Universidad de Alcalá

Estudio Propio: **CERTIFICADO DE FORMACIÓN PERMANENTE EN DIRECCIÓN DE SEGURIDAD DIGITAL Y GESTIÓN DE CRISIS**

Código Plan de Estudios: **FA34**

Año Académico: **2023-2024**

ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS:

CURSO	Obligatorios		Optativos		Prácticas Externas	TFM/Memoria/ Proyecto	Créditos Totales
	Créditos	Nº Asignaturas	Créditos	Nº Asignaturas	Créditos	Créditos	
1º	22	3				8	30
2º							
3º							
ECTS TOTALES	**22**	**3**				**8**	**30**

PROGRAMA TEMÁTICO:

ASIGNATURAS OBLIGATORIAS

Código Asignatura	Curso	Denominación	Carácter OB/OP	Créditos
706841	1	INTRODUCCIÓN A LA CIBERSEGURIDAD	OB	6
706842	1	GESTIÓN Y REGULACIÓN EN CIBERSEGURIDAD	OB	6
706843	1	LA CIBERSEGURIDAD DESDE UNA PERSPECTIVA 360º	OB	10

TRABAJO FIN DEMÁSTER/MEMORIA /PROYECTO

Código Asignatura	Curso	Denominación	Carácter OB/OP	Créditos
706844	1	TRABAJO FIN DE ESTUDIO	OB	8

Carácter: OB - Obligatoria; OP – Optativa

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2023-2024	
Estudio	Certificado de Formación Permanente en Dirección de Seguridad Digital y Gestión de Crisis	
Nombre de la asignatura	INTRODUCCIÓN A LA CIBERSEGURIDAD	
Carácter (Obligatoria/Optativa)	Obligatoria	
Créditos (1 ECTS=25 horas)	6	
Modalidad (elegir una opción)		Presencial (más del 80% de las sesiones son presenciales)
	X	Híbrida (sesiones on-line entre el 40% y 60%, resto presencial)
		Virtual (al menos el 80% de las sesiones son on-line o virtuales)
Profesor/a responsable	José Javier Martínez Herráiz Pablo Blanco Íñigo	
Idioma en el que se imparte	Español	

PROFESORES IMPLICADOS EN LA DOCENCIA

José Javier Martínez, Pablo Blanco Íñigo, Ángel Gómez de Agreda, Eduardo Ferrero.

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor/a	60
Número de horas de trabajo personal del estudiante	90
Total horas	150

CONTENIDOS (Temario)

Objetivo: *Establecer los conocimientos necesarios para identificar el espacio dirigido a la seguridad digital, como frente de nuevas amenazas corporativas dentro de la organización.*

1.- Introducción a la Ciberseguridad
- La biosfera digital Seguridad, ética y filosofía
- ¿Cuáles son las preocupaciones en las compañías?
- Consejos para tener vidas digitales más seguras
- Ciberseguridad y conceptos generales I
- La convergencia de la seguridad entre los mundos físicos y lógicos
- Ciberseguridad ¿Qué se nos avecina?
- Las dimensiones de la Ciberseguridad

COMPETENCIAS ESPECÍFICAS (indicar un mínimo de tres y máximo de cinco)

- Conocimientos técnicos necesarios para entender que pasa en su organización entorno a la seguridad digital.

- Conocimientos de la visión del negocio que debe de tener de su empresa para ponderar correctamente la inversión en Ciberseguridad.
- Adquirir habilidades directivas para responsables en Ciberseguridad tales como liderazgo, negociación, comunicación, gestión de personas y habilidades interculturales.

EVALUACIÓN

- Realización de ejercicios tipo test.
- Proyecto parcial a desarrollar: Casos Prácticos.

BIBLIOGRAFÍA

- Mundo Orwell. Ariel.
- Enciclopedia de la Seguridad Informática. Madrid: RA-MA.
- Los hombres que susurraban a las máquinas. Booket
- Ciberseguridad: consejos para tener vidas digitales más seguras. Monica Valle
- X1Red+Seguridad Informando y Educando V1.0. Angel-Pablo Avilés.
- Seguridad Informática para empresas y particulares. Madrid: McGRawHill.
- El libro del hacker. ANAYA MULTIMEDIA
- Ciberdiccionario: Conceptos de ciberseguridad en lenguaje entendible. Javier Zubieta

