# Escuela de Ingeniería de Telecomunicación

## (*)Páxina web

(*)

www.teleco.uvigo.es

## (*)Presentación

La Escuela de Enxeñaría de Telecomunicación, con acreditación institucional desde el 28/01/2019 (RD 420/2015), oferta un grado y cuatro másteres totalmente adaptados al Espacio Europeo de Educación Superior, verificados por la ANECA y que se ajustan a las Órdenes Ministeriales CIN/352/2009 y CIN/355/2009.

**Grado en Ingeniería de Tecnologías de Telecomunicación (GETT) - Bachelor□s Degree in Telecommunication Technologies Engineering**

**(Acreditado EUR-ACE®, 15/04/2019; Plan de Excelencia Ultreia 2020 de la  Xunta de Galicia).**

El Grado en Ingeniería de Tecnologías de Telecomunicación habilita para el ejercicio de las profesiones reguladas de ingeniería técnica. Las profesiones reguladas son aquellas para las que para su ejercicio se requiere cumplir una condición especial que, normalmente, es estar en posesión de un determinado título académico. En la actualidad, se rigen por el Real Decreto 1837/2008. El Espacio Europeo de Educación Superior (EEES) determinó que las atribuciones profesionales se pueden adquirir con la titulación de grado (Ingenieros e Ingenieras Técnicos) o con la titulación de máster universitario (Ingenieros e Ingenieras).

El GETT ha sido seleccionado para participar en el Plan de Excelencia del Sistema Universitario de Galicia Ultreia 2020, en el que se recogen un conjunto de acciones que tienen como objetivo que las universidades gallegas puedan dar un nuevo salto de calidad. Al amparo de este plan, a partir del curso 2018/19 **se oferta un itinerario en inglés para que, los alumnos y alumnas que así lo deseen, puedan cursar en esta lengua hasta el 80% de los créditos de la titulación**.

http://teleco.uvigo.es/images/stories/documentos/gett/diptico-uvigo-eet-grao-gal.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/gett

**Máster en Ingeniería de Telecomunicación**

Determinadas profesiones reguladas necesitan un nivel de estudios mayor y así, para poder ejercerlas, se requiere haber cursado un máster universitario habilitante. El Máster en Ingeniería de Telecomunicación es un máster con atribuciones profesionales plenas de Ingeniero e Ingeniera de Telecomunicación, regulado por la Orden Ministerial CIN/355/2009 de 9 de febrero de 2009 y publicado en el BOE nº 44 de 20/02/2009.

http://teleco.uvigo.es/images/stories/documentos/met/diptico-uvigo-eet-master-gal.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/mit

**Másteres Interuniversitarios**

La oferta educativa actual del centro se completa con diferentes másteres interuniversitarios  interrelacionados con el sector empresarial.

Master Interuniversitario en Ciberseguridad; www: https://www.munics.es/

Máster Interuniversitario en Matemática Industrial: www: http://m2i.es

Máster Interuniversitario en Visión por Computador: www: https://www.imcv.eu/

**(*)Equipo directivo**

EQUIPO DIRECTIVO DEL CENTRO

Director: Íñigo Cuíñas Gómez (teleco.direccion@uvigo.es)

Subdirección de Relaciones Internacionales: Enrique Costa Montenegro (teleco.subdir.internacional@uvigo.es)

Subdirección de Extensión: Francisco Javier Díaz Otero (teleco.subdir.extension@uvigo.es)

Subdirección de Organización Académica: Manuel Fernández Veiga (teleco.subdir.academica@uvigo.es )

Subdirección de Calidad: Loreto Rodríguez Pardo (teleco.subdir.calidade@uvigo.es )

Secretaría y Subdirección de Infraestructuras: Miguel Ángel Domínguez Gómez (teleco.subdir.infraestructuras@uvigo.es )

COORDINACIÓN DEL GRADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

Coordinadora General: Rebeca Díaz Redondo (teleco.grao@uvigo.es)

http://teleco.uvigo.es/images/stories/documentos/comisions/membros_comisions_grao.pdf

COORDINACIÓN DEL MÁSTER EN INGENIERÍA DE TELECOMUNICACIÓN

Coordinador General: Manuel Fernández Iglésias (teleco.master@uvigo.es)

http://teleco.uvigo.es/images/stories/documentos/comisions/membros_comisions_master.pdf

COORDINACIÓN DEL MÁSTER INTERUNIVERSITARIO EN CIBERSEGURIDAD

Coordinadora General: Ana Fernández Vilas (camc@uvigo.es)

http://teleco.uvigo.es/images/stories/documentos/comisions/membros_comisions_master_ciberseguridade.pdf

COORDINACIÓN DEL MÁSTER INTERUNIVERSITARIO EN MATEMÁTICA INDUSTRIAL

Coordinadora General: Elena Vázquez Cendón (USC)

Coordinador UVIGO: José Durany Castrillo (durany@dma.uvigo.es)

http://www.m2i.es/?seccion=coordinacion

COORDINACIÓN DEL MÁSTER INTERUNIVERSITARIO EN VISIÓN POR COMPUTADOR

Coordinador General: Xose Manuel Pardo López (USC)

Coordinador UVIGO: José Luis Alba Castro (jalba@gts.uvigo.es)

https://www.imcv.eu/legal-notice/

# Máster Universitario en Ciberseguridad

**Asignaturas**

**Curso 1**

| Código | Nombre | Cuatrimestre | Cr.totales |
|---|---|---|---|
| V05M175V01101 | Gestión de la seguridad de la información | 1c | 6 |
| V05M175V01102 | Seguridad de la información | 1c | 6 |
| V05M175V01103 | Seguridade en comunicacións | 2c | 6 |
| V05M175V01104 | Seguridad de aplicaciones | 1c | 6 |
| V05M175V01105 | Redes Seguras | 1c | 6 |
| V05M175V01201 | Conceptos y leyes en ciberseguridad | 2c | 3 |
| V05M175V01202 | Fortificación de sistemas operativos | 1c | 5 |
| V05M175V01203 | Tests de intrusión | 2c | 5 |
| V05M175V01204 | Análisis de malware | 2c | 5 |
| V05M175V01205 | Seguridad como negocio | 2c | 3 |
| V05M175V01206 | Seguridad en dispositivos móviles | 2c | 3 |
| V05M175V01207 | Análisis forense de equipos | 2c | 3 |
| V05M175V01208 | Seguridad ubicua | 2c | 3 |
| V05M175V01209 | Ciberseguridad en entornos industriales | 2c | 3 |
| V05M175V01210 | Gestión de incidentes | 2c | 3 |

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Gestión de la seguridad de la información** | | | | |
| Asignatura | Gestión de la seguridad de la información | | | |
| Código | V05M175V01101 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 6 | OB | 1 | 1c |
| Lengua Impartición | Castellano<br>Gallego | | | |
| Departamento | | | | |
| Coordinador/a | Caeiro Rodríguez, Manuel | | | |
| Profesorado | Caeiro Rodríguez, Manuel<br>Fernández Vilas, Ana<br>López Rivas, Antonio Daniel | | | |
| Correo-e | mcaeiro@det.uvigo.es | | | |
| Web | http://moovi.uvigo.es | | | |
| Descripción general | En esta asignatura se introducen los conceptos fundamentales relacionados con la gestión de la seguridad de la información (e.g. vulnerabilidad, amenaza, riesgo) y se estudian las metodologías, herramientas y especificaciones que se ocupan del análisis de riesgos y del desarrollo de sistemas de gestión de seguridad de la información. | | | |

| Competencias | |
|---|---|
| Código | |
| A2 | Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio |
| A3 | Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. |
| B1 | Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación |
| B2 | Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones. |
| C5 | Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia |
| C7 | Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros |
| C13 | Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes |
| D4 | Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad |
| D5 | Tener capacidad para comunicarse oralmente y por escrito en inglés. |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
| Conocer los conceptos fundamentales relacionados con la Gestión de la Seguridad de la Información: vulnerabilidad, amenaza, riesgo, contramedida, política de seguridad, plan de seguridad, auditoría | A2<br>A3<br>D4<br>D5 |
| Conocer las diferentes metodologías de Gestión de Seguridad de la Información, comúnmente aceptadas | B1<br>B2<br>C5<br>D5 |
| Conocer las herramientas propias para llevar a cabo tareas relacionadas con el análisis de riesgos y la auditoría de seguridad, así como saber cuáles son las más adecuadas a cada entorno | B1<br>B2<br>C7<br>C13<br>D5 |

| Contenidos |
|---|

| Tema | |
|---|---|
| Fundamentos | Conceptos básicos: Confidencialidad, Integridad, Disponibilidad, amenaza, riesgo, etc.<br>Marco legal de la ciberseguridad<br>Normalización: estándares y especificaciones<br>Centros de operaciones de seguridad |
| Análisis de riesgos, gestión y certificación | ISO 27005 e ISO 31000<br>Metodologías y herramientas de análisis de riesgos<br>Estrategia Nacional de Seguridad |
| Sistemas de Gestión de Seguridad de la Información | ISO27000, 27001 y 27002<br>Esquema Nacional de Evaluación y Certificación de las Tecnologías de la Información<br>Clasificación de información<br>Formación y concienciación |
| Impacto de negocio | Roles de ciberseguridad<br>Secuencia típica de un ataque<br>Resilencia<br>Gestión de la continuidad del negocio<br>Plan de contingencia |
| Auditoría de seguridad | Objetivos de control<br>Marcos y estándares para la auditoría<br>Auditoría de seguridad de los datos personales<br>Delegado de protección de datos |

**Planificación**

| | Horas en clase | Horas fuera de clase | Horas totales |
|---|---|---|---|
| Lección magistral | 19 | 29 | 48 |
| Trabajo tutelado | 0.5 | 10 | 10.5 |
| Prácticas de laboratorio | 18 | 57 | 75 |
| Examen de preguntas objetivas | 1.5 | 3 | 4.5 |
| Estudio de casos | 3 | 9 | 12 |

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

**Metodologías**

| | Descripción |
|---|---|
| Lección magistral | Presentación por parte del profesorado del temario de la materia. Con esta metodología se trabajan las competencias: CE5, CE7, CE13, CT4 y CT5. |
| Trabajo tutelado | Cada alumno de forma individual realizará un trabajo sobre uno de los temas de la asignatura a presentar en el grupo A. Con esta metodología se trabajarán las competencias CG1, CG2, CT4 y CT5. |
| Prácticas de laboratorio | En el laboratorio se desarrollarán prácticas guiadas y se plantearán casos de estudio prácticos. Con esta metodología se trabajarán las competencias CB2, CB3, CG1, CG2, CE5, CE7, CE13 y CT5. |

**Atención personalizada**

| Metodologías | Descripción |
|---|---|
| Lección magistral | El profesorado de la asignatura proporcionará atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Las dudas se atenderán de forma presencial o en línea (durante la propia sesión magistral, o durante lo horario establecido para las tutorías). El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura. |
| Prácticas de laboratorio | El profesorado de la materia proporcionará atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Así mismo, el profesorado orientará y guiará al alumnado durante la realización de las tareas que tienen asignadas en las prácticas de laboratorio. Las dudas se atenderán de forma presencial (durante las prácticas, o durante el horario establecido para tutorias). El horario de tutorias se establecerá al principio del curso y se publicará en la página web de la asignatura. |
| Trabajo tutelado | El profesorado de la materia proporcionará atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Así mismo, el profesorado orientará y guiará al alumnado durante la realización de las tareas que tienen asignadas en las prácticas de laboratorio. Las dudas se atenderán de forma presencial (durante las prácticas, o durante el horario establecido para tutorias). El horario de tutorias se establecerá al principio del curso y se publicará en la página web de la asignatura. |

**Evaluación**

| | Descripción | Calificación | Resultados de Formación y Aprendizaje | | |
|---|---|---|---|---|---|
| Trabajo tutelado | Cada alumno de forma individual realizará un trabajo sobre uno de los temas de la asignatura a presentar en el grupo A. | 10 | B1<br>B2 | | D4<br>D5 |
| Examen de preguntas objetivas | Examen de conocimientos teóricos y de desarrollo práctico | 50 | B1<br>B2 | C5<br>C7<br>C13 | D4<br>D5 |
| Estudio de casos | Se desarrollarán ejercicios de casos prácticos sobre el análisis de riesgos y la realización de planes de seguridad | 40 | A2<br>A3 | C5<br>C7<br>C13 | D5 |

**Otros comentarios sobre la Evaluación**

Los estudiantes pueden decidir ser evaluados según un modelo de evaluación continua o bien de evaluación única. Todos los alumnos que entreguen el primer estudio de casos están optando por la evaluación continua. Una vez los estudiantes opten por el modelo de evaluación continua su calificación no podrá ser nunca "No presentado".

En el modelo de evaluación continua, la calificación será el resultado de aplicar la media ponderada entre os resultados: (i) examen escrito (50%),  (ii) estudio de casos (40%) y (iii) trabajo tutelado (10%).

En el modelo de evaluación única, la calificación será el resultado de aplicar la media ponderada entre los resultados: (i) examen escrito (50%),  (ii) estudio de casos (50%).

**Examen escrito:** tendrá lugar en las fechas publicadas en el calendario oficial.

**Parte práctica:**

1- Modelo de evaluación continua. Sendos informes de  2 casos prácticos y 2 evaluaciones del informes de compañeros que se entregarán en las semanas indicadas en el documento que se facilitará a los alumnos el primer día de clase. Un informe será sobre análisis de riesgos y el otro sobre el desarrollo de un plan de seguridad (SGSI). Cada informe tendrá un peso en la nota final del 15% y cada evaluación del 5%. Los informes se desarrollarán en grupo y todos los alumnos del mismo grupo recibirán la misma calificación. Las evaluaciones se realizarán de forma individual. También es necesario realizar un trabajo tutelado sobre un tema de la asignatura a presentar en el grupo A.

