

GUÍA DOCENTE

1. DATOS BÁSICOS

Asignatura	Ciberseguridad y Blockchain
Titulación	Ingeniería de la Empresa (GIE) Ingeniería en Sistemas Inteligentes (GSI)
Escuela/ Facultad	Facultad de Ingeniería y Tecnología Empresarial
ECTS	6
Carácter	Obligatoria
Idioma/s	Español
Modalidad	Presencial /Presencial Síncrono
Semestre	Primero
Docente coordinador	Álvaro Gómez Vieites

2. PRESENTACIÓN

La asignatura Ciberseguridad y Blockchain tiene como principales objetivos analizar la importancia de la seguridad de los datos y los activos informáticos en la actual Economía Digital, así como las múltiples aplicaciones de blockchain. La asignatura se compone de cuatro unidades:

- Fundamentos de ciberseguridad.
- Seguridad en los accesos, en el software, en las redes y en los equipos.
- Blockchain y criptomonedas.
- Protección de datos personales y marco legal.

Al finalizar la asignatura estarás en capacidad de aplicar los fundamentos de la ciberseguridad en la protección de los datos y los activos tecnológicos, diseñar y elaborar planes de respuesta a incidentes, aplicar las soluciones basadas en blockchain en distintos casos de uso empresarial, y garantizar el cumplimiento del marco normativo y de protección de datos.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias vinculadas con la asignatura

Competencias	Código	Descripción
Básicas	CB02	Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
Generales	CG02	Determinar eficazmente los objetivos, prioridades, métodos y controles para desempeñar tareas mediante la organización de las actividades con los plazos y los medios disponibles en el ámbito de la gestión empresarial.
	CG05	Utilizar el potencial de las tecnologías de vanguardia para contribuir a la mejora de la competitividad de la empresa u organización.
	CG06	Conocer y aplicar la normativa local autonómica nacional e internacional en el ámbito de la gestión empresarial
Transversales	CT05	Resolver problemas y tomar decisiones aplicando los conocimientos, métodos y herramientas en su ámbito académico y profesional.
	CT07	Demostrar habilidades y actitudes para el trabajo autónomo y el trabajo en equipo.
	CT08	Utilizar conocimientos, habilidades, destrezas y actitudes para comunicarse en entornos digitales.
	CT09	Demostrar capacidad para escribir y/o exponer informes con rigor académico y profesional.
Específicas	CE	Aplicar los principios rectores de la ciberseguridad para diseñar políticas y planes estratégicos para la seguridad digital empresarial.
	CE	Utilizar plataformas de blockchain y criptomonedas en el ámbito empresarial.

Resultados de aprendizaje de la asignatura

Código	Descripción
RA01	Aplicar los fundamentos de la ciberseguridad, las vulnerabilidades, amenazas y atacantes, riesgos y controles.
RA02	Utilizar los diferentes mecanismos de control de acceso.
RA03	Diseñar planes para prevenir ataques al software empresarial, la web y usuarios y activar acciones de contingencia
RA04	Utilizar la tecnología blockchain, las criptomonedas y sus usos empresariales.
RA05	Aplicar el marco regulatorio de la seguridad de datos de personas y empresas.
RA06	Utilizar herramientas de software en el ámbito de la asignatura.
RA07	Elaborar un trabajo final de aplicación de los contenidos.

4. CONTENIDOS

- **Unidad I Fundamentos de Ciberseguridad.**

1. Gestión de la Seguridad de la Información.
2. Impacto de los incidentes de seguridad.
3. Análisis y gestión de riesgos.
4. Certificación de la seguridad.
5. Plan de respuesta a incidentes de seguridad.
6. Profesionales de la ciberseguridad.

- **Unidad II Seguridad en los accesos, en el software, en las redes y en los equipos.**

7. Autenticación y control de accesos.
8. Biometría.
9. Criptografía, firma electrónica y certificación digital.
10. Seguridad en el software y en redes de ordenadores.
11. Análisis de vulnerabilidades.
12. Seguridad en smartphones y en otros dispositivos.
13. Tipos de ataques informáticos.
14. Virus y malware.
15. Seguridad industrial.
16. El factor humano y la ingeniería social.

- **Unidad III Blockchain y Criptomonedas.**

17. Fundamentos y aplicaciones de Blockchain.
18. Características de las criptomonedas. Funcionamiento de Bitcoin.
19. Criptomonedas: regulación, cotización y otros aspectos a tener cuenta.

- **Unidad IV Protección de datos personales y marco legal.**

20. La recopilación masiva de datos personales y la privacidad.
21. El marco legal de la protección de datos: RGPD y LOPD.

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. El profesor se convierte en un facilitador y gestor del conocimiento y saber hacer.

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	Actividad	Tipo	Modalidad E-A	Modo
MD01	Primer Contacto y Motivación	I	Introductoria	PR
MD02	Presentación, Plan de Trabajo y Compromiso	I		
MD03	Clase Magistral	T/P	Expositiva y Participativa	PR
MD06	Resolución de Problemas y Ejercicios	P	Guiada / Autónoma	PR / NP
MD07	Actividad en el Campus Virtual UIE	T/P		
MD09	Elaboración de Proyectos y Trabajos	T/P	Guiada / Autónoma	PR/NP
MD10	Estudio de Casos	P	Guiada	PR
MD12	Debates y Discusiones	P		
MD16	Uso de Herramientas de Software	P		
MD19	Aprendizaje Servicio (ApS)	T/P	Aprendizaje Servicio	PR
MD20	Tutorías	T/P	Personalizada (Individual / Grupal)	PR
MD21	Contrato de Aprendizaje	I/T/P	Personalizada (Individual / Grupal)	PR
MD22	Portafolio (Portfolio Assessment)	T/P	Autónoma	NP
MD23	Foros de Discusión	T/P		
MD25	Seguimiento y Finalización	C	Autoevaluación continua	NP

I: Informativa T: Teórica P: Práctica C: Complementaria PR: Presencial NP: No presencial

6. ACTIVIDADES FORMATIVAS

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

Código	Nombre	Modalidad	Tipo
AF01	Introductoria	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 EEES, 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	50	Discreta	E
AE03	Proyectos	20	Discreta	E
AE05	Participación en el Campus Virtual	5	Continua	E
AE06	Participación, Actividades diarias y Voluntariado	5	Continua	O/E
AE09	Portafolio Digital	20	Discreta	CD
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.

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.