Guía Docente
Curso Académico 2026/27

Datos Generales

Asignatura: GOBERNANZA, REGULACIÓN Y ESTÁNDARES.
Titulación: GRADO EN CIBERSEGURIDAD
Carácter: OBLIGATORIA.
Créditos ECTS: 6 ECTS
Curso: 2º
Distribución temporal: 1º SEMESTRE.
Idioma de impartición: CASTELLANO.
Equipo docente: Marcos Ubiria marcos.ubiria@euneiz.com
Aula(s): Aula informatizada

Presentación de la asignatura:

Asignatura teórica para conocer los aspectos relacionados con la gobernanza de los datos, la regulación y los estándares nacionales e internacionales que permitan al alumno adquirir, entender y poner en contexto los aprendizajes enfocados a la ciberseguridad.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)[1]

Contenidos o conocimientos (C)	C2	Reconocer estructuras y protocolos para implementar soluciones de seguridad a nivel de arquitectura de redes de la ciberseguridad.
	C10	Entender las responsabilidades profesionales, éticas y legales a partir de las normas y reglamentos en el ámbito de la ciberseguridad.
	C11	Conocer las diferentes topologías de malware para su posterior análisis y mitigación.
Competencias (CO)	CO11	Gestionar evidencias de vulnerabilidades.
	CO13	Gestionar auditorías sobre marcos y estándares del mercado.
Destrezas o	H2	Desarrollar habilidades para el análisis, la elaboración y la

[1] La clasificación de los RFA corresponde a la definida en el RD822/2021 y se encuentran definidos en la memoria de verificación del título.

* Extender el contenido utilizando para ello la programación docente. La extensión debe estar en punto intermedio, es decir, ampliar la información en la guía docente pero no llegar a los límites de la programación docente. Se debe incluir el índice de temas a tratar punto por punto (sin desarrollar). Se pueden incluir hasta tres subapartados con ideas claves/subtemas. La extensión máxima será de 2 páginas.

habilidades (H)		colaboración en proyectos, partiendo de las necesidades propias del mercado.
	H5	Comunicar de forma clara y concisa, a todo tipo de audiencias, conocimientos, ideas, soluciones, datos, etc. en el ámbito del estudio.
	H6	Ser capaz de trabajar con información técnica en inglés, tanto a nivel de consulta como de su elaboración.

Contenido de la Asignatura*

- Unidad 1: Sistemas de Gestión de Seguridad de la Información
  - o Tema 1: Fundamentos de la gestión de la seguridad de la información
  - o Tema 2: Implantación de un Sistema de Gestión de Seguridad de la Información (SGSI): la norma ISO/IEC 27001
  - o Tema 3: Introducción a los controles de seguridad de la información en la ISO 27001
- Unidad 2: Esquema Nacional de Seguridad
  - o Tema 1: Introducción al ENS
  - o Tema 2: Medidas de Seguridad y requisitos mínimos
- Unidad 3: Normativa sobre protección de datos personales
  - o Tema 1: Introducción
  - o Tema 2: Principios de protección de datos
  - o Tema 3: La obligación de seguridad de los datos
  - o Tema 4: Brechas de datos personales
  - o Tema 5: Infracciones y Sanciones
- Unidad 4: Otras normas relacionadas con la ciberseguridad
  - o Tema 1: Cómo identificar normativas
  - o Tema 2: Otras normas jurídicas
  - o Tema 3: Código Penal: delitos relacionados con la ciberseguridad

Metodologías Docentes y Actividades Formativas[2]

Metodologías docentes utilizadas en esta asignatura son:

MD1	Método expositivo.
MD2	Estudios de caso.

[2] Se deberán extraer de la memoria verificada del título las metodologías docentes, actividades formativas y sistemas de evaluación. (1 ECTS = 25 horas de trabajo del estudiante).

MD3	Aprendizaje basado en problemas.
MD4	Aprendizaje basado en proyectos.
MD5	Aprendizaje cooperativo.
MD6	Tutorías.