2- Modelo de evaluación única. Entrega individual de los 2 informes de  los dos casos prácticos en la misma fecha del examen escrito publicado en el calendario oficial. En este caso no se realizará la evaluación de informes de compañeros y cada informe tendrá un peso en la nota final del 25%.

En la evaluación en segunda oportunidad los estudiantes serán evaluados utilizando la modalidad de evaluación única.

Si se detecta plagio en cualquiera de las pruebas de evaluación, la calificación final de la asignatura será de "suspenso (0)", hecho que se comunicará a la dirección de la escuela para adoptar las medidas oportunas.

**Fuentes de información**

**Bibliografía Básica**


Campbell, Tony, **Practical Information Security Management: A Complete Guide to Planning and Implementation**, Apress, 2016

UNE-EN ISO, **Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones. (ISO 22301:2012).**, AENOR, 2015

UNE-EN ISO, **Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Directrices. (ISO 22313:2012).**, AENOR, 2015

UNE-EN ISO, **Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015)**, AENOR, 2017

UNE-EN ISO, **Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015).**, AENOR, 2017

ISO/IEC, **Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (ISO/IEC 27000:2018)**, ISO/IEC, 2018

ISO/IEC, **Information technology -- Security techniques -- Information security management systems -- Guidance (ISO/IEC 27003:2017)**, ISO/IEC, 2017

ISO/IEC, **Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation (ISO/IEC 27004:2016)**, ISO/IEC, 2016

ISO/IEC, **Information technology -- Security techniques -- Information security risk management (ISO/IEC 27005:2011)**, ISO/IEC, 2011


**Bibliografía Complementaria**

Gómez Fernández, Luis y Fernández Rivero, Pedro Pablo, **Como implantar un SGSI según UNE-ISI/IEC 27001:2014 y su aplicación en el ENS**, AENOR, 2015

Fernández Sánchez, Carlos Manuel y Piatiini Velthuis, Mario, **Modelo para el gobierno de las TIC basado en las normas ISO**, AENOR, 2012

ISO, **Risk management -- Principles and guidelines (ISO/IEC 31000:2009)**, ISO, 2009

Alan Calder Steve Watkins, **IT Governance: An International Guide to Data Security and ISO27001/ISO27002**, 5, Kogan Page, 2012

Alan Calder, **Nine Steps to Success - North American edition: An ISO 27001:2013 Implementation Overview**, 1, IT Governance Publishing, 2017

Edward Humphreys, **Implementing the ISO / IEC 27001 ISMS Standard**, 2, Artech House, 2016

**Recomendaciones**

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Seguridad de la información** | | | | |
| Asignatura | Seguridad de la información | | | |
| Código | V05M175V01102 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 6 | OB | 1 | 1c |
| Lengua Impartición | Inglés | | | |
| Departamento | | | | |
| Coordinador/a | Fernández Veiga, Manuel | | | |
| Profesorado | Fernández Veiga, Manuel<br>Gestal Pose, Marcos<br>Vázquez Padín, David | | | |
| Correo-e | mveiga@det.uvigo.es | | | |
| Web | http://moví.uvigo.gal | | | |
| Descripción general | En esta asignatura se estudian las técnicas de criptografía y criptoanálisis, la generación de números y funciones aleatorias, los métodos de integridad de mensajes, el cifrado autenticado, el cifrado asimétrico, los métodos de privacidad y anonimato de la información, los esquemas de computación segura y la estenografía. Todas las anteriores son herramientas básicas para la protección de la información en redes y sistemas | | | |

| Competencias | |
|---|---|
| Código | |
| A2 | Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio |
| A5 | Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo |
| C1 | Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras |
| C4 | Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información |
| C10 | Conocer los fundamentos matemáticos de las técnicas criptográficas y comprender su evolución y tendencias futuras. |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
| Conocer los conceptos de cifrado Shannon, seguridad perfecta y seguridad semántica | C1<br>C10 |
| Conocer y saber utilizar los métodos de cifrado en flujo | C1<br>C4<br>C10 |
| Conocer y saber utilizar los métodos de cifrado en bloque, las funciones seudoaleatorias y los estándares DES y AES | C1<br>C4<br>C10 |
| Comprender, saber construir y saber utilizar las funciones de hash, las funciones hash universales y con ellas los mecanismos de integridad de la información | C1<br>C4<br>C10 |
| Comprender y saber utilizar los principios del cifrado asimétrico y los esquemas criptigráficos Diffie-Hellman, RSA y ElGamal. Comprender y saber utilizar las firmas digitales | C1<br>C4<br>C10 |
| Conocer los fundamentos de técnicas de cifrado avanzado: cifrado con curvas elípticas y sobre retículos | A2<br>A5<br>C1<br>C4<br>C10 |
| Conocer y saber utilizar los protocolos de intercambio de claves y de comunicaciones interactivas seguras | A5<br>C1<br>C4<br>C10 |

| | |
|---|---|
| Conocer, comprender y saber utilizar las técnicas de anonimización de datos | A5<br>C1<br>C4<br>C10 |
| Conocer, comprender y saber aplicar las técnicas básicas de esteganografía, marcado digital y forenses | A2<br>A5<br>C1<br>C4<br>C10 |
| Conocer y comprender las ideas básicas de la computación segura | A2<br>A5<br>C1<br>C4<br>C10 |

| **Contenidos** | |
|---|---|
| Tema | |
| 1. Cifrado | Cifrado de Shannon<br>Seguridad perfecta<br>Seguridad semántica y computacional |
| 2. Cifrado en flujo | Generadores pseudo aleatorios simples y compuestos<br>Ataques<br>Casos de estudio |
| 3. Cifrado en bloques | Cifrado en bloques. Seguridad<br>DES. AES<br>Funciones pseudoaleatorias<br>Construcción de PRF y cifrado en bloques |
| 4. Integridad | Códigos de autenticación e integridad. Definición de seguridad. MAC con claves. Funciones pseudoaleatorias y MAC. Funciones hash. Hashing universal y hashing resistente a colisiones. Casos de estudio |
| 5. Cifrado autenticado | Definición. Composición. Ataques. ejemplos y casos de estudio |
| 6. Cifrado con clave pública | Definición. Seguridad semántica. Funciones de una dirección. Esquemas RSA, ElGamal, Diffie-Hellman. Firmas digitales. Casos de estudio |
| 7. Cifrado avanzado | Cifrado sobre curvas elípticas. Retículos. Cifrado sobre retículos. RLWE. Ataques cuánticos. Computación homomórfica |
| 8. Protocolos de identificaciín | Definición. Contraseñas (de un solo uso). Challenge-response. Sigma-protocolos. Esquemas de Okamoto y Schnorr. Casos de estudio |
| 9. Anonimización | Definición. t-integridad, divergencia. Análisis. Casos de estudio |
| 10. Esteganografía y watermarking | Definiciones. Marcado de agua mediante espectro ensanchado. Codificación de papel sucio. Forensía digital. |
| 11. Computación segura | Funciones computables. Computación segura a dos vías. Computación segura a varias vías. Computación interactiva segura. Computación homomórfica. Aplicaciones |
| (*)1. Cifrado | (*)Cifrado Shannon. Seguridade perfecta. Seguridade semántica. Seguridade baseada na teoría da información. A canle wiretap |

| **Planificación** | | | |
|---|---|---|---|
| | Horas en clase | Horas fuera de clase | Horas totales |
| Resolución de problemas | 0 | 24 | 24 |
| Prácticas de laboratorio | 18 | 36 | 54 |
| Lección magistral | 17 | 51 | 68 |
| Examen de preguntas de desarrollo | 2 | 0 | 2 |
| Resolución de problemas y/o ejercicios | 1 | 0 | 1 |
| Proyecto | 1 | 0 | 1 |

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

| **Metodologías** | |
|---|---|
| | Descripción |
| Resolución de problemas | Los estudiantes resolverán problemas y ejercicios sobre los contenidos de las lecciones. Entrega por escrito y corrección.<br><br>Con esta metodología se trabajan las competencias CB2, CB4, CB5, CE1, CE 4, CE10 y CT5. |

| | |
|---|---|
| Prácticas de laboratorio | Los estudiantes desarrollarán en el laboratorio prácticas de seguridad de los datos y un proyecto de programación sobre cifrado, firma, anonimato o forenses digital. Las prácticas o proyectos serán supervisadas por los profesores.<br><br>Con esta metodología se trabajan las competencias CB2, CB4, CB5, CE1, CE 4, CE10 y CT4. |
| Lección magistral | Exposición sistemática de los contenidos del curso: conceptos, resultados, algoritmos, ejemplos y casos de uso.<br><br>Con esta metodología se trabajan las competencias CB2, CB4, CB5, CE1, CE 4, CE10 y CT5 |

**Atención personalizada**

| Metodologías | Descripción |
|---|---|
| Lección magistral | Se dispensará atención individual a los estudiantes que precisen orientación para el estudio, explicación adicional sobre los contenidos de la disciplina, aclaración o guía sobre la resolución de problemas. |
| Resolución de problemas | Se atenderán individualmente las consultas sobre la resolución de problemas y ejercicios planteados en las clases o trabajados de forma autónoma |
| Prácticas de laboratorio | Se responderán individualmente las cuestiones relativas a las prácticas de laboratorio y al desarrollo del proyecto. |

**Evaluación**

| | Descripción | Calificación | Resultados de Formación y Aprendizaje |
|---|---|---|---|
| Examen de preguntas de desarrollo | Examen escrito. Resolución de cuestiones, problemas o ejercicios. | 50 | A2 C1<br>A5 C4<br>C10 |
| Resolución de problemas y/o ejercicios | Resolución de cuestiones, problemas y ejercicios a lo largo del curso (2 o 3 cuestionarios). Entrega individual por escrito | 25 | A2 C1<br>A5 C4<br>C10 |
| Proyecto | Desarrollo de un proyecto de implementación de un sistema de protección de información. Pruebas funcionales y de rendimiento | 25 | A2 C1<br>A5 C4<br>C10 |

**Otros comentarios sobre la Evaluación**

Se dejan a discreción de los alumnos dos métodos de evaluación alternativos en la asignatura: evaluación continua y evaluación única.

La evaluación continua consistirá en la realización de un examen final (50% de la calificación), el desarrollo de prácticas y proyecto (25% de la calificación) que se presentará antes del último día hábil anterior al periodo oficial de exámenes y en la entrega a lo largo del curso de ejercicios resueltos (25%). La evaluación única consistirá en la realización de un examen final escrito (60% de la calificación) y en el desarrollo de proyectos de ingeniería a escala (40% de la calificación) que se presentará antes del último día hábil anterior al periodo oficial de exámenes. Las pruebas escritas de las modalidades de evaluación única y continua no serán necesariamente iguales.

Los alumnos podrán optarán por una u otra modalidad de evaluación hasta la fecha del examen escrito del curso.

Quienes no superen la asignatura en la primera oportunidad de la convocatoria disponen de una segunda oportunidad al final del curso en la que se reevaluarán sus conocimientos con una prueba escrita o se reevaluará su proyecto si se hubiera mejorado o modificado éste. Los pesos de cada una de las pruebas (examen y proyecto) serán los mismos que en el periodo ordinario de evaluación conforme a la modalidad que se hubiese elegido.

La calificación de las pruebas solo surte efecto en el curso académico en que se obtengan, con independencia del itinerario de evaluación escogido.

**Fuentes de información**

**Bibliografía Básica**

D. Boneh, V. Shoup, **A graduate course in applied cryptography**, http://toc.cryptobook.us, 2018

**Bibliografía Complementaria**

O. Goldreich, **Foundation of cryptography, vol. I**, Cambridge University Press, 2007

O. Goldreich, **Foundation of cryptography, vol. ii**, Cambridge University Press, 2009

J. Katz, Y. Lindell, **Introduction to modern cryptography**, 2, CRC Press, 2015

A. Menezes, P. van Oorschot, S. Vanstone., **Handbook of applied cryptography**, CRC Press, 2001
C. Dwork, A. Roth, **The algorithmic foundations of differential privacy**, NOW Publishers, 2014
W. Mazurczyk, S. Wenzel, S. Zander, A. Houmansadr, K. Szczypiorski, **Information hiding in communications networks: Fundamentals, mechanisms, applications, and countermeasures**, Wiley, 2016
I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kolker, **Digital watermarking and steganography**, 2, Morgan Kaufmann, 2008
A. El-Gamal, Y. Kim, **Network Information Theory**, Cambridge University Press, 2011

**Recomendaciones**

**Otros comentarios**

La asignatura se imparte en inglés. Es recomendable aptitud para el razonamiento matemático.

