UAB
Universitat Autònoma de Barcelona

# Gestión de la Seguridad de los Sistemas de Información

2026/2027

Código: 102161
Créditos: 6

| Titulación | Tipo | Curso |
|---|---|---|
| Empresa y Tecnología | OP | 4 |
| Gestión Aeronáutica | OP | 4 |

## Profesor/a de contacto

Nombre : Miguel Angel Cara Ruiz

Correo electrónico : miguelangel.decara@uab.cat

## Equipo docente

Miguel Angel Cara Ruiz

## Idiomas de los grupos

Puede consultar esta información al final del documento.

## Prerrequisitos

A pesar de no haber prerequisitos, se recomienda cursar la asignatura 102169-Redes.

## Objetivos

### Objetivos de la asignatura

La asignatura tiene como objetivo proporcionar al alumnado una visión global, aplicada y progresiva de la seguridad de la información en las organizaciones, combinando fundamentos técnicos, gobierno de la seguridad, gestión del riesgo y aplicación práctica mediante un caso de trabajo continuo.

- Comprender los fundamentos de la ciberseguridad y de la seguridad de la información en un contexto organizativo.
- Analizar el estado de la seguridad de la información de una organización desde una perspectiva global, teniendo en cuenta activos, procesos, riesgos, controles y necesidades del negocio.
- Dotar al alumnado de las habilidades técnicas y de gestión necesarias para comprender el entorno tecnológico de la seguridad de la información.
- Entender las necesidades de seguridad de la información en las organizaciones y transmitirlas a la Dirección

- Conocer los marcos legales, estándares internacionales, normativas y buenas prácticas que afectan a la seguridad de la información.
- Identificar y valorar riesgos de seguridad de la información, proponiendo medidas de mitigación adecuadas y priorizadas.
- Comprender los principales ámbitos técnicos de la seguridad: gestión de identidades, contraseñas y criptografía, redes, protección del dato, nube, IoT, seguridad en aplicaciones y respuesta a incidentes.
- Evaluar el impacto de la seguridad de la información en la continuidad del negocio, la protección del dato, el cumplimiento normativo y la toma de decisiones de la Dirección.
- Aplicar los conocimientos adquiridos en un caso práctico mediante entregables progresivos: inventario de activos y procesos, valoración inicial, análisis de riesgos, plan de proyectos, arquitectura de seguridad y propuestas de mejora..

## Competencias detalladas

- Demostrar una visión global de la seguridad de la información en las organizaciones.
- Comprender el alineamiento entre los objetivos de la organización y los objetivos de seguridad de la información.
- Identificar el estado de la seguridad tanto desde un punto de vista de gestión organizativa como desde un punto de vista técnico.
- Identificar carencias en el gobierno de la seguridad corporativa y proponer líneas de actuación para su mejora.
- Identificar riesgos de seguridad de la información y plantear medidas de tratamiento adecuadas.
- Comprender los principales ámbitos técnicos de la seguridad de la información, incluyendo identidad, criptografía, redes, protección del dato, nube, IoT, aplicaciones y respuesta a incidentes.
- Demostrar habilidades para comunicar conceptos técnicos de seguridad a destinatarios sin conocimiento especializado, tanto de forma oral como escrita.
- Aplicar los conocimientos adquiridos en ejercicios de evaluación continuada, presentaciones y entregables vinculados al caso práctico de la asignatura.

## Resultados de aprendizaje detallados

- Evaluar el estado de la seguridad de la información de una organización, en coherencia con su sector de actividad, contexto legal, exposición y nivel de riesgo asumible por la Dirección.
- Definir la estrategia inicial de implantación o mejora de un sistema de gestión de la seguridad de la información.
- Aplicar una metodología básica de análisis de riesgos para identificar amenazas, vulnerabilidades, impactos y medidas de mitigación.
- Definir un plan de proyectos de seguridad priorizado, justificando las acciones propuestas según criterios de riesgo, impacto y alineamiento con el negocio.
- Explicar el papel de los marcos de referencia, estándares y buenas prácticas en la organización, gestión y mejora continua de la seguridad de la información.
- Valorar la importancia de la protección del dato, la gestión de identidades, la criptografía y la seguridad en aplicaciones dentro de una estrategia corporativa de seguridad.
- Comprender los riesgos y criterios de seguridad asociados al uso de soluciones cloud, entornos IoT y tecnologías emergentes, incluyendo la seguridad en inteligencia artificial.
- Analizar situaciones de respuesta a incidentes desde una perspectiva organizativa y técnica, identificando necesidades de detección, contención, comunicación y mejora posterior.

