# FICHA DESCRIPTIVA DE MATERIA

| INFORMACIÓN GENERAL | | | |
|---|---|---|---|
| **Denominación de la materia:** | *(En castellano)*<br>Especialidad en Ciberseguridad | | |
| | (En Inglés)<br>Intensification in Cibersecurity | | |
| **Número de créditos ECTS:** | *18* | **Ubicación temporal** | 3º |
| **Idioma de impartición:** | Español, inglés | | |
| **Carácter:** | Optativa | | |
| **Módulo en el que se integra:** | *Complementos en Tecnologías Informáticas* | | |

## SISTEMA DE EVALUACIÓN

| *Descripción de los Sistemas de Evaluación* | *Ponderación Mínima (%)* | *Ponderación Máxima (%)* |
|---|---|---|
| Presentación de trabajos | 0 | 100 |
| Entrega de prácticas | 0 | 100 |
| Examen Escrito | 0 | 100 |

## ACTIVIDADES FORMATIVAS

**Horas totales Trabajo del Alumno (25 h. x número de créditos): *450* horas.**
**Horas Presencialidad Máxima (30 % de las horas, salvo para Practicas Externas y TFM): *135* horas.**

| *Descripción de la Actividad Formativa* | *Horas Activ.* | *Presencialidad (%)* |
|---|---|---|
| Actividades presenciales | 121,5 | 100 |
| Actividades evaluación | 13,5 | 100 |
| Actividades no presenciales | 315 | 0 |

## METODOLOGÍAS DOCENTES

Clases Magistrales.

Aprendizaje basado en proyectos.
Trabajo en Grupo

**RESULTADOS DE APRENDIZAJE**

- Aprender a realizar actividades de informática forense a partir de la recolección y extracción de evidencias electrónicas en distintos tipos de dispositivos.
- Ser capaz de realizar labores de análisis con el objetivo de detectar y descubrir la instalación de malware en distinto tipo de equipos informáticos, y la acciones a realizar como contramedidas.
- Diseñar sistemas software seguros caracterizando los procesos existentes para la ingeniería y el desarrollo de estos sistemas a través del correcto análisis de requisitos de seguridad y su especificación.
- Establecer metodologías para la detección de vulnerabilidades, y seleccionar herramientas y recursos para resolverlas, así como llevar a cabo prácticas para minimizarlas.
- Conocer técnicas criptográficas de soporte para aplicaciones, y comprender los criterios de diseño de las mismas, así como el análisis de sus características para seleccionar las más adecuadas a cada tipo de aplicación.
- Comprender los problemas de seguridad en sistemas industriales, identificar los puntos vulnerables de las redes de control, y seleccionar las soluciones óptimas de protección de sistemas ciberfísicos.

**Breve descripción de los CONTENIDOS**

En esta materia se introduce al alumno en las técnicas y metodologías existentes para la realización de trabajos en informática forense como una de las bases de la ciberseguridad actual, presentando mecanismos para la extracción de evidencias electrónicas, también en dispositivos móviles, así como metodologías que permitan garantizar su integridad a lo largo de todo el proceso, desde su recolección hasta su presentación final.

Parte del contenido anterior permitirá al alumno afrontar el trabajo del análisis de malware y, más concretamente, introducir los mecanismos específicos de ciberseguridad relativos a análisis estático y dinámico, que permiten al analista descubrir la funcionalidad y objetivos del malware ya sea de manera pasiva mediante análisis de ficheros, o de manera activa a través de la ejecución en un entorno controlado.

También se introducirá al alumno en el problema de la creación de sistemas software seguros, incidiendo en el enfoque de ingeniería y sistematización, y presentando los principios que rigen la ingeniería de tales sistemas. Se presentarán los procesos existentes para la ingeniería y el desarrollo, así como la problemática del descubrimiento de requisitos de seguridad, de su especificación, y del modelado y diseño de sistemas software seguros.

Se incidirá también en las vulnerabilidades del software como origen y causa de los incidentes de ciberseguridad en las empresas. El estudio de las vulnerabilidades más habituales permitirá al alumno establecer las metodologías de desarrollo necesarias para paliar las que no pueden ser detectadas en la fase de diseño, haciendo hincapié en las herramientas y recursos para identificar y resolver tales problemas.

Otro aspecto a abordar dentro de la materia será el conocimiento, diseño y análisis de sistemas y técnicas criptográficas avanzadas que dan soporte a aplicaciones de amplio uso. Ente ellas, la transmisión de información a través de sistemas de comunicaciones de alta velocidad, las implementaciones criptográficas ligeras de sistemas RFID, NFC, etc., y el uso de protocolos de

realización de firmas a grupos de usuarios y para transferir la propiedad electrónica.

Además, el alumno conocerá la problemática de ciberseguridad de los sistemas industriales y sus sistemas de monitorización, desde los dispositivos de campo tradicionales (ej., RTU, IED, PLC, sensores y actuadores) hasta las aplicaciones de control basadas en tecnología móvil. También se explorará la diversidad y seguridad de las redes de control, así como las soluciones de protección, resistencia y seguridad propuestas en la iniciativa de la Industria 4.0.

| **COMPETENCIAS** | |
|---|---|
| **Competencias básicas** | CB1, CB2, CB3, CB4, CB5 |
| **Competencias generales:** | CG1, CG2, CG4, CG8, CG9, CG10 |
| **Competencias Transversales:** | CT2 |
| **Competencias específicas:** | ETI1, ETI2, ETI3, ETI4, ETI5, ETI8 |