Proyecto docente

Asignatura	Derecho en Seguridad de datos		
Materia	Derecho		
Titulación	Máster Universitario en Inteligencia de Negocio y Big Data en Entornos Seguros		
Plan	2018	**Código**	
Periodo de impartición	Primer semestre	**Tipo/Carácter**	Obligatoria
Nivel/Ciclo	Máster	**Curso**	1
Créditos ECTS	3		
Lengua en que se imparte	Castellano		
Profesor/es responsable/s	Profesora responsable: Álvarez Cuesta, Henar Profesores: Álvarez Rodríguez, Aurelia Díaz Y García-Conlledo, Miguel Fernández Fernández, Roberto Fuertes López, María De Las Mercedes Luis Ángel Ballesteros Moffa Seijas Villadangos, María Esther Carrizo Aguado, David		
Datos de contacto (e-mail, teléfono…)	halvc@unileon.es : Henar Álvarez Cuesta aalvr@unileon.es mdiag@unileon.es rferf@unileon.es mmfuel@unileon.es luis.ballesteros@unileon.es meseiv@unileon.es dcara@unileon.es		
Horario de tutorías	Previa solicitud por correo electrónico. Horario acordado con el estudiante		
Coordinador	Henar Álvarez Cuesta		
Departamento	Derecho Privado y de la Empresa (Universidad de León)		
Web			
Descripción General	La asignatura ofrecerá a los estudiantes una panorámica general del derecho en protección de datos desde distintas perspectivas jurídicas.		

1. Situación / Sentido de la asignatura

1.1 Contextualización

El derecho a la protección de datos regulado por el Reglamento 2016/679 y la Ley Orgánica 3/2018 hacen necesario un examen multidisplinar de los distintos sectores del ordenamiento jurídico en presencia (Derecho Constitucional, Administrativo, Penal, Laboral e Internacional Privado). Asimismo, quienes vayan a desarrollar su actividad productiva en este campo precisan de un conocimiento somero de la legislación aplicable al efecto.

1.2 Relación con otras asignaturas

La asignatura presenta un contenido transversal que servirá para conocer las implicaciones legales del trabajo realizado en el resto de asignaturas.

1.3 Prerrequisitos

No existe ningún prerrequisito

2. Competencias

2.1 Generales del título

CG1. Adquisición de competencias teóricas y prácticas para el análisis y diseño de soluciones empresariales en Big Data (almacenamiento y procesamiento de grandes volúmenes de información heterogénea).
CG2. Capacidad de planificar y construir sistemas que permitan una gestión segura de los datos.
CG3. Capacidad de diseñar e implementar sistemas capaces de extraer conocimiento práctico de grandes volúmenes de datos aplicado al mundo de la empresa (Inteligencia de Negocio/Business Intelligence)

2.2 Específicas materia

CSD1. Capacidad para utilizar los conceptos básicos de ciberseguridad en proyectos de Big Data.
CSD4. Capacidad para acceder, analizar y aplicar la información generada en Centros de Respuesta a Incidentes de Seguridad, así como conocer sus principios de funcionamiento y normativas.
CSD5. Capacidad de diseñar y aplicar soluciones relativas a los aspectos relativos a temas de la seguridad y privacidad en entornos de Big Data.

3. Resultados de aprendizaje

Al finalizar la asignatura, el estudiante será capaz de:

Saber conocer y aplicar la distinta normativa existente en materia de protección de datos

Saber resolver los problemas jurídicos producidos en el ámbito de la protección de datos

Conocer las principales amenazas a la seguridad en el ciberespacio, así como los principales tipos de cibercrimen

Conocerá y aprenderá a aplicar la normativa existente en materia de ciberseguridad

Aprenderá a analizar las distintas implicaciones jurídicas que plantea el trabajo en el ámbito de Big Data y la protección de datos

4. Contenido / Programa de la asignatura

Bloque 1: Derecho constitucional y derechos digitales

Carga de trabajo en créditos ECTS: 0.6

a. Contextualización y justificación

La necesidad de conocer y distinguir las distintas normas aplicables al ámbito de la protección de datos hace necesaria la implementación del primero de los bloques que conforman la asignatura Derecho en seguridad de datos. Es así que se abordarán los contextos nacional, supranacional e internacional para que el alumno sea conocedor de los distintos órdenes que se afectan mutuamente y que inciden no solo en la protección de datos sino en el estatus mismo de ciudadanía. A su vez se tratará de facilitar los conocimientos necesarios para afrontar el resto de bloques.

b. Objetivos de aprendizaje

Conocer el marco normativo de los derechos digitales a nivel internacional y nacional

