

# Máster en Transformación Digital de Empresas – Módulo 1: Sistemas de Información y Analítica de Datos

Ciberseguridad y blockchain

## GUÍA DOCENTE



Curso Académico:	2022-2023					
Máster:	Máster en Transformación Digital de Empresas					
Denominación de la asignatura	Ciberseguridad y blockchain					
Módulo	Módulo 1: Sistemas de Información y Analítica de Datos					
Curso académico	2022-2023					
Tipología	Obligatoria					
ECTS	<b>Teoría:</b>	3.00	<b>Práctica:</b>	0.00	<b>Total:</b>	3.00
Periodo de impartición	de enero a marzo de 2023					
Modalidad	VIRTUAL					
Web universidad coordinadora	<a href="https://www.unia.es/master.transformacion.digital">https://www.unia.es/master.transformacion.digital</a>					
Web universidad colaboradora	<a href="https://www.uma.es/master-en-transformacion-digital-de-empresas/info/129778/master-en-transformacion-digital-de-empresas/">https://www.uma.es/master-en-transformacion-digital-de-empresas/info/129778/master-en-transformacion-digital-de-empresas/</a>					
Idiomas de impartición	Español					

**Profesorado (profesores correspondientes al curso 2021-22. Por confirmar para el curso 2022-23)**

Nombre y apellidos	Email	Universidad	Créditos
Cristina Alcaraz Tello		UNIVERSIDAD DE MALAGA	3.00

**TUTORIAS (Coordinador/a de asignatura): Horario y localización**
**COMPETENCIAS**

Básicas y Generales	<p>CB8. 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.</p> <p>CG2. Demostrar dominio en la utilización de bibliografía científica y bases de datos, así como en el análisis de documentos científico-técnicos, en el ámbito de la Transformación Digital de Empresas.</p>
---------------------	--

Transversales	CT3. Aplicar la igualdad de género y la reducción de desigualdades en la sociedad a través del conocimiento y la educación y desarrollar un compromiso ético como ciudadano y como profesional.
Específicas	CE4. Identificar las principales amenazas en los diferentes campos de aplicación y evaluar y gestionar los riesgos asociados. CE5. Comparar los servicios, los mecanismos y las herramientas de seguridad y privacidad existentes, y saber aplicarlos, implementarlos o integrarlos en los diversos entornos o escenarios de aplicación, ya sean convencionales o críticos, y de acuerdo con las actuales normativas, estándares y tecnologías.

### RESULTADOS DE APRENDIZAJE

Se espera que al final de este curso el estudiante haya adquirido las siguientes habilidades y conocimientos en materia de ciberseguridad y Blockchain:

- Aprender cuáles son las características específicas de los nuevos paradigmas y las tecnologías habilitadoras, como la red de Blockchain, que ayuden a modernizar los procesos industriales y los sectores estratégicos. Competencias relacionadas: **CB8**.
- Conocer cómo los Sistemas Ciberfísicos, la (I)IoT y otras tecnologías relacionadas se convierten en los bloques de construcción de las infraestructuras críticas, y cómo sus infraestructuras y sistemas de información podrían construirse con dichos bloques de construcción. Competencias relacionadas: **CB8**.
- El estudiante será capaz de entender y clasificar nuevos tipos de ataques emergentes, especialmente aquellos que provengan de la convergencia tecnológica y aplicados a entornos específicos. Para ello, el alumnado aprenderá las características específicas de determinados tipos de ataques e identificar posibles riesgos e impacto, a nivel de infraestructura, de negocio, social o a nivel económico. Competencias relacionadas: **CE4**.
- Comprender la existencia de soluciones y servicios avanzados de seguridad y privacidad, necesarios para la protección de infraestructuras críticas y procesos industriales teniendo en cuenta los nuevos marcos regulatorios, estándares y normativas. Competencias relacionadas: **CE5**.
- Aprender a identificar cuáles son los mecanismos de seguridad y privacidad más adecuados que debería aplicarse en una determinada infraestructura crítica. Competencias relacionadas: **CE5**.
- Entender cómo las características y limitaciones específicas de una infraestructura crítica concreta (ej. una industria inteligente, un sistema de control de energía) y las tecnologías habilitadoras influyen en el diseño, implementación e integración de mecanismos de seguridad específicos. Competencias relacionadas: **CE5**.
- Conocer en detalle la tecnología de Blockchain y su utilidad en entornos estratégicos y en procesos industriales, así como sus problemas de seguridad y privacidad asociados. Competencias relacionadas: **CB8, CE4, CE5**.
- Aprender a integrar mecanismos de seguridad y privacidad para infraestructuras complejas y distribuidas, y saber probar y comprobar la integración de tales mecanismos. Competencias relacionadas: **CE5**.
- Aprender a revisar e identificar el estado del arte de las soluciones y estándares de seguridad y privacidad, y especialmente en el ámbito de la transformación digital de empresas y procesos industriales.