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Seguridade en comunicacións** | | | | |
| Asignatura | Seguridade en comunicacións | | | |
| Código | V05M175V01103 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 6 | OB | 1 | 2c |
| Lengua Impartición | Castellano | | | |
| Departamento | | | | |
| Coordinador/a | Rodríguez Rubio, Raúl Fernando | | | |
| Profesorado | Fernández Iglesias, Diego<br>Rodríguez Rubio, Raúl Fernando<br>Suárez González, Andrés | | | |
| Correo-e | rrubio@det.uvigo.es | | | |
| Web | http://https://moovi.uvigo.gal | | | |
| Descripción general | Esta materia realiza un repaso por las capas de la arquitectura de comunicaciones de Internet, mostrando sus principales debilidades desde el punto de vista de la seguridad y proporcionando las técnicas y herramientas necesarias para mitigarlas. Los estudiantes conocerán en detalle los protocolos de red que aportan seguridad a la transmisión de la información, y las implicaciones derivadas del lugar que ocupan dentro de la arquitectura en que se organiza el software de comunicaciones. | | | |

| Competencias | |
|---|---|
| Código | |
| A2 | Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio |
| A4 | Que los estudiantes sepan comunicar sus conclusiones ---y los conocimientos y razones últimas que las sustentan--- a públicos especializados y no especializados de un modo claro y sin ambigüedades |
| A5 | Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo |
| B1 | Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación |
| B3 | Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones |
| B5 | Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos |
| C1 | Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras |
| C2 | Conocer en profundidad las técnicas de ciberataque y ciberdefensa |
| C4 | Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información |
| C8 | Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad |
| D4 | Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad |
| D5 | Tener capacidad para comunicarse oralmente y por escrito en inglés. |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
| Saber identificar qué solución/protocolo es el adecuado para asegurar un entorno determinado | A5<br>B1<br>B3<br>B5<br>C1<br>C2<br>C4<br>D4<br>D5 |

| | |
|---|---|
| Conocer las soluciones que se esconden tras ciertos servicios de red y/o aplicaciones universalmente utilizadas | A5<br>C2<br>C8<br>D4<br>D5 |
| Ser capaces de configurar las diferentes herramientas (paquetes software) que los distintos sistemas operativos/plataformas nos aportan para activar la seguridad en las comunicaciones. | A2<br>A5<br>B5<br>D4<br>D5 |
| Adquirir la capacidad de redactar informes técnicos justificando la idoneidad de una solución de ciberseguridad para un problema o entorno determinado | A4<br>B1<br>B3 |

## Contenidos

| Tema | |
|---|---|
| Arquitectura y protocolos de Internet | Conceptos fundamentales. |
| Seguridad en el nivel de enlace | Seguridad en redes cableadas/Ethernet:<br>Control de acceso y autenticación basada en puertos<br>Confidencialidad en redes Ethernet<br><br>Seguridad en redes inalámbricas/WiFi:<br>WPA/2/3 seguridad personal<br>WPA/2/3 seguridad empresarial |
| Seguridad en el nivel de red | IPsec<br>Protocolos de seguridad<br>Gestión dinámica de claves<br>Mecanismos de autenticación |
| Asegurando la infraestructura de Internet | Encaminamiento seguro<br>Seguridad en DNS<br>Seguridad en TCP |
| Seguridad en la transmisión de los datos | El protocolo TLS<br>Suites criptográficas<br>Infraestructura WebPKI<br>Validación de certificados |
| Seguridad en redes móviles | Arquitectura del sistema<br>Asociación y autenticación del terminal/usuario<br>Privacidad |

## Planificación

| | Horas en clase | Horas fuera de clase | Horas totales |
|---|---|---|---|
| Lección magistral | 21 | 21 | 42 |
| Prácticas de laboratorio | 19 | 19 | 38 |
| Prácticas con apoyo de las TIC | 0 | 58 | 58 |
| Examen de preguntas de desarrollo | 2 | 0 | 2 |
| Informe de prácticas, prácticum y prácticas externas | 0 | 10 | 10 |

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

## Metodologías

| | Descripción |
|---|---|
| Lección magistral | Las sesiones magistrales siguen el esquema habitual para este tipo de docencia. En estas sesiones se trabajan las competencias CG3, CE1, CE2, CE4, CE8 |
| Prácticas de laboratorio | Se realizarán varias sesiones prácticas guiadas por los profesores donde se asentarán los conceptos aprendidos en las clases teóricas. En dichas prácticas se utilizarán dispositivos de red reales (routers y switches) y/o software de virtualización que permitirá al alumno su instrucción y entrenamiento en su propia casa. De forma natural, las actividades definidas podrán incluir apartados/retos adicionales que complementarán el trabajo autónomo del estudiante, que se describe en el siguiente item. Los alumnos deben adquirir en las prácticas las competencias CB2, CB4, CG1, CG3, CG5, CE1, CE4, CE8 |
| Prácticas con apoyo de las TIC | Más allá de las prácticas guiadas, el alumno tendrá que desplegar/configurar/implementar algunas soluciones particulares, para ciertos escenarios, de forma autónoma.En estas actividades se trabajan las competencias CB2, CB4, CB5, CG1, CG3, CG5, CE1, CE4, CE8 |

## Atención personalizada

| Metodologías | Descripción |
|---|---|
| Lección magistral | Durante las horas de tutoría los docentes realizarán una atención personalizada para fortalecer u orientar al alumno en la comprensión de los conceptos teóricos explicados en las clases magistrales o en las sesiones demostrativas de carácter práctico; y para corregir o reorientar los pequeños trabajos prácticos optativos derivados de dichas clases de laboratorio. |
| Prácticas de laboratorio | Esta actividad es interactiva por definición, por lo que se espera que las cuestiones fluyan con naturalidad entre docentes y estudiantes, pudiendo involucrar a otros estudiantes en las respuestas buscadas. |
| Prácticas con apoyo de las TIC | Aunque el trabajo autónomo está orientado a que el estudiante resuelva por si mismo situaciones/retos que se encontrará en los sistemas reales, en las horas de tutoría los docentes podrán orientarlo cuestionando los soluciones elegidas o sugiriendo caminos alternativos. |

## Evaluación

| | Descripción | Calificación | Resultados de Formación y Aprendizaje |
|---|---|---|---|
| Prácticas de laboratorio | Serán calificadas como apto/no apto. El alumno será apto si asiste a todas las sesiones de este tipo. Si por algún motivo se perdiese alguna, deberá suplirla realizando alguna práctica complementaria que el profesor definirá en su momento.<br>En algunas de las sesiones/actividades se podrá solicitar al alumno un trabajo autónomo adicional (y su informe asociado) que se evaluará cuantitativamente dentro del ítem más general que denominamos "Prácticas autónomas a través de TIC" | 0 | A2 A4 A5 B5 C4 C8 D4 D5 |
| Prácticas con apoyo de las TIC | Los estudiantes tendrán que realizar, ante los profesores, la demostración práctica que muestre la resolución de los distintos retos técnicos planteados, enfrentándose a preguntas sobre las soluciones adoptadas y su grado de completitud. Esta defensa/entrevista tendrá lugar, por término general, tras la entrega de la última tarea encargada y antes del periodo oficial de exámenes de cada convocatoria; consensuándose la fecha concreta entre alumnos y profesores con antelación suficiente.<br><br>Todo reto o actividad autónoma exigirá un informe escrito, cuya estructura, composición y legibilidad tendrán su peso en la valoración final. | 40 | A2 A4 A5 B5 C1 C4 C8 D4 D5 |
| Examen de preguntas de desarrollo | Se realizará un exámen escrito al final del cuatrimestre, donde se evalúan tanto los conceptos teóricos impartidos en las sesiones magistrales, como los fundamentos prácticos derivados de las clases/trabajos prácticos acometidos. | 60 | A4 C1 C2 C4 D4 |
| Informe de prácticas, prácticum y prácticas externas | El trabajo autónomo del alumno deberá ser recogido en el/los informes de prácticas pertinentes, y su valoración formará parte de la valoración integral de aquél. | 0 | A4 B1 B3 D4 D5 |

## Otros comentarios sobre la Evaluación

La evaluación de la materia podrá seguir el canal de evaluación continua o bien evaluación única. Un alumno elegirá evaluación continua al entregar la solución e informe del primer reto o trabajo autónomo que se le plantee durante el devenir normal del curso. Los porcentajes expresados en el epígrafe anterior sólo reflejan el máximo obtenible en cada tipo de prueba en la modalidad de evaluación continua; y son sólo orientativos. La forma de evaluación detallada se expresa a continuación:

Para la evaluación continua (primera oportunidad), la nota final será la media geométrica ponderada entre la nota del trabajo autónomo (TA, 40%) y la calificación correspondiente al examen de preguntas de desarrollo (E, 60%). La nota TA será la media aritmética de las calificaciones asociadas a cada uno de los retos/prácticas autónomas que el alumno tendrá que resolver a lo largo del cuatrimestre.

NOTA FINAL(EC)=(TA^0.4)×(E^0.6)

Si las prácticas de laboratorio fueron calificadas como no aptas, la nota será la mínima entre la nota del examen escrito (E) y 3.

Los alumnos que opten por la evaluación única deberán presentarse a un examen final que consistirá de tres partes: una prueba escrita análoga a la prueba de evaluación continua (E), una prueba de aptitud en el laboratorio y uno o varios trabajos prácticos (T). La nota final, en este caso, es la media geométrica ponderada entre la nota de teoría (E, 80%) y el trabajo práctico (T, 20%), con la condición de que se supere la prueba de aptitud. Si el alumno no supera la prueba de

aptitud, la nota final será el mínimo entre E y 3.

NOTA FINAL(EU)=(T^0.2)×(E^0.8)

Finalmente, para la segunda oportunidad (junio/julio), el alumno podrá proseguir con el modo de evaluación que ya había elegido (conservándosele la nota de la parte -E o TA/T- que hubiera superado, y afrontando únicamente la parte suspensa -con posibles modificaciones en las especificaciones de los trabajos prácticos), o afrontar desde cero una evaluación que tendrá las mismas características que el examen final que acabamos de describir. La prueba de aptitud sólo será necesaria si no asistió a todas las sesiones del laboratorio.

## Fuentes de información

### Bibliografía Básica


I. Ristic, **Bulletproof SSL and TLS, ser. Computers/Security**, London: Fesity Duck, 2015

A. Liska and G. Stowe, **DNS Security: Defending the Domain Name System**, Boston: Syngress, 2016

Yago Fernández Hansen, Antonio Angel Ramos Varón, Jean Paul García-Moran Maglaya, **RADIUS / AAA / 802.1x**, RA-MA Editorial, 2008

Graham Bartlett, Amjad Inamdar, **IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS**, CISCO PRESS, 2016

Madhusanka Liyanage, Ijaz Ahmad, Ahmed Abro, Andrei Gurtov, Mika Ylianttila, **A Comprehensive Guide to 5G Security**, Wiley, 2018


### Bibliografía Complementaria


D. J. D. Touch, **Defending TCP Against Spoofing Attacks**, IETF, 2007

R. R. Stewart, M. Dalal, and A. Ramaiah, **Improving TCP□s Robustness to Blind In-Window Attacks**, IETF, 2010

D. J. Bernstein, **SYN cookies**,

P. McManus, **Improving syncookies**, 2008

C. Pignataro, P. Savola, D. Meyer, V. Gill, and J. Heasley, **The Generalized TTL Security Mechanism (GTSM)**, IETF, 2007

D. J. D. Touch, R. Bonica, and A. J. Mankin, **The TCP Authentication Option**, IETF, 2010

S. Rose, M. Larson, D. Massey, R. Austein, and R. Arends, **DNS Security Introduction and Requirements**, IETF, 2005

R. Arends, R. Austin, M. Larson, D. Massey, S. Rose, **Resource Records for the DNS Security Extensions**, IETF, 2005

R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, **Protocol Modifications for the DNS Security Extensions**, IETF, 2005

Cloudflare Inc., **How DNSSEC works**,

P. E. Hoffman and P. McManus, **DNS Queries over HTTPS (DOH)**, IETF, 2018

E. Jones and O. L. Moigne, **OSPF security vulnerabilities analysis**, IETF, 2006

M. Khandelwal and R. Desetti, **OSPF security: Attacks and defenses**, 2016

J. Durand, I. Pepelnjak, and G. Doering, **BGP operations and security**, IETF, 2015

R. Kuhn, K. Sriram, and D. Montgomery, **Border gateway protocol security**, NIST, 2007

C. Pelsser, R. Bush, K. Patel, P. Mohapatra, and O. Maennel, **Making route flap damping usable**, IETF, 2014

Y. Rekhter, J. Scudder, S. S. Ramachandra, E. Chen, and R. Fernando, **Graceful restart mechanism for BGP**, IETF, 2007

IEEE 802.1 Working Group, **IEEE Std 802.1X - 2010. Port-Based Network Access Control**, IEEE Computer Society, 2010

Security Task group of IEEE 802.1, **IEEE Std 802.1AE. Medium Access Control Security**, IEEE Computer Society, 2018

S. Kent, K. Seo, **Security Architecture for the Internet Protocol**, IETF, 2005

S. Kent, **IP Authentication Header**, IETF, 2005

S. Kent, **IP Encapsulating Security Payload**, IETF, 2005

C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, **Internet Key Exchange Protocol Version 2 (IKEv2)**, IETF, 2014

