Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Experto en Ciberseguridad para Criminólogos (Título Propio asociado a Criminología)
Rama de Conocimiento:	Ciencias Sociales y Jurídicas
Facultad/Escuela:	Derecho, Empresa y Gobierno
Asignatura:	Introducción a la Ciberseguridad
Tipo:	Propia Obligatoria
Créditos ECTS:	3
Curso:	1
Código:	61110
Periodo docente:	Primer semestre
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	75

Equipo Docente	Correo Electrónico
Jorge Noguerales Bautista	jorge.noguerales@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

El avance de la sociedad de la información y la transformación digital hacen cobrar una importancia creciente a los aspectos de seguridad informática y de seguridad de la información. En un mundo globalizado e interconectado, la seguridad en la red y en las tecnologías de la información debe ser un elemento primordial, que garantice un efectivo y real desarrollo social y económico, protegiendo a empresas y particulares de las amenazas que afecten a sus elementos tecnológicos y a los datos e información de que dispongan.

El empleo de términos como delincuencia informática, cibercriminalidad, delitos informáticos, etc., se ha convertido en una constante en nuestra sociedad actual. El nacimiento y la rápida difusión de las redes informáticas, están propiciando que la cibercriminalidad sea uno de los ámbitos delictivos con más rápido crecimiento en España. Por ello se hace evidente la necesidad de acercar el mundo digital a los alumnos estudiantes de criminología. A lo largo de la asignatura realizaremos un aproximación al panorama general sobre ciberseguridad: Controles posibles, amenazas existentes, ataques y riesgos. También introduciremos los conceptos de IC -Infraestructuras Críticas- e IoT -Internet de la Cosas- así como los distintos elementos cibernéticos suceptibles de ser atacados: mensajes cifrados, protocolos de comunicación, aplicaciones, etc.

En el año 2016 España sufrió 115.000 ataques informáticos según estimaciones del Instituto Nacional de Ciberseguridad (INCIBE), lo que nos obliga a hacer una reflexión que plantee la problemática real de las nuevas ciberamenazas, mayoritariamente ciberdelitos (ciberdelincuencia, ciberterrorismo, hacktivismo y ciberespionaje), planteándolas como un conjunto múltiple de técnicas y vulnerabilidades que en manos de la delincuencia tradicional, transforman el ciberespacio y todo lo que este “alberga” como objetivos potenciales de la acción ilícita.

El avance de la sociedad de la información y la transformación digital hacen cobrar una importancia creciente a los aspectos de seguridad informática y de seguridad de la información. En un mundo globalizado e interconectado, la seguridad en la red y en las tecnologías de la información debe ser un elemento primordial, que garantice un efectivo y real desarrollo social y económico, protegiendo a empresas y particulares de las amenazas que afecten a sus elementos tecnológicos y a los datos e información de que dispongan.

El empleo de términos como delincuencia informática, cibercriminalidad, delitos informáticos, etc., se ha convertido en una constante en nuestra sociedad actual. El nacimiento y la rápida difusión de las redes informáticas, están propiciando que la cibercriminalidad sea uno de los ámbitos delictivos con más rápido crecimiento en España. Por ello se hace evidente la necesidad de acercar el mundo digital a los alumnos estudiantes de criminología. A lo largo de la asignatura realizaremos un aproximación al panorama general sobre ciberseguridad: Controles posibles, amenazas existentes, ataques y riesgos. También introduciremos los conceptos de IC -Infraestructuras Críticas- e IoT -Internet de la Cosas- así como los distintos elementos cibernéticos suceptibles de ser atacados: mensajes cifrados, protocolos de comunicación, aplicaciones, etc.

En el año 2020 España sufrió 40.000 ataques informáticos incremento del 125% con respecto al año anterior (COVID), lo que nos obliga a hacer una reflexión que plantee la problemática real de las nuevas ciberamenazas, mayoritariamente ciberdelitos (ciberdelincuencia, ciberterrorismo, hacktivismo y ciberespionaje), planteándolas como un conjunto múltiple de técnicas y vulnerabilidades que en manos de la delincuencia tradicional, transforman el ciberespacio y todo lo que este “alberga” como objetivos potenciales de la acción ilícita.

OBJETIVO

El objetivo de la asignatura es dar a conocer la exposición digital actual, la correlación que existe entre el mundo físico y virtual, así como adquirir conocimientos de ciberseguridad (ataques y defensas) al alumno criminólogo. La formación en seguridad es clave para construir un mundo más seguro que contribuya al desarrollo de la sociedad.

CONOCIMIENTOS PREVIOS

No son necesarios conocimientos previos específicos salvo los propios de un estudiante de primer curso de criminología. La aproximación de la asignatura a la ciberseguridad se realizará desde un enfoque jurídico y no técnico.

