

# **GUÍA DOCENTE**

## **PROTECCION DE INFRAESTRUCTURAS CRITICAS**

### **GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD**

**CURSO 2026-27**

Fecha de publicación: 07-07-2026



| I.-Identificación de la Asignatura |                      |
|------------------------------------|----------------------|
| Tipo                               | OBLIGATORIA          |
| Período de impartición             | 4 curso, 2Q semestre |
| Nº de créditos                     | 3                    |
| Idioma en el que se imparte        | Castellano           |

| II.-Presentación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>La Ley 8/2011 establece que las Infraestructuras Críticas o Estratégicas (las que proporcionan servicios esenciales) son aquellas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. En un mundo que está en plena transformación digital, proteger las Infraestructuras Críticas de ciberataques es fundamental para el correcto funcionamiento de los servicios y de los estados. El objetivo de esta asignatura es ofrecer una visión global acerca de qué es una infraestructura crítica, qué mecanismos existen para protegerlas.</p> <p>Se espera que los alumnos y alumnas que cursen la asignatura obtengan las siguientes capacidades:</p> <ul style="list-style-type: none"> <li>•Comprender el concepto de infraestructura crítica, cuáles son consideradas como tal, su relación con la informática industrial y los sistemas SCADA y sus particularidades.</li> <li>•Analizar la importancia de los efectos de cascada y aprenderán a simularlos.</li> <li>•Conocer la legislación nacional e internacional que obliga a proteger las infraestructuras críticas y las contramedidas específicas que se proponen para proteger la seguridad de los ciudadanos en relación con las mismas.</li> <li>•Comunicar de forma efectiva conocimientos, técnicas, resultados e ideas relacionados con el contenido de la asignatura.</li> <li>•Ser capaces de interpretar documentación técnica relacionada con la materia.</li> </ul> |
| II.B-Presentación en inglés                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <p>Spanish Law 8/2011 establishes that Critical or Strategic Infrastructures are those whose operation is indispensable and does not allow alternative solutions, so that their disruption or destruction would have a serious impact on essential services. In a world in full digital transformation, protecting Critical Infrastructures from cyber-attacks is essential for the proper functioning of services and states. The objective of this course is to provide an overview of what is a critical infrastructure, which technologies do they use, and what mechanisms exist to protect them. Students taking this course are expected to obtain the following skills: Understand the concept of critical infrastructure and their particularities, including industrial computing and SCADA systems. Analyze the importance of cascade effects and learn how to simulate them. Know the national and international legislation requiring the protection of critical infrastructures and the specific countermeasures proposed to protect the security of citizens in relation to them. Effectively communicate knowledge, techniques, results and ideas related to the content of the course. Be able to interpret technical documentation related to the subject. Translated with DeepL.com (free version)</p>                                                                                                                                                                                                                                              |



### III.-Resultados de Aprendizaje

CG3. Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar documentos que tengan por objeto definir, planificar, especificar, resumir proyectos y planes en el ámbito de la ciberseguridad.

CG6. Capacidad para conocer, comprender y aplicar la legislación y código ético necesario para la labor profesional en el sector de la ciberseguridad.

CG7. Capacidad para evaluar y asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos.

CG8. Capacidad para definir, evaluar y seleccionar contramedidas para la protección de los activos tecnológicos, entendiendo las peculiaridades de los distintos contextos en los que deben desplegarse.

CG9. Conocimiento y aplicación de elementos básicos de economía y de gestión de recursos humanos, organización y planificación de proyectos, así como de legislación, regulación y normalización en el sector de la ciberseguridad.

CG11. Conocimiento para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos.

CG12. Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad en el ámbito de la ciberseguridad.

CE13. Comprender y analizar las implicaciones que para la seguridad tiene desarrollar, desplegar y utilizar aplicaciones y servicios basados en tecnologías de red, incluyendo: Internet, web, comercio electrónico, multimedia, servicios interactivos, redes sociales, computación móvil, Internet de las cosas.

CE28. Diseñar, desplegar, configurar y gestionar soluciones de seguridad física de las instalaciones

CE35. Comprender el concepto de infraestructura crítica, analizar los riesgos específicos que pueden sufrir y ser capaz de desplegar las contramedidas adecuadas para gestionarlos adecuadamente y teniendo en cuenta la legislación vigente.