Competencias relacionadas: **CG2**.

- Ser crítico y hábil para analizar y evaluar los nuevos retos de seguridad que están por aparecer en las próximas generaciones industriales. Competencias relacionadas: **CB8, CG2**.
- Saber trabajar de forma individual y en sociedad. Competencias relacionadas: **CT3**.

**CONTENIDOS**

Esta asignatura estará compuesto de tres principales bloques:

- **Bloque 1:** Problemas de seguridad y privacidad en la transformación digital.
- **Bloque 2:** Servicios avanzados de protección en entornos estratégicos.
- **Bloque 3:** Blockchain y su aplicación en entornos estratégicos.

**ACTIVIDADES FORMATIVAS Y METODOLOGÍAS DOCENTES**

AF1. Actividades dirigidas expositivas y prácticas (presenciales, síncronas y/o asíncronas) (18 horas)

Como metodología docente en esta parte de actividades se van a aplicar:

- Principalmente clases magistrales y estudios de casos.
- Aprendizaje basado en proyectos/problemas incluyendo el trabajo académico y el proyecto.

AF2. Actividades dirigidas y/o supervisadas académicamente (4,5 horas)

Como metodología docente se van a utilizar:

- Aprendizaje basado en proyectos/problemas incluyendo el trabajo académico y el proyecto.
- Estudios de casos y discusión de trabajos académicos.
- Tutorías personalizadas y supervisión de trabajos.

AF3. Actividades autónomas del estudiante (52,5 horas)

Con respecto al trabajo autónomo y en grupo del alumnado, éste deberá realizar:

- Desarrollo individual de un trabajo académico y la elaboración de su correspondiente informe.
- Desarrollo en equipo de un proyecto y la elaboración de su correspondiente informe.
- Asimilación de los conocimientos derivados de las materias impartidas en las clases teóricas.
- Realización de las pruebas o cuestionarios a realizar al final de cada uno de los bloques teóricos.

Las actividades formativas se impartirán mediante videoconferencia, en sesiones online haciendo uso de Microsoft Teams, Google Meet o cualquier herramienta similar que decida la coordinación del título, además del Campus Virtual (Moodle) (uso del chat, foros, e-mail, etc.).

Actividad formativa	Modalidad de enseñanza	Dedicación (horas de trabajo autónomo del estudiante)	Dedicación (horas de trabajo del estudiante con apoyo del profesor)
Presentación de la asignatura	SEMIPRESENCIAL	0	0.5
Bloque 1 - Problemas de seguridad y privacidad en la transformación digital	SEMIPRESENCIAL	7	4

Prueba de Bloque 1 - virtual	VIRTUAL	0.5	0
Bloque 2 - Problemas de seguridad y privacidad en la transformación digital	SEMIPRESENCIAL	10	6
Prueba de Bloque 2 - virtual	VIRTUAL	0.5	0
Trabajo académico	SEMIPRESENCIAL	8	2
Bloque 3 - Blockchain y su aplicación en entornos estratégicos	SEMIPRESENCIAL	11	8
Prueba de Bloque 3 - virtual	VIRTUAL	0.5	0
Proyecto académico	SEMIPRESENCIAL	15	2

### SISTEMA DE EVALUACIÓN

Para la evaluación de los contenidos de la asignatura se tendrá en cuenta: (i) el desarrollo del trabajo académico (a nivel individual) y del proyecto (a nivel grupal), por lo que se seguirá una metodología basada en proyectos, (ii) la participación del alumnado en las clases (ya sean en modo síncrono, asíncrono y dirigido) y en las actividades propuestas, así como (iii) la superación de pruebas específicas de los contenidos teóricos y prácticos.

