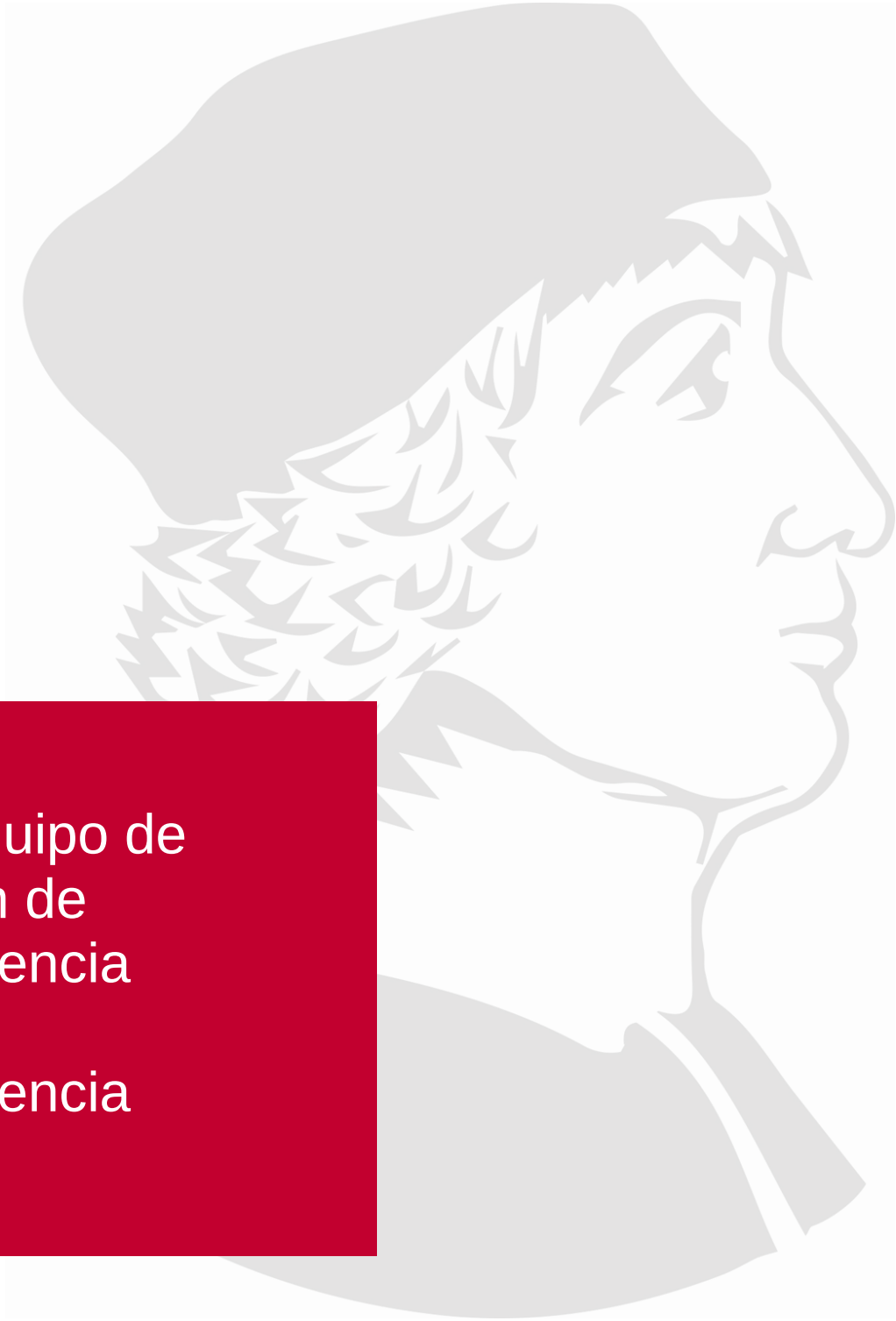
Entorno y equipo de investigación de Ciberdelincuencia Máster en Ciberdelincuencia



UNIVERSIDAD NEBRIJA

GUÍA DOCENTE

Asignatura: Entorno y equipo de investigación de Ciberdelincuencia

Titulación: Master Universitario en Ciberdelincuencia

Carácter: Obligatoria

Idioma: Castellano

Modalidad: presencial/semipresencial/a distancia

Créditos: 6

Curso: 1º

Semestre: 2º

Profesores/Equipo Docente: D. Bernardino Cortijo Fernández/Dr. D. Luis Armando Garcia Segura/ Dra. Dª Susana Checa Prieto.

1. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

1.1. Competencias

COMPETENCIAS GENERALES

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.
CG7.- El alumno debe ser capaz de desempeñar diferentes roles dentro de un equipo de la ciberseguridad y ciberdelincuencia, en particular el de líder.
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.
CG10.- El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia

COMPETENCIAS ESPECIFICAS

CE1 – Ser capaz de analizar y desarrollar sistemas de seguridad web aplicado a la prevención de la ciberdelincuencia.
CE2 - Ser capaz de asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad.
CE3 – Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.
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.

1.2. Resultados de aprendizaje

Que los estudiantes hayan demostrado:

- Elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática aplicados a la ciberdelincuencia e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.
- Investigación de fraudes relacionados con la informática.

- Detectar evidencias de la debilidad de los sistemas de información con carácter preventivo y con carácter correctivo.
- Comprender y saber aplicar las técnicas y funciones de la investigación de los Sistemas de Información.

2. CONTENIDOS

2.1. Requisitos previos

Ninguno.

2.2. Descripción de los contenidos

Los riesgos inherentes dentro de la actividad en los Sistemas de Información, la especialización de muchas empresas en el desarrollo de software, así como la gran inversión hecha en hardware y software, nos obligan cada vez más a maximizar el control y mejorar los procedimientos de investigación sobre estas tareas del departamento de investigación. El entorno de profesionales especializados en revisar el control y llevar a cabo un seguimiento de los estándares de procedimientos, estudiando y analizando los controles organizativos y operativos investigando y analizando los sistemas de aplicación que se están desarrollando o que ya están implantados sobre datos reales y resultados de los sistemas que se estén utilizando. Teniendo en cuenta la gran cantidad de aspectos que puede abarcar el control llevado a cabo por los equipos de investigación, es un proceso normal que exista un equipo que se especialice en entornos o actividades que requieran conocimientos muy particulares sobre los distintos fenómenos de la ciberdelincuencia. Además de lo anterior, la investigación informática 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.

El Módulo consta de cuatro temas:

I. Introducción a los Ciberataques. Ejemplos y casos. Técnicas utilizadas.

II. Estructura de un ciberataque: “Cyber Kill Chain”.

III. Revisiones y Auditorías de Seguridad en relación con los Ciberataques.

IV. Entornos y Herramientas.

A lo largo de los cuatro temas se verá, dentro del entorno tecnológico necesario, las herramientas y los casos relacionados con un Ciberataque, la estructura y todo lo relacionado con las revisiones de seguridad de Ciberataques y metodologías.

El Tema I introduce el concepto de ciberataque, mediante la revisión histórica de los principales ataques cibernéticos ocurridos en los últimos años, revisando sus características y peculiaridades, que técnicas utilizaron, a quién afectaron y qué objetivos perseguían, a través de ejemplos que se analizarán detalladamente.

En el Tema II se aborda el análisis más riguroso, conceptual y detallado de los ciberataques. Para ello, se usará la estructura definida como “Cyber Kill Chain”, término acuñado inicialmente por analistas de la empresa Lockheed Martin Corporation, que actualmente se ha convertido en un estándar de facto para entender las fases genéricas y comunes que componen los ciberataques más avanzados.

Una vez familiarizados con los elementos de un ciberataque, el Tema III expone la otra cara de esa misma moneda, analizando cómo poder utilizar las mismas

técnicas que usan los cibercriminales, pero en lugar de para llevar a cabo una acción hostil, en este caso para mejorar la protección del sistema, mediante la realización de auditorías de seguridad. En el Tema se revisarán los diferentes tipos de auditorías, así como las principales metodologías y buenas prácticas para llevarlas a cabo.

Finalmente, en el Tema IV se analizan los diferentes entornos en los que llevar a cabo las auditorías de ciberseguridad: sistemas operativos, web, redes, comunicaciones inalámbricas, etc.; así como las herramientas de apoyo, indispensables para poder realizarlas con éxito.

Al finalizar el estudio de estos cuatro temas, el alumno dispondrá de información suficiente para poder comprender los aspectos principales de los ciberataques y las auditorías de seguridad, así como de las herramientas asociadas a ambos.