CE37. Comprender y analizar los retos y las repercusiones que las diferentes ciberamenazas representan para la Seguridad Nacional

- Leyenda para las titulaciones no adaptadas al RD 822/21: **CB** - competencias básicas, **CG** - competencias generales, **CE** - competencias específicas, **CT** - competencias transversales.
- Leyenda para las titulaciones adaptadas al RD 822/21: **CON** - conocimientos, **COM** - competencias, **HAB** - habilidades.



#### IV.-Contenido

##### IV.A.-Temario de la asignatura

**Tema 1.** Introducción. Infraestructuras críticas y sistemas industriales

- Definiciones. Infraestructuras críticas. Sistemas industriales.
- Ley de Protección de infraestructuras críticas.
- Protección de infraestructuras críticas a nivel europeo e internacional.

**Tema 2.** Metodologías y estrategias para la protección de infraestructuras críticas y sistemas industriales. Análisis de riesgos

- Niveles ISA.
- SCADA.
- Análisis de riesgos.

**Tema 3.** Protección de infraestructuras críticas y sistemas industriales

- Defensa en profundidad. Estructura de capas.
- Security Awareness.

**Tema 4.** Ataque a infraestructuras críticas y sistemas industriales

- Técnicas de ataque.
- Efectos en cascada.
- Casos de estudio.

##### IV.B.-Actividades formativas

| Tipo                                       | Descripción                             |
|--------------------------------------------|-----------------------------------------|
| Tutorías académicas                        | Tutorías                                |
| Resolución de ejercicios, problemas, casos | Resolución de casos prácticos           |
| Prácticas                                  | Prácticas obligatorias de la asignatura |
| Realización de Pruebas                     | Pruebas                                 |



**V.-Tiempo de trabajo del alumnado (30h grado y 25h máster)**

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| Clases teóricas                                                               | 11 |
| Clases de resolución de ejercicios, problemas, casos, etc.                    | 0  |
| Prácticas en laboratorios experimentales, tecnológicos, clínicos, campo, etc. | 15 |
| Realización de pruebas                                                        | 4  |
| Tutorías académicas                                                           | 9  |
| Actividades relacionadas: jornadas, seminarios, etc.                          | 15 |
| Preparación de clases teóricas                                                | 8  |
| Preparación de prácticas/ejercicios/casos                                     | 16 |
| Preparación de pruebas                                                        | 12 |
| Total de horas de trabajo del alumnado                                        | 90 |

**VI.-Metodología y plan de trabajo**

| Tipo                | Periodo              | Contenido                                                                         |
|---------------------|----------------------|-----------------------------------------------------------------------------------|
| Clases Teóricas     | Semana 1 a Semana 15 | Sesiones de clases teóricas del temario de la asignatura.                         |
| Prácticas           | Semana 1 a Semana 15 | Sesiones de prácticas para profundizar en los contenidos explicados en la teoría. |
| Tutorías académicas | Semana 1 a Semana 15 | Tutorías académicas, previa solicitud por correo.                                 |
| Pruebas             | Semana 6 a Semana 9  | Prueba de evaluación.                                                             |



**VII.-Método de evaluación**

El modelo de evaluación general es la evaluación continua, tal como establece el Reglamento de evaluación de los resultados de aprendizaje de la Universidad Rey Juan Carlos.

Deberán utilizarse todos los sistemas de evaluación establecidos para la asignatura en la memoria de la titulación, excepto aquellos que tuviesen una ponderación mínima del 0%, que podrán utilizarse en los cursos académicos en los que el profesorado lo considere oportuno. Cada uno de los sistemas de evaluación podrá ser aplicado mediante una o más actividades de evaluación, coherentes con ese sistema. Ninguna de las actividades de evaluación podrá superar individualmente el 60% de la calificación global de la asignatura.

La suma de las actividades de evaluación no revaluables no podrá superar el 40% de la calificación global de la asignatura y, en general, no deberían tener nota mínima (salvo en el caso de actividades de carácter práctico en las que, estrictamente, no pudieran reproducirse en la convocatoria extraordinaria las condiciones de evaluación de la convocatoria ordinaria).

El alumnado que no consiga superar la asignatura en la convocatoria ordinaria, o no se hayan presentado, podrán presentarse a la convocatoria extraordinaria únicamente a las actividades de evaluación revaluables no superadas.

El uso de herramientas basadas en inteligencia artificial está prohibido en cualquier ejercicio y prueba de evaluación de la asignatura salvo que el profesor lo indique de forma explícita en el enunciado o en el material de esta. En caso de que esté permitido, se darán indicaciones precisas de qué usos están permitidos y cuáles no.

