MUNDO CIBERNÉTICO, SEGURIDAD Y DEFENSA

UNIVERSIDAD NEBRIJA

GUÍA DOCENTE

Asignatura: Mundo Cibernético, Seguridad y Defensa.

Titulación: Master universitario en Seguridad y defensa.

Idioma: Castellano.

Carácter: Obligatoria

Modalidad: Presencial, Semipresencial y a Distancia

Créditos: 5

Semestre: 1º

Profesor titular: José Duran; Marco Valbuena

Equipo Docente:

1. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

1.1. Competencias Generales:

- CGi2. Organizar y gestionar la actividad y el tiempo propios.
- CGi3. Reunir e interpretar con mentalidad científica los datos relevantes; transmitir la información elaborada de forma correcta y con los argumentos adecuados.
- CGi4.Exponer argumentaciones de forma ordenada y comprensible.
- CGi7 Capacidad para elaborar ideas y soluciones utilizando un lenguaje profesional adecuado.
- CGp1. Trabajar en equipos multidisciplinares y específicamente de Seguridad y Defensa.
- CGp2. Coordinar y dirigir equipos de trabajo en el ámbito de la seguridad y defensa.
- CGp5. Aumentar la sensibilidad e interés respecto a los temas de interés social y políticas públicas referidas a seguridad y defensa.
- CGs1. Adquirir una conciencia crítica para la promoción del respeto y los derechos humanos.
- CGs2. Desarrollar habilidades para el aprendizaje autónomo en el ámbito de la seguridad y la defensa.
- CGs3. Potenciar la capacidad de iniciativa, creatividad, liderazgo y superación en el desarrollo de la vida profesional.
- CGs4. Potenciar la visión estratégica en el desarrollo de la profesión.
- CGs5. Desenvolverse con eficacia en un entorno de presión.

1.2. Competencias Específicas:

- CE1. Conocer los instrumentos jurídicos y marcos institucionales en el ámbito de la seguridad y defensa.
- CE2. Aplicar instrumentos de análisis del entorno geopolítico actual y de las relaciones internacionales en materia de Defensa.
- CE3. Emplear y analizar los sistemas de inteligencia estratégica internacional y sus sistemas de funcionamiento, con especial incidencia en situaciones de crisis.

- CE6. Conocer los procesos de Marketing y sistemas de comercialización aplicables a los Programas de Seguridad y Defensa en el ejercicio de la actividad profesional.
- CE7- Aplicar e interpretar técnicas de estimación y optimación de procesos en los Programas de Seguridad y Defensa.
- CE11. Crear y administrar sistemas de gestión de información (Bases de datos) sobre datos referidos a la seguridad y defensa
- CE15. Tomar conciencia de los problemas temporales y espaciales en el ámbito de la seguridad y defensa.
- CE19. Conocer la gestión y la aplicación de los sistemas de control de crisis en el entorno de la Seguridad Privada.
- CE21. Adquirir habilidades para analizar y documentar situaciones de crisis, catástrofes humanitarias y conflictos.
- CE23. Conocer cómo se gestionan las empresas de seguridad y los departamentos de seguridad de las grandes empresas, en la consecución de objetivos organizativos.

1.3.- Resultados de aprendizaje

El alumno podrá demostrar poseer y comprender conocimientos sobre los fundamentos sobre los que se basa el ciberespacio, las vulnerabilidades intrínsecas que estos implican, así como las amenazas a las que se enfrenta. El alumno podrá aplicar conocimientos y comprensión a través de capacidades de análisis y gestión de riesgos cibernéticos. El alumno adquirirá la capacidad de emitir juicios sobre medidas de seguridad a aplicar a partir de la información sobre las ciberamenzas que pueden afectar a los activos cibernéticos objeto de análisis. El alumno adquirirá la capacidad de comunicar sus conclusiones, conocimientos y las razones que las sustentan sobre riesgos y amenazas cibernéticas a otros compañeros de profesión, al público en general o a responsables de gestionar e implementar estrategias de ciberseguridad. El alumno adquirirá habilidades de aprendizaje necesarias para mantenerse al día en un mundo tan terriblemente cambiante como es el de la seguridad en el ciberespacio, en el que las tecnologías, las vulnerabilidades y las amenazas cambian y se renuevan a diario.