J. Cichonski, J. M. Franklin, M. Bartock, **Guide to LTE Security**, NIST Special Publication 800-187,


## Recomendaciones

### Asignaturas que se recomienda haber cursado previamente

Redes Seguras/V05M175V01105
Seguridad de la información/V05M175V01102

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Seguridad de aplicaciones** | | | | |
| Asignatura | Seguridad de aplicaciones | | | |
| Código | V05M175V01104 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 6 | OB | 1 | 1c |
| Lengua Impartición | Castellano | | | |
| Departamento | | | | |
| Coordinador/a | López Nores, Martín | | | |
| Profesorado | Bellas Permuy, Fernando<br>López Nores, Martín<br>Losada Pérez, José | | | |
| Correo-e | mlnores@det.uvigo.es | | | |
| Web | http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530005&any_academic=2020_21&idioma_assig=cast | | | |
| Descripción general | Desarrollar aplicaciones seguras no es una tarea trivial. Conocer las vulnerabilidades que habitualmente sufren las aplicaciones, los mecanismos de autenticación, autorización y control de acceso, así como la incorporación de la seguridad al ciclo de vida de desarrollo, es esencial para poder construir y mantener aplicaciones seguras con éxito. En esta materia se estudian de forma práctica todos estos aspectos, con especial énfasis en el desarrollo de aplicaciones y servicios web. | | | |

| Competencias |
|---|
| Código |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |

| Contenidos |
|---|
| Tema |

| Planificación | | | |
|---|---|---|---|
| | Horas en clase | Horas fuera de clase | Horas totales |
| *Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado | | | |

| Metodologías |
|---|
| Descripción |

| Atención personalizada |
|---|

| Evaluación | | |
|---|---|---|
| Descripción | Calificación | Resultados de Formación y Aprendizaje |

| Otros comentarios sobre la Evaluación |
|---|

| Fuentes de información |
|---|
| **Bibliografía Básica** |
| **Bibliografía Complementaria** |

| Recomendaciones |
|---|

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Redes Seguras** | | | | |
| Asignatura | Redes Seguras | | | |
| Código | V05M175V01105 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 6 | OB | 1 | 1c |
| Lengua Impartición | Castellano | | | |
| Departamento | | | | |
| Coordinador/a | Rodríguez Rubio, Raúl Fernando | | | |
| Profesorado | Nóvoa de Manuel, Francisco Javier<br>Rodríguez Rubio, Raúl Fernando | | | |
| Correo-e | rrubio@det.uvigo.es | | | |
| Web | http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530006&any_academic=2022_23&idioma_assig=cast | | | |
| Descripción general | a materia Redes Seguras tiene como objetivo principal que los estudiantes aprendan a diseñar e implementar infraestructuras de red que sean capaces de proporcionar los servicios de seguridad necesarios en un entorno corporativo moderno. Deberán conocer las arquitecturas de seguridad de referencia y ser capaces de configurarlas y administrarlas, utilizando para ello tecnologías como VPN, IDS/IPS y Firewalls, entre otras. La materia esta concebida para que las prácticas de laboratorio, con equipos físicos y virtuales tengan una importancia capital en el proceso de aprendizaje. | | | |

| Competencias |
|---|
| Código |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |

| Contenidos |
|---|
| Tema |

| Planificación | | | |
|---|---|---|---|
| | Horas en clase | Horas fuera de clase | Horas totales |
| *Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado | | | |

| Metodologías |
|---|
| Descripción |

| Atención personalizada |
|---|

| Evaluación | | |
|---|---|---|
| Descripción | Calificación | Resultados de Formación y Aprendizaje |

| Otros comentarios sobre la Evaluación |
|---|

| Fuentes de información |
|---|
| **Bibliografía Básica** |
| **Bibliografía Complementaria** |

| Recomendaciones |
|---|

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Conceptos y leyes en ciberseguridad** | | | | |
| Asignatura | Conceptos y leyes en ciberseguridad | | | |
| Código | V05M175V01201 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 3 | OB | 1 | 2c |
| Lengua Impartición | Castellano<br>Gallego<br>Inglés | | | |
| Departamento | | | | |
| Coordinador/a | Rodríguez Vázquez, Virgilio | | | |
| Profesorado | Faraldo Cabana, Patricia<br>Rodríguez Vázquez, Virgilio | | | |
| Correo-e | virxilio@uvigo.es | | | |
| Web | http://moovi.uvigo.gal/ | | | |
| Descripción general | En esta materia se hará una aproximación a la normativa relativa a la ciberseguridad. A continuación se realizará un estudio criminológico de los principales delitos informáticos. El bloque central está formado por una revisión sistemática de la regulación de los delitos informáticos contenida en el Código Penal español. Además, se analizará la jurisprudencia existente en esta materia. | | | |

| Competencias | |
|---|---|
| Código | |
| A3 | Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. |
| C3 | Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información |
| C8 | Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad |
| D1 | Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria. |
| D5 | Tener capacidad para comunicarse oralmente y por escrito en inglés. |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
| Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. | A3 |
| Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información | C3 |
| Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad. | C8 |
| Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria. | D1 |
| Tener capacidad para comunicarse oralmente y por escrito en inglés. | D5 |

| Contenidos | |
|---|---|
| Tema | |
| 1. Introducción al Derecho sobre ciberseguridad. Revisión de las normativas en materia de seguridad informática y gestión de riesgos. | 1.1. La normativa de la UE.<br>1.2. La Ley de Seguridad Nacional: la estrategia de ciberseguridad nacional y el esquema de seguridad nacional.<br>1.3. El Reglamento (UE) 2016/679 de 27 de abril de 2016, Reglamento General de Protección de Datos (RGPD). La Ley Orgánica de Protección de Datos y el Reglamento de desarrollo. El Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).<br>1.4. El Código Penal en materia de delitos informáticos. |

| | |
|---|---|
| 2. Aproximación criminológica a los delitos informáticos. | 2.1. Fuentes estadísticas: principales organismos nacionales e internacionales.<br>2.2. Análisis de los principales informes sobre cibercriminalidad.<br>2.3. Identificación de los principales recursos tecnológicos utilizados. |
| 3. La vulneración de la ciberseguridad a través de conductas delictivas. | 3.1. Precisiones terminológicas: delitos informáticos y cibercrimen<br>3.2. La utilización de las TIC para cometer delitos y cuando las TIC son el objeto del delito.<br>3.3. El Código Penal español, LO 10/1995, de 23 de noviembre, la Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, Convenio sobre cibercriminalidad o Convenio de Budapest, del Consejo de Europa, de 23 de noviembre de 2001. |
| 4. Las principales conductas delictivas que afectan a la ciberseguridad. | 4.1. Delitos de descubrimiento y revelación de secretos (I). Riesgos frecuentes: el ransomware y el robo de información.<br>4.2. Delitos de descubrimiento y revelación de secretos (II). Acceso e interceptación ilícita. El acceso a ficheros o soportes informáticos, electrónicos o telemáticos. Especial atención al responsable de los ficheros o soportes. La interceptación de transmisiones de datos informáticos. La utilización de malware (virus, troyanos y spyware).<br>4.3. Delitos de descubrimiento y revelación de secretos (III). Producir, adquirir, importar o facilitar programas informáticos para cometer los delitos anteriores o contraseñas de ordenador o códigos de acceso.<br>4.4. Delitos contra la intimidad y el derecho a la propia imagen: el uso indebido de cookies.<br>4.5. Delitos contra la propiedad (I). Estafas valiéndose de alguna manipulación informática. Producir, poseer o facilitar programas informáticos destinados a ese fin.<br>4.6. Delitos contra la propiedad (II). Defraudación utilizando señal de telecomunicaciones ajena. Uso de terminal de telecomunicaciones sin consentimiento del titular.<br>4.7. Delitos contra la propiedad (III). Daños en datos informáticos, programas informáticos o documentos electrónicos. Daños a sistemas informáticos. Daños a sistemas informáticos de una infraestructura crítica (breve referencia a los operadores de infraestructuras críticas, a los planes de seguridad del operador y a los planes de protección específicos). Obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. Fabricar, poseer o facilitar a terceros programas informáticos con tal fin. Especial referencia a la responsabilidad penal de las personas jurídicas.<br>4.8. Delitos contra la propiedad intelectual e industrial. A través de la prestación de servicios de la sociedad de la información o a través de un portal de acceso a internet.<br>4.9. Delitos relativos al mercado y a los consumidores. Descubrimiento de secretos de empresa a través de las TIC. Acceso inteligible a un servicio de radiodifusión sonoro o televisivo, a servicios interactivos prestados a distancia por vía electrónica.<br>4.10. Delitos contra la fe pública: falsedades electrónicas. |
| 5. Delitos cometidos contra las personas utilizando las TIC. | 5.1. Delitos contra la libertad. Amenazas y coacciones utilizando redes sociales u otras TIC. Ciberstalking.<br>5.2. Delitos contra la libertad e indemnidad sexuales. Child grooming y pornografía infantil.<br>5.3. Delitos contra la intimidad y la privacidad.<br>5.4. Delitos contra el honor. Lesión de la reputación digital. |
| 6. El ciberterrorismo. | 6.1. Concepto.<br>6.2. Delitos informáticos realizados con una finalidad específica del art. 573 del Código Penal.<br>6.3. Delito de colaboración con organización o grupo terrorista a través de la prestación de servicios tecnológicos. |
| 7. Delitos relativos a la Defensa nacional y otros. | Breve aproximación. |
| 8. Análisis de la jurisprudencia española en relación con delitos informáticos. | 8.1. Especial atención a la jurisprudencia del Tribunal Supremo.<br>8.2. Acuerdos del pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo relativos a delitos informáticos.<br>8.3. El Ministerio Fiscal y la Fiscalía especialista en materia de criminalidad informática. |

| **Planificación** | | | |
|---|---|---|---|
| | Horas en clase | Horas fuera de clase | Horas totales |
| Lección magistral | 13 | 32 | 45 |

| | | | |
|---|---|---|---|
| Prácticas de laboratorio | 5 | 22 | 27 |
| Examen de preguntas objetivas | 2 | 0 | 2 |
| Resolución de problemas y/o ejercicios | 1 | 0 | 1 |

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

**Metodologías**

| | Descripción |
|---|---|
| Lección magistral | Exposición por parte del profesor de los contenidos sobre la materia objeto de estudio, bases teóricas y/o directrices de un trabajo, ejercicio que el/la estudiante tiene que desarrollar |
| Prácticas de laboratorio | Actividades de aplicación de los conocimientos a situaciones concretas y de adquisición de habilidades básicas y procedimentales relacionadas con la materia objeto de estudio. |

**Atención personalizada**

| Metodologías | Descripción |
|---|---|
| Lección magistral | El alumnado será atendido nos horarios de tutorías que serán publicados en la web del Máster. Podrá atenderse, previa cita -concertada mediante correo electrónico-, o bien a través de correo electrónico o bien a través de despacho virtual en el campus remoto. |
| Prácticas de laboratorio | El alumnado será atendido nos horarios de tutorías que serán publicados en la web del Máster. Podrá atenderse, previa cita -concertada mediante correo electrónico-, o bien a través de correo electrónico o bien a través de despacho virtual en el campus remoto. |

**Evaluación**

| | Descripción | Calificación | Resultados de Formación y Aprendizaje |
|---|---|---|---|
| Examen de preguntas objetivas | El sistema de evaluación continua consistirá en tres exámenes escritos: los dos primeros, de resolución de pruebas objetivas parciales ("exámenes de preguntas objetivas", tipo test, a los que se refiere este apartado de la Guía), y el tercero, de "resolución de problemas" (referido en el siguiente apartado de la guía).<br>Los exámenes correspondientes a la "resolución de preguntas objetivas", pruebas tipo test:<br>- se celebrarán a lo largo del curso, en horario de clase magistral. La planificación de las diferentes pruebas de evaluación intermedia se aprobará en una Comisión Académica de Máster Interuniversitaria (CAMI) y estará disponible al principio del cuatrimestre.<br>- cada examen comprenderá la parte del temario que respectivamente se indique al inicio del cuatrimestre por parte del coordinador de la materia<br>- consistirán en pruebas tipo test, para cuya calificación, de 0 a 2,5 puntos cada una de ellas, las respuestas correctas suman 0,1 y las incorrectas restan 0,05, no puntuando las dejadas en blanco<br>- Ambos exámenes se ponderarán al 50% para la calificación final, correspondiendo el otro 50% a la "resolución de problemas" (que se describe en el apartado siguiente).<br>Para superar la materia por el sistema de evaluación continua es necesario que la nota resultante de los tres exámenes, de acuerdo con la ponderación indicada, sea igual o superior a 5 puntos. Quien acuda a la primera prueba parcial (al primer examen de preguntas objetivas, tipo test), manifestando así su interés por acogerse a este sistema de evaluación continua, será evaluado en esta oportunidad de acuerdo con los criterios previamente establecidos y no tendrá derecho a ser evaluado mediante un examen final que constituya el 100% de la calificación de la materia. Por lo tanto, realizada la primera prueba parcial, no es posible renunciar al sistema de evaluación continua. Si realizada la primera prueba<br>parcial, la alumna o alumno no se presentase a la siguiente o siguientes, la calificación de estas será de 0 puntos. | 50 | A3 C3 C8 D1 |

| | | | | | |
|---|---|---|---|---|---|
| Resolución de problemas y/o ejercicios | El sistema de evaluación continua consistirá en tres exámenes escritos: los dos primeros, de resolución de pruebas objetivas parciales ("exámenes de preguntas objetivas", tipo test, a los que se refiere el apartado anterior de la Guía), y el tercero, de "resolución de problemas" (referido en este apartado de la guía).<br>El citado examen correspondiente a la "resolución de problemas":<br>- Se celebrará en la fecha oficial de examen final de la convocatoria ordinaria: primera oportunidad, según el calendario oficial aprobado por la Comisión Académica del Máster en el curso 2022-2023<br>- consistirá en la resolución de uno o varios casos prácticos y se calificará de 0 a 5 puntos<br>- los problemas que planteen los casos prácticos pueden afectar a cuestiones comprendidas en la totalidad del temario<br>- Se ponderará al 50% para la calificación final, correspondiendo el otro 50% a los dos exámenes citados de preguntas objetivas, de tipo test.<br>Para superar la materia por el sistema de evaluación continua es necesario que la nota resultante de los tres exámenes, de acuerdo con la ponderación indicada, sea igual o superior a 5 puntos. Quien acuda a la primera prueba parcial, manifestando así su interés por acogerse a este sistema de evaluación continua, será evaluado en esta oportunidad de acuerdo con los criterios previamente establecidos y no tendrá derecho a ser evaluado mediante un examen final que constituya el 100% de la calificación de la materia. Por lo tanto, realizada la primera prueba parcial, non es posible renunciar al sistema de evaluación continua. Si realizada la primera pruba parcial, la alumna o alumno no se presenta a la siguiente o siguientes, la calificación de estas será de 0 puntos. | 50 | A3 | C3<br>C8 | D1<br>D5 |

**Otros comentarios sobre la Evaluación**

**1. PRIMERA OPORTUNIDADa) SISTEMA DE EVALUACIÓN CONTINUASe describe en los apartados anteriores.**
**b) SISTEMA DE EXAMEN FINAL**

Para quien no opte por el sistema de evaluación continua, la evaluación de la materia consistirá en un único examen final, en la fecha fijada en el calendario oficial aprobado por la Comisión Académica del Máster para el curso 2022-2023.

