbito internacional para, posteriormente aportar una visión a nivel internacional fundamentalmente en el ámbito europeo, de afección a España. Se repasan elementos fundamentales para situar al alumno en el marco correcto de los aspectos generales que en ciberseguridad deben ser considerados. Posteriormente se centra el contenido en aquellos aspectos más relevantes desde el prisma de la actividad terrorista, que hace uso de las tecnologías de la información y la comunicación, facilitando estas actividades o haciendo uso de las mismas como herramientas.

El Tema II realiza una introducción de las infraestructuras estratégicas nacionales desde la perspectiva de la ciberseguridad, así como recoge los conceptos fundamentales de las infraestructuras críticas de la información como elemento constituyente de conjunto de las IIEE. Se ofrece una visión al alumno de la respuesta que se realiza en España para la gestión de la ciberseguridad así como otras iniciativas en las que el gobierno español participa. En el mismo

sentido se identifican iniciativas que a nivel europeo se mantienen en este marco, así como los agentes que participan en estas cuestiones.

Se remarca y se recoge la importancia de los sistemas SCADA en el ámbito PIC reconociendo los componentes de estos sistemas y analizando los elementos más importantes y sus vulnerabilidades generales.

En el Tema III se estudiarán las bases de las infraestructuras críticas nacionales y su protección, realizando una introducción sobre sus principios básicos así como la importancia de las interdependencias que se generan entre estas y otros sistemas.

Del mismo modo se realiza una aproximación al ciberespionaje y el ciberterrorismo desde el prisma PIC, describiendo algunos de los ataques más comunes, y las distintas motivaciones que pueden estar detrás de dichos ataques.

En Tema IV realiza un repaso del ciclo de inteligencia, desde una perspectiva real y comparada, así como identifica aspectos de interés para la obtención de inteligencia a través de fuentes abiertas o las herramientas que posibilitan dicha obtención.

Po último se exponen análisis de posibles casos prácticos en los cuales el alumno debe ser capaz de identificar la solución posible a las cuestiones planteadas en base a las cuestiones planteadas, así como la puesta en práctica de situaciones mediante el manejo de la información facilitada.

Contenido detallado

Presentación de la asignatura.

1. LA REGULACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO NACIONAL.

2. ASPECTOS NORMATIVOS ESPECÍFICOS.

3. CIBERSEGURIDAD EN EL ÁMBITO DE LA UNIÓN EUROPEA.

4. USO DE INTERNET CON FINES TERRORISTAS. INTRODUCCIÓN.

5. USO DE INTERNET COMO FACILITADOR DE LA ACTIVIDAD TERRORISTA.

6. USO DE INTERNET COMO MEDIO PARA ATACAR OTROS SISTEMAS INFORMÁTICOS.

7. ASPECTOS JURÍDICOS DEL USO DE INTERNET CON FINES TERRORISTAS.

8. INTRODUCCIÓN IIEE.

9. MODELO ESPAÑOL DE RESPUESTA.

10. INICIATIVAS DE LA UNIÓN EUROPEA.

11. AGENTES A NIVEL EUROPEO.

12. ANTECEDENTES SISTEMAS SCADA.

13. INTRODUCCIÓN A LOS SISTEMAS SCADA.

14. IC Y SCADA.

15. COMPONENTES DE LOS SISTEMAS SCADA.

16. TIC VS. SCADA.

17. VULNERABILIDADES.

18. RECOMENDACIONES SEGURIDAD.

19. APROXIMACIÓN A LAS INFRAESTRUCTURAS ESTRATÉGICAS. CONCEPTOS BÁSICO.

20. INTERDEPENDENCIAS.

21. ANTECEDENTES SOBRE CIBERESPIONAJE Y CIBERTERRORISMO.

22. CIBERSEGURIDAD.

23. TIPOS DE ATAQUES.

24. ORIGEN DE LOS ATAQUES.

25. MOTIVACIÓN DEL ATACANTE (OBJETIVOS).

26. FASES DE UN ATAQUE.

27. INTRODUCCIÓN CICLO INTELIGENCIA.

28. OSINT.

29. HERRAMIENTAS.

30. ANÁLISIS DE CASOS PRÁCTICOS.

2.3. 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	53	0%
AF5	30	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	58	0%
AF5	25	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	35	0%

AF5	48	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	40	40
SE2	10	10
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 y textos legales

Ley 8/2011

RD 704/2011

Guías de contenidos mínimos para el desarrollo de los Planes de Seguridad del Operador y de los Planes de Protección Específicos

5. DATOS DEL PROFESOR

Nombre y Apellidos	Maria Riesco Garcia
Titulación académica	Ingeniera de Telecomunicaciones
Correo electrónico	mriesco@nebrija.es
Localización	Campus de Princesa. Sala de Profesores
Tutoría	Contactar con el profesor previa petición de hora por e-mail

Nombre y Apellidos	Antonio Nicolas Marchal Escalona
Titulación académica	Doctor en Derecho
Correo electrónico	amarchale@nebrija.es
Localización	Campus de Princesa. Sala de Profesores
Tutoría	Contactar con el profesor previa petición de hora por e-mail

Nombre y Apellidos	Antonio Esteban Lopez
Titulación académica	Licenciado en Derecho/Ingeniero informático
Correo electrónico	aesteban@nebrija.es
Localización	Campus de Princesa. Sala de Profesores
Tutoría	Contactar con el profesor previa petición de hora por e-mail