

GUÍA DOCENTE

Ciberseguridad I

GRADO EN INTELIGENCIA, SEGURIDAD Y DIPLOMACIA

CURSO 2026-27

Fecha de publicación: 14-07-2026



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

En esta asignatura se estudiarán los conceptos fundamentales relacionados con la seguridad informática y la protección de la información, los sistemas, las aplicaciones y las redes frente a posibles amenazas y ataques.

Se abordarán los principios básicos de la seguridad de la información, como la confidencialidad, la integridad y la disponibilidad, así como los principales riesgos, vulnerabilidades y medidas de protección. También se estudiarán las distintas fases de un ataque informático, desde la búsqueda inicial de información hasta el acceso a los sistemas y la respuesta ante un incidente. Durante el curso se introducirán los fundamentos de la criptografía y sus principales aplicaciones en la protección de datos y comunicaciones. Además, se analizarán las técnicas de ingeniería social utilizadas para engañar a los usuarios y obtener información o accesos no autorizados. La asignatura también tratará las vulnerabilidades más habituales de las aplicaciones y las principales medidas de seguridad aplicadas a redes, equipos y servidores.

Los alumnos, tras cursar esta asignatura, deberán:

- Conocer y comprender los conceptos básicos de seguridad informática y seguridad de la información.
- Identificar activos, amenazas, vulnerabilidades, riesgos e incidentes de seguridad.
- Conocer los principios de confidencialidad, integridad y disponibilidad de la información.
- Comprender las principales fases de un ataque informático y reconocer sus posibles señales.
- Conocer las medidas básicas de prevención, detección y respuesta ante incidentes de seguridad.
- Comprender los fundamentos del cifrado simétrico y asimétrico, las funciones hash, las firmas digitales y los certificados digitales.
- Identificar las principales técnicas de ingeniería social y aplicar medidas básicas para prevenirlas.
- Reconocer las vulnerabilidades más habituales relacionadas con la seguridad de las aplicaciones.
- Conocer las principales medidas de protección de redes, equipos y servidores.
- Comprender la importancia de las actualizaciones, el control de acceso, las copias de seguridad y la monitorización de los sistemas.
- Aplicar medidas básicas para proteger la información, las aplicaciones, las comunicaciones y los sistemas informáticos.

II.B-Presentación en inglés



This course will cover the fundamental concepts related to cybersecurity and the protection of information, systems, applications, and networks against potential threats and attacks. The course will address the basic principles of information security, such as confidentiality, integrity, and availability, as well as the main risks, vulnerabilities, and protection measures. It will also examine the different stages of a cyberattack, from the initial gathering of information to gaining access to systems and responding to an incident. Throughout the course, students will be introduced to the fundamentals of cryptography and its main applications in the protection of data and communications. In addition, the course will analyse the social engineering techniques used to deceive users and obtain information or unauthorised access. It will also cover the most common application vulnerabilities and the main security measures applied to networks, computers, and servers. After completing this course, students should be able to:

- * Know and understand the basic concepts of cybersecurity and information security.
- * Identify assets, threats, vulnerabilities, risks, and security incidents.
- * Know the principles of confidentiality, integrity, and availability of information.
- * Understand the main stages of a cyberattack and recognise possible signs of an attack.
- * Know the basic measures for preventing, detecting, and responding to security incidents.
- * Understand the fundamentals of symmetric and asymmetric encryption, hash functions, digital signatures, and digital certificates.
- * Identify the main social engineering techniques and apply basic measures to prevent them.
- * Recognise the most common vulnerabilities related to application security.
- * Know the main measures used to protect networks, computers, and servers.
- * Understand the importance of updates, access control, backups, and system monitoring.
- * Apply basic measures to protect information, applications, communication

III.-Resultados de Aprendizaje

COM6. Evaluar la eficacia del ciclo de inteligencia utilizando una variedad de medidas y criterios que les permita hacer recomendaciones para mejorar la eficacia de dicho ciclo.

CON13. Conocer los desafíos que la sobreinformación y la Inteligencia artificial plantean a la humanidad.

CON14. Comprender cómo se utilizan la tecnología de la información y la comunicación (TIC) en el ámbito de la seguridad. Conocer las amenazas cibernéticas y cómo proteger la información y las infraestructuras críticas

HAB6. Utilizar eficazmente la tecnología de inteligencia moderna. Esto incluye el uso de software de análisis de datos y plataformas de vigilancia para recopilar y analizar información.