El citado examen, que comprenderá la totalidad del temario y que constituye el 100% de la calificación de la materia, constará de
dos partes, una teórica y otra práctica, que se calificarán de 0 a 5 puntos cada una de ellas. La parte teórica consistirá en pruebas tipo test, para cuya calificación las respuestas correctas suman el doble que restan las incorrectas, no puntuando las dejadas en blanco. La parte práctica consistirá en la resolución de uno o varios casos prácticos. La calificación final del examen
será la suma de las calificaciones obtenidas en cada una de las partes. Para superar la materia es necesario obtener un mínimo de 5 puntos en la suma de la calificación de ambas partes.

**2. SEGUNDA OPORTUNIDAD Y CONVOCATORIA EXTRAORDINARIA**

La evaluación de la materia consistirá en un único exame final, en la fecha fijada en el calendario oficial aprobado por la Comisión Académica del Máster para el curso 2022-2023.

El citado examen, que comprenderá la totalidad del temario y que constituye el 100% de la calificación de la materia, constará de
dos partes, una teórica y otra práctica, que se calificarán de 0 a 5 puntos cada una de ellas. La parte teórica consistirá en pruebas tipo test, para cuya calificación las respuestas correctas suman el doble que restan las incorrectas, no puntuando las dejadas en blanco. La parte práctica consistirá en la resolución de uno o varios casos prácticos. La calificación final del examen
será la suma de las calificaciones obtenidas en cada una de las partes. Para superar la materia es necesario obtener un mínimo de 5 puntos en la suma de la calificación de ambas partes.

**Fuentes de información**

**Bibliografía Básica**

DE LA CUESTA ARZAMANDI, José Luis (dir.), **Derecho penal informático**, 1.ª, Civitas, 2010

LUZÓN PEÑA, Diego-Manuel (dir.), **Código Penal**, 5.ª, Reus, 2017

**Bibliografía Complementaria**

BARONA VILAR, Silvia, **Justicia civil y penal en la era global**, 1.ª, Tirant lo Blanch, 2017

BARRIO ANDRÉS, Moisés, **Ciberdelitos : amenazas criminales del ciberespacio : adaptado reforma Código Penal 2015**, 1.ª, Reus, 2017

CRESPO SANCHÍS, Carolina (coord.), **Fraude electrónico : panorámica actual y medios jurídicos para combatirlo**, 1.ª, Civitas, 2013

CRUZ DE PABLO, José Antonio, **Derecho penal y nuevas tecnologías : aspectos sustantivos : adaptado a la reforma operada en el Código penal por la Ley orgánica 15-2003 de 25 de noviembre, especial referencia al arículo 286 CP**, 1.ª, Difusión Jurídica y Temas de actualidad, 2006

CUERDA ARNAU, María Luisa (coord.), **Menores y redes sociales : ciberbullying, ciberstalking, cibergrooming, pornografía, sexting, radicalización y otras formas de violencia en la red**, 1.ª, Tirant lo Blanch, 2016

DAVARA RODRÍGUEZ, Miguel Ángel, **Manual de derecho informático**, 11.ª, Thomson-Aranzadi, 2015

DE NOVA LABIÁN, Alberto José, **Delitos contra la propiedad intelectual en el ámbito de Internet : especial referencia a los sistemas de intercambio de archivos**, 1.ª, Dykinson, 2010

DE URBANO CASTRILLO, Eduardo et al., **Delincuencia informática : tiempos de cautela y amparo**, 1.ª, Aranzadi, 2012

FARALDO CABANA, Patricia, **Las Nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico**, 1.ª, Tirant lo Blanch, 2009

FERNÁNDEZ TERUELO, Javier Gustavo, **Cibercrimen, los delitos cometidos a través de Internet : estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y ot**, 1.ª, Constitutio Criminalis Carolina, 2017

FLORES PRADA, Ignacio, **Criminalidad informática : (aspectos sustantivos y procesales)**, 1.ª, Tirant lo Blanch, 2012

GALÁN MUÑOZ, Alfonso, **El Fraude y la estafa mediante sistemas informáticos : análisis del artículo 248.2 C.P**, 1.ª, Tirant lo Blanch, 2005

GIANT, Nikki, **Ciberseguridad para la i-generación : usos y riesgos de las redes sociales y sus aplicaciones**, 1.ª, Narcea, 2016

GÓMEZ RIVERO, M.ª del Carmen (dir.), **Nociones fundamentales de Derecho penal. Parte especial. Volumen I**, 2.ª, Tecnos, 2015

GÓMEZ RIVERO, M.ª del Carmen (dir.), **Nociones fundamentales de Derecho penal. Parte especial. Volumen II**, 2.ª, Tecnos, 2015

GÓMEZ TOMILLO, Manuel, **Responsabilidad penal y civil por delitos cometidos a través de Internet : especial consideración del caso de los proveedores de contenidos, servicios, acceso y enlaces**, 2.ª, Thomson-Aranzadi, 2006

GONZÁLEZ CUSSAC, José Luis (coord.), **Derecho penal. Parte especial**, 5.ª, Tirant lo Blanch, 2016

GONZÁLEZ CUSSAC, José Luis/CUERDA ARNAU, M.ª Luisa (dirs.), **Nuevas amenazas a la seguridad nacional : terrorismo, criminalidad organizada y tecnologías de la información y la comunicación**, 1.ª, Tirant lo Blanch, 2013

GOODMAN, Marc, **Future crimes : inside the digital underground and the battle for our connected world**, 1.ª, Pegasus Books, 2016

HILGENDORF, Eric, **Computer- und Internetstrafrecht : ein Grundriss**, 1.ª, Springer, 2005

Instituto Español de Estudios Estratégicos, Grupo de Trabajo número 03/10, **Ciberseguridad : retos y amenazas a la seguridad nacional en el ciberespacio**, 1.ª, Ministerio de Defensa, Dirección General de Relaci, 2011

LUZÓN PEÑA, Diego-Manuel, **Lecciones de Derecho penal. Parte general**, 3.ª, Tirant lo Blanch, 2016

MARZILLI, Alan, **The Internet and crime**, 1.ª, Chelsea House, 2010

MATA Y MARTÍN, Ricardo M., **Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago : el uso fraudulento de tarjetas y otros instrumentos de pago**, 1.ª, Thomson-Aranzadi, 2007

MORÓN LERMA, Esther, **Internet y derecho penal : "hacking" y otras conductas ilícitas en la red**, 2.ª, Aranzadi, 2002

MUÑOZ CONDE, Francisco/GARCÍA ARÁN, Mercedes, **Derecho penal. Parte general**, 9.ª, Tirant lo Blanch, 2015

ORENES, Eduardo, **Ciberseguridad familiar : cyberbullying, hacking y otros peligros en Internet**, 1.ª, Círculo Rojo, 2013

ORTS BERENGUER, Enrique/ROIG TORRES, Margarita, **Delitos informáticos y delitos comunes cometidos a través de la informática**, 1.ª, Tirant lo Blanch, 2001

QUERALT JIMÉNEZ, Joan Josep, **Derecho penal español. Parte especial**, 7.ª, Tirant lo Blanch, 2015

QUINTERO OLIVARES, Gonzalo (dir.), **Comentarios a la Parte especial del Derecho penal**, 10.ª, Aranzadi, 2016

RALLO LOMBARTE, Artemi, **El derecho al olvido en Internet : Google**, 1.ª, Centro de Estudios Políticos y Constitucionales, 2014

RODRÍGUEZ MESA, M.ª José, **Los delitos de daños**, 1.ª, Tirant lo Blanch, 2017

ROMEO CASABONA, Carlos M.ª (coord.), **El Cibercrimen : nuevos retos jurídico-penales, nuevas respuestas político-criminales**, 1.ª, Comares, 2006

RUEDA MARTÍN, M.ª Ángeles, **Protección penal de la intimidad personal e informática : (los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código penal)**, 1.ª, Atelier, 2004

SAIN, Gustavo, **Delitos informáticos : investigación criminal, marco legal y peritaje**, 1.ª, B de f, 2017

SÁINZ PEÑA, Rosa M.ª (coord.), **Ciberseguridad, la protección de la información en un mundo digital**, 1.ª, Fundación Telefónica, Ariel, 2016

SEGURA SERRANO, Antonio/GORDO GARCÍA, Fernando (coords.), **Ciberseguridad global : oportunidades y compromisos en el uso del ciberespacio**, 1.ª, Universidad de Granada, 2013

SILVA SÁNCHEZ, Jesús María (dir.)/RAGUÉS I VALLÉS, Ramón (coord.), **Lecciones de Derecho penal: Parte especial**, 5.ª, Atelier, 2018

SINGER, Peter Warren, **Cybersecurity and cyberwar : what everyone needs to know**, 1.ª, Oxford University Press, 2014

TOURIÑO, Alejandro, **El derecho al olvido y a la intimidad en Internet**, 1.ª, Los Libros de la Catarata, 2014

VALLS PRIETO, Javier, **Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial**, 1.ª, Dykinson, 2017

VELASCO NÚÑEZ, Eloy (dir.), **Delitos contra y a través de las nuevas tecnologías : ¿cómo reducir su impunidad?**, 1.ª, Consejo General del Poder Judicial,Centro de Docu, 2006

VELASCOS SAN MARTÍN, Cristos, **La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet**, 1.ª, Tirant lo Blanch, 2012

WALDEN, Ian, **Computer crimes and digital investigations**, 1.ª, Oxford University Press, 2007

## Recomendaciones

### Asignaturas que se recomienda haber cursado previamente

Gestión de la seguridad de la información/V05M175V01101

## DATOS IDENTIFICATIVOS

**Fortificación de sistemas operativos**

| | | | | |
|---|---|---|---|---|
| Asignatura | Fortificación de sistemas operativos | | | |
| Código | V05M175V01202 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 5 | OB | 1 | 1c |
| Lengua Impartición | Castellano | | | |
| Departamento | | | | |
| Coordinador/a | Blanco Fernández, Yolanda | | | |
| Profesorado | Blanco Fernández, Yolanda<br>Yáñez Izquierdo, Antonio Fermín | | | |
| Correo-e | yolanda@det.uvigo.es | | | |
| Web | http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530007&any_academic=2021_22&idioma_assig=eng | | | |
| Descripción general | A newly installed Operating system is inherently insecure. It has a certain number of vulnerabilities, depending on such things such as the age of the O.S., the amount of services it provides, the existence of initial backdoors not already patched, and the use of default policies designed without security in mind By Hardening Operating Systems we refer to the act of configuring an operating system with the aim of making it as secure as possible, so thet we minimize the risk of getting it compromised. This usually implies applying patches, changing default O.S. policies, and removing (or disabling) non-essential aplications and/or services. In this course we'll try to identify common O.S. vulnerabilities and how to defend the O.S. against them. Both UNIX (linux) and Windows type O.S. will be considered. | | | |

## Competencias

| Código |
|---|

## Resultados de aprendizaje

| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
|---|---|

## Contenidos

| Tema |
|---|

## Planificación

| | Horas en clase | Horas fuera de clase | Horas totales |
|---|---|---|---|

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

## Metodologías

| | Descripción |
|---|---|

## Atención personalizada

## Evaluación

| Descripción | Calificación | Resultados de Formación y Aprendizaje |
|---|---|---|

## Otros comentarios sobre la Evaluación

## Fuentes de información

**Bibliografía Básica**

**Bibliografía Complementaria**

## Recomendaciones

## DATOS IDENTIFICATIVOS

### Tests de intrusión

| | | | | |
|---|---|---|---|---|
| Asignatura | Tests de intrusión | | | |
| Código | V05M175V01203 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 5 | OB | 1 | 2c |
| Lengua Impartición | Castellano | | | |
| Departamento | | | | |
| Coordinador/a | Costa Montenegro, Enrique | | | |
| Profesorado | Carballal Mato, Adrián<br>Costa Montenegro, Enrique | | | |
| Correo-e | kike@gti.uvigo.es | | | |
| Web | http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530008&idioma=cast&idioma_assig=cast&any_academic=2022_23 | | | |
| Descripción general | No hay una mejor forma de probar la fortaleza de un sistema que atacarlo. Los Test de Intrusión sirven para reproducir intentos de acceso de un atacante valiéndose de las vulnerabilidades que puedan existir en una determinada infraestructura. En este curso se cubrirán los temas fundamentales orientados a los test de intrusión (pentesting) cubriendo las distintas fases de un ataque y explotación (desde el reconocimiento y el control de acceso hasta el borrado de huellas). | | | |

## Competencias

| Código |
|---|

## Resultados de aprendizaje

| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
|---|---|

## Contenidos

| Tema |
|---|

## Planificación

| | Horas en clase | Horas fuera de clase | Horas totales |
|---|---|---|---|

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

## Metodologías

| | Descripción |
|---|---|

## Atención personalizada

## Evaluación

| Descripción | Calificación | Resultados de Formación y Aprendizaje |
|---|---|---|

