



## Datos Generales

---

Asignatura: INTRODUCCIÓN A LA CIBERSEGURIDAD.

Titulación: GRADO EN CIBERSEGURIDAD

Carácter: OBLIGATORIA.

Créditos ECTS: 6 ECTS

Curso: 1º

Distribución temporal: 1ER SEMESTRE.

Idioma de impartición: CASTELLANO.

Equipo docente: UNAI AYÚCAR CARBAJO [unai.ayucar@euneiz.com](mailto:unai.ayucar@euneiz.com)

Aula(s): Aula informatizada

### Presentación de la asignatura:

Introducción a la ciberseguridad es una asignatura teórico-práctica para adquirir una visión de conjunto de la ciberseguridad que permita posteriormente al alumno adquirir, entender y poner en contexto los aprendizajes ligados a la ciberseguridad.

## Datos Específicos

---

### Resultados del proceso de formación y aprendizaje (RFA)<sup>1</sup>

|                                |     |                                                                                                                |
|--------------------------------|-----|----------------------------------------------------------------------------------------------------------------|
| Conocimientos o contenidos (C) | C3  | Aplicar los conocimientos de protección de datos y seguridad de la información en distintos niveles.           |
|                                | C4  | Ejecutar técnicas de desarrollo y prenetración analizando las mejoras técnicas, soluciones y buenas prácticas. |
|                                | C5  | Realizar desarrollos seguros y aplicar contramedidas a nivel de código.                                        |
|                                | C9  | Identificar los fundamentos teóricos y arquitecturas de los SSOO.                                              |
|                                | C12 | Conocer la nube, su seguridad y sus aplicaciones.                                                              |

---

<sup>1</sup> La clasificación de los RFA corresponde a la definida en el RD822/2021 y se encuentran definidos en la memoria de verificación del título.

\* Extender el contenido utilizando para ello la programación docente. La extensión debe estar en punto intermedio, es decir, ampliar la información en la guía docente pero no llegar a los límites de la programación docente. Se debe incluir el índice de temas a tratar punto por punto (sin desarrollar). Se pueden incluir hasta tres subapartados con ideas claves/subtemas. La extensión máxima será de 2 páginas.

|                             |      |                                                                                                                                            |
|-----------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Competencias (CO)           | CO1  | Usar y programar ordenadores, sistemas operativos, redes, bases de datos y el entorno de la nube para su aplicación en la ciberseguridad.  |
|                             | CO3  | Llevar a cabo distintos procesos de análisis en las diferentes áreas de la ciberseguridad.                                                 |
|                             | CO4  | Realizar diseños de ingeniería aplicados a la ciberseguridad.                                                                              |
|                             | CO5  | Aplicar técnicas de prevención, detección y protección de ataques en un sistema informático.                                               |
|                             | CO6  | Utilizar de forma segura los lenguajes de programación más utilizados para su implementación en situaciones reales.                        |
|                             | CO7  | Implementar soluciones criptográficas.                                                                                                     |
|                             | CO9  | Integrar de forma eficaz soluciones basadas en TI en el entorno del usuario.                                                               |
|                             | CO11 | Gestionar evidencias de vulnerabilidades.                                                                                                  |
| Habilidades o destrezas (H) | H1   | Trabajar en grupo transmitiendo conocimientos y habilidades adquiridos.                                                                    |
|                             | H2   | Desarrollar habilidades para el análisis, la elaboración y la colaboración en proyectos, partiendo de las necesidades propias del mercado. |
|                             | H6   | Ser capaz de trabajar con información técnica en inglés, tanto a nivel de consulta como de su elaboración.                                 |

### Contenido de la Asignatura\*

- TEMA 1:
  - INTRODUCCIÓN A LA CIBERSEGURIDAD
- TEMA 2:
  - HISTORIA DE LA CIBERSEGURIDAD
- TEMA 3:
  - CIA + AT
- TEMA 4:
  - TIPOS DE ATAQUES
- TEMA 5:
  - CRITICIDAD DE VULNERABILIDADES
- TEMA 6:
  - CONCEPTOS BÁSICOS DE REDES
- TEMA 7:
  - CRIPTOGRAFIA
- TEMA 8:
  - NORMATIVA Y ORGANISMOS GUBERNAMENTALES
- TEMA 9:
  - METASPLOIT

- TEMA 10:
  - FIREWALLING
- TEMA 11:
  - CONCEPTOS BÁSICOS DE RED
- TEMA 12:
  - SOLUCIONES DE MONITORIAZACIÓN DEL MERCADO
- TEMA 13:
  - INGENIERÍA SOCIAL
- TEMA 14:
  - CIBER CRIMINALES VS HACKERS ETICOS
- TEMA 15:
  - PROTOCOLOS WIFI
- TEMA 16:
  - OTRAS TECNOLOGÍAS
- TEMA 17:
  - THREAT MODELING

### Metodologías Docentes y Actividades Formativas<sup>2</sup>

Metodologías docentes utilizadas en esta asignatura son:

|     |                                  |
|-----|----------------------------------|
| MD1 | Método expositivo.               |
| MD2 | Estudios de caso.                |
| MD3 | Aprendizaje basado en problemas. |
| MD4 | Aprendizaje basado en proyectos. |
| MD5 | Aprendizaje cooperativo.         |
| MD6 | Tutorías.                        |