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2023-2024	
Estudio	Certificado de Formación Permanente en Dirección de Seguridad Digital y Gestión de Crisis	
Nombre de la asignatura	GESTIÓN Y REGULACIÓN EN CIBERSEGURIDAD	
Carácter (Obligatoria/Optativa)	Obligatoria	
Créditos (1 ECTS=25 horas)	6	
Modalidad (elegir una opción)		Presencial (más del 80% de las sesiones son presenciales)
	X	Híbrida (sesiones on-line entre el 40% y 60%, resto presencial)
		Virtual (al menos el 80% de las sesiones son on-line o virtuales)
Profesor/a responsable	José Javier Martínez Herráiz Pablo Blanco Íñigo	
Idioma en el que se imparte	Español	

PROFESORES IMPLICADOS EN LA DOCENCIA

Carmen Pagés Arévalo, Pablo Blanco Iñigo, Vicente Moret, Francisco Pérez Bes, Alonso Hurtado

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor/a	60
Número de horas de trabajo personal del estudiante	90
Total horas	150

CONTENIDOS (Temario)

Objetivo: *Adquirir por parte del alumno todos los conocimientos y terminología básica, para profundizar en un curso práctico de ciberseguridad aplicada al entorno corporativo de una compañía.*

Con objeto de cubrir las características propias de esta área se cubrirán, entro otros, los siguientes temas:

2.- Gestión y Regulación en Ciberseguridad

- Derecho y ciberseguridad
- Gobierno corporativo, riesgos y cumplimiento en ciberseguridad
- Cumplimiento Legal y Normativo
- Marco Jurídico y procesal de la Ciberseguridad
- Principios y buenas prácticas en ciberseguridad
- Gobernanza y ordenación institucional de la ciberseguridad en España, ¿qué deberíamos tener y hacia dónde vamos?

COMPETENCIAS ESPECÍFICAS (indicar un mínimo de tres y máximo de cinco)

- Comprender el papel crítico de la Ciberseguridad en todos los planos de la sociedad actual, como garantía última de fiabilidad y resiliencia, adquiriendo competencias y visión en la materia.
- Adquirir destrezas prácticas para la gestión de crisis de Ciberseguridad.
- Conocer las amenazas y vulnerabilidades más importantes en materia de Ciberseguridad, mediante una visión estratégica.

EVALUACIÓN

- Realización de ejercicios tipo test.
- Proyecto parcial a desarrollar: Casos Prácticos.

BIBLIOGRAFÍA

- COBIT 5 for Risk. ISACA
- Cibersecurity Framework NIST
- Computación forense. Descubriendo los rastros informáticos. Alfaomega
- Escenarios de Riesgo: Utilizando COBIT 5 para Riesgos. ISACA
- Gestión de Proveedores: Utilizando COBIT® 5. ISACA
- Implementación del Marco de Ciberseguridad de NIST. ISACA
- Derecho digital: De la protección de datos a la ciberseguridad. The Valley Digital Business School.
- ISO 27001:2013 e ISO 27002:2013

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2023-2024	
Estudio	Certificado de Formación Permanente en Dirección de Seguridad Digital y Gestión de Crisis	
Nombre de la asignatura	La Ciberseguridad desde una Perspectiva 360º	
Carácter (Obligatoria/Optativa)	Obligatoria	
Créditos (1 ECTS=25 horas)	10	
Modalidad (elegir una opción)		Presencial (más del 80% de las sesiones son presenciales)
	X	Híbrida (sesiones on-line entre el 40% y 60%, resto presencial)
		Virtual (al menos el 80% de las sesiones son on-line o virtuales)
Profesor/a responsable	Carmen Pagés Arévalo Pablo Blanco Íñigo	
Idioma en el que se imparte	Español	

PROFESORES IMPLICADOS EN LA DOCENCIA

José Javier Martínez Herráiz, Joaquín del Toro, Pablo Blanco Iñigo, Andrés Ruiz Vázquez, Elvira Tejada, Enrique Cubeiro. Ramses Gallego, Julio San José, Pablo Montoliu, José Maria Blanco, Pau Bernar, Ricardo Barrasa, Israel Hernández, Ricardo Cañizares

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor/a	100
Número de horas de trabajo personal del estudiante	150
Total horas	250

CONTENIDOS (Temario)

Objetivo: *Adquirir los conocimientos necesarios para gestionar una dirección de ciberseguridad y poder hacer frente a cada uno de los aspectos propios en la gestión de crisis ciber.*
Para ello se establecen cinco bloques basados en las buenas prácticas de gestión en ciberseguridad y crisis corporativa:

3.- La Ciberseguridad desde una Perspectiva 360º

- Identificar
  - La importancia de conocer la compañía, ¿Cuál es el corazón de nuestro negocio?
  - Análisis y gestión del Riesgo tecnológico
  - De la inteligencia a la Ciber Inteligencia
  - El poder de la ciberinteligencia para la identificación de los riesgos y amenazas
  - Identificación de ciberdelitos ¿Qué son y cómo se persiguen?
  - Perfil del ciber delincuente

- Proteger
  - El acceso a nuestros sistemas, nuestra puerta de entrada
  - Medidas de protección cotidianas de ciberseguridad
  - La Estrategia de Ciberseguridad Nacional ¿Cómo nos protegen?
  - El empleado como el eslabón más débil de la cadena de la ciberseguridad
  - ¿Quién nos protege en el mundo digital?
  - ¿Cómo se protege el delito?

- Identificar
  - Procesos de detección de anomalías y eventos
  - Centro de Operaciones de Ciberseguridad (SOC)
  - Exposición digital y riesgos derivados
  - Procedimientos de gestión de incidentes y crisis
  - Forense informático ¿A qué problemas nos enfrentamos?
  - Enfoque de periciales informáticas

- Responder
  - Gobierno y gestión de la seguridad en entornos complejos e internacionales
  - Plan de gestión de Crisis de Ciberseguridad
  - Noticias falsas, ¿Cómo afectan a nuestra organización?
  - Plan de gestión de Crisis Reputacional
  - Plan de comunicación de crisis reputacional
  - Plan de gestión de crisis Corporativa

- Recuperar
  - Plan de continuidad de negocio
  - Plan de Recuperación de desastres en el sector Banca
  - Plan de Recuperación de desastres en el sector Seguros
  - Estrategia de la transferencia del riesgo Ciberseguros
  - Lecciones aprendidas después de la crisis Auditando la mejora

COMPETENCIAS ESPECÍFICAS (indicar un mínimo de tres y máximo de cinco)

- Adquirir las habilidades necesarias para gestionar y comunicarte con los colectivos técnicos.
- Aprender a elaborar mecanismos preventivos en materia de Ciberseguridad, así como a desarrollar instrumentos de comunicación y control posteriores a crisis.
- Conseguir una visión global para desarrollar en crisis la actividad directiva con la máxima eficacia

EVALUACIÓN

- Realización de ejercicios tipo test.
- Proyecto parcial a desarrollar: Casos Prácticos.

BIBLIOGRAFÍA

- Amenazas persistentes avanzadas: Cómo gestionar el riesgo para su negocio. ISACA
- El cisne Negro: el impacto de lo altamente improbable. Booket
- Respuesta a los ataques cibernéticos dirigidos. ISACA
- Diseño de un plan de recuperación ante desastre (DRP). Editorial Académica Española
- Evaluación de la madurez del SGCN en el sector financiero bancario. Editorial Académica Española

- El plan de continuidad de negocio: Una guía práctica para su elaboración. Ediciones Díaz de Santos, S.A.
- Planes de contingencia: la continuidad del negocio en las organizaciones. Ediciones Diaz de Santos
- ISO 22301

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2023-2024	
Estudio	Certificado de Formación Permanente en Dirección de Seguridad Digital y Gestión de Crisis	
Nombre de la asignatura	TRABAJO FIN DE ESTUDIO	
Carácter (Obligatoria/Optativa)	Obligatoria	
Créditos (1 ECTS=25 horas)	8	
Modalidad (elegir una opción)		Presencial (más del 80% de las sesiones son presenciales)
	X	Híbrida (sesiones on-line entre el 40% y 60%, resto presencial)
		Virtual (al menos el 80% de las sesiones son on-line o virtuales)
Profesor/a responsable	José Javier Martínez Herráiz Carmen Pagés Arévalo	
Idioma en el que se imparte	ESPAÑOL	

PROFESORES IMPLICADOS EN LA DOCENCIA

José Javier Martínez Herráiz
Carmen Pagés Arévalo

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor/a	80
Número de horas de trabajo personal del estudiante	120
Total horas	200

CONTENIDOS (Temario)

- Proyecto Final de curso, el cual se desarrolla a lo largo de la segunda parte del calendario académico como culminación del trabajo realizado durante todo el curso.

EVALUACIÓN

Presentación presencial ante tribunal.

BIBLIOGRAFÍA

La que consta en cada una de las disciplinas a desarrollar en el estudio y de aplicación al trabajo final de curso