Concretamente, el 70% de la nota final corresponderá a la evaluación continua en el que se desarrollará un trabajo académico que implique la elaboración escrita de un informe de investigación que resuelva o aborde un determinado problema, y el desarrollo de un proyecto durante el periodo lectivo. La asignación porcentual de cada una de estas partes será el 20% (trabajo académico) y el 50% (el proyecto), respectivamente. El 30% restante de la nota final corresponderá a una evaluación específica: un 5% a la participación e interés, y un 25% a las pruebas y cuestionarios (ej. tests de respuesta múltiple) realizados al final de cada uno de los bloques teóricos. Se requiere superar por separado tanto la parte específica (correspondiente al 30%: participación + bloques teóricos) como la evaluación continua (correspondiente al 70%).

Dada la especificidad de las actividades prácticas de esta asignatura, no será posible plantear un sistema de evaluación diferente para los estudiantes a tiempo parcial o los deportistas universitarios de alto nivel, incluyendo otro tipo de alumnos/alumnas especiales como los que realizan prácticas o estancias en el extranjero. Todos ellos/ellas deberán entregar todas las actividades (incluyendo ejercicios, estudios de casos, etc.) o trabajos relacionados. En este caso, es imprescindible tener en cuenta las siguientes condiciones: la calidad de la descripción de los informes (trabajo/proyecto), el cumplimiento de los objetivos y la entrega de las actividades propuestas en el plazo establecido.

La evaluación del resto de convocatorias, se realizará mediante un examen de adquisición de conocimientos en modo online síncrono (ej., un test online a través del campus virtual), en el que se evaluará cada parte (la parte teórica (25%) y/o la parte práctica (70%)) que no haya sido superada en la primera convocatoria ordinaria. Por tanto, se guarda la nota de evaluación continua (70%) y la participación realizada por el alumnado durante el curso lectivo (5%). Si el alumno/a desea ir al 100% de la asignatura para su recuperación, en ese caso, deberá superar por separado tanto la parte teórica (30%) como la parte de evaluación continua (70%), mediante preguntas teóricos-prácticos.

<b>OBSERVACIONES</b>	
None	
<b>Estrategias/metodologías de evaluación</b>	<b>Porcentaje de valoración sobre el total</b>
Trabajo académico o de investigación individual	20%
Trabajo grupal	50%
Participación activa en clase	5%
Cuestionarios (tests online) después de cada bloque	25%
<b>BIBLIOGRAFÍA</b>	
<ul style="list-style-type: none"> <li>• Hands-On Industrial Internet of Things: Create a powerful Industrial IoT infrastructure using Industry 4.0. Giacomo Veneri y Antonio Capasso, Packt Publishing, version Kindle, ISBN: 978-1789537222, 2018.</li> <li>• Digital Transformation, Cyber Security and Resilience of Modern Societies. Tagarev, T., Atanassov, K.T., Kharchenko, V., Kacprzyk, J. (Eds.), Springer, series volumen 84, ISBN: 978-3-030-65721-5, 2021.</li> <li>• Handbook of Research on Advancing Cybersecurity for Digital Transformation, IGI Global, Kamaljeet Sandhu (University of New England, Australia), ISBN: 9781799869757, 2021.</li> <li>• Blockchain Cybersecurity, Trust and Privacy. Choo, Kim-Kwang Raymond, Dehghantanha, Ali, Parizi, Reza M. (Eds.), Springer, series volumen 79, ISBN: 978-3-030-38180-6, 2020.</li> <li>• Blockchain Enabled Applications. Dhillon, Vikram, Metcalf, David, Hooper, Max (Autores), Springer, ISBN: 978-1-4842-6533-8, 2021.</li> <li>• Security and Privacy Trends in the Industrial Internet of Things. C. Alcaraz (Ed.), Springer, ISBN: 978-3-030-12329-1, 2019.</li> <li>• Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing. Autor: Thames, Editores: Lane Thames y Dirk Schaefer, Springer Series in Advanced Manufacturing, 1st ed. 2017 Edición, Edición Kindle, ISBN: 978-3319506593, 2017.</li> <li>• Blockchain: la revolución industrial de internet (Sin colección). Gestión 2000, ISBN: 978-8498754476, 2017.</li> <li>• Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum &amp; Smart Contracts. David Gerard, versión Kindle, 2017.</li> <li>• Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity. Dr. Erdal Ozkaya (Autor), Packt Publishing, ISBN: 978-1789616194, 2019.</li> </ul>	
<b>PLAN DE CONTINGENCIA</b>	
<p><b>Metodología de aprendizaje</b>            En caso de alerta sanitaria, todas las sesiones tendrán lugar en modo online síncrono, incluidas las que puntualmente se hubiera decidido realizar de forma presencial en el laboratorio.</p> <p><b>Procedimiento de evaluación</b>            Se mantendrá lo indicado en el apartado de evaluación.</p>	