## Resultados de aprendizaje

Empresa y Tecnología

- CM26 (Cumplir los principios éticos, legales y de propiedad intelectual con relación al tratamiento de la

información privada en el ámbito empresarial.) Cumplir los principios éticos, legales y de propiedad intelectual con relación al tratamiento de la información privada en el ámbito empresarial.
- KM22 (Identificar a partir de las necesidades de una organización los sistemas de gestión y comunicación de datos, así como su gobernanza.) Identificar a partir de las necesidades de una organización los sistemas de gestión y comunicación de datos, así como su gobernanza.
- SM16 (Distinguir las actividades de gestión de la seguridad y su implicación en el diseño e implementación de sistemas de información.) Distinguir las actividades de gestión de la seguridad y su implicación en el diseño e implementación de sistemas de información.

## Contenidos

### Seguridad de la Información y Ciberseguridad

- Comprender qué se entiende por seguridad de la información y ciberseguridad en el contexto de las organizaciones.
- Identificar la importancia de la seguridad de la información en entornos corporativos, considerando su impacto en el negocio, la continuidad operativa, la protección del dato y la toma de decisiones.
- Analizar los principales conceptos de confidencialidad, integridad, disponibilidad, autenticación, trazabilidad y responsabilidad.
- Comprender la evolución de las amenazas y riesgos de ciberseguridad en las organizaciones actuales.

### Gobierno, marcos de referencia y gestión de la seguridad

- Conocer los principales marcos de referencia, estándares y buenas prácticas aplicables a la seguridad de la información.
- Comprender el papel de los marcos de referencia en la organización, gestión y mejora continua de la seguridad.
- Identificar cómo se alinean los objetivos de seguridad de la información con los objetivos estratégicos y operativos de la organización.
- Analizar las carencias de seguridad de una organización y proponer líneas de actuación para su mejora.
- Entornos tecnológicos de Cloud Computing

### Análisis y gestión de riesgos

- Comprender la importancia del análisis de riesgos en la gestión de la seguridad de la información.
- Identificar activos, procesos, amenazas, vulnerabilidades, impactos y controles dentro de un entorno corporativo.
- Aplicar una metodología básica de análisis de riesgos para valorar el estado de seguridad de una organización.
- Definir medidas de mitigación y planes de actuación priorizados según criterios de riesgo, impacto y viabilidad.

### Gestión de identidades, contraseñas y criptografía

- Comprender la importancia de la gestión de identidades y accesos en la seguridad corporativa.
- Analizar los riesgos asociados al uso de contraseñas, autenticación débil y mala gestión de privilegios.
- Conocer los principios básicos de la criptografía y su aplicación en la protección de la información.
- Diferenciar entre cifrado simétrico, cifrado asimétrico, funciones hash, certificados digitales y firma digital.

### Seguridad en redes y entornos tecnológicos

- Comprender los fundamentos de la seguridad en redes de comunicaciones.
- Identificar riesgos habituales en arquitecturas de red corporativas y posibles medidas de protección.
- Analizar el papel de los controles de seguridad en redes, segmentación, monitorización y protección perimetral.
- Relacionar la seguridad de red con el resto de ámbitos de la seguridad corporativa.

### Protección del dato y cumplimiento normativo

- Comprender la importancia de la protección del dato dentro de una estrategia de seguridad de la información.
- Identificar los principales requisitos legales, normativos y regulatorios que afectan a la seguridad y protección de la información.
- Analizar el impacto del cumplimiento normativo en la gestión de la seguridad corporativa.
- Comprender la relación entre protección del dato, gobierno de la seguridad, riesgos y controles técnicos.