- 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 informática.
 Tema 2. Anatomía de un ataque.
 Tema 3. Criptografía y sus aplicaciones.
 Tema 4. Ingeniería social.
 Tema 5. Introducción a las vulnerabilidades típicas relacionadas con la seguridad de las aplicaciones
 Tema 6. Seguridad en Redes, Equipos y Servidores.

IV.B.-Actividades formativas

Tipo	Descripción
Asistencia a clases teóricas	Tienen como objetivo transmitir conocimiento y activar procesos cognitivos en el estudiante (método expositivo/lección magistral). Las exposiciones serán por parte del profesor y la participación de los estudiantes en las actividades propuestas.
Resolución de ejercicios, problemas, casos	Desarrollo de actividades prácticas destinadas a aplicar los contenidos teóricos mediante la resolución de ejercicios guiados, el análisis de incidentes de seguridad y el estudio de casos reales o simulados. Estas actividades permitirán identificar amenazas, vulnerabilidades, riesgos y posibles medidas de protección
Prácticas	Actividades presenciales realizadas en el aula de informática en las que el alumnado utilizará herramientas y entornos controlados para analizar problemas de seguridad, configurar medidas de protección, revisar vulnerabilidades y observar el funcionamiento de distintas técnicas de seguridad informática. Estas sesiones estarán orientadas a consolidar las competencias técnicas mediante el trabajo autónomo o colaborativo
Tutorías académicas	Sesiones individuales o en grupo destinadas a la orientación, resolución de dudas y seguimiento del progreso del alumnado en relación con los contenidos y actividades de la asignatura.
Trabajos colectivos	Elaboración de actividades a realizar de manera colectiva sobre el análisis de amenazas, vulnerabilidades, incidentes o medidas de protección en contextos reales o simulados. Estos trabajos estarán dirigidos a aplicar los conocimientos adquiridos y a desarrollar la autonomía, la capacidad de análisis y la toma de decisiones relacionadas con la seguridad informática.

Realización de Pruebas

Realización de pruebas teóricas y prácticas destinadas a evaluar el grado de comprensión y aplicación de los contenidos de la asignatura. Estas pruebas podrán realizarse de forma parcial o global e incluirán cuestiones conceptuales, resolución de ejercicios y análisis de situaciones relacionadas con la ciberseguridad.

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

Clases teóricas	22
Clases de resolución de ejercicios, problemas, casos, etc.	12
Prácticas en laboratorios experimentales, tecnológicos, clínicos, campo, etc.	24
Realización de pruebas	2
Tutorías académicas	48
Actividades relacionadas: jornadas, seminarios, etc.	0
Preparación de clases teóricas	20
Preparación de prácticas/ejercicios/casos	30
Preparación de pruebas	22
Total de horas de trabajo del alumnado	180

VI.-Metodología y plan de trabajo

Tipo	Periodo	Contenido
Clases Teóricas	Semana 1 a Semana 15	Tienen como objetivo transmitir conocimiento y activar procesos cognitivos en el estudiante (método expositivo/lección magistral). Las exposiciones serán por parte del profesor y la participación de los estudiantes en las actividades propuestas
Resolución de ejercicios, problemas, casos	Semana 1 a Semana 15	Sesiones de resolución de problemas: Tienen como objetivo la aplicación directa de los conocimientos adquiridos durante las sesiones teóricas. Se plantean una serie de problemas que los estudiantes deben resolver, principalmente de manera individual
Prácticas	Semana 4 a Semana 15	Sesiones prácticas con las herramientas vistas en el temario de la asignatura. Tienen como objetivo mostrar al estudiante cómo resolver problemas prácticos para que el estudiante tome contacto con problemas reales y lo resuelva o bien tome decisiones haciendo uso de lo aprendido.