y acompañando copia de su documento acreditativo de identidad. La solicitud podrá hacerse mediante escrito en formato papel o por medios electrónicos.

Caso de no obtener contestación o ver desestimada su solicitud puede dirigirse al Delegado de Protección de Datos de la Universidad (rgpd@unia.es Tfno 954 462299) o en reclamación a la Agencia Española de Protección de Datos a través de los formularios que esa entidad tiene habilitados al efecto y que son accesibles desde su página web: <https://sedeagpd.gob.es>

Como responsable, la Universidad le informa que exclusivamente tratará los datos personales que Ud. le facilite para dar cumplimiento a los siguientes fines:

- a) Gestión académica y administrativa de:
- Participación en procesos de acceso y admisión a las enseñanzas oficiales(Grado, Máster y Doctorado) o de formación Continua de la Universidad Internacional de Andalucía.
  - Inscripción y/o matrícula como alumno en cualquiera de las titulaciones oficiales(Grado, Máster y Doctorado), Formación Continua u otras actividades académicas ofrecidas por la Universidad Internacional de Andalucía.
- Participación en convocatorias de becas y ayudas al estudio de la Universidad Internacional de Andalucía, la Admón. General del Estado o la de las Comunidades Autónomas y de otras entidades públicas o privadas.
- Participación en convocatorias de programas de movilidad de carácter nacional o internacional.
  - Obtención y expedición de títulos oficiales, títulos propios y otros títulos académico
- b) Gestión de su participación como estudiante en prácticas y actividades formativas nacionales o internacionales en instituciones, empresas, organismos o en otros centros.
- c) Utilización de servicios universitarios como obtención del carné universitario, bibliotecas, actividades deportivas u otros.

La Universidad se encuentra legitimada para tratar estos datos al ser necesarios para la ejecución de la relación jurídica establecida entre Ud. y la Universidad y para que ésta pueda cumplir con sus obligaciones legales establecidas en la Ley Orgánica 6/2001, de Universidades.

Usted responde de la veracidad de los datos personales que ha proporcionado a la Universidad y de su actualización.

La Universidad comunicará los datos personales que sean indispensables, y nunca en otro caso, a las siguientes categorías de destinatarios:

- A otras Administraciones y organismos públicos para el ejercicio de las competencias que les sean propias y compatibles con las finalidades arriba enunciadas(Así - a modo enunciativo y no limitativo - a Ministerios con competencias en educación y ciencia, a otras administraciones, a otras Universidades o Centros formativos equivalentes para la gestión de traslados, a empresas para la realización de prácticas)
- A entidades bancarias para la gestión de pagos y cobros.
- A organismos públicos o privados en virtud de la celebración de convenios de colaboración o contratos, conforme a lo dispuesto en la legislación vigente en materia de Protección de Datos.
- A los servicios de la propia Universidad que sean adecuados para gestionar la utilización de los servicios universitarios ofertados.

Sus datos de carácter personal se tratarán y conservarán por la Universidad conforme a la legislación vigente en materia de protección de datos, pasando luego a formar parte -previo expurgo - del Archivo Histórico Universitario conforme a lo dispuesto en la legislación sobre Patrimonio Histórico.

La Universidad sólo prevé la transferencia de datos a terceros países en el caso de su participación como alumno en alguno de los programas de formación o becas de carácter internacional. La transferencia se realizará siguiendo las directrices establecidas al respecto por el Reglamento Europeo de Protección de Datos y normativa de desarrollo.

El Servicio de Protección de Datos de la Universidad Internacional de Andalucía cuenta con una página en la que incluye legislación, información y modelos en relación con la Protección de Datos Personales a la que puede acceder desde el siguiente enlace: <https://www.unia.es/protecciondatos>