### Seguridad en nube, IoT y tecnologías emergentes

- Comprender los principales riesgos asociados al uso de soluciones cloud en entornos corporativos.
- Identificar criterios de seguridad aplicables a servicios cloud, modelos de responsabilidad compartida y protección de la información en la nube.
- Analizar los riesgos específicos de entornos IoT y dispositivos conectados.
- Comprender los riesgos emergentes vinculados a nuevas tecnologías, incluyendo la seguridad en inteligencia artificial.

### Seguridad en aplicaciones

- Comprender los fundamentos de la seguridad en aplicaciones y su importancia en el ciclo de vida tecnológico.
- Identificar riesgos habituales en aplicaciones corporativas y servicios expuestos.
- Relacionar la seguridad en aplicaciones con la protección del dato, la identidad, la red y la gestión de vulnerabilidades.

### Respuesta a incidentes

- Comprender el ciclo de gestión y respuesta ante incidentes de seguridad.
- Identificar las fases principales de detección, análisis, contención, erradicación, recuperación y mejora posterior.
- Analizar incidentes de seguridad desde una perspectiva técnica y organizativa.
- Comprender la importancia de la comunicación, la documentación y la toma de decisiones durante un incidente.

### Caso práctico aplicado

- Aplicar los conocimientos adquiridos en un caso práctico continuo de seguridad de la información.
- Elaborar un inventario de activos, procesos y valoración inicial del caso.
- Realizar una valoración de riesgos y definir un plan de proyectos de seguridad.
- Proponer una arquitectura de seguridad coherente con las necesidades del caso.
- Identificar mejoras adicionales y justificar su prioridad en función del riesgo, impacto y alineamiento con el negocio.
- Presentar y defender las conclusiones del caso práctico de forma clara, estructurada y orientada a perfiles técnicos y no técnicos.

## Actividades formativas y Metodología

| Título | Horas | ECTS | Resultados de aprendizaje |
|---|---|---|---|
| Trabajo en grupo | 20 | 0,8 | |
| Estudio | 50 | 2 | |
| Problemas y Ejercicios | 15 | 0,6 | |
| | | | |

| | | |
|---|---|---|
| Clases magistrales y casos | 30 | 1,2 |
| redacción de trabajos y preparación de casos | 32 | 1,28 |

## Aspectos Generales

### 1. Relación profesorado-alumnado

La información general y relevante de la asignatura se publicará en el Campus Virtual, o espacio equivalente habilitado por la universidad. En este espacio se detallarán los contenidos de la guía docente, las fechas de evaluación continuada, las fechas y condiciones de entrega de trabajos, los materiales de apoyo y cualquier otra información necesaria para el seguimiento de la asignatura.

La planificación de la asignatura podrá estar sujeta a ajustes por motivos organizativos, académicos o por incidencias sobrevenidas. En caso de producirse cambios en la programación, estos serán comunicados a través del Campus Virtual, que se considerará el canal habitual de comunicación entre el profesorado y el alumnado.

### 2. Idiomas

Las clases se realizarán mayoritariamente en catalán o castellano, aunque será habitual la aparición de términos técnicos en inglés. El material escrito o de apoyo a la asignatura, como apuntes, bibliografía, referencias, enunciados de prácticas, ejercicios o casos, podrá facilitarse en catalán, castellano o inglés. En este sentido, el uso de la lengua inglesa podrá ser habitual, especialmente en materiales técnicos o referencias especializadas.

La prueba final y la reevaluación estarán redactadas en catalán o castellano. Las respuestas a las pruebas, ejercicios, prácticas y presentaciones podrán entregarse indistintamente en catalán, castellano o inglés

## Actividades durante el curso

### Clases magistrales, casos y sesiones de resolución de ejercicios

Durante las sesiones teóricas se presentarán los contenidos fundamentales de la asignatura, necesarios para comprender los principales ámbitos de la seguridad de la información en las organizaciones.

