Universidad Rey Juan Carlos

GUÍA DOCENTE

SEGURIDAD INFORMATICA

GRADO EN INGENIERÍA INFORMÁTICA

CURSO 2026-27

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

Fecha de publicación: 06-07-2026

I.-Identificación de la Asignatura	
Tipo	OBLIGATORIA
Período de impartición	3 curso, 1Q semestre
Nº de créditos	6
Idioma en el que se imparte	Castellano

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

II.-Presentación

En una sociedad tecnológica y en red como la actual la Seguridad Informática afecta prácticamente a todas las facetas de la vida cotidiana de personas y organizaciones. En esta asignatura se garantiza una formación básica en los aspectos más importantes de la ciberseguridad.

Se comienza el semestre analizando la importancia de la Seguridad Informática y los tres pilares básicos que la garantizan, la disponibilidad, la confidencialidad y la integridad. A continuación, se introducen los conceptos básicos de la materia que permitirán abordar con éxito el resto de la asignatura: vulnerabilidad, riesgo, amenaza, incidente, ataque, contramedida, etc. Después se analizan los principales ataques que pueden sufrir las redes y los protocolos y las aplicaciones y servicios, realizando un estudio por "familias" o patrones de ataque. A partir de este análisis se profundiza en el estudio de las contramedidas que pueden evitar estos ataques o minimizar su impacto, haciendo especial hincapié en los mecanismos criptográficos, las contramedidas a nivel de red y las metodologías de desarrollo seguro. Para finalizar, se realiza un recorrido por las nuevas tendencias en seguridad informática (APTs, seguridad en entonos cloud y móviles, etc.), ya que es necesario que el alumno adquiera la capacidad de adaptarse en cada momento a un entorno tan rápidamente cambiante como es el de la Informática, sobre todo en lo que se refiere a este campo. Se resumirán los últimos avances así como los retos que se plantean para el futuro.

Prerrequisitos: Se recomienda haber cursado previamente las asignaturas Introducción a la Programación, Estructuras de datos, Programación Orientada a Objetos, Bases de Datos y Redes de Computadores.

II.B-Presentación en inglés

In today's technological and networked society, computer security affects practically all facets of the daily lives of people and organizations. This course provides basic training in the most important aspects of cybersecurity. The semester begins by analyzing the importance of Computer Security and the three basic pillars that guarantee it: availability, confidentiality and integrity. Next, the basic concepts of the subject are introduced, which will allow to approach successfully the rest of the course: vulnerability, risk, threat, incident, attack, countermeasure, etc. Afterwards, the main attacks that networks and protocols, applications and services may suffer are analyzed, carrying out a study by "families" or attack patterns. Based on this analysis, the countermeasures that can prevent these attacks or minimize their impact are studied in depth, with special emphasis on cryptographic mechanisms, network countermeasures and secure development methodologies. Finally, a tour of the new trends in computer security (APTs, security in cloud and mobile environments, etc.) will be made, as it is necessary for the student to acquire the ability to adapt at all times to such a rapidly changing environment as IT, especially in this field. The latest developments as well as the challenges for the future will be summarized. Prerequisites: It is recommended to have previously taken the subjects Introduction to Programming, Data Structures, Object Oriented Programming, Databases and Computer Networks.

III.-Resultados de Aprendizaje

CG03. Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
CG04. Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas, de acuerdo con los conocimientos adquiridos según lo establecido en el apartado 5 del Anexo II de la Resolución de 8 de junio de 2009 de la Secretaría General de Universidades, que da publicidad al acuerdo del Consejo de Universidades por el que se establecen recomendaciones para la propuesta por las universidades de memorias de solicitud de títulos oficiales en los ámbitos de la Ingeniería Informática y la Ingeniería Técnica Informática.
CG06. Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes de acuerdo con los conocimientos adquiridos según lo establecido en el apartado 5 del Anexo II de la Resolución de 8 de junio de 2009 de la Secretaría General de Universidades, que da publicidad al acuerdo del Consejo de Universidades por el que se establecen recomendaciones para la propuesta por las universidades de memorias de solicitud de títulos oficiales en los ámbitos de la Ingeniería Informática y la Ingeniería Técnica Informática.
CG09. Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.
CE01. Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.
CE02. Capacidad para planificar, concebir, desplegar y dirigir proyectos, servicios y sistemas informáticos en todos los ámbitos, liderando su puesta en marcha y su mejora continua y valorando su impacto económico y social.
CE05. Conocimiento, administración y mantenimiento de sistemas, servicios y aplicaciones informáticas.
CE12. Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.
CE13. Capacidad de describir las características de los últimos avances en hardware y software y sus correspondientes aplicaciones prácticas.

