UNIVERSIDAD DEL ATLÁNTICO MEDIO

GUÍA DOCENTE

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

MÁSTER UNIVERSITARIO EN SISTEMAS INTEGRADOS DE GESTIÓN QHSE

MODALIDAD VIRTUAL

CURSO ACADÉMICO 2022-2023

ÍNDICE

RESUMEN 3
DATOS DEL PROFESORADO 3
REQUISITOS PREVIOS 3
COMPETENCIAS 4
RESULTADOS DE APRENDIZAJE 6
CONTENIDOS DE LA ASIGNATURA 6
METODOLOGÍA 7
ACTIVIDADES FORMATIVAS 9
EVALUACIÓN 9
BIBLIOGRAFÍA 11

RESUMEN

Centro	Facultad de Ciencias Sociales y Jurídicas		
Titulación	Master Universitario en Sistemas Integrados de Gestión QHSE		
Asignatura	Sistemas de gestión de seguridad de la información SO 27001	**Código**	F1C3M03004
Materia	Sistemas de gestión		
Carácter	Obligatorio		
Curso	1º		
Semestre	1º		
Créditos ECTS	6		
Lengua de impartición	Castellano/inglés		
Curso académico	2022-2023		

DATOS DEL PROFESORADO

Responsable de Asignatura	José Javier Rainer Granados
Correo electrónico	josejavier.rainer@pdi.atlanticomedio.es
Teléfono	828.019.019
Tutorías	Consultar horario de tutorías en el campus virtual. El horario de atención al estudiante se publicará al inicio de curso en el Campus Virtual. En caso de incompatibilidad con las franjas horarias establecidas pueden ponerse en contacto a través del *mail* para concertar una tutoría fuera de este horario. Se ruega que se solicite la tutoría a través del Campus Virtual o a través del correo electrónico.

REQUISITOS PREVIOS

Sin requisitos previos.

COMPETENCIAS

Competencias básicas:

CB6

Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.

CB7

Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8

Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9

Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10

Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Competencias generales:

CG01

Desarrollar y mantener una estructura documentada de los sistemas de gestión, que asegure la permanente actualización, distribución, registro y buen uso de los documentos tanto internos como externos, utilizando las fuentes y cauces adecuados y desarrollando una cultura tecnológica mediante la utilización de aplicaciones de las TICs.

CG02

Establecer procedimientos con controles operacionales que recojan los criterios y directrices a seguir para asegurar que las actividades no se desvían de la política, los objetivos y metas establecidos, asegurando la plena satisfacción de todas las partes interesadas.

Competencias transversales:

CT01

Capacidad de los estudiantes para fundamentar sus planteamientos en una deontología profesional que incorpore el respeto por el medio ambiente, la seguridad y salud de los trabajadores, y la confidencialidad e integridad de la información.

CT02

Conocer y utilizar con habilidad los mecanismos básicos de uso de la comunicación bidireccional entre profesores, alumnos, foros, etc.

CT03

Utilizar las herramientas para buscar, analizar y comprender la información que les permita transformarla en conocimiento.

CT04

Investigar y comunicar los resultados de la investigación en el lenguaje apropiado.

CT05

Innovar y aplicar la flexibilidad necesaria en entornos nuevos de aprendizaje como es la enseñanza online.

Competencias específicas:

CE01

Analizar y saber interpretar la Estructura de Alto Nivel (HSL), común a todas las normas ISO, que facilita la integración de sistemas de gestión, estableciendo una estructura organizativa, definiendo las funciones y responsabilidades que aseguren la disponibilidad de recursos y su adecuado funcionamiento.

CE06

Analizar e interpretar los requisitos establecidos por la norma ISO 27001, para su cumplimiento en la implantación de un sistema de gestión de la seguridad de la información en cualquier tipo de organización, independientemente de su tamaño o actividad.

CE16

Identificar las características del proceso de certificación que asegura a las empresas y a sus partes interesadas que sus sistemas de gestión son acordes con las normas de referencia.

RESULTADOS DE APRENDIZAJE

Cuando el estudiante supere esta asignatura será capaz de:

- Aplicar adecuadamente la Norma ISO 27001, básica en el desarrollo del proceso de implantación de un sistema de gestión de seguridad de la información.
- Implementar correctamente en una organización un sistema de gestión de seguridad de la información.
- Verificar la información del Sistema de Gestión de Seguridad de la Información y cumplimentar las posibles notas de aplicación.