CONTENIDOS

1.Concepto de Riesgo, Amenaza, Vulnerabilidad, Probabilidadl, Impacto
2.Ciberseguridad, la seguridad en el ciberespacio
3.Ciberamenazas, las nuevas amenazas transnacionales del s.XXI
3.1.Cibercrimen: Delito Informático o ciberdelito
3.2.Ciberterrorismo
3.3.Hactivismo
3.4.Ciberespionaje
3.5.Ciberguerra
4. Estrategias, de Seguridad y Ciberseguridad. Introducción al Plan Director de Seguridad
5. Introducción al Reglamento General de Protección de Datos y Ley de Servicios de la Sociedad de la Información 34/2002

ACTIVIDADES FORMATIVAS

Se realizarán diferentes actividades formativas a lo largo del curso;
Sesiones de invitados de reconocido prestigio en el mundo de la Ciberseguridad. Al menos dos, una de Inteligencia y otra de Hacking.
Gamificación. Trivial de Ciberseguridad. El ganador tendrá recompensa.

Las actividades formativas, así como la distribución de los tiempos de trabajo, pueden verse modificadas y adaptadas en función de los distintos escenarios establecidos siguiendo las indicaciones de las autoridades sanitarias.

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
30 horas	45 horas

COMPETENCIAS

- Identificar la estructura de la Administración de Justicia y los operadores jurídicos en el ámbito penal y de los cuerpos y fuerza de seguridad del Estado así como sus principales instituciones para poder conocerlos y utilizarlos correctamente en su quehacer profesional del criminólogo.
- Conocer los fundamentos de la ciberseguridad y su relación con la función del criminólogo.
- Conocer el entorno global de las ciberamenazas para comprender y valorar el entorno delictivo.
- Conocer la importancia que desempeña la seguridad como uno de los pilares básicos para el desarrollo de las sociedades.

RESULTADOS DE APRENDIZAJE

Usa los recursos bibliográficos y/o informáticos en la obtención de la información para el desarrollo de un trabajo de investigación, comentario crítico o resolución de cuestiones teórico-prácticas planteadas.
Utiliza el lenguaje técnico-jurídico a través del recorrido del entorno digital actual.
Conoce las principales instituciones jurídicas, judiciales y de las fuerzas y cuerpos de seguridad nacionales e internacionales en la lucha contra las ciberamenazas.

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

El sistema de evaluación será de evaluación continua constando de dos exámenes, uno parcial (20%) y un final (50%), así como la elaboración de un trabajo (10%). Igualmente se valorará la asistencia y participación en clase y a las diferentes actividades planteadas (20%). Para poder aprobar la asignatura el examen final debe estar aprobado con un 5 sobre 10. el examen parcial no elimina materia para el final. El examen final será en su mayor parte, 75% tipo test.

Se podrá establecer un mecanismo de evaluación excepcional por causa de fuerza mayor o para alumnos con dispensa académica de asistencia, siempre y cuando sea solicitada por el alumno antes de finalizar las dos primeras sesiones desde el inicio de curso y el profesor verifique la existencia y valoración de la misma causa. Este sistema se aplicará igualmente a los alumnos de convocatoria extraordinaria y se basará en la realización de un trabajo final relacionado con la materia impartida. Todo el proceso constará por escrito en los plazos y fechas previstas.

En el caso de que las recomendaciones sanitarias nos obliguen a volver a un escenario donde la docencia haya que impartirla exclusivamente en remoto, las clases serán a través de las plataformas on line que pone a nuestra disposición para tal fin la UFV siendo obligatoria su asistencia y participación en las mismas. La asistencia y participación en las clases on line supondrá un 25% de la nota final, sólo se realizará un examen presencial (los exámenes se realizarán de manera presencial) con un peso sobre la nota final del 50%, además han de realizarse dos trabajos que supondrán un 25% de la nota final y serán llave para poder realizar el examen final, es decir sí no se realizan los trabajos no se podrá presentar al examen final y la asignatura tendrá la calificación de

suspensa.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

- BARRIO, M. "Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet". Editorial Tirant lo Blanch, Valencia, 2018.
- BARRIO, M. "Ciberdelitos: amenazas criminales del ciberespacio". Editorial Reus, Madrid, 2017.
- CANO, J. "Computación forense - Descubriendo los rastros informáticos". Editorial Alfa y Omega, 2015.
- Gómez de Ageda, A. "Mundo Orwell". Editorial Planeta y Ariel, 2016.

Complementaria

- ISACA, CSX, CISM, CRISC.
- Reglamento General de Protección de Datos. Ley 34/2002 LSSI.
- www.incibe.es
- https://www.ccn-cert.cni.es/
- CCN-CERT_IA1319 Informe. Amenazas y Tendencias Resumen Ejecutivo.
- Google_Panorama-actual-de-la-ciberseguridad-en-España
- M-Trends-Report-2020-ESP