## Otros comentarios sobre la Evaluación

## Fuentes de información

### Bibliografía Básica

### Bibliografía Complementaria

## Recomendaciones

## DATOS IDENTIFICATIVOS

**Análisis de malware**

| | | | | |
|---|---|---|---|---|
| Asignatura | Análisis de malware | | | |
| Código | V05M175V01204 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 5 | OB | 1 | 2c |
| Lengua Impartición | Inglés | | | |
| Departamento | | | | |
| Coordinador/a | Burguillo Rial, Juan Carlos | | | |
| Profesorado | Burguillo Rial, Juan Carlos<br>Hernández Pereira, Elena María<br>Rivas López, Jose Luis | | | |
| Correo-e | jrial@uvigo.es | | | |
| Web | http://moovi.uvigo.gal/ | | | |
| Descripción general | El malware utiliza los sistemas y las redes de comunicaciones para propagar virus, secuestrar dispositivos o robar datos confidenciales. El objetivo de esta asignatura es dotar al alumno de la capacidad para analizar, detectar y eliminar malware. Para ello se explorarán y ejemplificarán, de forma práctica y con casos reales, las técnicas actuales de ocultación y persistencia de malware, así como las tendencias más novedosas para su detección y eliminación.<br><br>Esta asignatura se impartirá en inglés. | | | |

## Competencias

| Código | |
|---|---|
| A1 | Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación. |
| B1 | Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación |
| C8 | Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad |
| C11 | Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones. |
| C13 | Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes |
| D4 | Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad |
| D5 | Tener capacidad para comunicarse oralmente y por escrito en inglés. |

## Resultados de aprendizaje

| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
|---|---|
| Analizar, detectar y eliminar malware en sistemas y redes. | B1<br>C11<br>C13<br>D5 |
| Conocer, detectar y luchar contra las técnicas de ocultación y persistencia de malware en sistemas y redes. | A1<br>B1<br>C8<br>C11<br>C13<br>D5 |
| Estudiar sistemas y redes para detectar y eliminar las vulnerabilidades susceptibles de ser utilizadas por el malware. | B1<br>C8<br>C11<br>C13<br>D5 |
| Conocer las tendencias actuales en malware y las experiencias aprendidas de casos reales. | A1<br>B1<br>D4<br>D5 |

## Contenidos

| Tema | |
|---|---|
| Introducción al análisis e ingeniería de malware. | a) ¿Qué es el malware?<br>b) ¿Cómo detectarlo y eliminarlo?<br>c) ¿En qué consiste la ingeniería de malware? |
| Tipos de malware. | a) Estructura.<br>b) Componentes.<br>c) Vectores de infección. |
| Ingeniería de malware. | a) Técnicas de propagación.<br>b) Procesos de infección.<br>c) Persistencia del malware.<br>d) Técnicas de ocultación. |
| Ingeniería inversa de malware. | a) ¿Cómo analizar e inferir el funcionamiento del malware?<br>b) Comprensión del funcionamiento de nuevos tipos de malware. |
| Herramientas de análisis de malware. | a) Herramientas para la detección de malware.<br>b) Herramientas para la eliminación de malware. |

**Planificación**

| | Horas en clase | Horas fuera de clase | Horas totales |
|---|---|---|---|
| Actividades introductorias | 2 | 2 | 4 |
| Lección magistral | 10 | 30 | 40 |
| Prácticas de laboratorio | 15 | 40 | 55 |
| Foros de discusión | 0 | 2 | 2 |
| Estudio de casos | 5 | 4 | 9 |
| Examen de preguntas objetivas | 2 | 4 | 6 |
| Resolución de problemas y/o ejercicios | 3 | 6 | 9 |

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

**Metodologías**

| | Descripción |
|---|---|
| Actividades introductorias | Hacer una introducción genérica a los objetivos, contenidos globales generales de la asignatura y resultados esperados. Esta actividad será realizada individualmente. |
| Lección magistral | Se introducen los distintos temas de la asignatura proporcionando el material docente necesario para su seguimiento.<br><br>Con esta metodología se trabajan las competencias CB1, CG1, CE8, CE11, CE13, CT4 y CT5. Esta actividad será realizada individualmente. |
| Prácticas de laboratorio | Se realizan prácticas de laboratorio para comprender mejor los contenidos vistos en las clases magistrales.<br><br>Con esta metodología se trabajan las competencias CG1, CE8, CE11, CE13 y CT5. Algunas prácticas se realizarán de forma individual y otras en grupos (dependiendo del número de estudiantes). |
| Foros de discusión | Los estudiantes deben participar en el foro dentro de la plataforma MOOVI.<br><br>Con esta metodología se trabajan las competencias CE8, CE11, CE13 y CT5. Esta actividad será realizada individualmente. |
| Estudio de casos | Durante las clases magistrales se realizarán presentaciones de casos de estudio típicos de amenazas, problemas de seguridad conocidos o tecnologías actuales.<br><br>Con esta metodología se trabajan las competencias CG1, CE11, CE13 y CT5. Esta actividad se realizará en grupo. |

**Atención personalizada**

| Metodologías | Descripción |
|---|---|
| Actividades introductorias | En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. |

| | |
|---|---|
| Lección magistral | En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. |
| Estudio de casos | En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. |
| Prácticas de laboratorio | En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. |
| Foros de discusión | En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. |

## Evaluación

| | Descripción | Calificación | Resultados de Formación y Aprendizaje | | | |
|---|---|---|---|---|---|---|
| Prácticas de laboratorio | Los alumnos realizarán prácticas de laboratorio, donde se trabajará con los conceptos estudiados en las clases teóricas. | 45 | A1 | B1 | C8 C11 C13 | D5 |
| Foros de discusión | Los estudiantes deben participar en el foro de la plataforma MOOVI. | 5 | A1 | B1 | C11 C13 | D4 D5 |
| Estudio de casos | El alumnado realizará presentaciones de casos de estudio, seleccionados por ellos, para analizar amenazas actuales. | 15 | | B1 | C11 C13 | D5 |
| Examen de preguntas objetivas | Dos test de evaluación sucesivos para el contenido parcial de la materia impartida hasta ese momento. Los tests serán individuales y de tiempo limitado. | 30 | A1 | B1 | C11 C13 | D5 |
| Resolución de problemas y/o ejercicios | Durante las clases magistrales se realizarán preguntas a los estudiantes para conocer su comprensión del tema bajo estudio. | 5 | A1 | | C11 C13 | D5 |

## Otros comentarios sobre la Evaluación

Los elementos que forman parte de la evaluación de la asignatura son los siguientes:
- **Cuestionarios**: a lo largo del curso se realizarán dos cuestionarios que aportarán un 15% de la nota final (cada uno).
- **Presentación de casos de estudio**: cada alumno deberá realizar una presentación original que aportará un 15% de la nota final.
- **Prácticas de laboratorio**: cada alumno deberá realizar individualmente y/o en grupo un conjunto de prácticas propuestas en el laboratorio que aportará un 45% de la nota final.
- **Participación en clase**: los estudiantes participarán y discutirán sobre las exposiciones realizadas por el profesor y esto contribuirá hasta un 5% a la nota final.
- **Participación en el foro**: los estudiantes deben participar en el foro de la asignatura, de forma individual, y esto contribuirá hasta un 5% a la nota final. Para conseguir dicho porcentaje se deben proporcionar, como mínimo, dos contribuciones relevantes.

Así tenemos:
**Nota Final** = Cuestionarios (2x15 = 30%) + Presentación de caso de estudio (15%) + Prácticas de lab. (45%) + Participación en clase (5%) + Foro (5%) = 100%.
Los estudiantes deben obtener al menos 4 puntos sobre 10 en la nota de los cuestionarios y la práctica para poder calcular la nota media final. Si cualquiera de estas notas estuviese por debajo de 4, entonces la nota final obtenida nunca será superior a un 4 sobre 10.
La planificación de las diferentes pruebas de evaluación intermedia se aprobará en una Comisión Académica de Máster (CAM) y estará disponible al principio del cuatrimestre.
En caso de detección de plagio en cualquiera de las pruebas (pruebas cortas, exámenes parciales o examen final), la

calificación final será de SUSPENSO (0) y el hecho será comunicado a la dirección del Centro para los efectos oportunos.
Siguiendo las directrices propias de la titulación se ofrecerá a los alumnos que cursen esta materia dos sistemas de evaluación: evaluación continua y evaluación única (fin del cuatrimestre).
**Evaluación continua**: el estudiante sigue la evaluación continua desde el momento en que se presenta a dos cuestionarios de la asignatura. Un alumno que opta por la evaluación continua se considera que se ha presentado a la asignatura, independientemente de que se presente o no a la evaluación única.
**Evaluación única**: el alumno deberá realizar un examen teórico que sustituye a los cuestionarios realizados a lo largo del curso, además de entregar las prácticas y los trabajos equivalentes a los que se han realizado como parte de la evaluación continua.
**Segunda oportunidad**: el alumno deberá realizar la parte que no haya superado. En el caso de no haber superado los cuestionarios deberá realizar un examen equivalente.
Los trabajos y tareas prácticas propuestas y realizadas en este curso no son recuperables y sólo son válidas para el curso actual.

## Fuentes de información

### Bibliografía Básica

Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, **The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory**, 1, John Wiley & Sons Inc, 2014

Michael Sikorski / Andrew Honig, **Practical Malware Analysis**, 1, William Pollock, 2012

### Bibliografía Complementaria

## Recomendaciones

### Asignaturas que se recomienda cursar simultáneamente

Análisis forense de equipos/V05M175V01207
Fortificación de sistemas operativos/V05M175V01202
Seguridad en dispositivos móviles/V05M175V01206

### Asignaturas que se recomienda haber cursado previamente

Seguridad de aplicaciones/V05M175V01104

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Seguridad como negocio** | | | | |
| Asignatura | Seguridad como negocio | | | |
| Código | V05M175V01205 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 3 | OB | 1 | 2c |
| Lengua Impartición | Castellano | | | |
| Departamento | | | | |
| Coordinador/a | Fernández Vilas, Ana | | | |
| Profesorado | Carneiro Díaz, Victor Manuel<br>Fernández Vilas, Ana | | | |
| Correo-e | avilas@det.uvigo.es | | | |
| Web | http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530010&any_academic=2022_23&idioma_assig=cast | | | |
| Descripción general | Seguridad como negocio aborda las competencias necesarias para comprender el funcionamiento de un Security Operation Centre (SOC), desde el punto de vista tecnológico, operacional y de inteligencia. Se profundizará en la infraestructura, organización, operación y mecanismos de métrica necesarios para la explotación empresarial de los servicios asociados a un SOC. Se estudiarán diferentes entornos de especialización como el sector bancario, administración pública o el ámbito militar. CONSULTA DE LA GUÍA EN UDC. | | | |

| Competencias |
|---|
| Código |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |

| Contenidos |
|---|
| Tema |

| Planificación | | | |
|---|---|---|---|
| | Horas en clase | Horas fuera de clase | Horas totales |
| *Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado | | | |

| Metodologías | |
|---|---|
| | Descripción |

| Atención personalizada |
|---|

| Evaluación | | |
|---|---|---|
| Descripción | Calificación | Resultados de Formación y Aprendizaje |

| Otros comentarios sobre la Evaluación |
|---|

| Fuentes de información |
|---|
| **Bibliografía Básica** |
| **Bibliografía Complementaria** |

| Recomendaciones |
|---|

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Seguridad en dispositivos móviles** | | | | |
| Asignatura | Seguridad en dispositivos móviles | | | |
| Código | V05M175V01206 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 3 | OP | 1 | 2c |
| Lengua Impartición | Castellano<br>Gallego<br>Inglés | | | |
| Departamento | | | | |
| Coordinador/a | López Bravo, Cristina | | | |
| Profesorado | Fernández Caramés, Tiago Manuel<br>López Bravo, Cristina<br>Rivas López, Jose Luis | | | |
| Correo-e | clbravo@det.uvigo.es | | | |
| Web | http://moovi.uvigo.gal | | | |
| Descripción general | En esta asignatura se muestra una visión general de la seguridad en dispositivos móviles con diferentes características. Partiendo del estudio de la arquitectura de estos dispositivos, descubriremos su funcionamiento interno y cuáles son las principales herramientas de seguridad que incluyen, junto con los riesgos y amenazas que sufren. Estudiaremos cómo encontrar, analizar y mitigar las vulnerabilidades que afectan a los dispositivos móviles, usando herramientas de análisis forense, de desarrollo de aplicaciones seguras y de gestión de dispositivos en entornos empresariales.<br><br>La documentación de esta materia estará en inglés. | | | |

| Competencias | |
|---|---|
| Código | |
| A2 | Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio |
| A3 | Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. |
| A4 | Que los estudiantes sepan comunicar sus conclusiones ---y los conocimientos y razones últimas que las sustentan--- a públicos especializados y no especializados de un modo claro y sin ambigüedades |
| B1 | Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación |
| B2 | Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones. |
| B5 | Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos |
| C4 | Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información |
| C6 | Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad |
| C9 | Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados |
| C15 | Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de estos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad. |
| D4 | Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad |
| D5 | Tener capacidad para comunicarse oralmente y por escrito en inglés. |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |

| | |
|---|---|
| Conocer los conceptos fundamentales asociados con la seguridad en los sistemas operativos móviles y el desarrollo de apps seguras. | A2<br>B1<br>C4<br>C15<br>D4<br>D5 |
| Identificar una app con comportamiento malicioso y vulnerabilidades en sistemas operativos y apps | A4<br>B2<br>C4<br>D4<br>D5 |
| Ser capaz de realizar un análisis forense de un dispositivo móvil | A3<br>B2<br>C6<br>D5 |
| Conocer los sistemas gestión de dispositivos móviles | A2<br>B1<br>B2<br>B5<br>C9<br>D5 |

| **Contenidos** | |
|---|---|
| Tema | |
| Introducción: Amenazas y vulnerabilidades que afectan a los dispositivos móviles | |
| Arquitecturas de dispositivos móviles | |
| Modelos de seguridad de dispositivos móviles | |
| Desarrollo de aplicaciones seguras | Permisos<br>Gestión de paquetes<br>Gestión de usuarios<br>APIs |
| Seguridad de los datos | |
| Seguridad de los dispositivos | |
| Seguridad de la red | |
| Vulnerabilidades, exploits y aplicaciones maliciosas | |
| Análisis forense de sistemas operativos móviles | |
| Sistemas para la gestión de la movilidad empresarial (EMM) | |

