

GUÍA DOCENTE

1. DATOS DE LA ASIGNATURA

Asignatura	TECNOLOGÍAS DE SEGURIDAD Y CIBERSEGURIDAD					
Código asignatura	A23PGR008.04			Modalidad	Presencial	
Créditos ECTS	6	Lengua	Castellano	Campus	A Coruña	
Curso	1		Semestre	1	Período	Del 25/09/2023 al 22/12/2023
Carácter	Obligatoria		Módulo	Formación Básica	Materia	Informática
Horario de clase	Grupo		Día	Hora		Aula
	1		Jueves	10:00 - 14:00		Aula correspondiente a la asignatura en cada campus
Profesor	Álvaro Gómez Vieites			E-mail	alvaro.gomez@uie.edu	

2. PRESENTACIÓN

La asignatura Tecnologías de Seguridad y Ciberseguridad tiene como principales objetivos analizar la importancia de la seguridad de los datos y los activos informáticos en la actual Economía Digital. La asignatura se compone de tres unidades:

- Fundamentos de ciberseguridad.
- Seguridad en los datos, en los accesos, en los equipos y en las redes.
- Tópicos especiales de seguridad de bases de datos.

Al finalizar la asignatura estarás en capacidad de aplicar los fundamentos de la ciberseguridad en la protección de los datos y los activos tecnológicos, analizar riesgos y definir las distintas funciones y estrategias de seguridad, diseñar y elaborar planes de respuesta a incidentes, y conocer las principales herramientas para garantizar la seguridad en las bases de datos.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias vinculadas con la asignatura

Competencias	Código	Descripción
Básicas	CB06	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
	CB07	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
	CB08	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
	CB09	Que los estudiantes sepan comunicar sus conclusiones, y los conocimientos y razones últimas que las sustentan, a públicos especializados y no especializados de un modo claro y sin ambigüedades.
	CB10	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
Generales	CG01	Utilizar las técnicas que permiten obtener y analizar la información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto empresarial.
	CG02	Utilizar el potencial de las tecnologías de vanguardia para contribuir a la mejora de la competitividad de la empresa u organización.
	CG03	Tratar situaciones complejas e impredecibles de forma sistemática, creativa y con juicio crítico, tomando decisiones con información incompleta y asumiendo riesgos.
	CG04	Comunicarse de forma correcta, tanto oralmente como por escrito, en cualquier ámbito y con el apoyo de la tecnología más actual.
Transversales	CT05	Demostrar habilidades y actitudes para el trabajo autónomo y el trabajo en equipo.
	CT06	Utilizar conocimientos, habilidades, destrezas y actitudes para comunicarse en entornos digitales.
Específicas	CE05	El titulado o titulada podrá definir planes de seguridad y contingencia para garantizar la protección y seguridad de los datos empresariales.

Código	Descripción
RA01	Reconocer los problemas de seguridad de los datos empresariales.
RA02	Utilizar funciones, métodos y técnicas para garantizar la seguridad de los datos empresariales.
RA03	Identificar y utilizar herramientas de análisis de seguridad para bases de datos.
RA04	Elaborar el modelo y estrategias para garantizar la seguridad de los datos empresariales.
RA05	Analizar y valorar razonadamente un artículo científico sobre tendencias actuales de la seguridad de datos.
RA06	Elaborar un proyecto final de seguridad de datos.

4. CONTENIDOS

- **Unidad I Fundamentos de Ciberseguridad.**
 1. Gestión de la Seguridad de la Información.
 2. Problemas de seguridad e impacto de los incidentes de seguridad.
 3. Análisis y gestión de riesgos.
 4. Modelos estandarizados de estrategias de seguridad.
 5. Plan de respuesta a incidentes de seguridad.
 6. Profesionales de la ciberseguridad.

- **Unidad II Seguridad en los datos, en los accesos, en los equipos y en las redes.**
 7. Autenticación y control de accesos.
 8. Biometría.
 9. Criptografía, firma electrónica y certificación digital.
 10. Seguridad en el software, bases de datos y equipos informáticos.
 11. Análisis de la seguridad de los datos.
 12. Seguridad en smartphones y en otros dispositivos IoT.
 13. Tipos de ataques informáticos.
 14. El factor humano y la ingeniería social.

- **Unidad III Tópicos especiales de seguridad de bases de datos.**
 15. Fundamentos y aplicaciones de Blockchain.
 16. Características de las criptomonedas. Funcionamiento de Bitcoin.
 17. La recopilación masiva de datos personales y la privacidad.

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

La UIE desarrolla un modelo académico innovador centrado en el sujeto que aprende, combinando diferentes corrientes filosóficas de Enseñanza-Aprendizaje (E-A), una amplia variedad de actividades de aprendizaje, en especial aquellas donde el estudiante asume un rol activo en la construcción del conocimiento, el acompañamiento permanente y el uso intensivo de las tecnologías, como herramienta facilitadora del proceso, conformando un ecosistema de aprendizaje único e innovador.

La formación se desarrolla en la modalidad presencial, incluyendo la modalidad virtual síncrona, con un campus virtual vanguardista, que proporciona flexibilidad y personalización, en un modelo ubicuo de aprendizaje (U-Learning).