La distribución y características de las actividades de evaluación son las que se describen a continuación.

**VII.A.- Descripción de las actividades de evaluación y su ponderación**

| Sistema de Evaluación                                   | Revaluable en Extraordinaria                                      | Ponderación | Actividad de evaluación               | Nota mínima | Contenidos        | Fecha                                   |
|---------------------------------------------------------|-------------------------------------------------------------------|-------------|---------------------------------------|-------------|-------------------|-----------------------------------------|
| SE1 - Prueba escrita de respuestas abiertas o tipo test | Sí. Todas las pruebas seguirán el mismo formato que en ordinaria. | 60%         | Prueba 1 (30%) - parcial eliminatorio | 5           | Temas 1 y 2       | Semana 8                                |
|                                                         |                                                                   |             | Prueba 2 (30%)                        | 5           | Temas 3 y 4       | Fecha oficial de convocatoria ordinaria |
| SE2 - Resolución de problemas y casos prácticos         | Sí. Todas las pruebas seguirán el mismo formato que en ordinaria. | 20%         | Práctica 1                            | 5           | Temas 1, 2 y 3    | Semana 8                                |
| SE6 - Valoración y presentación de trabajos / Proyectos | Sí. Todas las pruebas seguirán el mismo formato que en ordinaria. | 20%         | Práctica 2                            | 5           | Temas 1, 2, 3 y 4 | Fecha oficial de convocatoria ordinaria |

#### Cálculo de la nota final

- La **nota final** se calcula como la **media ponderada** de las notas de las pruebas evaluables según los porcentajes indicados, siempre y cuando se hayan superado con la nota mínima indicada para cada una de ellas.
- Si alguna de las pruebas evaluables no se ha superado con la nota mínima necesaria, la nota final será el mínimo entre 4,5 y la media ponderada de las pruebas de evaluación.
- Si no se ha presentado a alguna de las pruebas evaluables, la nota en esa prueba será 0.
- Si no se ha presentado a ninguna prueba evaluable, la nota final será **"No presentado"**.

#### Convocatoria extraordinaria

En convocatoria extraordinaria los estudiantes solamente se presentarán a la reevaluación de las pruebas no superadas, de manera que para el cálculo de la nota final en esta convocatoria se utilizará la calificación de las pruebas aprobadas en convocatoria ordinaria y las notas obtenidas en las pruebas revaluadas. El cálculo de la nota final se realiza tal y como se indica en el apartado anterior.

La reevaluación de las pruebas se realizará en la fecha oficial indicada para la convocatoria extraordinaria.

#### Conducta académica

En el caso de **fraude académico** en alguna actividad de evaluación, se otorgará una calificación de cero puntos en dicha actividad lo que, para aquellas actividades con nota mínima superior a cero implica el suspenso en la convocatoria correspondiente.

Se recuerda además que, atendiendo al artículo 9.d). de la **Normativa de Convivencia de la Universidad Rey Juan Carlos** (<https://www.urjc.es/images/Universidad/Presentacion/normativa/normativa%20convivencia%20universitaria.pdf>) el **fraude académico** en alguna actividad de evaluación se considera **falta grave**. Las sanciones correspondientes a las faltas graves, según el artículo 11 de la referida normativa, son la expulsión temporal de la Universidad, o la pérdida al derecho de la convocatoria ordinaria.

#### VII.B.- Evaluación del alumnado con dispensa académica de asistencia a clase



La concesión de Dispensa Académica de Asistencia a Clase (DAAC) no implica que se quede automáticamente eximido de participar en las actividades de evaluación continua ni en las actividades formativas presenciales de asistencia obligatoria establecidas en la guía docente. Una vez concedida la dispensa, el alumnado deberá contactar con el docente, que podría proponerle las adaptaciones que considere convenientes, siempre que garanticen la adquisición y adecuada evaluación de los resultados de aprendizaje previstos. El alumnado deberá mantener a lo largo de curso una comunicación fluida con el docente para que este le proporcione información sobre las fechas en que se realizarán esas actividades formativas y de evaluación, en caso de que su programación no estuviese ya fijada y a disposición del alumnado en el momento de la concesión de la dispensa.

Asignatura con posibilidad de dispensa: Sí

#### **VII.C.- Revisión y reclamación de las actividades de evaluación**

Se realizará conforme al Reglamento de evaluación de los resultados de aprendizaje de la Universidad Rey Juan Carlos.