**Planificación**

| | Horas en clase | Horas fuera de clase | Horas totales |
|---|---|---|---|
| Lección magistral | 9 | 9 | 18 |
| Prácticas con apoyo de las TIC | 10 | 10 | 20 |
| Examen de preguntas objetivas | 2 | 14 | 16 |
| Resolución de problemas y/o ejercicios | 0 | 11 | 11 |
| Informe de prácticas, prácticum y prácticas externas | 0 | 10 | 10 |

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

**Metodologías**

| | Descripción |
|---|---|
| Lección magistral | Exposición, por parte del profesorado, de los principales contenidos teóricos relacionados con la seguridad en dispositivos móviles. Con esta metodología se contribuirá a la adquisición de las competencias CB3, CG1, CE4, CE15, CT4 y CT5. |
| Prácticas con apoyo de las TIC | Realización por parte del alumnado de prácticas guiadas y supervisadas. Con esta metodología se trabajarán las competencias CG2, CG5, CB2, CB4, CE4, CE6, CE9 y CT5. |

**Atención personalizada**

| **Metodologías** | **Descripción** |
|---|---|

| | |
|---|---|
| Prácticas con apoyo de las TIC | El conjunto de profesores de la materia proporcionará atención individual y personalizada a los alumnos y alumnas durante el curso, solucionando sus dudas y preguntas. Así mismo, el profesorado orientará y guiará al alumnado durante la realización de las tareas que tienen asignadas en las prácticas con apoyo de las TIC. Las dudas se atenderán de forma presencial o telemática (durante las propias prácticas, durante el horario establecido para las tutorías o durante el horario acordado con los alumnos y alumnas para tutorías). El horario de tutorías se fijará al inicio del curso y se publicará en la página web de la asignatura. Fuera de este horario, será necesario reservar las tutorías mediante cita previa. |
| Lección magistral | El conjunto del profesores de la materia proporcionará atención individual y personalizada a los alumnos y alumnas durante el curso, solucionando sus dudas y preguntas. Las dudas se atenderán de forma presencial o telemática (durante la propia sesión magistral, durante el horario establecido para las tutorías o durante el horario acordado con los alumnos y alumnas para tutorías). El horario de tutorías se fijará al inicio del curso, y se publicará en la web de la asignatura. Fuera de este horario, será necesario reservar las tutorías mediante cita previa. |

## Evaluación

| | Descripción | Calificación | Resultados de Formación y Aprendizaje | | | |
|---|---|---|---|---|---|---|
| Examen de preguntas objetivas | Examen de preguntas cortas sobre los contenidos teóricos y prácticos revisados a lo largo del curso, tanto en las sesiones magistrales como en las prácticas de laboratorio. Este examen se realizará al final del bimestre. | 50 | A3<br>A4 | | C4 | |
| Resolución de problemas y/o ejercicios | Resolución de problemas en los que se haga uso de los conocimientos adquiridos tanto en las sesiones de teoría como de prácticas. Esta prueba se realizará a lo largo del bimestre, con entregas parciales en las fechas indicadas por el profesorado. | 20 | A2<br>A4 | B1<br>B2 | C4 | |
| Informe de prácticas, prácticum y prácticas externas | El alumnado completará de forma individual cuestionarios y/o informes de prácticas donde se mostrará la correcta realización y comprensión de las prácticas. | 30 | A4 | B5 | C4<br>C6<br>C9<br>C15 | D4 |

## Otros comentarios sobre la Evaluación

**PRIMERA OPORTUNIDAD**

Siguiendo las directrices propias de la titulación se ofertará a quienes cursen esta materia dos sistemas de evaluación: evaluación continua y evaluación única.

Antes de que finalice la segunda semana del curso, los estudiantes deberán indicar al profesorado de la asignatura el sistema de evaluación elegido. Quienes opten por el sistema de evaluación continua no podrán ser calificados como "no presentados" si realizan una entrega o prueba de evaluación con posterioridad a la comunicación de su decisión.

**Sistema de evaluación continua**

La calificación global de la asignatura será igual a la media aritmética ponderada de las pruebas indicadas previamente. Para superar la asignatura la calificación global debe ser mayor o igual que cinco.

**Sistema de evaluación única**

La calificación global de la asignatura será igual a la media aritmética ponderada de las tareas indicadas previamante. En este caso, la prueba de resolución de problemas se hará en un única prueba al finalizar el bimestre. Para superar la asignatura la calificación global debe ser mayor o igual que cinco.

**SEGUNDA OPORTUNIDAD**

La evaluación consistirá en realizar un examen de preguntas objetivas, un examen de resolución de problemas y entregar los informes de prácticas de todas las prácticas realizadas a lo largo del curso.

**OTROS COMENTARIOS**

Las puntuaciones obtenidas solo son válidas para el curso académico en vigor.

El uso de cualquier material durante la realización de los exámenes y pruebas de evaluación tendrá que ser autorizado explícitamente por el profesorado de la asignatura.

En caso de detección de plagio en alguno de los trabajos/pruebas realizadas la calificación final de la asignatura será de

suspenso (0) y los profesores comunicarán a la dirección de la escuela el asunto para que tome las medidas que considere oportunas.

## Fuentes de información

### Bibliografía Básica

Dominic Chell, **The mobile application hacker´s handbook**, 1, Jonh Wiley & Sons, 2015

### Bibliografía Complementaria

Joshua Drake, **Android hacker's handbook**, 1, John Wiley & Sons, 2014

Charles Miller, **iOS hacker's handbook**, 1, John Wiley & Sons, 2012

Abhishek Dubey, Anmol Misra, **Android security: attacks and defenses**, 1, CRC Press, 2013

David Thiel, **iOS application security: the definitive guide for hackers and developers**, 1, No Starch Press, 2016

Nikolay Elenkov, **Android security internals: an in-depth guide to Android's security architecture**, 1, No Starch Press, 2015

Andrew Hoog, **iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices**, 1, Syngress/Elsevier, 2011

## Recomendaciones

### Otros comentarios

Se recomienda tener conocimientos básicos sobre el S.O. Linux y conocimientos de programación en Java. Así mismo, si bien no es imprescindible, se recomienda tener conocimientos de programación de dispositivos móviles Android.

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Análisis forense de equipos** | | | | |
| Asignatura | Análisis forense de equipos | | | |
| Código | V05M175V01207 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 3 | OP | 1 | 2c |
| Lengua Impartición | Castellano | | | |
| Departamento | | | | |
| Coordinador/a | Suárez González, Andrés | | | |
| Profesorado | Suárez González, Andrés<br>Vázquez Naya, José Manuel | | | |
| Correo-e | asuarez@det.uvigo.es | | | |
| Web | http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530012&any_academic=2020_21&any_academic=2020_21 | | | |
| Descripción general | El análisis forense de equipos consiste en la aplicación de técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. La materia "Análisis Forense de Equipos" tiene una fuerte componente práctica. Se comenzará con una introducción a este campo, explicando conceptos clave. A continuación, se estudiarán fundamentos y metodologías de análisis forense desde un punto de vista genérico y aplicable a nuevos casos, pero también se estudiarán ejemplos concretos basados en casos reales. Paralelamente, en las prácticas de laboratorio el/la alumno/a aprenderá a manejar diferentes herramientas de análisis forense y realizará prácticas simulando problemas reales. | | | |

| Competencias |
|---|
| Código |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
| Nueva | |

| Contenidos |
|---|
| Tema |

| Planificación | | | |
|---|---|---|---|
| | Horas en clase | Horas fuera de clase | Horas totales |
| *Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado | | | |

| Metodologías |
|---|
| Descripción |

| Atención personalizada |
|---|

| Evaluación | | |
|---|---|---|
| Descripción | Calificación | Resultados de Formación y Aprendizaje |

| Otros comentarios sobre la Evaluación |
|---|

| Fuentes de información |
|---|
| **Bibliografía Básica** |
| **Bibliografía Complementaria** |

| Recomendaciones |
|---|

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Seguridad ubicua** | | | | |
| Asignatura | Seguridad ubicua | | | |
| Código | V05M175V01208 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 3 | OP | 1 | 2c |
| Lengua Impartición | Castellano<br>Gallego | | | |
| Departamento | | | | |
| Coordinador/a | Gil Castiñeira, Felipe José | | | |
| Profesorado | Gil Castiñeira, Felipe José<br>Martínez Pérez, María<br>Rabuñal Dopico, Juan Ramón | | | |
| Correo-e | felipe@uvigo.es | | | |
| Web | http://moovi.uvigo.gal | | | |
| Descripción general | Los dispositivos inteligentes nos están proporcionando cada vez más servicios casi sin que seamos conscientes de su presencia: el coche ha dejado de ser una máquina simplemente mecánica para convertirse en un sistema conectado y con un enorme control electrónico; en los hoteles ya no utilizamos una llave, sino que podemos abrir nuestra habitación con una tarjeta o incluso con el móvil; los termostatos de nuestra casa se pueden conectar con un servicio de predicción meteorológica y adecuarse al tiempo de las próxima horas. Son todos ejemplos de las aplicaciones que permiten las tecnologías "embedded", las redes de comunicación inalámbricas, y en definitiva, la "Internet of Things" (IoT). Esta asignatura analiza los problemas y las mejores prácticas a la hora de hacer que este tipo de sistemas sean seguros. | | | |

| Competencias | |
|---|---|
| Código | |
| A2 | Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio |
| A3 | Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. |
| A4 | Que los estudiantes sepan comunicar sus conclusiones ---y los conocimientos y razones últimas que las sustentan--- a públicos especializados y no especializados de un modo claro y sin ambigüedades |
| B1 | Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación |
| B2 | Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones. |
| B5 | Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos |
| C4 | Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información |
| C9 | Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados |
| D4 | Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad |
| D5 | Tener capacidad para comunicarse oralmente y por escrito en inglés. |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
| Conocer la seguridad en las diferentes capas relacionadas con los sistemas ubicuos y las tecnologías que se utilizan. | A2<br>A3<br>A4<br>B1<br>B2<br>B5<br>C4<br>C9<br>D4<br>D5 |

| | |
|---|---|
| Entender los problemas de seguridad asociados al mundo ubicuo. | A2<br>A3<br>A4<br>B1<br>B2<br>B5<br>C4<br>C9<br>D4<br>D5 |
| Conocer casos reales de ataques a sistemas ubicuos. | A2<br>A3<br>A4<br>B5<br>C4<br>D4<br>D5 |

| **Contenidos** | |
|---|---|
| Tema | |
| Seguridad física | Elementos de hardware. Componentes.<br>- Buses de comunicación.<br>- Interfaces.<br>- Hardware criptográfico.<br>Ataques. |
| Seguridad en el middleware | Seguridad en el proceso de arranque.<br>Seguridad en el sistema operativo.<br>Control de acceso.<br>Cifrado.<br>Actualización del firmware. |
| Seguridad en las comunicaciones | Comunicaciones inalámbricas.<br>Riesgos y amenazas en las comunicaciones. |
| Seguridad en la percepción del entorno | Ataques en los sistemas de posicionamiento.<br>Ataques a las medidas de los sensores.<br>Privacidad. |

| **Planificación** | | | |
|---|---|---|---|
| | Horas en clase | Horas fuera de clase | Horas totales |
| Aprendizaje basado en proyectos | 10 | 35 | 45 |
| Lección magistral | 10 | 20 | 30 |
| *Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado | | | |

| **Metodologías** | |
|---|---|
| | Descripción |
| Aprendizaje basado en proyectos | Realización en grupo del diseño, implementación y prueba de un sistema IoT, poniendo un énfasis especial en la seguridad.<br><br>Realización en grupo de ataques a la seguridad de lo sistemas implementados por otros compañeros/as o de terceros.<br><br>Con esta metodología se trabajarán las competencias CB2, CB3, CB4, CG1, CG2, CG5, CE4, CE9, CT4 y CT5. |
| Lección magistral | Exposición, por parte del profesorado, de los principales contenidos teóricos relacionados con la seguridad para sistemas ubicuos (seguridad empotrada, en las comunicaciones y en los backends)<br><br>Con esta metodología se contribuirá a la adquisición de las competencias CB2, CB3, CB4, CG1, CG2, CE4 y CE9. |

| **Atención personalizada** | |
|---|---|
| **Metodologías** | **Descripción** |
| Lección magistral | El profesorado de la asignatura proporcionarán atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Las dudas se atenderán durante la propia sesión magistral, o durante el horario establecido para tutorías. El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura. |

| | |
|---|---|
| Aprendizaje basado en proyectos | El profesorado de la materia proporcionará atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Así mismo, el profesorado orientará y guiará al alumnado durante la realización del proyecto. Las dudas se atenderán durante las sesiones de tutoría en grupo, o durante el horario establecido para las tutorías. El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la materia. |

## Evaluación

| | Descripción | Calificación | Resultados de Formación y Aprendizaje |
|---|---|---|---|
| Aprendizaje basado en proyectos | El alumnado se dividirá en grupos para la realización del diseño, implementación y prueba de un sistema IoT, poniendo un énfasis especial en la seguridad y/o realizará ataques a la seguridad de los sistemas implementados por otros compañeros/as o por terceros.<br><br>El proyecto realizado, y el informe que contiene el resultado de los ataques completados (en cuanto a su calidad y a su éxito) serán evaluados después de su entrega valorando aspectos como la corrección, la calidad, las prestaciones y las funcionalidades. Se deberá entregar el código, prototipos y documentación realizados. Asimismo, será necesario realizar una presentación de los resultados.<br><br>Durante la realización del proyecto se realizará un seguimiento continuo del diseño y de la evolución de la implementación. Si los resultados intermedios no son satisfactorios, se podrá aplicar una penalización de hasta el 20% de la nota.<br><br>El seguimiento será grupal e individual: cada uno de lo miembros del grupo debe documentar las tareas desarrolladas dentro de su equipo y responder sobre ellas. | 80 | A2 B1 C4 D4<br>A3 B2 C9 D5<br>A4 B5 |
| Lección magistral | Se realizarán uno o varios exámenes para evaluar la comprensión de los contenidos presentados en las sesiones magistrales. Si hay más de un examen, la nota final será la media aritmética de las distintas pruebas. | 20 | A2 B1 C4<br>A3 B2 C9<br>A4 |

## Otros comentarios sobre la Evaluación

Para superar la asignatura es necesario completar las distintas partes en las que se divide (examen o exámenes acerca de los contenidos expuestos en la sesión magistral y el proyecto). La nota final será el resultado de aplicar la **media geométrica ponderada** de la nota de cada una de las partes.