- 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.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

IV.-Contenido

IV.A.-Temario de la asignatura

Bloque temático	Tema	Apartados
I.- Introducción a la seguridad informática	1. Introducción	Introducción a la seguridad informática. Los tres pilares de la seguridad. Políticas y procedimientos. El factor humano. El Plan Director de Seguridad. Normativas y legislación.
	2. Conceptos básicos y definiciones	Riesgos y amenazas. Vulnerabilidades. Exploits. Incidentes de seguridad.
II.- Ataques y contramedidas	3. Anatomía de un ataque	Tipos de adversario. Fases de un ataque. Técnicas de recogida de información. Anonimato.
	4. Ataques a redes IP y protocolos	Envenenamientos, suplantación y Man in the Middle. Secuestro de sesión. Denegación de servicio volumétrica. Ataques a IPv6.
	5. Ataques a aplicaciones y servicios	Desbordamiento de buffer. Inyecciones de comandos y código. Forgeries (XSS y XSRF).
	6. Malware	Tipos de malware. Vectores de infección. Mecanismos de defensa del malware. Evolución del malware.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

	7. Mecanismos criptográficos	Sistemas de cifrado de clave pública y de clave privada. DES, AES y RSA. Mecanismos de autenticación. Firma digital y funciones hash. Kerberos. Sistemas de certificados.
	8. Contramedidas en redes y protocolos	Mecanismos para la protección del perímetro y nuevos modelos. Firewalls y DMZs. VPNs seguras e IPSec. TLS y SSL.
	9. Contramedidas de usuario, administrador y desarrollador	Buenas prácticas para el usuario. Buenas prácticas para el administrador. Codificación segura. Metodologías de desarrollo seguro.
III.- Nuevas tendencias en seguridad informática	10. Presente y futuro de la seguridad informática	APTs. Protección de infraestructuras críticas. Cibercrimen y ciberguerra. Seguridad en entornos Cloud. Seguridad en entornos móviles y BYOD.

IV.B.-Actividades formativas	
Tipo	**Descripción**
Prácticas	Resolución de problemas prácticos en ordenador.
Resolución de ejercicios	Resolución de problemas prácticos en ordenador.

V.-Tiempo de trabajo del alumnado (30h grado y 25h máster)	
Clases teóricas	36
Clases de resolución de ejercicios, problemas, casos, etc.	10
Prácticas en laboratorios experimentales, tecnológicos, clínicos, campo, etc.	10
Realización de pruebas	4
Tutorías académicas	18
Actividades relacionadas: jornadas, seminarios, etc.	0
Preparación de clases teóricas	30
Preparación de prácticas/ejercicios/casos	48
Preparación de pruebas	24
Total de horas de trabajo del alumnado	180

VI.-Metodología y plan de trabajo		
Tipo	**Periodo**	**Contenido**
Prácticas	Semana 1 a Semana 15	Desarrollo de pruebas prácticas para profundizar en los contenidos teóricos vistos en la teoría.
Pruebas	Semana 14 a Semana 15	Prueba de evaluación. Resolución de ejercicios teórico-prácticos.
Pruebas	Semana 6 a Semana 9	Prueba de evaluación. Resolución de ejercicios teórico-prácticos.
Clases Teóricas	Semana 1 a Semana 15	Contenidos teórico-prácticos de las unidades didácticas del programa de la asignatura

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

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

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737batdf33be031ec6c760beee14869.

Sistema de evaluación	Revaluable en extraordinaria	Ponderación	Actividad de evaluación	Nota mínima	Contenidos	Fecha
SE1 – Prueba escrita de respuesta abierta o tipo test o selección	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria.	Prueba 1 (35%)	Prueba individual y escrita de respuesta abierta o tipo test o selección.	4	Temas 1 al 5	Semana 6 a semana 10
		Prueba 2 (35%)	Prueba individual y escrita de respuesta abierta o tipo test o selección.	4	Temas 6 al 10	Fecha del examen de convocatoria ordinaria
S E 3 – Prácticas en ordenador	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria	Práctica 1 (10%)	Prueba individual y escrita de respuesta abierta o tipo test o selección	4	Temas 1 al 3	Semana 3 a semana 8
		Práctica 2 (10%)	Prueba individual y escrita de respuesta abierta o tipo test o selección	4	Temas 3 al 6	Semana 5 a semana 12
		Práctica 3 (10%)	Prueba individual y escrita de respuesta abierta o tipo test o selección	4	Temas 1 al 10	Semana 10 a semana 15

Cálculo de la nota final o global

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. La **nota final** para aprobar deberá ser de 5 puntos sobre 10.