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	Reevaluación Extraordinaria	Ponderación	Actividad de evaluación	Nota mínima	Contenidos	Fecha
SE2 - Entrega de trabajos/proyectos/portafolios/individuales o colectivos	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria.	20%	Prueba 1 (20%)	4	Temas 1 y 2	Semana 5 o 6
SE4 - Resolución de problemas o casos prácticos	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria.	40%	Prueba 2 (20%)	4	Temas 3 y 4	Semana 11 o 12
			Prueba 3 (20%)	4	Temas 5 y 6	Semana 14 o 15
SE1 - Prueba escrita de respuesta abierta o tipo test	Sí. Todas las pruebas seguirán el mismo formato que en ordinaria.	40%	Prueba 4	5	Temas 1, 2, 3, 4, 5 y 6	Fecha del examen de convocatoria ordinaria

Cálculo de la nota final

- La calificación global de la asignatura será la media ponderada de las calificaciones obtenidas por el estudiante en cada una de las actividades de evaluación, siempre que se haya superado la nota mínima en cada una de las pruebas.
- 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 el mínimo entre la nota media ponderada y un 4.
- Si no se ha presentado a alguna de las pruebas evaluables en la convocatoria, la nota final será el mínimo entre la media ponderada, considerando un 0 en las pruebas no presentadas, y un 4.
- Si no se ha presentado a ninguna prueba evaluable, la nota final será **No presentado**.

Convocatoria extraordinaria

En convocatoria extraordinaria las estudiantes y los estudiantes se presentarán a la re-evaluación de las pruebas no superadas (no han alcanzado la nota mínima o las no presentadas). En el caso especial de que en la convocatoria ordinaria se alcanzasen las notas mínimas exigidas en todas las pruebas, pero la nota final fuera inferior a 5 puntos, en la convocatoria extraordinaria las y los estudiantes podrán presentarse a subir nota en alguna o en todas las pruebas reevaluables en las que hubiesen obtenido menos de 5 puntos. La calificación obtenida en la convocatoria extraordinaria sustituirá a la obtenida previamente, con independencia de si es mayor o menor.

Si no se ha presentado a ninguna prueba no superada en convocatoria ordinaria, la nota final de la asignatura en convocatoria extraordinaria será **No presentado**.

Para el cálculo de la nota final en esta convocatoria se utilizará la calificación de las pruebas superadas en convocatoria ordinaria y las notas obtenidas en las pruebas reevaluadas. El cálculo de la nota final se realiza tal y como se indica en el apartado anterior

La re-evaluación de las pruebas se realizará en la fecha oficial indicada para la convocatoria extraordinaria.

Se considerará aprobada la asignatura cuando la nota media ponderada es igual o superior a 5.

Convocatoria adelantada

La convocatoria adelantada sigue los mismos sistemas de evaluación establecidos para la convocatoria ordinaria y 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** (<http://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: Computer Security Fundamentals. 5ª Edición

Autor: W. Easttom

Editorial: Pearson IT Certification

Año: 2024

Título: Ciberseguridad: prevención, análisis y respuesta a incidentes

Autora: María Teresa Moreno García

Editorial: RA-MA

Año: 2024

Título: Seguridad de equipos informáticos. Edición 2024

Autor: Arturo Enrique Mata García

Editorial: RA-MA

Año: 2023

Título: Ciberinteligencia de la amenaza en entornos corporativos

Autor: Mario Guerra Soto

Editorial: RA-MA

Año: 2023

Título: Ciberseguridad. Manual práctico

Autor: J. M. Ortega Candel

Editorial: Paraninfo

Año: 2021

Bibliografía complementaria

Título: Seguridad informática. Edición 2020

Autor: A. Postigo Palacios

Editorial: Paraninfo

Año: 2020

Orion Intelligence. (s. f.). *Repositorio*. Recuperado el 22 de junio de 2026, de <https://orionintel.es/repositorio/>

IX.-Profesorado

Nombre y apellidos	CARLOS VILLARRUBIA MARTÍN
Correo electrónico	carlos.villarrubia@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Madrid - Quintana
Categoría	Profesor/a Ayudante Doctor/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	0



Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	1
Nombre y apellidos	CRISTIAN GÓMEZ MACÍAS
Correo electrónico	cristian.gomez@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Madrid - Quintana
Categoría	Profesor/a Ayudante Doctor/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	0
Nº de Sexenios	1
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	0
Nombre y apellidos	FRANCISCO JAVIER PÉREZ BLANCO
Correo electrónico	francisco.perez@urjc.es
Departamento	Informática y Estadística
Campus de impartición	Madrid - Quintana
Categoría	Profesor/a Ayudante Doctor/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	1
Nº de Sexenios	1
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	2