Así, si la nota de las sesiones magistrales es NT,  y la nota del proyecto es NP, la nota final será:

$$\textbf{Nota} = NT^{0.2} \times NP^{0.8}$$

Durante el primer mes, el estudiantado deberá indicar explícitamente y por escrito su deseo de cursar la materia siguiendo la evaluación única. En otro caso se considerará que siguen la evaluación continua.  Quienes sigan la evaluación continua no se podrán considerar "no presentados" así que hayan realizado la entrega del primer cuestionario o tarea.

El alumnado que opte por la evaluación única deberá presentar adicionalmente  un *dossier* que deberá defender presencialmente ante el profesorado, en el que se incluyan todos los detalles sobre la realización de las distintas tareas, y muy especialmente el proyecto. En el caso de seguir la evaluación única, los alumnos/as deberán realizar el trabajo de forma individual, salvo que el profesorado les comunique explícitamente la autorización para realizarlo en grupo.

**Segunda oportunidad**

Solo podrán optar a al segunda oportunidad quien no supere la primera oportunidad (al finalizar el cuatrimestre).  La evaluación será la descrita en los apartados anteriores, pero adicionalmente será necesario presentar un *dossier,* que deberá ser defendido presencialmente ante el profesorado, en el que se incluyan todos los detalles sobre la realización de las distintas tareas, muy especialmente el proyecto.

Quien hubiese seguido la evaluación continua puede optar por mantener las notas obtenidas en la primera oportunidad para las distintas partes de la asignatura o descartarlas.

**Otros comentarios**

Las puntuaciones obtenidas solo son válidas para el curso académico en vigor. Aunque el proyecto se desarrollará (en la

medida de lo posible) en grupos, el alumnado debe guardar evidencias de su trabajo individual dentro del grupo. En el caso en el que el rendimiento de un alumno o alumna no sea acorde al de sus compañeros de grupo, se considerará su expulsión del mismo y/o podrá ser evaluado/a de forma completamente individual en esta parte.

El uso de cualquiera material durante la realización de los exámenes tendrá que ser autorizado explícitamente por el profesorado.

En caso de detección de plagio o de comportamiento no ético en alguno de los trabajos/pruebas realizadas, la calificación de la materia será de "suspenso (0)" y los profesores comunicarán el asunto a las autoridades académicas para que tomen las medidas oportunas.

## Fuentes de información

### Bibliografía Básica

Brian Russell, Drew Van Duren, **Practical Internet of Things Security**, 978-1788625821, 2, Packt Publishing, 2018

### Bibliografía Complementaria

Houbing Song, Glenn A. Fink, Sabina Jeschke, **Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.**, 978-1-119-22604-8, 1, Wiley, 2018

Bruce Schneider, **Applied Cryptography: Protocols, Algorithms and Source Code in C**, 978-1119096726, 2, Wiley, 2015

Adam Shostack, **Threat Modeling. Designing for Security.**, 978-1118809990, 1, Wiley, 2014

## Recomendaciones

### Asignaturas que se recomienda haber cursado previamente

Fortificación de sistemas operativos/V05M175V01202
Redes Seguras/V05M175V01105
Seguridad de aplicaciones/V05M175V01104
Seguridad de la información/V05M175V01102
Seguridade en comunicacións/V05M175V01103
Tests de intrusión/V05M175V01203

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Ciberseguridad en entornos industriales** | | | | |
| Asignatura | Ciberseguridad en entornos industriales | | | |
| Código | V05M175V01209 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 3 | OP | 1 | 2c |
| Lengua Impartición | Castellano | | | |
| Departamento | | | | |
| Coordinador/a | Diaz-Cacho Medina, Miguel Ramón | | | |
| Profesorado | Diaz-Cacho Medina, Miguel Ramón<br>Fernández Caramés, Tiago Manuel | | | |
| Correo-e | mcacho@uvigo.es | | | |
| Web | http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530014&any_academic=2022_23 | | | |
| Descripción general | El concepto de la Industria 4.0 dio lugar a que cada vez sean más los dispositivos industriales conectados a la rede y a procesos físicos. Esta asignatura, además de repasar los sistemas industriales tradicionales (i.e., sistemas de control industrial, control de accesos, sistemas de comunicaciones o de gestión de la información), se enfocará en la seguridad de las tecnologías de la Industria 4.0: sistemas IoT/IIoT, sistemas robotizados, cloud/edge computing, realidad aumentada, blockchain o AGVs. | | | |

| Competencias |
|---|
| Código |

| Resultados de aprendizaje | |
|---|---|
| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |

| Contenidos | |
|---|---|
| Tema | |
| Introducción | Políticas de seguridad industrial<br><br>Implicaciones de la ciberseguridad industrial y de infraestructuras críticas<br><br>Casos prácticos |
| Sistemas de control de acceso físico a dependencias industriales | Sistemas de proximidad<br><br>Sistemas de acceso remoto<br><br>Sistemas biométricos |
| Sistemas de control industrial | Arquitecturas de comunicaciones<br><br>Sistemas tradicionales<br><br>Sistemas ciberfísicos |
| Sistemas de la Industria 4.0 | Introducción a la Industria 4.0<br><br>Sistemas IoT/IIoT<br><br>Seguridade en otras tecnologías 4.0 (e.g., realidad aumentada, cloud/edge computing, blockchain, AGVs) |
| Sistemas de gestión de información en entornos industriales | Bases de datos tradicionales<br><br>ERPs<br><br>PLMs<br><br>Sistemas MES |

| | |
|---|---|
| Sistemas de comunicaciones industriales | Arquitectura de comunicaciones |
| | Tecnologías de comunicación cableadas |
| | Tecnologías de comunicación inalámbricas |

**Planificación**

| | Horas en clase | Horas fuera de clase | Horas totales |
|---|---|---|---|
| Prácticas con apoio de las TIC (Repetida, non usar) | 10 | 10 | 20 |
| Trabajo tutelado | 0 | 20 | 20 |
| Lección magistral | 9 | 9 | 18 |
| Examen de preguntas objetivas | 1 | 15 | 16 |

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

**Metodologías**

| | Descripción |
|---|---|
| Prácticas con apoio de las TIC (Repetida, non usar) | Realización por parte del alumnado de prácticas guiadas y supervisadas. |
| Trabajo tutelado | Realización por parte del alumnado de trabajos de componente tanto teórica como práctica. |
| Lección magistral | Exposición por parte del profesorado de los principales contenidos teóricos relacionados con la ciberseguridad en contornos industriales. |

**Atención personalizada**

| Metodologías | Descripción |
|---|---|
| Prácticas con apoio de las TIC (Repetida, non usar) | Los profesores de la materia proporcionarán atención individual y personalizada a los alumnos durante el curso, solucionando sus dudas y preguntas. Asimismo, los profesores orientarán y guiarán a los alumnos durante la realización de las tareas que tengan asignadas, tanto en las prácticas como en los distintos trabajos tutelados. Las dudas se atenderán ya sea durante las propias clases o durante el horario establecido para tutorías. Se buscará flexibilizar dicho horario para atender las dudas del alumnado con reconocimiento de dedicación a tempo parcial y dispensa académica de exención de asistencia. |

**Evaluación**

| | Descripción | Calificación | Resultados de Formación y Aprendizaje |
|---|---|---|---|
| Prácticas con apoio de las TIC (Repetida, non usar) | Resolución de prácticas y realización de informes con los resultados obtenidos. | 30 | |
| Trabajo tutelado | Realización de un trabajo con parte teórica y parte práctica. | 30 | |
| Examen de preguntas objetivas | Examen escrito sobre los contidos teóricos y prácticos impartidos durante el curso. | 40 | |

**Otros comentarios sobre la Evaluación**

PRIMERA OPORTUNIDAD

Se ofrecerán dos alternativas de evaluación: continua y única.

La evaluación contínua implicará la realización de las prácticas, de un trabajo tutelado y una prueba mixta que serán evaluados en los porcentajes arriba indicados (30, 30, 40), siendo necesario obtener un cinco sobre diez en la evaluación total. Igualmente, será necesario obtener un dos sobre cuatro en la prueba mixta para poder aprobar la asignatura. En caso de optar a la evaluación continua, el alumnado que realice cualquier tipo de entrega (práctica, trabajo, prueba mixta), no podrá calificarse como "no presentado".

En el caso de la evaluación única, toda la puntuación vendrá dada por una única prueba mixta que incluirá parte teórica y práctica. Dicha prueba se realizará al final del bimestre y deberá obterse en total al menos un cinco sobre diez para poder aprobar la asignatura.

La selección de la alternativa de evaluación deberá indicarse como muy tarde al final de la segunda semana de clase.

Para cualquiera de las dos alternativas se facilitará flexibilidad horaria para el alumnado con reconocimiento de dedicación a tiempo parcial y dispensa académica de exención de asistencia.

SEGUNDA OPORTUNIDAD Y CONVOCATORIAS EXTRAORDINARIAS

Los alumnos que hayan optado en la primera oportunidad por la evaluación continua tendrán la opción de conservar las notas de prácticas y trabajos tutelados realizados durante el curso académico. Dicho alumnado realizará una prueba mixta, estableciéndose la nota en los porcentajes indicados arriba (30, 30, 40). El resto de alumnos (incluido el alumnado con reconocimiento de dedicación a tiempo parcial y dispensa académica de exención de asistencia) se tratarán como alumnos de evaluación única y realizarán una prueba mixta que mezcle parte teórica y práctica.

OTROS COMENTARIOS

No se conservará ninguna de las notas obtenidas para los cursos académicos posteriores.

En el caso de detección de plagio durante alguna de las entregas, se calificará al alumno/a con suspenso (0) y se comunicará la situación a la dirección del máster y a las autoridades universitarias correspondientes de cara a tomar las medidas oportunas.

**Fuentes de información**

**Bibliografía Básica**

Eric Knapp, Joel Thomas Langill, **Industrial Network Security.**, Elsevier, 2014

Junaid Ahmed Zubairi, **Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies.**, IGI Global, 2012

Tyson Macaulay, **Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.**, Auerbach Publications, 2012

Josiah Dykstra, **Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems.**, O'Reilly, 2015

Pascal Ackerman, **Industrial Cybersecurity**, Packt, 2017

**Bibliografía Complementaria**

Peng Cheng, Heng Zhang, Jiming Chen, **Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop.**, CRC Press, 2016

**Recomendaciones**

## DATOS IDENTIFICATIVOS

**Gestión de incidentes**

| | | | | |
|---|---|---|---|---|
| Asignatura | Gestión de incidentes | | | |
| Código | V05M175V01210 | | | |
| Titulacion | Máster Universitario en Ciberseguridad | | | |
| Descriptores | Creditos ECTS | Seleccione | Curso | Cuatrimestre |
| | 3 | OP | 1 | 2c |
| Lengua Impartición | Castellano | | | |
| Departamento | | | | |
| Coordinador/a | Álvarez Sabucedo, Luis Modesto | | | |
| Profesorado | Álvarez Sabucedo, Luis Modesto<br>Dafonte Vázquez, José Carlos<br>López Rivas, Antonio Daniel | | | |
| Correo-e | lsabucedo@det.uvigo.es | | | |
| Web | http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530015&any_academic=2021_22&idioma_assig=cast&idioma_assig=cast | | | |
| Descripción general | La gestión de incidentes de ciberseguridad se centra en manejar la proactividad para prevenir y atenuar posibles consecuencias. Se obtendrá el conocimiento necesario sobre herramientas que pueden facilitar la gestión de los incidentes y las recuperaciones, la justificación de los planes propuestos para recuperación y resiliencia, la identificación y clasificación de los posibles incidentes y la definición de los cauces para su gestión y resolución. | | | |

## Competencias

| Código |
|---|

## Resultados de aprendizaje

| Resultados previstos en la materia | Resultados de Formación y Aprendizaje |
|---|---|

## Contenidos

| Tema |
|---|

## Planificación

| | Horas en clase | Horas fuera de clase | Horas totales |
|---|---|---|---|

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

## Metodologías

| | Descripción |
|---|---|

## Atención personalizada

## Evaluación

| Descripción | Calificación | Resultados de Formación y Aprendizaje |
|---|---|---|

## Otros comentarios sobre la Evaluación

## Fuentes de información

**Bibliografía Básica**

**Bibliografía Complementaria**

## Recomendaciones