Si alguna de las pruebas o práticas evaluables no se ha superado con la nota mínima necesaria para hacer media, la nota final de la asignatura será:

•Si la media ponderada <=4, la nota final será la media ponderada.

•Si la media ponderada >4, la nota final será un 4.

•Si no se ha presentado a alguna prueba, se le pondrá un 0 en esa prueba.

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 y prácticas no superadas, de manera que, para el cálculo de la nota final en esta convocatoria se utilizará la calificación de las pruebas y prácticas aprobadas en convocatoria ordinaria junto con las obtenidas en esta convocatoria.

En caso de presentarse a una prueba que ya hubiera superado, se mantendrá la nota obtenida en la convocatoria extraordinaria, independientemente de si es superior o inferior a la nota de la convocatoria ordinaria.

El calculo de la nota se hara con los mismos pesos y otas mínimas que durante la convocatoria ordinaria.

Convocatoria adelantada

El procedimiento y criterios de evaluación para los estudiantes que soliciten la convocatoria adelantada, será igual que en las convocatorias ordinaria y extraordinaria

Otras observaciones o aclaraciones
Los estudiantes podrán no revaluarse de las pruebas y prácticas con una calificación >= 4 puntos y <5 puntos, conservando la calificación obtenida en la convocatoria ordinaria.
El cálculo de la nota final en la convocatoria extraordinaria se realizará del mismo modo que en la convocatoria ordinaria.
La revaluación de las pruebas escritas y las prácticas se realizará en la fecha oficial indicada para la convocatoria extraordinaria.
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.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

VIII.-Recursos y materiales didácticos

Bibliografía básica

Título
Computer Security Handbook
Autor
Seymour Bosworth, Eric Whyne y M.E. Kabay
Editorial
John Wiley & Sons, 2009

Título
Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach
Autor
Charles P. Pfleeger y Shari Lawrence Pfleeger
Editorial
Prentice Hall, 2011

Título
Computer Security Fundamentals (tercera edición)
Autor
Chuck Easttom
Editorial
Pearson, 2016

Título
Seguridad Informática
Autor
Antonio Postigo Palacios
Editorial
Paraninfo, 2020

Bibliografía complementaria

Título
Hacking Exposed 7: Network Security Secrets & Solutions
Autor
Stuart McClure, Joel Scambray y George Kurtz
Editorial
McGraw-Hill, 2012

Título
Computer Security and Cryptography
Autor
Alan G. Konheim
Editorial
Wiley-Interscience, 2007

Título Information Security The Complete Reference Autor Mark Rhodes-Ousley Editorial McGraw-Hill, 2013

IX.-Profesorado	
Nombre y apellidos	ÁLVARO ALFONSO EVERLET FERNÁNDEZ
Correo electrónico	alvaro.everlet@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Móstoles
Categoría	Profesor/a Asociado/a
Responsable de asignatura	No
Horario de tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	0
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docentia	0
Nombre y apellidos	JORGE ÁNGEL COLINAS GARCÍA
Correo electrónico	jorge.colinas@urjc.es
Campus de impartición	Madrid - Vicálvaro
Categoría	Investigador
Responsable de asignatura	No
Horario de tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	0
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docentia	0

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 23/10/2026 15:38 | Hash: 0737bafdf33be031ec6c760beee14869.

Nombre y apellidos	JUAN MARTÍN MANSILLA
Correo electrónico	juan.martin@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Móstoles
Categoría	Profesor/a Asociado/a
Responsable de asignatura	Si
Horario de tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	1
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docentia	2
Nombre y apellidos	MIGUEL ÁNGEL MUÑOZ MOHEDANO
Correo electrónico	miguel.munoz@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Madrid - Vicálvaro
Categoría	Profesor/a Ayudante Doctor/a
Titulación académica	Doctor
Responsable de asignatura	No
Horario de tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	0
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docentia	0