CONTENIDOS DE LA ASIGNATURA

1. Concepto de seguridad informática.
2. El sistema de información y procesos de informatización de los sistemas de información.
3. Origen, evolución y utilidad de la norma ISO 27001.
4. Estructura, objetivos y controles de la norma ISO 27001.
5. Comprender las necesidades y expectativas de la organización.
6. Liderazgo y compromiso de la alta dirección.
7. Entender la planificación y la gestión de recursos para el sistema de gestión de seguridad de la información.
8. Entender la evaluación del desempeño y los procesos de mejora.
9. Entender el proceso de implementación de la Norma ISO 27001 en un sistema de gestión de seguridad de la información.

METODOLOGÍA

Las metodologías de enseñanza-aprendizaje utilizadas en este Máster Universitario están basadas en el Desarrollo de Competencias a través del modelo de formación a distancia que utiliza Internet como herramienta de aprendizaje, junto con un apoyo tutorial permanente.

Además, en esta asignatura se impartirán 0,4 ECTS en inglés.

Las actividades formativas y metodologías docentes son las siguientes:

Actividades Formativas	Finalidad / Descripción de la Actividad	Metodologías Docentes
Clases virtuales	Visualización, análisis, comprensión y participación en sesiones expositivas, explicativas y/o demostrativas a cargo del profesor o expertos invitados.	Método Expositivo. Lección Magistral.
Estudio individual	Lectura, análisis y comprensión de los contenidos teóricos disponibles en la Plataforma, los facilitados por los Profesores y con la utilización de las TICs. Realización de ejercicios individuales interactivos on-line de autoevaluación, que permiten el refuerzo de los conocimientos adquiridos a lo largo del estudio. Preparación de exámenes.	Aprendizaje autónomo dirigido por el profesor.
Trabajo individual	Resolución de ejercicios individuales mediante el análisis, recopilación de información y resolución individual de situaciones de estudio con la utilización de las TICs.	Resolución de ejercicios y problemas.
Trabajo de casos prácticos en grupo	Realización en grupo de casos prácticos mediante el análisis, recopilación de información, puesta en común de las conclusiones y resolución de casos reales,	Estudio de Casos. Aprendizaje cooperativo.

Actividades Formativas	Finalidad / Descripción de la Actividad	Metodologías Docentes
	experiencias y situaciones de estudio relacionados con las asignaturas y bajo la supervisión de los Profesores, con la utilización de las TICs.	
Tutorías individuales y grupales	Relación personalizada para el seguimiento, orientación, apoyo y resolución de consultas por parte del Equipo Docente para uno o varios alumnos, mediante correo electrónico y reuniones virtuales tipo chat y/o videoconferencia.	Tutorías y seguimiento mediante atención personalizada virtual.
Foros de discusión	Participación en Foros de Discusión. Reflexión, profundización y debate colectivo en inglés, acerca de cuestiones de interés relacionadas con las asignaturas, bajo la supervisión del Profesor, con la utilización de las TICs.	Aprendizaje cooperativo.
Examen presencial	Actividad destinada a la realización de pruebas de evaluación para valorar la adquisición de las competencias en las asignaturas teóricas por parte de los estudiantes	Pruebas de evaluación.

ACTIVIDADES FORMATIVAS

Actividad Formativa	Horas	Presencialidad
Clases virtuales	6	0
Estudio individual	87	0
Trabajo individual	18	0
Trabajo de casos prácticos en grupo	15	0
Tutorías individuales y grupales	12	8,3%
Foros de discusión	9	0
Examen presencial	3	100%

EVALUACIÓN

Criterios de evaluación

Actividad	% Calificación Final
Test de Evaluación on line por UC	15%
Trabajos Individuales	15%
Casos Prácticos	25%
Foro de discusión	5%
Examen presencial de la asignatura	40%

Sistemas de evaluación

Se realizarán dos tipos de evaluaciones diferenciadas, con la siguiente distribución porcentual sobre la nota global de la asignatura:

Evaluación continua	60%
Examen de evaluación final	40%
TOTAL	100%

- **Evaluación continua:** Se evaluará el seguimiento constante que cada estudiante desarrolla de la asignatura, y su participación en las distintas actividades formativas planificadas.

