COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

GUÍA DOCENTE
2025 - 2026

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Gobierno, Riesgo y Cumplimiento de la Seguridad
Código	DTC-MCS-513
Impartido en	Máster en Ciberseguridad [Primer Curso]
Nivel	Master
Cuatrimestre	Anual
Créditos	6,0 ECTS
Carácter	Obligatoria
Departamento / Área	Departamento de Telemática y Computación
Responsable	Juan Francisco Cornago Baratech
Horario	Miercoiles de 17:00 a 19:00 y Viernes de 18:00 a 20:00
Horario de tutorías	Por petición previa a través de correo
Descriptor	La disciplina de GRC dota al alumnado de un marco práctico para gobernar la ciberseguridad, gestionar riesgos y cumplir regulaciones en organizaciones reales. Integra negocio, tecnología y normativa (por ejemplo, ISO/IEC 27001, ISO 31000/27005, NIST CSF 2.0, ENS, NIS2, DORA, RGPD y AI Act), conectando el trabajo del CISO Office, auditoría, legal/compliance, continuidad de negocio y equipos operativos (SOC/IR). La asignatura prepara para implantar programas GRC medibles, auditables y sostenibles, alineados con la estrategia corporativa y el apetito de riesgo.

Datos del profesorado	
Profesor	
Nombre	David Estévez Maestre
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	destevez@icai.comillas.edu
Profesor	
Nombre	Juan Francisco Cornago Baratech
Departamento / Área	Departamento de Telemática y Computación
Despacho	Cualquier duda o aclaración por correo electrónico
Correo electrónico	jfcornago@icai.comillas.edu
Profesor	
Nombre	Valentín López Sotomayor
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	vlsotomayor@icai.comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

GUÍA DOCENTE
2025 - 2026

Aportación al perfil profesional de la titulación

Al cursar esta asignatura, el estudiante estará capacitado para desempeñar funciones de:

- **Analista/Manager de GRC** en CISO Office y/o Compliance.
- **Risk Owner / Risk Analyst** con enfoque **ISO 31000** y cadena de suministro.
- **Consultor/a y auditor/a** de marcos de control (ISO 27001, NIST, ENS, etc.).
- **Responsable de proyectos de cumplimiento** (NIS2, DORA, RGPD, AI Act) con orientación a evidencia.
- **BCM & Crisis**: integración de continuidad de negocio (**ISO 22301**), DRP y gestión de crisis cibernética.
- **Reporting a dirección**: cuadros de mando, KRIs/KPIs, comités y comunicación ejecutiva.

Prerrequisitos

- **Recomendados**: fundamentos de sistemas y redes, nociones de seguridad de la información, gestión de proyectos y bases de derecho TIC/protección de datos.
- **Habilidades deseables**: pensamiento crítico, comunicación ejecutiva, manejo avanzado de Excel/Docs y lectura de normativa técnica.

Competencias - Objetivos

Competencias

Competencias específicas

1. Diseñar y gobernar un **programa GRC** alineado con la estrategia y el apetito de riesgo.
2. Aplicar **ISO 31000/27005** PARa identificar, analizar, valorar y tratar riesgos; definir **KRIs** y planes de mitigación.
3. Mapear y evaluar **controles** frente a marcos de referencia (ISO 27001, NIST CSF/800-53, ENS, COBIT, ISO 22301).
4. Planificar y desplegar **programas de cumplimiento** (NIS2, DORA, RGPD, AI Act), con enfoque de **accountability** y evidencias auditables.
5. Integrar GRC con **SOC/IR**, continuidad y gestión de crisis; diseñar **procedimientos** y **RACI**.
6. Elaborar **cuadros de mando** y **reporting** ejecutivo comprensibles para Comité de Dirección.
7. Evaluar riesgos de **terceros y cadena de suministro** (TPRM) y definir cláusulas y controles contractuales.
8. Dirigir **auditorías internas** y planes de mejora continua.

Competencias transversales

- Comunicación escrita y oral orientada a negocio.
- Trabajo en equipo y liderazgo situacional.
- Pensamiento crítico y toma de decisiones bajo incertidumbre.
- Ética profesional y cumplimiento de la normativa académica.