2. CONTENIDOS

Las tecnologías de la información aplicadas al ciberespionaje y el ciberterrorismo se identifican hoy como un factor esencial para la Seguridad a nivel nacional, internacional y global, como a su vez constituyen un elemento esencial para la vigilancia y la ofensiva en beneficio de la Seguridad en dichos tres ámbitos. En la asignatura Mundo cibernético, seguridad y defensa el estudiante se enfrentará al análisis y profundización avanzada de los retos que la sociedad de la información supone para el mundo de la seguridad, y en particular a la detección y protección frente amenazas tales como virus, troyanos, ataques de denegación de servicio, espionaje, intercepción de telecomunicaciones, etc. La protección de infraestructuras críticas frente ataques informáticos, la organización española del mando conjunto de ciberdefensa y la revisión de los aspectos legales asociados a la supervisión de sistemas informáticos en el ámbito de la empresa son algunos de los temas que igualmente recibirán tratamiento en dicha asignatura.

2.1. Requisitos previos

Ninguno.

2.2. Contenido detallado.

Unidad 1. Introducción al tema de estudio

Tema 1: INTRODUCCIÓN AL CIBERESPACIO

- **Características destacables del ciberespacio**
  - Ámbitos de la confrontación
  - Evolución
  - Activos a proteger
  - Transversalidad e influencia
  - Atribución
  - Legislación

- **Infraestructuras críticas**
  - Normativa y definiciones
  - Sectores
  - Ciberdependencia
  - Diferencias entre IT y OT

- **Protección de IC,s**
  - Cert,s
  - Relaciones entre actores
  - Normativa
  - Ejemplos de ataque y consecuencias

Tema 2: CARACTERIZACIÓN DE LAS CIBERAMENAZAS

- **Seguridad**
  - Definición
  - Objetivos a proteger
  - Pilares de la seguridad

- **Análisis de riesgos**
  - Definiciones
  - Metodología Magerit
  - Impacto
  - Herramientas

- **Ciberamenazas**
  - Hacktivismo
  - Cibercrimen
  - Ciberespionaje
  - Ciberterrorismo
  - Ciberguerra

- **Ciberataques**
  - Tipos de ciberataque
  - Código avanzado

Unidad 2. Ciberespionaje y ciberterrorismo

Tema 3: CIBERESPIONAJE

- **Campañas de ciberespionaje**
  - Historia
  - Evolución
  - Importancia e influencia en las estrategias
  - Ejemplos

- **Estudio de un ciberataque - Stuxnet**
  - Historia
  - Objetivo
  - Tácticas, técnicas y procedimientos
  - Atribución

Tema 4: CIBERTERRORISMO

- **Características de ciberterrorismo**
  - Las TIC como objetivo
  - Las TIC como medio / uso de internet con fines terroristas
  - Ventajas e inconvenientes

- **TIC como objetivo**
  - Historia y evolución
  - Importancia y peligrosidad
  - Ciberterrorismo vs ciberguerra
  - Ejemplos; caso Estonia

- **TIC como medio / uso de internet con fines terroristas**
  - Historia y evolución
  - Comunicación
  - Obtención de información
  - Publicidad
  - Captación, adoctrinamiento y formación
  - Financiación
  - Logística

3. Sistemas de evaluación

Criterio General para toda la titulación:

La evaluación contemplará todos los aspectos integrados en la docencia, siendo una evaluación integral de toda la actividad del alumno, y garantizando un criterio de seriedad y rigor académico. Habrá una prueba objetiva final en todas las asignaturas (que puntuará al menos un 40 % de la nota global) y se puntuarán también las actividades prácticas, los trabajos entregados, la participación en clase, exposiciones, etc.

3.1.- FORMA DE EVALUACIÓN PREVISTA EN LA MODALIDAD PRESENCIAL:

Convocatoria Ordinaria:

3.1.1.Participación	10%
3.1.2.Prácticas, proyectos o trabajo de asignatura	40%
3.1.3. Prueba objetiva final……	50%

3.1.4.Restricciones y explicación de la ponderación.

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

3.2.- FORMA DE EVALUACIÓN PREVISTA EN LA MODALIDAD A DISTANCIA Y SEMIPRESENCIAL:

Convocatoria Ordinaria:

3.2.1.Participación en las discusiones planteadas en los foros	10%
3.2.2.Trabajos individuales o en grupo	40%
3.2.3.Prueba objetiva final.	50%

3.2.4.Restricciones y explicación de la ponderación.

