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 2024-2025

Índice

RESUMEN

Centro	Universidad del Atlántico Medio
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	2024-2025

DATOS DEL PROFESORADO

Responsable de Asignatura	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

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

El sistema de calificaciones (R.D. 1125/2003, de 5 de septiembre) será:

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 que hayan obtenido una calificación igual o superior a 9,0. Se podrá conceder una matrícula por cada 20 alumnos o fracción.

Criterios de Calificación

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

Si el alumno no aprueba el examen de la asignatura, en actas aparecerá el porcentaje correspondiente a la calificación obtenida en la prueba.

Los alumnos podrán examinarse en convocatoria extraordinaria atendiendo al mismo sistema de evaluación de la convocatoria ordinaria.

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