Conocer los derechos constitucionales y su desarrollo en la LO 3/2018 referidos a los derechos digitales

c. Contenidos y materiales de aprendizaje

LECCIÓN 1: MARCO NORMATIVO DE LOS DERECHOS DIGITALES EN EL ENTORNO SUPRA E INTERNACIONAL

1. NIVEL GLOBAL:

1.1 Declaración Universal de los Derechos Humanos

1.2 Soft Law

2. NIVEL EUROPEO:

2.1 Derecho Originario

2.2 Derecho Derivado

LECCIÓN 2: DERECHOS DIGITALES Y CONSTITUCIÓN ESPAÑOLA

2.1. Contexto político y analítico: protección de datos, privacidad y habeas data

2.2. Constitución española: art. 18.4

2. 3. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

2.4 Jurisprudencia del Tribunal Constitucional

d. Métodos docentes

Se expondrán en remoto y de forma asíncrona los contenidos teórico-prácticos de la asignatura

Formulación, análisis, resolución y debate de un problema o ejercicio relacionado con el contenido de la asignatura.

e. Bibliografía básica

- Declaración Universal de Derechos Humanos (DUDH), PIDCP y PIDESC.
- Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), Tratado de la UE (TUE) y Tratado de Funcionamiento de la UE (TFUE).
- Reglamento (UE) 2016/679 General de Protección de Datos (RGPD).
- Constitución Española (CE).
- Ley Orgánica 3/2018, 5 diciembre, Protección de Datos Personales y garantía de derechos digitales (LOPDGDD).
- Código de Protección de Datos de Carácter persona. Disponible en: https://www.boe.es/legislacion/codigos/codigo.php?id=55&modo=1&nota=0&tab=2

- Código de Derecho de la Ciberseguridad. Disponible en: https://www.boe.es/legislacion/codigos/codigo.php?id=173&modo=1&nota=0&tab=2
- ÁLVAREZ ROBLES, T. "Derechos digitales: especial interés en los derechos de acceso a Internet y a la ciberseguridad como derechos constitucionales sustantivo". Juventud y constitución: un estudio de la Constitución española por los jóvenes en su cuarenta aniversario. coord. por Andrés Iván Dueñas Castrillo, Daniel Fernández Cañueto, Gabriel Moreno González, 2018, ISBN 9788494620140, págs. 135-158.

f. Bibliografía complementaria

- BUSTAMANTE DONAS, J. "Hacia la cuarta generación de derechos humanos: repensando la condición humana en la sociedad tecnológica". CTS+I: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación, ISSN-e 1681-5645, Nº. 1, 2001.
- FUERTES LÓPEZ, M. "En defensa de la neutralidad de la red", R.V.A.P. núm. especial 99-100. Mayo-Diciembre 2014. Págs. 1397-1412.
- Carta de derechos humanos y principios para Internet del Internet Governance Froum UN. Disponible en: http://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf
- Carta de derechos humanos y principios para Internet. Naciones Unidas, Internet Governance Forum. 2015. Disponible en: http://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf
- Guías de la Agencia Española de Protección de Datos. Disponibles en: https://www.aepd.es/es/guias-y-herramientas/guias

g. Recursos necesarios

- Plataforma docente
- Herramientas de comunicación:
  - Asíncronos: foros existente en cada bloque, correos electrónicos
  - Videoconferencia

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
0.5	Primera semana

Bloque 2: "Consecuencias administrativas de los retos planteados por la protección de datos y la ciberseguridad"

Carga de trabajo en créditos ECTS: 0.6

a. Contextualización y justificación

La multiplicación de riesgos y amenazas en el ciberespacio hacen indispensable establecer instrumentos jurídicos que garanticen la identidad personal, eviten suplantaciones o suplantaciones, protejan, en fin, tantos datos personales que se trasladan por las redes o se almacenan en servidores. De ahí que resulte indispensable que los estudiantes conozcan los organismos e instituciones básicas que se dirigen a garantizar el entorno seguro de las comunicaciones y relaciones en el ciberespacio.

b. Objetivos de aprendizaje

Conocer las competencias y organización de las entidades competentes en protección de datos.

Comprender y conocer los objetivos y prioridades en materia de ciberseguridad

c. Contenidos y materiales de aprendizaje

LECCIÓN 3: Derecho público y protección de datos.

1. Régimen jurídico de privacidad: Derecho común y Derechos especiales (el conflicto con la seguridad)
2. Ámbito de la protección de datos
3. Competencias y organización administrativa (CEPD y AEPD). Las funciones de supervisión, inspección y sanción
4. El refuerzo de la e-Administración y el tratamiento de datos por las Administraciones públicas
5. La privacidad en las comunicaciones electrónicas. El impacto de las tecnologías disruptivas

LECCIÓN 4.- Objetivos y prioridades en materia de ciberseguridad.

