

## GUÍA DOCENTE 2021-2022

### DATOS GENERALES DE LA ASIGNATURA

<b>ASIGNATURA:</b>	Seguridad Electrónica y Legislación
<b>PLAN DE ESTUDIOS:</b>	Máster Universitario en Dirección Estratégica en Tecnologías de la Información
<b>FACULTAD:</b>	Escuela Politécnica Superior
<b>CARÁCTER DE LA ASIGNATURA:</b>	Obligatoria
<b>ECTS:</b>	5 ECTS
<b>CURSO:</b>	Primero
<b>SEMESTRE:</b>	Primero
<b>IDIOMA EN QUE SE IMPARTE:</b>	Castellano
<b>PROFESORADO:</b>	Dr. Jon Arambarri
<b>DIRECCIÓN DE CORREO ELECTRÓNICO:</b>	<a href="mailto:jon.arambarri@uneatlantico.es">jon.arambarri@uneatlantico.es</a>

### DATOS ESPECÍFICOS DE LA ASIGNATURA

<b>REQUISITOS PREVIOS:</b>
No aplica
<b>CONTENIDOS:</b>
<ul style="list-style-type: none"> <li>• Tema 1. Confianza, Seguridad y Sociedad de la Información             <ul style="list-style-type: none"> <li>- Confianza y Seguridad en la Información</li> <li>- Seguridad de Información y Desarrollo Económico</li> <li>- Seguridad, Confianza y Negocio Electrónico</li> </ul> </li> <li>• Tema 2. Tecnología y Organización de la Seguridad de la Información             <ul style="list-style-type: none"> <li>- Medida del Riesgo y Gestión de la Seguridad</li> </ul> </li> </ul>

- Salvaguardad Generales para la Información
- Mecanismos de Control de Accesos e Intrusiones
- Mecanismos de Cifrado y Negocio Electrónico
- Firma Digital
- Infraestructura de Clave Pública
- Tema 3. La Infraestructura para la Construcción de la Confianza
  - Evaluación y certificación de Seguridad de las TI
  - Reconocimiento Internacional de Evaluaciones y Certificados de Seguridad de Tecnologías
  - Evaluación y Certificación de la Gestión de la Seguridad en las Organizaciones
  - Firma y Comercio Electrónico Europeo
- Tema 4. Marco Normativo y Regulatorio de la Seguridad y del Comercio Electrónico. Firma Digital, Protección de Datos Personales y Delitos Informáticos
  - Privacidad, Seguridad y Confidencialidad
  - Leyes, Recomendaciones y Declaraciones Generales en el Contexto de la Seguridad y del Comercio Electrónico
  - Leyes de Firma Electrónica en el Marco de la UNCITRAL
  - Leyes de Firma Electrónica en el Marco de la Legislación de Latinoamérica
  - Leyes de Protección de Datos Personales y Resguardo de la Privacidad Online en Europa y España
  - Leyes de Protección de datos en Latinoamérica
  - Tipificación de Delitos Informáticos: Sanciones Penales a las Vulneraciones en Materia de Seguridad de Sistemas y Confidencialidad de la Información
  - El Papel de las Administraciones Públicas

## COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

### COMPETENCIAS GENERALES:

Que los estudiantes sean capaces de:

CG1 - Organizar y planificar el trabajo en el ámbito de la dirección estratégica en tecnologías de la información.

CG2 - Realizar un análisis crítico en el ámbito de la dirección estratégica en tecnologías de la información.

CG3 - Gestionar la información y el conocimiento vinculados al ámbito de la dirección estratégica en tecnologías de la información.

CG4 - Tener la habilidad para comunicarse con expertos de otras áreas en el ámbito de la dirección estratégica en tecnologías de la información.

CG5 - Trabajar en equipo, y en contexto de trabajo en un equipo interdisciplinar en el ámbito de la dirección estratégica en tecnologías de la información.

CG6 - Generar nuevas ideas en el ámbito de la dirección estratégica en tecnologías de la información.

CG7 - Desarrollar la capacidad de liderazgo en el ámbito de la dirección estratégica en tecnologías de la información.

#### **COMPETENCIAS ESPECÍFICAS:**

Que los estudiantes sean capaces de:

- CE12 - Gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

#### **COMPETENCIAS PROPIAS DE LA ASIGNATURA:**

No Aplica

#### **RESULTADOS DE APRENDIZAJE:**

En esta asignatura se espera que alumnos alcancen los siguientes resultados de aprendizaje:

- Mejorar y corregir los procesos.
- Integrar las leyes y normativas adecuadas en el funcionamiento del negocio electrónico, en función del ámbito de acción de dicho negocio
- Diferenciar información y mensajes fraudulentos así como intentos de phishing, pharming, spoofing, XSS etc.
- Distinguir entre sitios web seguros y no seguros.
- Adecuar la tecnología existente en base a un código de buenas prácticas que incluyan: adoptar medidas de seguridad, creación de copias de respaldo y reorganización del sistema de gestión de forma que sea escalable.
- Generar sistemas de información encriptados.