2.3. Contenido detallado

Presentación de la asignatura.

I. Introducción a los Ciberataques. Ejemplos y casos. Técnicas utilizadas.

II. Estructura de un ciberataque: “Cyber Kill Chain”.

III. Revisiones y Auditorías de Seguridad en relación con los Ciberataques.

IV. Entornos y Herramientas.

2.4. Actividades Formativas

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	63	0%
AF5	20	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	43	0%
AF5	40	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

METODOLOGÍAS DOCENTES		
Código	METODOLOGÍA DOCENTE	
MD1	Método del Caso	Metodología centrada en la investigación del estudiante sobre un problema real y específico que ayuda al alumno a adquirir la base para un estudio inductivo (Boehrer, y Linsky, 1990). Parte de la definición de un caso concreto para que el alumno sea capaz de comprender, de conocer y de analizar todo el contexto y las variables que intervienen en el caso
MD2	Aprendizaje Cooperativo	Metodología basada en el trabajo en equipo de los estudiantes. Incluye técnicas en las que los

		alumnos trabajan conjuntamente para lograr determinados objetivos comunes de los que son responsables todos los miembros del equipo
MD3	Aprendizaje Basado en Problemas (ABP)	Metodología centrada en el aprendizaje, en la investigación y reflexión que siguen los alumnos para llegar a una solución o posibles soluciones, ante un problema planteado
MD4	Clase magistral	Metodología de enseñanza centrada en la transmisión de conocimientos por parte del docente. Exposición de contenidos ante los estudiantes, que tienen la oportunidad de preguntar.

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 y textos legales

Pastor, Oscar. «STUXNET, una amenaza sin precedentes». En Ciberseguridad: amenazas y oportunidades en el cuarto espacio, 77-84. Revista Seguridad Global 01. CHOISEUL, 2011. http://www.choiseul.es/images/stories/choiseul/revistas/SG1-contenidos.pdf.

Hutchins, Eric M., Michael J. Cloppert, y Rohan M. Amin.
«Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains». Leading Issues in Information Warfare & Security Research 1 (2011): 80.

INCIBE. «Cyber Kill Chain en Sistemas de Control Industrial». Blog. CERTSI, 27 de octubre de 2016. https://www.certsi.es/blog/cyber-kill-chain-sistemas- control-industrial.

Herzog, Pete. «OSSTMM 3 – The Open Source Security Testing Methodology Manual». ISECOM, 14 de diciembre de 2010. http://www.isecom.org/mirror/OSSTMM.3.pdf.

OWASP (Open Web Application Security Project). «OWASP Testing Guide v4.0», septiembre de 2014. https://www.right-technology.net/downloads/Owasp- Testing-Guide-4.pdf.

Pastor Acosta, Oscar. 2012. «Capacidades para la Defensa del Ciberespacio». En El Ciberespacio. Nuevo Escenario de Confrontación, 196-241. Monografías del CESEDEN 126. Madrid: Ministerio de Defensa, Subdirección General de Publicaciones y Patrimonio Cultural. http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL _CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf.

Pastor Acosta, Oscar. 2013. «La conciencia de ciberseguridad en las empresas». En Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario, 185-253. MONOGRAFÍAS del CESEDEN 137. Madrid: Ministerio de Defensa, Subdirección General de Publicaciones y Patrimonio Cultural.

http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/137_NECESIDAD_DE_UNA_CONCIENCIA_NACIONAL_DE_CIBERSEGURIDAD_LA_CIBERDEFENSA_UN_RETO_PRIORITARIO.pdf.

5. DATOS DEL PROFESOR

Nombre y Apellidos	Bernardino Cortijo Fernández
Titulación académica	Licenciado en Ciencias matemáticas. Especialidades de Investigación Operativa y Estadística
Correo electrónico	bcortijo@nebrija.es
Localización	Campus de Princesa. Sala de Profesores
Tutoría	Contactar con el profesor previa petición de hora por e-mail

Nombre y Apellidos	Luis Armando Garcia Segura
Titulación académica	Doctor en Derecho
Correo electrónico	lgarcise@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 Checa Prieto
Titulación académica	Doctor en Derecho
Correo electrónico	scheca@nebrija.es
Localización	Campus de Princesa. Sala de Profesores
Tutoría	Contactar con el profesor previa petición de hora por e-mail