Sistema de Evaluación Continua	Modo de Calificación	% Sobre Nota Final
Evaluación continua de la adquisición de los contenidos teóricos mediante Test online.	Nota de 0 a 10	15%
Evaluación continua del seguimiento de tareas individuales previstas en cada asignatura.	Nota de 0 a 10	15%
Evaluación continua de la realización de los Casos Prácticos Colaborativos.	Nota de 0 a 10	25%
Evaluación continua del seguimiento de tareas colaborativas previstas en cada asignatura.	Nota de 0 a 10	5%
TOTAL, Evaluación continua	60%	

- **Examen de evaluación final**: El estudiante deberá realizar un examen final presencial individual que se calificará con una nota de 0 a 10, teniendo un valor del 40% sobre la nota final de la asignatura. La superación con éxito de la asignatura está condicionada a aprobar el examen presencial individual (igual o superior a 5).

Criterios de calificación

De acuerdo con el Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en todo el territorio nacional, el sistema de calificaciones se expresará en función de la siguiente escala numérica de 0 a 10, con expresión de un decimal, a la que podrá añadirse su correspondiente calificación cualitativa:

- 0 a 4.9 - Suspenso
- 5.0 a 6.9 - Aprobado
- 7.0 a 8.9 - Notable
- 9.0 a 10 - Sobresaliente

BIBLIOGRAFÍA

- **Básica:**
  - BOE (2018). Ley Orgánica 3/2018 de 5 de diciembre de protección de datos personales y garantía de los derechos digitales.
  - BOE (2021). Ley Orgánica 7/2021 de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
  - DOCE (2016). Reglamento UE 2016/679. Reglamento Europeo de Protección de Datos relativo a la protección de las personas físicas en el tratamiento de datos personales. Parlamento Europeo
  - ISO (2017). Norma ISO/IEC 27001. Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
  - ISO (2022). Norma ISO/IEC 27002. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.

- **Complementaria:**
  - Calso Morales, N. y Pardo Álvarez. J.M. (2018). "Guía práctica para la integración de sistemas de gestión: ISO 9001, ISO 14001 e ISO 45001". AENOR Internacional S.A.U.
  - Centro Criptográfico Nacional (2015) Guía CCN-STIC- 2020)401 Glosario y Abreviaturas
  - Centro Criptográfico Nacional (2015) CCN-STIC-425 Ciclo de Inteligencia y Análisis de Intrusiones.
  - Centro Criptológico Nacional (2020): Ciberamenazas y tendencias
  - De Luz, S (2022). Análisis y estudio de los diferentes tipos de firewall que existen.
  - De Luz, S (2022). VLANS: Qué son, tipos y para qué sirven.
  - Gastaldi, S y Ocon, L (2021) Ciberdefensa. Taeda Editorial
  - ISO (2018). Norma ISO 31000. Gestión del riesgo. Principios y directrices. Publicada el 28/03/18
  - Lisa Institute (2020). ¿Qué es y para qué sirve la ciberinteligencia?
  - Orera Gracia, A y Soriano Sarrio, V (2012). Firewalls, informe profesional.
  - Pons, J (2021). Sistemas para ciberDefensa. Revista Española de Defensa
  - Sevillano, F (2021) Ciberdefensa y ciberataque: el papel de los directivos.

- Tech-Blog (2019). Segmentación de redes: ¿Por qué aplicar esta estrategia en tus sistemas?

- **Recursos web**:

- BOE (2022) Boletín Oficial del Estado. Protección de datos de carácter personal. Disponible en línea. https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=055_Proteccion_de_Datos_de_Caracter_Personal&tipo=C&modo=2
- INCIBE (2022) Instituto Nacional de CiberSeguridad en España. Desarrollar cultura en seguridad. Disponible en línea. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf
- INCIBE (2022) Instituto Nacional de CiberSeguridad en España. Cumplimiento legal
- Disponible en línea. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_cumplimientolegal.pdf
- INCIBE (2022) Instituto Nacional de CiberSeguridad en España.
- Normativa corporativa de software legal Disponible en línea.
- https://www.incibe.es/sites/default/files/contenidos/dosieres/proteccion-puesto-trabajo/proteccion-puesto-trabajo-normativa-corporativa-de-software-legal.pdf
- ISO (2022). Directivas ISO/IEC, Parte 1 — Suplemento ISO Consolidado — Procedimientos específicos de ISO. Recuperado de https://www.copant.org/index.php/es/catalogo-de-normas/directivas-iso-iec?download=525:directivas-iso-iec-parte-1-y-suplemento-iso-consolidado-limpio