

GUÍA DOCENTE SEGURIDAD EN REDES

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	2 curso, 2Q semestre
Nº de créditos	6
Idioma en el que se imparte	Castellano

II.-Presentación

Las redes de computadores tienen cada vez un alcance mayor y uno de los aspectos a los que más atención se le presta hoy en día es su seguridad. La capacidad de los atacantes para romper esa seguridad de red es cada vez mayor, por lo que se debe aumentar en consonancia la capacidad y conocimientos de seguridad de los servicios de informática de las organizaciones para hacer frente a esta amenaza creciente. En esta asignatura se verán las principales contramedidas que se deben emplear en las redes de una organización para protegerla frente a las amenazas. El estudiante aprenderá los distintos mecanismos y dispositivos que permiten segmentar redes y proteger su perímetro, así como los criterios que permiten escoger los más adecuados en cada caso. Además se analizarán los sistemas que permiten prevenir y detectar intrusiones en redes. El estudiante también analizará los protocolos específicos de seguridad en las comunicaciones, sus vulnerabilidades y escenarios, así como los mecanismos y tecnologías que permiten desplegar redes virtuales, accesos remotos y redes inalámbricas seguras. Además, en esta asignatura se cubrirán parte de los contenidos de la certificación Cisco CCNA Security y, dado que la ETSII-URJC es centro Cisco Academy, los estudiantes tendrán también acceso a los materiales de formación de esta certificación de seguridad en redes.

Para cursar esta asignatura es deseable que el estudiante haya cursado y aprobado las asignaturas de Introducción a la Ciberseguridad y Redes de Computadores.

II.B-Presentación en inglés

Computer networks are becoming increasingly more widespread and one of the aspects that receives the most attention today is their security. The ability of attackers to break this network security is increasing, so the security capacity and knowledge of the IT services of organizations must be increased accordingly to face this growing threat. In this course, the main countermeasures that must be used in an organization's networks to protect it from threats will be seen. The student will learn the different mechanisms and devices that allow segmenting networks and protecting their perimeter, as well as the criteria that allow choosing the most appropriate ones in each case. In addition, the systems that allow preventing and detecting intrusions in networks will be analyzed. The student will also analyze the specific security protocols in communications, their vulnerabilities and scenarios, as well as the mechanisms and technologies that allow deploying virtual networks, remote access and secure wireless networks. In addition, this course will cover part of the content of the Cisco CCNA Security certification and, since the ETSII-URJC is a Cisco Academy center, students will also have access to the training materials for this network security certification. To take this course, it is desirable that the student has taken and passed the Introduction to Cybersecurity and Computer Networks courses.



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.

CG5. Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

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.

CG13. Capacidad para concebir, desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería como instrumento para el aseguramiento de su calidad.

CE11. Diseñar, desarrollar y desplegar aplicaciones considerando las características, funcionalidades y estructura de Internet y los riesgos que éstas suponen para la ciberseguridad.

CE18. Ser capaz de gestionar el factor humano en ciberseguridad mediante la definición de políticas y procedimientos adecuados para cada contexto.

CE23. Diseñar, desplegar, configurar y gestionar soluciones que protejan el perímetro de una red, segmentarla y prevenir/detectar intrusiones en ella.

CE24. Diseñar, desplegar, configurar y gestionar soluciones que protejan los datos almacenados y en tránsito (las comunicaciones).

- 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 a la seguridad en redes
 Tema 2. Protección del perímetro: Firewalls y DMZs
 Tema 3. Segmentación de redes: VLANs.
 Tema 4. Prevención y detección de intrusos.
 Tema 5. Redes Privadas Virtuales: IPSec y TLS.
 Tema 6. Seguridad en redes inalámbricas.

IV.B.-Actividades formativas

Tipo	Descripción
Resolución de ejercicios, problemas, casos	Resolución de ejercicios en clase
Lecturas	Lectura y visionado de materiales
Realización de pruebas	Realización de pruebas de evaluación formativa de los temas
Asistencia a clases teóricas	Clases teóricas
Prácticas	Realización de prácticas con ordenador



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

Clases teóricas	14
Clases de resolución de ejercicios, problemas, casos, etc.	10
Prácticas en laboratorios experimentales, tecnológicos, clínicos, campo, etc.	30
Realización de pruebas	6
Tutorías académicas	46
Actividades relacionadas: jornadas, seminarios, etc.	2
Preparación de clases teóricas	14
Preparación de prácticas/ejercicios/casos	42
Preparación de pruebas	16
Total de horas de trabajo del alumnado	180