1.- Estrategia de ciberseguridad de la Unión Europea
2. ENISA y la certificación voluntaria de ciberseguridad
3. Estrategia nacional de ciberseguridad: principales objetivos y líneas de actuación
4. La protección de las infraestructuras críticas
5. La seguridad de las redes y sistemas de comunicación
6. La organización de la ciberseguridad
7. La comunicación de incidente

d. Métodos docentes

Se expondrán en remoto y de forma asíncrona los contenidos teórico-prácticos de la asignatura

Formulación, análisis, resolución y debate de un problema o ejercicio relacionado con el contenido de la asignatura.

e. Bibliografía básica

VVAA “Sociedad digital y Derecho”, BOE

Estrategia Nacional de Ciberseguridad

PIÑAR MAÑAS, J. L. (dir.), Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad, 2017.

LÓPEZ CALVO, J., Comentarios al Reglamento europeo de protección de datos, 2017.

DAVARA RODRÍGUEZ, M. A., La protección de datos personales en el sector de las comunicaciones electrónicas, 2003.

BALLESTEROS MOFFA, L. A., La privacidad electrónica. Internet en el centro de protección, 2005.

f. Bibliografía complementaria

Se facilitará durante el curso académico.

g. Recursos necesarios

- Plataforma docente
- Herramientas de comunicación:
  - Asíncronos: foros existente en cada bloque, correos electrónicos
  - Videos
  -

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
0.5	Segunda semana

Bloque 3: "Derecho Penal y ciberseguridad"

Carga de trabajo en créditos ECTS: 0.6

a. Contextualización y justificación

La proliferación de comportamientos punibles por el ordenamiento penal en el ámbito digital y en particular por cuanto afecta a la protección de datos hacen necesario realizar una aproximación a las fuentes del Derecho Penal, a sus principios de aplicación y a los tipos delictivos conectados con la protección de datos.

b. Objetivos de aprendizaje

Conocer los aspectos generales del Derecho Penal relacionados con la ciberseguridad y la protección de datos.
Comprender la regulación de los principales ciberdelitos

c. Contenidos y materiales de aprendizaje

LECCIÓN 5. Aspectos generales del Derecho Penal en relación con la ciberseguridad (I)
LECCIÓN 6. Aspectos generales del Derecho Penal en relación con la ciberseguridad (II): Panorámica de los principales ciberdelitos

d. Métodos docentes

Se expondrán en remoto y de forma asíncrona los contenidos teórico-prácticos de la asignatura
Formulación, análisis, resolución y debate de un problema o ejercicio relacionado con el contenido de la asignatura.

e. Bibliografía básica

Se proporcionará durante el curso

f. Bibliografía complementaria

g. Recursos necesarios

- Plataforma docente
- Herramientas de comunicación:
  - Asíncronos: foros existente en cada bloque, correos electrónicos
  - Videoconferencia

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
0.5	Tercera semana

Bloque 4: "Consecuencias jurídicas del big data en la empresa"

Carga de trabajo en créditos ECTS: 0.6

a. Contextualización y justificación

El impacto del derecho de protección de datos en el ámbito de las relaciones laborales, tanto individuales como colectivas, hacen preciso su estudio específico.

b. Objetivos de aprendizaje

Comprender los límites del control empresarial a través de la tecnología

Conocer las implicaciones que la normativa en protección de datos y derechos digitales plantea en el ámbito laboral.

c. Contenidos y materiales de aprendizaje

LECCIÓN 7: Relaciones laborales y sistemas tecnológicos.

1.- Selección de personal

2.- Teletrabajo o trabajo a distancia.

3.- Poderes del empresario.

4.- Derechos de los trabajadores

5.- Pactos típicos en la relación laboral

6.- Despido y sistemas tecnológicos

LECCIÓN 8: Relaciones laborales y protección de datos.

1.- Los nuevos derechos digitales de los trabajadores en la normativa de Protección de Datos.

2.- Repercusiones de la protección de datos en el contrato de trabajo

3.- Control empresarial de la actividad laboral y protección de datos

d. Métodos docentes

Se expondrán en remoto y de forma asíncrona los contenidos teórico-prácticos de la asignatura

Formulación, análisis, resolución y debate de un problema o ejercicio relacionado con el contenido de la asignatura.

e. Bibliografía básica

PRECIADO DOMENECH, C.H.: El derecho a la protección de datos en el contrato de trabajo, Cizur Menor, Aranzadi, 2017.