## METODOLOGÍAS DOCENTES Y ACTIVIDADES FORMATIVAS

### METODOLOGÍAS DOCENTES:

En esta asignatura se ponen en práctica diferentes metodologías docentes con el objetivo de que los alumnos puedan obtener los resultados de aprendizaje definidos anteriormente:

- Método expositivo
- Estudio y análisis de casos
- Resolución de ejercicios
- Aprendizaje cooperativo/trabajo en grupo
- Trabajo autónomo

### ACTIVIDADES FORMATIVAS:

A partir de las metodologías docentes especificadas anteriormente, en esta asignatura, el alumno participará en las siguientes actividades formativas:

Actividades formativas	
<b>Actividades supervisadas</b>	Actividades de foro
	Corrección de actividades
	Tutorías (individual / en grupo)
<b>Actividades autónomas</b>	Sesiones expositivas virtuales
	Preparación de actividades de foro
	Estudio personal y lecturas
	Elaboración de trabajos (individual-en grupo)
	Realización de actividades de autoevaluación

El día del inicio del período lectivo de la asignatura, el profesor proporciona información detallada al respecto para que el alumno pueda organizarse.

## SISTEMA DE EVALUACIÓN

### CONVOCATORIA ORDINARIA:

En la convocatoria ordinaria de esta asignatura se aplican los siguientes instrumentos de evaluación:

Actividades de evaluación		Ponderación
<b>Evaluación continua</b>	Resolución de un caso práctico (tipo Harvard)	20 %
	Participación en una actividad de debate	20 %
<b>Evaluación final</b>	Resolución de un examen (prueba tipo test)	60 %

Para más información consúltese [aquí](#)

#### CONVOCATORIA EXTRAORDINARIA:

En la convocatoria extraordinaria de esta asignatura se aplican los siguientes instrumentos de evaluación:

	Actividades de evaluación	Ponderación
Evaluación continua	Calificación obtenida en la actividad de debate de la convocatoria ordinaria	20%
	Realización de un trabajo individual	20%
Evaluación final	Resolución de un examen (prueba tipo test)	60%

Para más información consúltese [aquí](#)

## BIBLIOGRAFÍA Y RECURSOS DE REFERENCIA GENERALES

#### BIBLIOGRAFÍA BÁSICA:

Las siguientes referencias son de consulta obligatoria y están ordenadas por nivel de importancia:

Ortega, A. (s.f.). *Seguridad electrónica y legislación*. Material didáctico propio de la Institución.

Abril, A., Pulido, J., & Bohada, J. A. (2014). *Análisis de Riesgos en Seguridad de la Información*. *Ciencia, Innovación y Tecnología*, 1, 39-53.

Ordóñez, S., & Navarrete, D. (2016). *Industria de servicios de telecomunicaciones y reforma regulatoria en México*. *Problemas del desarrollo*, 47(184), 35-60.

#### BIBLIOGRAFÍA COMPLEMENTARIA:

Las siguientes referencias no se consideran de consulta obligatoria, pero su lectura es muy recomendable. Están ordenadas alfabéticamente

Aloul, F. (2012). *The Need for Effective Information Security Awareness*. *Journal of Advances in Information Technology*.

Arévalo Mutiz L & García Leguizamón M. & Navarro H. (2012). *Aproximación a problemáticas jurídicas de las redes sociales virtuales*. Revista Virtual Universidad Católica Del Norte, 62-92.

Burn-Murdoch, J. (2013). *Study: Less than 1% of the World's Data is Analyzed, over 80% is Unprotected*. The Guardian

Ordóñez, S. (2016). *Industria de telecomunicaciones y reforma regulatoria en México. Problemas Del Desarrollo*. Revista Latinoamericana De Economía, 35-60.

Peña Saffon, S. (2014). *Acceso a la órbita de los satélites geoestacionarios. Propuesta para un régimen jurídico especial*. Revista De Derecho Comunicaciones Y Nuevas Tecnologías. 2-25.

Velmurugan, M. (2009). *Security and Trust in e-Business: Problems and Prospects*. International Journal of Electronic Business Management

Zillmer, K. (. (2016). *Do your data security policies need a checkup?* Collector, 26- 29

#### WEBS DE REFERENCIA:

No Aplica

#### OTRAS FUENTES DE CONSULTA:

- Base de datos EBSCO – Acceso a través del campus virtual.