VI.-Metodología y plan de trabajo

Tipo	Periodo	Contenido
Clases Teóricas	Semana 1 a Semana 1	Tema 1. Introducción a la seguridad en redes
Clases Teóricas	Semana 2 a Semana 2	Tema 2. Protección del perímetro: Firewalls y DMZs
Pruebas	Semana 15 a Semana 15	Prueba 3
Seminarios	Semana 15 a Semana 15	Seminario sobre seguridad en redes
Pruebas	Semana 8 a Semana 8	Prueba 1
Pruebas	Semana 12 a Semana 12	Prueba 2
Clases Teóricas	Semana 13 a Semana 13	Tema 6. Seguridad en redes inalámbricas
Prácticas	Semana 2 a Semana 4	Práctica Tema 2
Clases Teóricas	Semana 5 a Semana 5	Tema 3. Segmentación de redes: VLANs
Clases Teóricas	Semana 7 a Semana 7	Tema 4. Prevención y detección de intrusos
Clases Teóricas	Semana 9 a Semana 9	Tema 5. Redes Privadas Virtuales: IPSec y TLS
Prácticas	Semana 7 a Semana 8	Práctica Tema 4



Prácticas	Semana 5 a Semana 6	Práctica Tema 3
Prácticas	Semana 9 a Semana 12	Práctica Tema 5
Prácticas	Semana 13 a Semana 15	Práctica Tema 6
Clases Teóricas	Semana 1 a Semana 1	Para motivar la asistencia a las clases prácticas, que son muchas, se ha gamificado la asignatura
Clases Teóricas	Semana 1 a Semana 1	Toda la asignatura se desarrolla trabajando en equipos con trabajo colaborativo

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

Convocatoria ordinaria

La asignatura se evaluará mediante **evaluación continua** según la siguiente distribución de actividades:

Sistema de Evaluación	Revaluable en Extraordinaria	Ponderación	Actividad de evaluación	Nota mínima	Contenidos	Fecha
SE1 – Pruebas de formato escrito de similar respuesta abierta o tipo test	Sí, con pruebas de formato escrito de similar respuesta abierta o tipo test adaptadas al tiempo disponible	40%	Prueba Teoría 1 (10%)	5	Temas 1 y 2	Semana 8
			Prueba Teoría 2 (15%)	5	Temas 3 y 4	Semana 12
			Prueba Teoría 3 (15%)	5	Temas 5 y 6	Fecha del examen de convocatoria ordinaria
SE2 – Resolución de problemas y casos prácticos	Sí, con pruebas de formato escrito de similar respuesta abierta o tipo test adaptadas al tiempo disponible	30%	Se incluirán problemas y casos prácticos a resolver en las pruebas de los temas	-	Temas 1-6	En las fechas de las pruebas de los temas
SE3 – Prácticas con ordenador	Sí, con pruebas de formato escrito de similar respuesta abierta o tipo test adaptadas al tiempo disponible	30%	Se incluirán pruebas prácticas en las pruebas de los temas	-	Temas 1-6	En las fechas de las pruebas de los temas

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.
- Para que la asignatura se considere superada será necesario obtener en alguna convocatoria una nota final igual o superior a 5.0 puntos sobre 10.0.
- Si alguna de las pruebas evaluables no se ha superado con la nota mínima necesaria para hacer media, la nota final de la asignatura será la calculada si esta está por debajo de 4,5, y será de 4,5 si es superior (es decir, se satura en 4,5).
- 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 revaluación de las pruebas no superadas o a las que no se haya presentado, 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 revaluación de las pruebas se realizará en la fecha oficial indicada para la convocatoria extraordinaria.

Conducta académica

En todas las pruebas de evaluación será necesario que el estudiante disponga de documentación identificativa (DNI/NIE, pasaporte, permiso de conducir o carnet de estudiante de la URJC) que le podrá ser requerida en cualquier momento. No estará permitido el uso de ningún material bibliográfico, así como el uso de dispositivos electrónicos o de comunicación como tablets, PCs, teléfonos móviles, e-books, etc., o cualquier otro tipo que el profesor no considere adecuados. Solo los estudiantes con necesidades especiales podrán hacer uso de este tipo de dispositivos, siempre que el profesor lo autorice expresamente. El estudiante se compromete a presentar en las pruebas una solución propia y original. En caso de plagio total o parcial de las soluciones, o cualquier otro tipo de fraude que considere el profesor en alguna actividad de evaluación, se otorgará una calificación de cero puntos en dicha actividad.

Se recuerda además que, atendiendo al artículo 8.g). 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**.

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

Bibliografía complementaria

Michael McLafferty, Warun Levesque, Arthur Salmon. Applied Network Security. Packt Publishing. 2017. (Disponible como libro electrónico en Safari)

IX.-Profesorado

Nombre y apellidos	CÉSAR CÁCERES TALADRIZ
Correo electrónico	cesar.caceres@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Móstoles
Categoría	Titular de Universidad
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	4
Nº de Sexenios	3
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	6
Nombre y apellidos	MARÍA TERESA GONZÁLEZ DE LENA ALONSO
Correo electrónico	mariateresa.gonzalezdelena@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Móstoles
Categoría	Profesor/a Colaborador/a
Titulación académica	Doctor
Responsable de asignatura	No
Horario de tutorías	Para consultar las tutorías póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	4
Nº de Sexenios	0



Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	4