



UNAM

UNIVERSIDAD DEL
ATLÁNTICO MEDIO

Guía Docente

Sistemas de gestión de la seguridad de la
información ISO 27001

**Máster Universitario en Sistemas Integrados
de Gestión QHSE**
MODALIDAD VIRTUAL

Curso Académico 2025-2026

Índice

RESUMEN

DATOS DEL PROFESORADO

REQUISITOS PREVIOS

RESULTADOS DEL APRENDIZAJE

CONTENIDOS DE LA ASIGNATURA

CRONOGRAMA ORIENTATIVO DE LA ASIGNATURA

ACTIVIDADES FORMATIVAS

EVALUACIÓN

NORMATIVA

BIBLIOGRAFÍA

RESUMEN

Centro	Escuela de Ingeniería en Sistemas de Información
Titulación	Máster Universitario en Sistemas Integrados de Gestión QHSE
Asignatura	Sistemas de gestión de seguridad de la información ISO 27001
Materia	Sistemas de gestión
Carácter	Obligatoria
Curso	1º
Semestre	1
Créditos ECTS	6
Lengua de impartición	Castellano
Curso académico	2025-2026

DATOS DEL PROFESORADO

Responsable de Asignatura	José Javier Rainer Granados
Correo Electrónico	josejavier.rainer@pdi.atlanticomedio.es
Tutorías	De lunes a viernes bajo cita previa

REQUISITOS PREVIOS

Sin requisitos previos.

RESULTADOS DEL APRENDIZAJE

Competencias

COM01

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.

COM02

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.

COM04

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.

COM08

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.

Conocimientos

CON04

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.

CONTENIDOS DE LA ASIGNATURA

Concepto de seguridad informática.

El sistema de información y procesos de informatización de los sistemas de información.

Origen, evolución y utilidad de la norma ISO 27001.

Estructura, objetivos y controles de la norma ISO 27001.

Comprender las necesidades y expectativas de la organización.

Liderazgo y compromiso de la alta dirección.

Entender la planificación y la gestión de recursos para el sistema de gestión de seguridad de la información.

Entender la evaluación del desempeño y los procesos de mejora.

Entender el proceso de implementación de la Norma ISO 27001 en un sistema de gestión de seguridad de la información.

Estos contenidos se desarrollarán por medio del siguiente programa:

Unidad 1 - Conocer la Importancia de la Norma ISO 27001 en el SGSI de una Empresa.

Unidad 2 - Analizar y Revisar la Norma ISO 27001.

Unidad 3 - Comprender Necesidades y Expectativas de la Organización: Liderazgo y Compromiso de la Alta Dirección.

Unidad 4 - Entender la Planificación y la Gestión de Recursos para el Sistema de Gestión de Seguridad de la Información.

Unidad 5 - Entender la Evaluación del Desempeño y los Procesos de Mejora.

Unidad 6 - Entender el Proceso de Implementación de la Norma ISO 27001 en un SGSI.

CRONOGRAMA ORIENTATIVO DE LA ASIGNATURA

Unidad 1

Semanas 1-2.

Unidad 2

Semanas 3-4.

Unidad 3

Semanas 5-7.

Unidad 4

Semanas 8-10.

Unidad 5

Semanas 11-14.

Unidad 6

Semanas 15-16.

RECOMENDACIONES

- Recomendación para realizar la actividad 1, haber estudiado las unidades 1 y 2.
- Recomendación para realizar la actividad 2, haber estudiado las unidades 3 y 4.
- Recomendación para realizar la actividad 2, haber estudiado las unidades 5 y 6.
- Recomendación para realizar los foros, participar desde la semana 1, leyendo y aportando sobre los comentarios de los demás estudiantes.

Nota: La distribución expuesta tiene un carácter general y orientativo, ajustándose a las características y circunstancias de cada curso académico y grupo clase.

ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	HORAS INTERACTIVIDAD SÍNCRONA
Clases virtuales	6	6
Estudio individual	87	0
Trabajo individual	18	0
Trabajo de casos prácticos en grupo	15	0
Tutorías individuales y grupales	12	3
Foros de discusión	9	0
Examen virtual	3	3

Según está establecido institucionalmente, todos los trabajos individuales y casos prácticos se deben entregar a través de las vías habilitadas en el campus virtual, dentro los plazos establecidos por el docente. No se aceptarán entregas en el correo electrónico del docente.

El estudiante es el responsable de garantizar dichas entregas y plazos en el campus virtual. Todos aquellos trabajos presentados fuera de fecha o por otras vías diferentes al campus virtual o a las indicadas por el docente contarán como no presentados.

El formato de entrega será el que indique para cada una de las actividades en particular.

Si por capacidad o formato, no se puede realizar una entrega por el Campus Virtual, el docente informará de la vía alternativa de almacenamiento que suministra la universidad y su mantenimiento será responsabilidad del estudiante.

En cualquier caso, el trabajo deberá permanecer accesible hasta que finalice el curso académico.

El docente deberá realizar una copia de todos aquellos trabajos que por su naturaleza no puedan estar almacenados en el Campus Virtual.

