

Estudio Propio: **FORMACIÓN SUPERIOR EN DIRECCIÓN DE SEGURIDAD DIGITAL Y GESTIÓN DE CRISIS CORPORATIVA**

Código Plan de Estudios: **EÑ84**

Año Académico: **2020-2021**

<b>ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS:</b>							
CURSO	Obligatorios		Optativos		Prácticas Externas	Memoria/ Proyecto	Créditos
	Créditos	Nº Asignaturas	Créditos	Nº Asignaturas	Créditos	Créditos	
1º	22	3				8	30
2º							
3º							
<b>ECTS TOTALES</b>	<b>22</b>	<b>3</b>				<b>8</b>	<b>30</b>

<b>PROGRAMA TEMÁTICO:</b>				
<b>ASIGNATURAS OBLIGATORIAS</b>				
Código Asignatura	Curso	Denominación	Carácter OB/OP	Créditos
705748	1	LA SEGURIDAD CORPORATIVA EN SU CONCEPTO GLOBAL	OB	6
705749	1	LA SEGURIDAD DIGITAL COMO PROCESO EN LAS ORGANIZACIONES	OB	6
705750	1	PRÁCTICA EN LA CRISIS DE LA SEGURIDAD DIGITAL	OB	10
<b>MEMORIA /PROYECTO</b>				
Código Asignatura	Curso	Denominación	Carácter OB/OP	Créditos
705751	1	TRABAJO FIN DE ESTUDIO	OB	8

Carácter: OB - Obligatoria; OP – Optativa

## GUÍA DOCENTE

Año académico	2020-2021	
Estudio	Formación Superior en Dirección de Seguridad Digital y Gestión de Crisis Corporativa (EÑ84)	
Nombre de la asignatura	LA SEGURIDAD CORPORATIVA EN SU CONCEPTO GLOBAL	
Carácter (Obligatoria/Optativa)	Obligatoria	
Créditos (1 ECTS=25 horas)	6	
Modalidad (elegir una opción)		Presencial
	X	Semipresencial
		On-line
Profesor responsable	José Javier Martínez Herráiz José Ricardo López García	
Idioma en el que se imparte	Español	

### DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor	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.

Temas:

1. Coordinación Seguridad privada Actual.
2. Evolución del Director de Seguridad en la organización de la Seguridad Corporativa. La seguridad como pieza clave para los negocios.
3. ROSI Retorno de la inversión en seguridad en la organización.
4. Legislación aplicable a Seguridad Digital.
5. La convergencia de la seguridad física y lógica. La seguridad integral corporativa.

### 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

## GUÍA DOCENTE

Año académico	2020-2021	
Estudio	Formación Superior en Dirección de Seguridad Digital y Gestión de Crisis Corporativa (EÑ84)	
Nombre de la asignatura	LA SEGURIDAD DIGITAL COMO PROCESO EN LAS ORGANIZACIONES	
Carácter (Obligatoria/Optativa)	Obligatoria	
Créditos (1 ECTS=25 horas)	6	
Modalidad (elegir una opción)		Presencial
	X	Semipresencial
		On-line
Profesor responsable	José Javier Martínez Herráiz José Ricardo López García	
Idioma en el que se imparte	Español	

### DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor	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, entre otros, los siguientes temas:

1. Ciberseguridad y Conceptos Generales. Principios Generales de la Seguridad (Confidencialidad, Integridad y Disponibilidad) (doble modulo)
2. Ciber-inteligencia (doble modulo)
3. Regulación aplicable a la Ciberseguridad. (ISSI. RGPD. ENS)
4. IOT. Seguridad industrial, seguridad tecnológica,
5. Buenas prácticas en Seguridad de la información. (Estándares)
6. Gobierno de la Ciberseguridad.
  - Niveles de reporting (C-Level), ¿Qué necesitamos saber?
  - Atacante, tipología y evolución.
  - Insiders, hacktivistas, atacantes y evolución.

### EVALUACIÓN

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

## BIBLIOGRAFÍA

- COBIT 5 for Risk. ISACA
- Cybersecurity 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

GUÍA DOCENTE

Año académico	2020-2021	
Estudio	Formación Superior en Dirección de Seguridad Digital y Gestión de Crisis Corporativa (EÑ84)	
Nombre de la asignatura	PRÁCTICA EN LA CRISIS DE LA SEGURIDAD DIGITAL	
Carácter (Obligatoria/Optativa)	Obligatoria	
Créditos (1 ECTS=25 horas)	10	
Modalidad (elegir una opción)		Presencial
	X	Semipresencial
		On-line
Profesor responsable	Carmen Pagés Arévalo Pablo Blanco Iñigo	
Idioma en el que se imparte	Español	

**DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)**

Número de horas presenciales/on-line asistencia profesor	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:

**1. Identificar. Estrategia en el Análisis y Gestión del Ciber-Riesgo.**

- Entendimiento de negocio
- Gestión de activos
  - o Clasificación de la información.
  - o CMDB
- Análisis de Riesgos
- Estrategia de Gestión del Riesgo.
  - o Gestión del Riesgo en la cadena de suministro (Proveedores, productos y Servicios)

**2. Proteger. Estrategia de Seguridad Digital.**

- Gestión de Identidades y control de Acceso.
- Seguridad en Capas (Tecnología de Protección.):
  - o Ciberseguridad Tecnológica.
  - o Ciberseguridad de la información.
  - o Ciberseguridad en las Redes e IOTs
  - o Ciberseguridad del Dato.
- Procesos y procedimientos de Protección de Información
- Formación y Concienciación; El usuario final como eslabón más débil. (1 bloque)

**3. Detectar.**

- Proceso de detección (Anomalías y eventos)
- Monitorización continua de Seguridad.
  - o Nivel 2.- ITGRC
  - o NIVEL 3.- Auditoria.
- Gestión de incidentes y crisis

**4. Responder. Estrategia en Ciber-Resiliencia.**

- Amenazas Cross-Sectoriales
- Planificar la respuesta, Comunicar, Analizar, Mitigar, Mejorar.
- Amenazas y Contramedidas.
- Plan de Gestión de Crisis y Continuidad de negocio.

**5. Recuperar. Mejora Continua.**

- Plan de Recuperación
- Mejora Continua y comunicación (Comunicación)

**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 Díaz de Santos
- ISO 22301

## GUÍA DOCENTE

Año académico	2020-2021	
Estudio	Formación Superior en Dirección de Seguridad Digital y Gestión de Crisis Corporativa (EÑ84)	
Nombre de la asignatura	TRABAJO FIN DE ESTUDIO	
Carácter (Obligatoria/Optativa)	Obligatoria	
Créditos (1 ECTS=25 horas)	8	
Modalidad (elegir una opción)	<input type="checkbox"/>	Presencial
	<input checked="" type="checkbox"/>	Semipresencial
	<input type="checkbox"/>	On-line
Profesor responsable	José Javier Martínez Herráiz Carmen Pagés Arévalo	
Idioma en el que se imparte	Español	

### DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor	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