Estas sesiones abordarán, entre otros aspectos, los fundamentos de la ciberseguridad, los marcos de referencia, el análisis de riesgos, la gestión de identidades, la criptografía, la seguridad en redes, la protección del dato, la seguridad en nube e IoT, la seguridad en aplicaciones, la respuesta a incidentes y las tecnologías emergentes, incluyendo la seguridad en inteligencia artificial.

Las clases podrán combinar explicación teórica, análisis de ejemplos, resolución de ejercicios, discusión de casos y actividades de evaluación continuada. Asimismo, se indicarán las vías necesarias para ampliar o profundizar los contenidos tratados en clase.

### Aprendizaje Basado en Problemas, aprendizaje cooperativo, talleres y ejercicios prácticos

Una parte de la asignatura utilizará metodologías de aprendizaje activo y ejercicios de carácter aplicado, en

los que el alumnado tendrá que enfrentarse a situaciones cercanas a la práctica profesional de la seguridad de la información en entornos corporativos.

Durante el curso se podrán realizar actividades individuales y en grupo, supervisadas por el equipo docente de la asignatura. Estas actividades estarán orientadas a la aplicación práctica de los contenidos trabajados en clase, especialmente mediante el desarrollo del caso práctico de la asignatura.

Se fomentará el trabajo en equipo y el intercambio colaborativo de información y herramientas para la resolución de problemas. No obstante, el proceso final de aprendizaje deberá ser individual, apoyado en la actividad autónoma de cada estudiante, que deberá complementar y enriquecer el trabajo iniciado en las sesiones dirigidas del curso.

La actividad supervisada, mediante tutorías regladas y consultas efectuadas durante el curso, será igualmente una herramienta importante para la adquisición de los conocimientos y competencias que proporciona la asignatura.

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

## Evaluación

### Actividades de evaluación continuada

| Título | Peso | Horas | ECTS | Resultados de aprendizaje |
|---|---|---|---|---|
| Prácticas, ejercicios y participación | 60% | 0 | 0 | CM26, KM22, SM16 |
| Exámenes | 40% | 3 | 0,12 | CM26, KM22, SM16 |

Esta asignatura no contempla la posibilidad de evaluación única.

La evaluación consta de dos partes complementarias:

(1) Prácticas, Ejercicios y Participación (6 puntos):

Ejercicio(s) de aprendizaje basado en problemas, trabajo en equipo o individual, presentación en clase de los resultados y otras pruebas que se determinen. Si el peso de la actividad es de 1 puntos o más, se publicará un aviso en el campus virtual con una anticipación de al menos una semana.

Estas actividades, por ser de evaluación continua no se podrán recuperar. Se entregarán en los plazos y condiciones establecidas que se harán públicas en el Campus Virtual de la asignatura.

(2) Teoría (4 puntos):

Prueba escrita final sobre conceptos y aspectos tratados a lo largo del curso que se realizará el día que determine la facultad en el calendario de exámenes.

Durante el curso se pueden hacer pruebas parciales liberadoras de materia. Para cada una de ellas se publicará un aviso en el campus virtual con una anticipación de al menos una semana

Condiciones generales para superar la asignatura:

Para aprobar la asignatura es necesario obtener 5 puntos habiendo alcanzado los mínimos siguientes:

- Prácticas Ejercicios y Participación: mínimo 2.5 puntos de 6 posibles
- Teoría: mínimo 1.5 puntos de 4 posibles

Cálculo de la nota final:

- Si se alcanzan los mínimos será el menos la suma de la obtenida en las dos partes. El profesor podrá, no obstante, aumentarla atendiendo a criterios objetivos y equitativos. Si después de la suma de los resultados obtenidos en ambas partes no alcanzaran los 5 puntos necesarios para aprobar la asignatura, el estudiante podrá efectuar el proceso de recuperación enlas condiciones que se describen más adelante.
- Si no se alcanzan los mínimos de la parte Prácticas, Ejercicios y Participación la nota final de la asignatura será la de esta parte y por tanto la asignatura quedará suspendida.
- Si no se alcanzan los mínimos de la parte Teoría y la suma de las partes es inferior a 3,5 puntos la nota final será la suma de las partes y por tanto la asignatura quedará suspendida
- Si no se alcanzan los mínimos de la parte Teoría y la suma de las partes es superior o igual a 3,5 puntos se podrá hacer la prueba de recuperación en las condiciones descritas más adelante.