Resultados de Aprendizaje

- RA1: Construye un **mapa de riesgos** y un **registro de riesgos** completo, con valoración cualitativa y cuantitativa básica.
- RA2: Entrega un **Plan de Tratamiento de Riesgos** con KRIs, responsables y plazos, justificando el coste/beneficio.
- RA3: Presenta un **programa GRC** y su **modelo de gobierno** (políticas, comités, RACI) para un sector concreto.
- RA4: Demuestra conformidad trazable entre **controles** y **exigencias normativas** (mapeo control–requisito–evidencia).
- RA5: Ejecuta una **simulación de comité de riesgos** defendiendo decisiones ante dirección.
- RA6: Elabora **dashboards ejecutivos** con indicadores de desempeño (KPIs) y de riesgo (KRIs).

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

Índice de contenido

  - Infraestructuras críticas, Servicios esenciales y Privacidad
- TEMA GRC 6. Sistema Integrado de Gestión.
  - Qué es. Por qué es necesario. Qué va a controlar. Quien es el responsable. Cómo se construye. Cómo se mantiene.
- TEMA GRC 7. Cuadro de mando de la ciberseguridad.
  - medir. A quién reporto. Cada cuánto tiempo. Cómo lo divulgo.
- TEMA GRC 8. Auditoría.
  - Metodología
  - Caso práctico. Auditando una Organización.
- TEMA GRC 9: CÓMO GESTIONAR EL RIESGO EN LAS ORGANIZACIONES
  - Análisis de riesgo mediante la metodología MAGERIT
  - Tratamiento de los riesgos.
  - Herramientas: PILAR, MOSLER
  - Otras metodologías de análisis de riesgo.
  - Caso práctico. Realización de un análisis de riesgo real en una organización.
- TEMA GRC 10: CULTURA DE LA CIBERSEGURIDAD
  - El usuario final, principal actor en materia de ciberseguridad.
  - Cómo atraer la atención del usuario.
- Persuasión frente a la simple comunicación.

- TEMA C1. Introducción a GID
  - ¿Qué es la Gestión de Identidades?
  - Áreas de la Gestión de Identidades y Accesos
  - Identidad Digital
- TEMA C2. Control de Acceso
  - Componentes del Control de Acceso
  - Modelos de Control de Acceso
  - Técnicas y Administración de Control de Acceso
  - Inicio de sesión único (single sign on)
  - Directorios
- TEMA C3. Access Manager
  - Federación de Identidades
  - SAML
  - Cl@ve
  - OAUTH
  - FIDO
  - CIAM
- TEMA C4. Gobierno de la Identidad
  - Gobierno de la Identidad
  - Ciclo de Vida JML
  - Segregación Funcional (SoD)
  - Recertificación de Accesos.
  - RBAC y ABAC
  - Perfilado
- TEMA C5 Cuentas Privilegiadas
  - Importancia de las cuentas privilegiadas

  - Controles adicionales
  - Soluciones dedicadas.
- TEMA C6. Cloud Access
  - La nube: nuevas amenazas
  - ¿Qué es diferente entre Gobierno de Cloud vs IGA?
  - Gobierno Cloud

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Aspectos metodológicos generales

- **Aprendizaje activo**: clases participativas con mini-casos, debates guiados y análisis de incidentes reales.
- **Prácticas posibles**: construcción de un **registro de riesgos**, **mapeo control-requisito**, **plan de tratamiento** y **dashboard**.
- **Trabajo en equipo**: participación en clase con **simulación de comité de riesgos** (rol de CISO/negocio/auditoría).
- **Lecturas dirigidas**: estándares y guías oficiales; resúmenes ejecutivos para discutir en clase.
- **Herramientas**: hojas de cálculo plantilladas, con opción de demo en **plataforma GRC** (no se exige licenciamiento).
- **Política de IA generativa**: se permite su uso **con cita explícita** de las herramientas empleadas; el/la estudiante **es responsable** del contraste de fuentes y de la autoría final. Cualquier plagio o generación no reconocida se considerará falta grave.
- **Accesibilidad**: materiales y evaluación adaptables a necesidades justificadas.