EVALUACIÓN

CRITERIOS DE EVALUACIÓN	PORCENTAJE CALIFICACIÓN FINAL
Evaluación continua de la adquisición de los contenidos teóricos mediante Test online	15%
Evaluación continua del seguimiento de tareas individuales previstas en cada asignatura	15%
Evaluación continua de la realización de los Casos Prácticos colaborativos	25%
Evaluación continua del seguimiento de tareas colaborativas previstas en cada asignatura	5%
Evaluación final a través de un examen virtual individual por asignatura	40%

Sistemas de evaluación

La calificación final se basará en una puntuación total de 10 puntos obtenida por el estudiante, de acuerdo con la siguiente escala:

Nota	Valor numérico
Suspenso:	0 - 4,9
Aprobado:	5 - 6,9
Notable:	7 - 8,9
Sobresaliente:	9 - 10
No Presentado	(NP)

Para optar a la **matrícula de honor** se debe haber obtenido sobresaliente, además de una mención especial a criterio del docente de la asignatura en función del rendimiento e implicación del estudiante en la asignatura. El número de matrículas a repartir por cada asignatura es calculado por la aplicación del campus.

PRIMERA MATRICULA

Criterios de Calificación

La superación con éxito de la asignatura está condicionada a aprobar el examen individual, obteniendo una calificación igual o superior a 5.

Si el alumno no aprueba el examen de la asignatura, en actas aparecerá la calificación obtenida en dicho examen.

Si el alumno no se presenta al examen en convocatoria oficial, figurará como “No Presentado” en actas.

El resto de las actividades evaluativas indicadas en la tabla “Criterios de evaluación” computarán para el cálculo de la nota final de la asignatura.

Se penalizarán las faltas de ortografía en la realización de los exámenes y trabajos escritos.

Convocatoria ordinaria:

La convocatoria ordinaria estará conformada por los elementos de evaluación reflejados en la Tabla: Criterios de evaluación.

Convocatoria extraordinaria:

La convocatoria extraordinaria estará conformada por los elementos de evaluación reflejados en la Tabla: Criterios de evaluación. El estudiante se presentará a aquellas partes que no superase en convocatoria ordinaria.

SEGUNDA Y SIGUIENTES MATRICULAS

Las segundas y siguientes matriculas poseerán una evaluación idéntica a la expuesta en primera matrícula en la que no se almacenarán entregas de cursos anteriores ni notas de pruebas de la matrícula anterior. A todos los efectos el estudiante debe volver a realizar y superar todas las partes reflejadas en la Tabla: Criterios de evaluación.

NORMATIVA

Evaluación

Todas las actividades formativas susceptibles de evaluación, así como la revisión de las calificaciones, estarán supeditadas a lo establecido en la Normativa de Evaluación, la Normativa de Permanencia y la Normativa de Convivencia de la Universidad del Atlántico Medio públicas en la web de la Universidad:

<https://www.universidadatlanticomedio.es/universidad/normativa>

Las conductas de plagio, así como el uso de medios ilegítimos en las pruebas de evaluación, serán sancionados conforme a lo establecido en estas normativas. El personal docente tiene a su disposición una herramienta informática antiplagio que puede utilizar según lo estime necesario. El estudiante estará obligado a aceptar los permisos de uso de la herramienta para que esa actividad sea calificada.

Exámenes

Los exámenes semestrales ordinarios y extraordinarios, se realizarán en modalidad virtual utilizando SMOWL como sistema de monitorización.

SMOWL es una herramienta de e-proctoring o supervisión remota que garantiza la integridad de las evaluaciones y exámenes online mediante la monitorización de la actividad del estudiante, la confirmación de su identidad y la detección de comportamientos sospechosos o no autorizados durante la prueba.

En caso de producirse alguna irregularidad durante la celebración del examen o prueba de evaluación, como puede ser hacer uso de cualquier elemento no autorizado o no cumplir las normas de comportamiento establecidas, SMOWL está programado para expulsar al estudiante del examen, lo que implica una calificación de suspenso.

El estudiante podrá solicitar la modificación de fechas en pruebas de evaluación por escrito a través de correo electrónico dirigido a Coordinación del Máster, únicamente en situaciones excepcionales debidamente justificadas, aportando la documentación correspondiente, dentro de los plazos indicados en cada caso en la Normativa de evaluación.

<https://universidadatlanticomedio.es/Static/Documentos//ES/Normativa-de-Evaluacion.pdf>

Se justificarán aquellas faltas sobrevenidas (solicitándose posteriormente documentación para dicha justificación) que sean debidas, únicamente, en caso de Ingreso hospitalario del estudiante o de un familiar de primer grado, lesión o incapacidad temporal del estudiante, fallecimiento de familiar o nacimiento de un hijo o hija.

Estudiantes con discapacidad o necesidades educativas especiales

A fin de garantizar la igualdad de oportunidades, la no discriminación, la accesibilidad universal y la mayor garantía de éxito académico, los y las estudiantes con discapacidad o con necesidades educativas especiales podrán solicitar adaptaciones curriculares para el seguimiento de sus estudios acorde con el Programa de Atención a la Diversidad de la UNAM:

https://www.universidadatlanticomedio.es/Static/Documentos/ES/Programa_atencion_diversidad.pdf

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_cumplimiento-legal.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>