Se considerará Evaluable cualquier estudiante que haya hecho al menos dos entregas en la evaluación continua.

Calendario de actividades de evaluación

Las fechas de las diferentes actividades de evaluación (ejercicios, entrega de trabajos, etc.) se anunciarán con suficiente antelación durante el semestre.

Las fechas de los exámenes parcial y final de la asignatura estan programadas en el calendario de exámenes de la Facultad.

\"*La programación de las pruebas de evaluación no se podrá modificar, salvo que haya un motivo excepcional y debidamente justificado por el cual no se pueda realizar un acto de evaluación. En estecaso, las personas responsables de las titulaciones, previa consulta al profesorado y al estudiantado afectado, propondrán una nueva programación dentro del período lectivocorrespondiente*.\" ***Apartado 1 del Artículo 115. Calendario de las actividades de evaluación (Normativa Académica UAB)***

Los y las estudiantes de la Facultad de Economía y Empresa que de acuerdo con el párrafo anterior necesiten cambiar una fecha de evaluación han de presentar la petición rellenando el documento Solicitud reprogramación prueba https://eformularis.uab.cat/group/deganat_feie/solicitud-reprogramacion-de-pruebas

Procedimiento de revisión de las calificaciones

Coincidiendo con el examen final se anunciará el día y el medio en que es publicarán las calificaciones finales. De la misma manera se informará del procedimiento, lugar, fecha y hora de la revisión de exámenes de acuerdo con la normativa de la Universidad.

Proceso de Recuperación

*"Para participar en el proceso de recuperación el alumnado debe haber sido previamente evaluado en un conjunto de actividades que represente un mínimo de dos terceras partes de la calificación total de la asignatura o módulo."****Apartado 3 del Artículo 112 ter. La recuperación(Normativa Académica UAB).*** Los y las estudiantes deben haber obtenido una calificación media de la asignatura entre 3,5 y 4,9.

La fecha de esta prueba estará programada en el calendario de exámenes de la Facultad. El estudiante que se presente y la supere aprobará la asignatura con una nota de 5. En caso contrario mantendrá la misma nota.

Irregularidades en actos de evaluación

Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, y de acuerdo con la normativa académica vigente, *"*en caso que el estudiante realice cualquier irregularidad que pueda conducir a una variación significativa de la calificación de un acto de evaluación, se calificará con un 0 este acto de evaluación, con independencia del proceso disciplinario que se pueda instruir. En caso que se produzcan*

*diversas irregularidades en los actos de evaluación de una misma asignatura, la calificación final de esta asignatura será 0\".* ***Apartado 10 del Artículo 116. Resultados de la evaluación. (Normativa Académica UAB)***

La realización de las actividades de evaluación está sujeta a lo establecido en esta guía docente y en la "Política de la Facultad de Economía y Empresa ante la detección de irregularidades durante la realización de actividades evaluativas", que regula las condiciones en las que se desarrollan las pruebas de evaluación y los procedimientos aplicables ante indicios de irregularidad. Se recomienda al estudiantado consultar su contenido.

## Bibliografía

Ver Campus Virtual

## Software

No se utiliza software excepto el que forma parte de la ofimática convencional

### Grupos e idiomas de la asignatura

La información proporcionada es provisional hasta el 30 de noviembre. A partir de esta fecha, podrá consultar el idioma de cada grupo a través de este enlace. Para acceder a la información, será necesario introducir el CÓDIGO de la asignatura

| Tipo de docencia | Grupo | Idioma | Semestre | Turno |
|---|---|---|---|---|
| (TE) Teoría | 20 | Catalán | primer cuatrimestre | tarde |
| (PAUL) Prácticas de aula | 201 | Catalán | primer cuatrimestre | tarde |