Por otra parte, en armonía con los principios fundacionales y corporativos de responsabilidad social, en la UIE además de promover la participación de toda su comunidad universitaria en actividades de voluntariado y servicio social, incorpora la actividad formativa “Aprendizaje Servicio (ApS)” y la habilita como parte de las estrategias de enseñanza-aprendizaje.

Código	Metodologías Docentes	Tipo	Actividad Formativa	Modo
MD01	Primer Contacto y Motivación	I	Introductoria	PR
MD02	Presentación, Plan de Trabajo y Compromiso	I		
MD03	Clase Magistral	T	Expositiva y Participativa	PR
MD04	Charlas Invitadas de Expertos	P	Guiada / Autónoma	PR / NP
MD07	Actividad en el Campus Virtual UIE	T/P		
MD08	Estudio de Contenidos	T	Autónoma	NP
MD09	Elaboración de Proyectos y Trabajos	T/P		
MD13	Exposiciones	P	Guiada	PR
MD16	Uso de Herramientas de Software	P		
MD20	Tutorías	T/P	Personalizada (Individual / Grupal)	PR
MD21	Contrato de Aprendizaje	I/T/P		
MD24	Análisis y Síntesis de Material Documental	T/P	Autónoma	NP
MD25	Seguimiento y Finalización	C	Autoevaluación continua	NP
I: Informativa T: Teórica P: Práctica C: Complementaria PR: Presencial NP: No presencial				

6. ACTIVIDADES FORMATIVAS UTILIZADAS EN LA ASIGNATURA

A continuación, se identifican los tipos de actividades formativas que se realizarán:

Código	Nombre	Modalidad	Tipo
AF01	Introdutoria	PR	Motivacional / Informativa
AF02	Expositiva y Participativa	PR	Teórica
AF03	Guiada	PR	Teórica / Práctica
AF04	Personalizada (Individual / Grupal)	PR	Teórica / Práctica
AF05	Autónoma	NP	Teórica / Práctica
AF06	Aprendizaje Servicio	PR	Aprendizaje Servicio
AF07	Autoevaluación continua	NP	Evaluación de la Calidad

PR: Presencial NP: No presencial

7. EVALUACIÓN

El modelo incluye además el proceso de evaluación continua como parte esencial de la verificación de las competencias adquiridas. Para la UIE y en armonía con la mejora del proceso de enseñanza-aprendizaje propuesto para el EEES2, el sistema de evaluación que se ha denominado Revisión de los Resultados de Aprendizaje (RRA) se desarrolla como un proceso más humanizado, alejado de los sistemas tradicionales en donde los estudiantes se juega su suerte en exámenes (convocatorias), en ocasiones con pesos porcentuales elevados y definitivos, con la consiguiente generación de estrés, frustración y en ocasiones la deserción.

El sistema RRA de la UIE es de carácter continuo, compartido y progresivo, permitiendo un seguimiento del aprendizaje a lo largo del todo el período, haciendo de ello un proceso natural al que los estudiantes acuden sin emociones negativas y conscientes de la necesidad de conocer su propio progreso.

Código	Actividad de Evaluación	Ponderación %	Tipo	Modo
AE01	Pruebas Parciales	30	Discreta	O/E
AE03	Proyectos	32	Discreta	E
AE04	Exposición	20	Discreta	O/E
AE05	Actividad en el Campus Virtual	15	Continua	E
AE06	Participación, Actividades diarias y Voluntariado	3	Continua	O/E
AE08	Aprendizaje Servicio ¹			O/E
AE10	Recuperar			E
		100		

O: Oral E: Escrito CD: Carpeta Digital

8. BIBLIOGRAFÍA

- Gómez, A. (2011). *Enciclopedia de la Seguridad Informática*. Ra-Ma.
- Gómez, A. (2010). *Seguridad Informática. Básico*. Starbook.
- MAGERIT versión 3 (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Ministerio de Hacienda y Administraciones Públicas. NIPO: 630-12-171-8.
- Mitnick, K; Simon, L. (2002). *Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. Wiley.
- O’Neil, C. (2017). *Weapons Of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Penguin Books.
- Szmigielski, A. (2016). *Bitcoin Essentials*. Pack Publishing.
- Tapscott, D (2017). *La revolución blockchain: Descubre cómo esta nueva tecnología transformará la economía global*. Deusto.
- The National Cyber Security Centre (2019). *The Cyber Security Body of Knowledge*. www.cybok.org
- Zuboff, S. (2018). *The Age Of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Hachette USA.

¹ Actividad que puede surgir durante el desarrollo del semestre

9. TUTORÍAS

MD20 Tutoría (2%): Los estudiantes deben asistir como mínimo de tres tutorías personalizadas a lo largo del semestre. Es una actividad del tipo todo o nada ("Pass- Fail"), es decir se deben completar las tres tutorías.

10. ENCUESTAS DE CALIDAD

MD25 Gestión de la calidad (2%): Los estudiantes deben rellenar a lo largo del semestre cuatro formularios referidos a la gestión de la calidad de la UIE. Es una actividad del tipo todo o nada ("Pass- Fail"), es decir se deben completar los cuatro formularios en los plazos previstos en el plan de actividades de la asignatura. La actividad tiene como objetivo valorar oportunamente el desarrollo del proceso de enseñanza-aprendizaje y la competencia transversal referida al pensamiento crítico y autocrítico.