#### **VII.D.- Alumnado con discapacidad o necesidades educativas especiales**

Con el fin de garantizar la igualdad de oportunidades, la no discriminación, la accesibilidad universal y la mayor garantía de éxito académico, las adaptaciones curriculares para alumnado con discapacidad o con necesidades educativas especiales serán pautadas por la Unidad de Atención a Personas con Discapacidad, de acuerdo con la normativa que regula el servicio de Atención a Estudiantes con Discapacidad, aprobada por Consejo de Gobierno de la Universidad Rey Juan Carlos.

Para que esas adaptaciones puedan realizarse, será requisito la emisión de un informe de adaptaciones curriculares por parte de dicha Unidad, por lo que el alumnado con discapacidad o necesidades educativas especiales deberán contactar con este servicio para analizar conjuntamente las distintas opciones.

#### **VII.E.- Conducta académica, integridad y honestidad académica**

La Universidad Rey Juan Carlos está plenamente comprometida con los más altos estándares de integridad y honestidad académica, por lo que estudiar en la URJC supone asumir y suscribir los valores de integridad y la honestidad académica recogidos en el Código Ético de la Universidad.

Para acompañar este proceso, la Universidad dispone de la Normativa de Convivencia de la Universidad Rey Juan Carlos y de diferentes herramientas (antiplagio, supervisión) que ofrecen una garantía colectiva para el completo desarrollo de estos valores esenciales.

Las herramientas basadas en inteligencia artificial pueden mejorar la experiencia de aprendizaje, pero debe utilizarse de forma ética, legal, honesta y transparente. Por este motivo, deben seguirse las recomendaciones de uso adecuado indicadas por los docentes de la asignatura.



## VIII.-Recursos y materiales didácticos

### Bibliografía básica

Título: Infraestructuras críticas y sistemas industriales: Auditorías de seguridad y fortificación.

Autor: Francisco Bolívar

Editorial: OxWord

Título: Industrial cybersecurity. Efficiently secure critical infrastructure systems.

Autor: Pascal Ackerman

Editorial: Packt

Título: Critical Infrastructure Security and Resilience. Theories, Methods, Tools and Technologies.

Autores: Dimitris Gritzalis, Marianthi Theocharidou, George Stergiopoulos

Editorial: Springer

### Bibliografía complementaria

## IX.-Profesorado

|                                       |                                                                                                     |
|---------------------------------------|-----------------------------------------------------------------------------------------------------|
| Nombre y apellidos                    | JOSÉ MANUEL VALERO ESTEBAN                                                                          |
| Correo electrónico                    | josemanuel.valero@urjc.es                                                                           |
| Departamento                          | Informática y Estadística                                                                           |
| Campus de impartición                 | Móstoles                                                                                            |
| Categoría                             | Profesor/a Asociado/a                                                                               |
| Titulación académica                  | Doctor                                                                                              |
| Responsable de asignatura             | Si                                                                                                  |
| Horario de tutorías                   | Para consultar las tutorías póngase en contacto con el/la profesor/a a través de correo electrónico |
| Nº de Quinquenios                     | 1                                                                                                   |
| Nº de Sexenios                        | 1                                                                                                   |
| Nº de Sexenios de transferencia       | 0                                                                                                   |
| Nº de evaluaciones positivas Docencia | 1                                                                                                   |
|                                       |                                                                                                     |
| Nombre y apellidos                    | LIDIA ANDRÉS ESPINAL                                                                                |
| Correo electrónico                    | lidia.andres@urjc.es                                                                                |
| Departamento                          | Informática y Estadística                                                                           |
| Campus de impartición                 | Móstoles                                                                                            |
| Categoría                             | Profesor/a Asociado/a                                                                               |
| Responsable de asignatura             | No                                                                                                  |



|                                              |                                                                                                     |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Horario de tutorías</b>                   | Para consultar las tutorías póngase en contacto con el/la profesor/a a través de correo electrónico |
| <b>Nº de Quinquenios</b>                     | 0                                                                                                   |
| <b>Nº de Sexenios</b>                        | 0                                                                                                   |
| <b>Nº de Sexenios de transferencia</b>       | 0                                                                                                   |
| <b>Nº de evaluaciones positivas Docencia</b> | 1                                                                                                   |
|                                              |                                                                                                     |

