Guía Docente
Curso Académico 2026/27

Datos Generales

Asignatura: PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Titulación: GRADO EN CIBERSEGURIDAD

Carácter: OPTATIVA.

Créditos ECTS: 6 ECTS

Curso: 3º

Distribución temporal: 2º SEMESTRE.

Idioma de impartición: CASTELLANO.

Equipo docente: Dr. Lorenzo Fanari lorenzo.fanari@euneiz.com

Aula(s): Aula informatizada

Presentación de la asignatura:

Asignatura orientada al análisis y diseño de estrategias para la protección de infraestructuras críticas frente a riesgos físicos y cibernéticos. Se estudiarán marcos normativos, modelos de evaluación de amenazas y vulnerabilidades, y sistemas de defensa aplicados a sectores esenciales como energía, agua, salud, transporte o telecomunicaciones.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)[1]

Contenidos o conocimientos (C)	C1	Desarrollar habilidades de cálculo para el análisis en los lenguajes de programación.
	C16	Entender el concepto de infraestructura crítica y elementos ciberfísicos para analizar los riesgos específicos que pueden sufrir y desplegar las contramedidas adecuadas para su gestión y teniendo en cuenta la legislación vigente.
	C17	Conocer los sistemas y las herramientas de los sistemas sanitarios, sus implicaciones y metodologías y herramientas

[1] 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.

		de protección.
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.
	CO4	Realizar diseños de ingeniería aplicados a la ciberseguridad.
	CO6	Utilizar de forma segura los lenguajes de programación más utilizados para su implementación en situaciones reales.
	CO9	Integrar de forma eficaz soluciones basadas en TI en el entorno del usuario.
	CO10	Aplicar técnicas y herramientas de desarrollo seguro para la verificación y validación del software.
Habilidades y 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.
	H4	Tomar decisiones en el ámbito profesional, aplicando los conocimientos y técnicas adquiridas a lo largo de la actividad académica.
	H5	Comunicar de forma clara y concisa, a todo tipo de audiencias, conocimientos, ideas, soluciones, datos, etc. en el ámbito del estudio.
	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 las Infraestructuras Críticas
  - o Definición de Infraestructuras Críticas y sectores asociados
  - o Impacto sistémico y dependencias entre sectores
  - o Evolución histórica de la protección de CI
- Tema 2. Amenazas y vulnerabilidades
  - o Conceptos de amenaza, vulnerabilidad y riesgo
  - o Vulnerabilidades específicas en sistemas ICS
  - o Ataques de ransomware y riesgos en la cadena de suministro
- Tema 3. ICS y SIS
  - o Arquitectura de sistemas ICS y SIS
  - o Diferencias entre BPCS y SIS

- Ciclo de vida de la seguridad (security) y seguridad funcional

• Tema 4. Diseño seguro en entornos industriales
- Estrategia Defense in Depth
- Modelo Purdue de segmentación industrial
- Zonas y conduits según estándares OT

• Tema 5. Análisis de ataques reales
- Caso Stuxnet
- Ataque a Colonial Pipeline
- Malware TRITON/TRISIS en sistemas de seguridad

• Tema 6. Gestión del riesgo en entornos industriales
- Evaluación de riesgos en SIS
- Metodología IEC 62443-3-2
- Técnicas BowTie y LOPA para análisis de riesgo

• Tema 7. Normativa y estándares
- IEC 61511 e IEC 62443
- NIST CSF y NIST SP 800-82
- Regulación NERC CIP en el sector energético

• Tema 8. Futuro de las Infraestructuras Críticas
- Zero Trust aplicado a entornos OT
- Inteligencia artificial y automatización en CI
- Resiliencia operativa y recuperación ante incidentes

Metodologías Docentes y Actividades Formativas[2]

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.

[2] 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).

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica.	18	100
AF2: Clase prácticas.	5	100
AF3: Realización de trabajos (individuales y/o grupales).	17	50
AF3: Tutorías (individuales y/o grupales).	2	50
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	96	0
AF6: Pruebas de evaluación.	2	40
AF9: Clase en laboratorio	10	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. Mín	Pond. Máx
SE1 Evaluación de la asistencia y participación del o la estudiante.	0	5
SE2 Evaluación de trabajos.	5	15
SE3 Pruebas de evaluación y/o exámenes	50	70
SE6: Evaluación de laboratorios	10	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.

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 continue 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.

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
Laboratorio Ciberseguridad

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- Robertson, E. (2021). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley.
- Stouffer, K., Falco, J., & Scarfone, K. (2018). Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Industrial Control System Foundations. NIST Special Publication.
- Johnson, C. (2022). Cyber Security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Routledge.

Bibliografía Complementaria

- Radvanovsky, R., & Brodsky, J. (2016). Handbook of SCADA/Control Systems Security. CRC Press.
- Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2019). Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures. ArXiv.
- Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for Industrial Control Systems: A Survey. ArXiv.

Otros Recursos de Aprendizaje Recomendados[3]

- NIST Cybersecurity Framework y NIST SP 800-82 (ICS Security) – marcos de referencia para gestión de riesgos y seguridad OT/IT .
- IEC 62443 – estándares internacionales esenciales para proteger infraestructuras industriales

[3] Entre otros recursos de aprendizaje pueden incluirse páginas web, software, materia audiovisual, etc.