Política de uso de IA generativa (ICAI)

- **Objetivo.** Potenciar el aprendizaje con IA sin sustituir el trabajo intelectual propio ni comprometer la evaluación.
- **Uso permitido (con condiciones):**
  - Apoyo a ideación, estructuración, síntesis y revisión lingüística.
  - Búsqueda de referencias y comparación de marcos (p. ej., ISO/NIST/ENS), siempre citando fuentes.
  - Prototipado de artefactos (p. ej., tablas de riesgos) que **deben** revisarse y adaptarse críticamente.
- **Uso prohibido:**
  - Generar total o parcialmente **entregas evaluables** (trabajos, prácticas, exámenes, TFM/TFG) sin declaración explícita y sin aportación crítica propia.
  - Introducir **datos personales o confidenciales** en herramientas de IA sin autorización

Transparencia obligatoria en cada entrega (si se usa IA): Incluye un anexo con: herramienta y versión, fecha, prompts principales, partes generadas o asistidas y cómo se han verificado/contrastado. La ausencia de esta declaración se considerará **uso indebido**.

Verificación y trazabilidad: Podrá requerirse el borrador de trabajo, historial de ediciones y una breve **defensa oral** para comprobar la autoría. Se podrán usar verificaciones de similitud.

Advertencia académica: Un uso indebido podrá conllevar sanciones conforme al Reglamento General de la Universidad Pontificia Comillas (ver **§ 6.3**). Prevalece siempre la normativa oficial.

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Método de evaluación

- Pruebas intermedias: 20%

- Comprensión de los conceptos teóricos.
- Aplicación de dichos conceptos para la resolución de problemas.
- Análisis e interpretación crítica de los resultados obtenidos en la resolución de problemas.

- Examen Final: 60%
  - Comprensión de los conceptos teóricos.
  - Aplicación de dichos conceptos para la resolución de problemas.
  - Análisis e interpretación crítica de los resultados obtenidos en la resolución de problemas.
- Proactividad, Actitud y esfuerzo: 20%
  - Iniciativa y proactividad en el trabajo, y colaboración en el trabajo en equipo.
  - Habilidades de comunicación en la escritura y en las presentaciones verbales.

Calificaciones

Cada parte de la asignatura de GRC se verá evaluada de forma independiente, atendiendo a los criterios del profesor responsable. La nota final de la asignatura será la media, en base a la proporción de horas de cada parte, que corresponda.

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

8.1 Bibliografía básica

1. **ISO/IEC 27001:2022** e **ISO/IEC 27002:2022** – Sistemas de gestión de seguridad de la información.
2. **ISO 31000:2018** e **ISO/IEC 27005:2022** – Gestión del riesgo / riesgo en SI.
3. **NIST Cybersecurity Framework 2.0** y extractos de **NIST SP 800-53 Rev.5**.
4. **ENS** (RD 311/2022, y guías CCN-CERT) – Esquema Nacional de Seguridad.
5. **Directiva NIS2 (UE) 2022/2555** y materiales de ENISA.
6. **Reglamento DORA (UE) 2022/2554** – Resiliencia operativa digital en el sector financiero.
7. **RGPD (UE) 2016/679** – tratamiento de datos y seguridad.
8. **AI Act (UE) 2024/1689** – requisitos de gobernanza de IA y gestión de riesgos.

8.2 Bibliografía complementaria

- **COBIT 2019** – Gobierno de TI y marcos de control.
- **ISO 22301:2019** – Continuidad de negocio.
- **IEC 62443 (familia)** – Seguridad en sistemas de automatización y control industrial.
- **NIST SP 800-37 Rev.2** – Risk Management Framework.
- **Measuring and Managing Information Risk (FAIR)**, Jones & Hood, 2015.
- **The CISO's Guide / Playbooks** (selección actualizada del curso).
- Guías ENISA y EDPB (complementos prácticos).

8.3 Recursos y materiales

- **Plantillas**: registro de riesgos, plan de tratamiento, mapeo control-requisito, dashboard KRIs/KPIs.
- **Casos reales**: informes públicos (post-mortem) y lecciones aprendidas.
- **Herramientas**: hojas de cálculo y demo opcional de plataforma GRC.
- **Normativa**: enlaces a textos consolidados y notas técnicas (aula virtual).

Se presenta una muestra de todas las normativas y buenas prácticas existentes en la actualidad, pero será necesario estar actualizado con cuantas actualizaciones o nuevas normas aparezcan o sean de interés.