Para poder hacer media con las ponderaciones anteriores es necesario obtener al menos una calificación de 6 en la prueba objetiva final. Si la prueba objetiva final es un examen, será presencial; y si es un trabajo que deba ser defendido ante tribunal o ante el profesor, la defensa será presencial o por videoconferencia.

3.2.5.- Convocatoria Extraordinaria:

La calificación final de la convocatoria extraordinaria se obtiene como suma ponderada entre la nota del Trabajo Fin de Máster (60%), siempre que su nota sea igual o superior a 5, y las calificaciones obtenidas en los trabajos escritos presentados en la convocatoria ordinaria (40%). Queda a criterio del profesor solicitar y evaluar de nuevo las prácticas o trabajos escritos, si éstos no han sido entregados en fecha, no han sido aprobados o se desea mejorar la nota obtenida en convocatoria ordinaria.

4.- Actividades formativas con su contenido en ECTS, su metodología de enseñanza y aprendizaje, y su relación con las competencias que debe adquirir el estudiante:

4.1.- Actividades formativas modalidad presencial:

4.1.1.- Docencia teórico-práctica:

Clases práctico-teóricas en las que se explicarán los fundamentos de las asignaturas, mediante el método del caso, notas técnicas, talleres específicos y la exposición y coloquio-debate de aspectos concretos.
Clases magistrales y fundamentos teóricos.
Explicación técnica para la resolución de casos.
Tutorías.
(14 ECTS/ 350 horas/ Presencialidad: 100%).

4.1.2.- Trabajo personal y en equipo:

Trabajos del alumno de forma individual y un trabajo en grupo, que se presentarán en clase, ayudándole a aplicar los conocimientos a través de los métodos y técnicas desarrollados. Asistencia presencial opcional.
Trabajos individuales y en grupo del estudiante.
Puesta en común de resultados y procedimientos.
Evaluación.
(6 ECTS/ 150 horas/ Presencialidad: 0%).

4.2.- Actividades formativas modalidad semipresencial y a distancia:

4.2.1.- Docencia teórico-práctica:

Los contenidos didácticos de los módulos de este Máster en Seguridad y Defensa son posicionados en el Campus Virtual Avanzado, en el apartado de “Itinerarios formativos”. Estos contenidos se ilustran con animaciones, vídeos y gráficos que hacen más amena su lectura y su estudio por los alumnos. En el apartado “Documentación” se integran los mismos textos, pero sin animaciones, para que los alumnos puedan imprimirlos, si así lo desean. Esto se completa con Tutorías con el profesor y por videoconferencia, en las horas y fechas establecidas. Incluye el aprendizaje basado en el método del caso, y en las notas técnicas. La discusión de aspectos específicos de dichos casos se lleva a cabo en el apartado de “Foros”, en el que los alumnos debaten sobre estos casos, así como aquellos temas relacionados que el profesor crea conveniente plantearles. La exposición, individualizada o en grupo, la presentan los alumnos a través del Buzón de Tareas y/o por videoconferencia. Cada módulo cuenta con su propio espacio en el Campus Virtual, que permite compartir documentación e imágenes, y mantener

debates por videoconferencia en tiempo real. Asistencia presencial obligatoria: 0%
Clase magistral y fundamentos teóricos.
Explicación técnica para la resolución de casos.
Tutoría.
(14 ECTS/ 350 horas/ Presencialidad: 50%).

4.2.2.- Trabajo personal y en equipo:

El alumno realizará y presentará dos trabajos individuales y otro en grupo, que muestren la aplicación de los métodos y técnicas desarrollados a través de los módulos, por los medios descritos anteriormente.
Trabajos individuales y en grupo del estudiante.
Puesta en común de resultados y procedimientos.
Evaluación.
(6 ECTS/ 150 horas/ Presencialidad: 0%).

5.- BIBLIOGRAFÍA

Bibliografía básica

Boletín Oficial del Estado, 2010. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

Centro Criptológico Nacional, 2019. Ciberamenazas y Tendencias. Edición 2020

Claver, J. (2019). De la flecha al ratón. Consideraciones jurídicas de las operaciones ofensivas en el ciberespacio. *Límites jurídicos de las operaciones actuales: nuevos desafíos*, 133-175.

European Cybercrime Centre (Europol), 2020. Internet Organized Crime ThreatAssessment.

European Network and Information Security Agency (ENISA), 2012. National CyberSecurity Strategies. Practical Guide on Development and Execution.

European Network and Information Security Agency (ENISA), 2012. National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace.