Actividades formativas utilizadas en esta asignatura son:

| Actividades formativas                                    | Horas previstas | % presencialidad |
|-----------------------------------------------------------|-----------------|------------------|
| AF1: Clase teórica.                                       | 30              | 100              |
| AF2: Clase prácticas.                                     | 6               | 100              |
| AF3: Realización de trabajos (individuales y/o grupales). | 6               | 100              |

<sup>2</sup> Se deberán extraer de la memoria verificada del título las metodologías docentes, actividades formativas y sistemas de evaluación. (1 ECTS = 25 horas de trabajo del estudiante).

|                                                                    |     |     |
|--------------------------------------------------------------------|-----|-----|
| AF3: Tutorías (individuales y/o grupales).                         | 3   | 50  |
| AF5: Estudio independiente y trabajo autónomo del o la estudiante. | 90  | 0   |
| AF6: Pruebas de evaluación.                                        | 3   | 100 |
| AF9: Clases en laboratorio                                         | 12  | 100 |
| Total                                                              | 150 | --  |

### Evaluación: Sistemas y Criterios de Evaluación

Las semanas de evaluación están definidas en el calendario académico publicado en la web de la universidad; la concreción de las fechas se realizará una vez que la docencia haya comenzado.

Sistemas de evaluación utilizados en esta asignatura son:

| Denominación                                                         | Pond.<br>Mín | Pond.<br>Máx |
|----------------------------------------------------------------------|--------------|--------------|
| SE1 Evaluación de la asistencia y participación del o la estudiante. | 0            | 2            |
| SE2 Evaluación de trabajos.                                          | 15           | 30           |
| SE3 Pruebas de evaluación y/o exámenes.                              | 20           | 40           |
| SE6: Evaluación de laboratorios                                      | 15           | 30           |

El estudiantado posee dos modalidades de evaluación para superar la asignatura:

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con 2 convocatorias/año.

En la Universidad Euneiz la evaluación continua (media ponderada de las diferentes actividades evaluables de la asignatura definidas por el profesorado) es la evaluación primordial; pero Euneiz permite al estudiantado acogerse a la evaluación única.



# Guía Docente

## Curso Académico 2026/27

No se permite el cambio de modalidad de evaluación (de continua a única) escogido por el estudiante a lo largo del curso.

El/la estudiante que desee acogerse a la modalidad de evaluación única deberá solicitarlo por escrito formal que lo justifique dirigido al profesorado responsable de la asignatura y a la Coordinación del título en las dos primeras semanas del inicio de la misma.

Si el/la estudiante no asiste un 80% a las clases presenciales, pasará directamente a la convocatoria extraordinaria de la evaluación única.

De manera excepcional, el/la docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del o la estudiante, etc., la posibilidad de permitir que el/la estudiante continúe en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.

Las faltas de asistencia deben justificarse al profesor/a responsable de la asignatura con un plazo máximo de 1 semana. El justificante oficial deberá ser presentado al profesor/a responsable mediante un correo electrónico.

El/la estudiante irá a la evaluación extraordinaria ÚNICAMENTE con las partes suspendidas.

El sistema de calificación de la asignatura sigue lo establecido en el RD 1125/2003 y los resultados obtenidos se calificarán siguiendo la escala numérica de 0 a 10, con expresión de un decimal.

- 0-4,9: Suspenso (SS).
- 5,0-6,9: Aprobado (AP).
- 7,0-8,9: Notable (NT).
- 9,0-10: Sobresaliente (SB).

La mención de «Matrícula de Honor» podrá ser otorgada a alumnos/as que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los/las alumnos/as matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos/as matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

Será considerado no presentado (NP) el estudiantado matriculado que no realice ninguna actividad evaluativa.

Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas ortotipográficas en la calificación final.



# Guía Docente

## Curso Académico 2026/27

El plagio está prohibido, tanto en los trabajos, como en los exámenes, en caso de detectarse la calificación será suspenso. Los trabajos entregados a través del campus virtual serán objeto de análisis por la herramienta Turnitin:

- Los informes con un índice de similitud entre el 20% y el 30% serán revisados por el profesor/a para analizar las posibles fuentes de plagio y evaluar si están justificadas.
- Cualquier trabajo con un índice de similitud superior al 30%, una vez realizado el análisis del o la docente, no será evaluado.

### Recursos materiales e infraestructuras necesarias

| Tipo de recurso material y/o infraestructura                 |
|--------------------------------------------------------------|
| Material docente (apuntes, presentaciones, guías, tareas...) |
| Recursos audiovisuales                                       |
| Material específico de la asignatura                         |
| Aula informatizada                                           |

### Bibliografía y otros Recursos de Aprendizaje

#### Bibliografía Básica

- Adam Shostack. Threat modeling designing of security.
- Michael Sikorski and Andrew Honig. Practical Malware Analysis.
- Simon Singh. The code book.

#### Bibliografía Complementaria

- Cristopher Hadnagy. Social Engineering,

#### Otros Recursos de Aprendizaje Recomendados<sup>3</sup>

- <https://www.nist.gov/>
- <https://www.shodan.io/>
- <https://www.wireshark.org/download.html>
- <https://www.first.org/cvss/>

<sup>3</sup> Entre otros recursos de aprendizaje pueden incluirse páginas web, software, materia audiovisual, etc.



# Guía Docente

## Curso Académico 2026/27

- <https://attack.mitre.org/>
- <https://www.cisecurity.org/>