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica.	25	100
AF2: Clase prácticas.	15	100
AF3: Realización de trabajos (individuales y/o grupales).	7,5	50
AF3: Tutorías (individuales y/o grupales).	5	0
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	91,5	0
AF6: Pruebas de evaluación.	6	100
Total	**150**	**--**

Evaluación: Sistemas y Criterios de Evaluación

Las semanas de evaluación están definidas en el calendario académico publicado en la web de la universidad; la concreción de las fechas se realizará una vez que la docencia haya comenzado.

Sistemas de evaluación utilizados en esta asignatura son:

Denominación	Pond. Mín	Pond. Máx
SE1 Evaluación de la asistencia y participación del o la estudiante.	0	5

SE2 Evaluación de trabajos.	10	30
SE3 Pruebas de evaluación y/o exámenes.	50	75

El estudiantado posee dos modalidades de evaluación para superar la asignatura:

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con 2 convocatorias/año.

En la Universidad Euneiz la evaluación continua (media ponderada de las diferentes actividades evaluables de la asignatura definidas por el profesorado) es la evaluación primordial; pero Euneiz permite al estudiantado acogerse a la evaluación única.

No se permite el cambio de modalidad de evaluación (de continua a única) escogido por el estudiante a lo largo del curso.

El/la estudiante que desee acogerse a la modalidad de evaluación única deberá solicitarlo por escrito formal que lo justifique dirigido al profesorado responsable de la asignatura y a la Coordinación del título en las dos primeras semanas del inicio de la misma.

Si el/la estudiante no asiste un 80% a las clases presenciales, pasará directamente a la convocatoria extraordinaria de la evaluación única.

De manera excepcional, el/la docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del o la estudiante, etc., la posibilidad de permitir que el/la estudiante continue en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.

Las faltas de asistencia deben justificarse al profesor/a responsable de la asignatura con un plazo máximo de 1 semana. El justificante oficial deberá ser presentado al profesor/a responsable mediante un correo electrónico.

El/la estudiante irá a la evaluación extraordinaria ÚNICAMENTE con las partes suspendidas.

El sistema de calificación de la asignatura sigue lo establecido en el RD 1125/2003 y los resultados obtenidos se calificarán siguiendo la escala numérica de 0 a 10, con expresión de un decimal.

- 0-4,9: Suspenso (SS).
- 5,0-6,9: Aprobado (AP).
- 7,0-8,9: Notable (NT).
- 9,0-10: Sobresaliente (SB).

La mención de «Matrícula de Honor» podrá ser otorgada a alumnos/as que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los/las alumnos/as matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos/as matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

Será considerado no presentado (NP) el estudiantado matriculado que no realice ninguna actividad evaluativa.

Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas ortotipográficas en la calificación final.

El plagio está prohibido, tanto en los trabajos, como en los exámenes, en caso de detectarse la calificación será suspenso. Los trabajos entregados a través del campus virtual serán objeto de análisis por la herramienta Turnitin:

- Los informes con un índice de similitud entre el 20% y el 30% serán revisados por el profesor/a para analizar las posibles fuentes de plagio y evaluar si están justificadas.
- Cualquier trabajo con un índice de similitud superior al 30%, una vez realizado el análisis del o la docente, no será evaluado.

Recursos materiales e infraestructuras necesarias

Tipo de recurso material y/o infraestructura
Material docente (apuntes, presentaciones, guías, tareas…)
Recursos audiovisuales
Material específico de la asignatura
Aula informatizada
Laboratorio de Ciberseguridad

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- ISO27001/ISO27002: Una guía de bolsillo. Calder, Alan, itgovernance, 2017
- UNE-ISO/IEC 27001:2023: Seguridad de la información, ciberseguridad
- Edwards, J., & Weaver, G. (2024). The Cybersecurity Guide to Governance, Risk, and Compliance. John Wiley & Sons. https://doi.org/10.1002/9781394250226

Bibliografía Complementaria

- Ciberseguridad: regulación, estándares y fundamentos: Jersain Zadamig LLamas Covarrubias, 2024

Otros Recursos de Aprendizaje Recomendados[3]

- Ladino, M. I., Villa, P. A., & María, A. L. E. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. Scientia et technica, 1(47), 334-339.
- Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Tecnura*, *19*(46), 123-134.

[3] Entre otros recursos de aprendizaje pueden incluirse páginas web, software, materia audiovisual, etc.