European Network and Information Security Agency (ENISA), 2013. Good Practice Guide on National Risk Assessment and Threat Modelling.

European Network and Information Security Agency (ENISA), 2016. NCSS Good Practice Guide. Designing and Implementing National Cyber Security Strategies.

European Network and Information Security Agency (ENISA), 2018. Threat LandscapeReport. 15 Top Cyber threats and Trends.

Félix Arteaga en Real Instituto Elcano, 2019. Capacidades Ofensivas, Disuasión y Ciberdefensa.

Gobierno de España, 2019. Estrategia Nacional de Ciberseguridad.

Instituto Español de Estudios Estratégicos. (2010). Ciberseguridad. Retos Y Amenazas a La Seguridad Nacional En El Ciberespacio. En *Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio- cuaderno de estudios estrategicos* (Número 149)

MacAfee, 2018. Economic Impact of Cybercrime— No Slowing Down

Mando Conjunto de Ciberdefensa en XIII Jornadas STIC CCN_CERT,2019. Presentación Peculiaridades del Combate en el Ciberespacio.

Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*.

Transactions, E., & Agency, D. (2019). Threat Group Cards : a Threat Actor Encyclopedia. Etda, 01(June), 1-275.

The White House, 2011. International Strategy for Cybercrime.

Bibliografía recomendada

Alperovitch, D. (2011). Revealed: Operation Shady RAT. *White Paper*, 1-14.

Alan Webber, Charlene Li, Jaimy Szymanski, 2012. Guarding the Social Gates: The Imperative for Social Media Risk Management. Altimeter Group.

Army, U. S. (2009). Headquarters Department of the Army Headquarters Department of the Army. *Headquarters, Department of the Army*, *FM 4-02.2*(30 July 2009), 206. www.us.army.mil

Comptroller and Auditor General, 2013. The UK cyber security strategy: Landscape review. National Audit Office, London.

Fernandez Vazquez, D., Pastor Acosta, O., Brown, S., Reid, E., Spirito, C., 2012. Conceptual framework for cyber defense information sharing within trust relationships, in: Cyber Conflict (CYCON), 2012 4th International Conference on. pp. 1–17.

Francisco Zea Pasquín, Óscar Pastor Acosta, 2013. La organización de la Ciberdefensa militar en España y el perfeccionamiento de sus capacidades. Revista SIC 84–86.

Gobierno de España, 2013a. Estrategia de Seguridad Nacional: Un proyecto compartido,NIPO 002130347.

Gobierno de España, 2013b. Estrategia de Ciberseguridad Nacional. Instituto Nacional de Tecnologías de la Comunicación (INTECO), 2012. Guía para empresas: seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA).Observatorio de la Seguridad de la Información.

Jefatura del Estado, 2011. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Joint Task Force Transformation Initiative, 2013. NIST SP 800-53r4 - Security and Privacy Controls for Federal Information Systems and Organizations (No. NIST SP 800-53r4). National

Institute of Standards and Technology.

Lawrence Orans, 2012. Securing BYOD With Network Access Control, a Case Study. SANS Institute.

Ministerio de Defensa. BOD, 2013. Orden Ministerial 10/2013, de 19 de febrero, por laque se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

Ministerio del Interior, 2011. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

OscarPastor Acosta, Javier Candau, 2014. Propuesta para un Esquema Nacional de Certificación de Profesionales en Ciberseguridad para España. Revista SIC 84–87.

SANS, 2013. A Brief History Of The 20 Critical Security Controls. SANS Institute.

Verizon RISK Team, 2012. Data Breach Investigations Report (DBIR) Snapshot:Intellectual Property Theft. Verizon.

ZDNet, TechRepublic, 2013. The Executive's Guide to BYOD and the Consumerizationof IT. TechRepublic.

6.- DATOS DEL PROFESOR

Nombre y Apellidos	José Durán
Departamento	Derecho, Área de Seguridad y Defensa
Titulación académica	Máster
Correo electrónico	jduran@nebrija.es
Localización	Facultad de Ciencias Sociales
Tutoría	Se puede realizar tanto en modalidad presencial, así como online, previa petición de fecha y hora por e-mail

Nombre y Apellidos	Marco Valbuena
Departamento	Derecho, Área de Seguridad y Defensa
Titulación académica	Máster
Correo electrónico	mvalbuena@nebrija.es
Localización	Facultad de Ciencias Sociales
Tutoría	Se puede realizar tanto en modalidad presencial, así como online, previa petición de fecha y hora por e-mail