RODRÍGUEZ ESCANCIANO, S.: Derechos laborales digitales: garantías e interrogantes, Aranzadi, 2019..

f. Bibliografía complementaria

g. Recursos necesarios

- Plataforma docente
- Herramientas de comunicación:
  - Asíncronos: foros existente en cada bloque, correos electrónicos
  - Videoconferencia

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
0.5	Cuarta semana

Bloque 5: Derecho internacional privado y ciberseguridad: "Los daños contra la personalidad cometidos en Internet y la protección de la privacidad en el espacio europeo"

Carga de trabajo en créditos ECTS: 0.6

a. Contextualización y justificación

Internet es un elemento clave de la llamada sociedad de la información, pues facilita los más variados servicios electrónicos interactivos y la comunicación de todo tipo de informaciones. El desarrollo de la red de redes ha ido unido a la expansión de plataformas de contenidos y servicios semicerradas que contrastan con el carácter abierto de la web y cuyos usuarios no acceden a los contenidos dentro de la plataforma a través de los navegadores web ni de los motores de búsqueda, pero que sí emplean Internet para la transferencia de grandes cantidades de datos. Así, las aplicaciones y servicios digitales se caracterizan por la presencia de técnicas que facilitan el acceso por terceros a datos personales y su tratamiento, con gran frecuencia sin el consentimiento -ni siquiera el conocimiento- de los afectados. De esta manera, la interconexión a nivel mundial de las redes digitales promueve la globalización de la información, de manera que Internet constituye un medio propicio para la circulación transfronteriza de información, lo que genera particulares riesgos respecto de los datos de carácter personal, vinculados a la diversidad de niveles de protección existentes a nivel comparado, donde cabe apreciar divergencias muy significativas en la protección jurídica de los datos personales entre los diversos ordenamientos, incluso de países con niveles tecnológicos parejos

b. Objetivos de aprendizaje

Conocer los aspectos internacionales de los daños contra la personalidad cometidos en Internet.
Comprender cuál es el foro y la Ley aplicable a los ilícitos civiles cometidos en la Red.
Saber conocer y aplicar la distinta normativa existente en materia de la protección de datos en el ámbito europeo.

c. Contenidos y materiales de aprendizaje

LECCIÓN 9: Aspectos internacionales de los daños contra la personalidad cometidos en Internet

1. Observaciones preliminares
2. Situaciones cubiertas por el Derecho internacional privado

2.1. Autoridad judicial competente

2.2. Derecho aplicable

2.3. Reconocimiento y ejecución de decisiones extranjeras

3. Aplicabilidad práctica

LECCIÓN 10: La protección de la privacidad en el contexto internacional

1. Ley aplicable

2. Competencia judicial internacional

3. Aplicabilidad práctica

d. Métodos docentes

Se expondrán en remoto y de forma asíncrona los contenidos teórico-prácticos de la asignatura

Formulación, análisis, resolución y debate de un problema o ejercicio relacionado con el contenido de la asignatura.

e. Bibliografía básica

AA.VV, Derecho TIC. Derecho de las tecnologías de la información y de la comunicación, LÓPEZ-TARRUELLA MARTÍNEZ, A. (Dir.), Tirant lo Blanch, 2016

CALVO CARAVACA, A-L. / CARRASCOSA GONZÁLEZ, J, Conflictos de Leyes y conflictos de Jurisdicción en Internet, Colex, 2001.

CORDERO ÁLVAREZ, C.I., Litigios internacionales sobre difamación y derechos de la personalidad, Dykinson, 2015.

DE MIGUEL ASENSIO, P.A., Derecho Privado de Internet, 5ª ed., Thomson Reuters Aranzadi, 2015.

ORTEGA GIMÉNEZ, A., Transferencias internacionales de Datos de Carácter Personal Ilícitas, Thomson Reuters Aranzadi, 2016.

f. Bibliografía complementaria

g. Recursos necesarios

- Plataforma docente
- Herramientas de comunicación:
  - Asíncronos: foros existente en cada bloque, correos electrónicos
  - Videoconferencia

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
0.5	Quinta semana

Añada tantas páginas como bloques temáticos considere realizar.

Añada tantas páginas como bloques temáticos considere realizar.

5. Metodología de enseñanza y dedicación del estudiante a la asignatura

Actividad Formativa	Competencias relacionadas	Horas	Presencialidad (%)
Clases, conferencias y técnicas expositivas		12	0
Actividades autónomas y en grupo (trabajos y lecturas dirigidas)		45	0
Pruebas de seguimiento y exposición de trabajos		10	50
Tutoría individual, participación en foros y otros medios colaborativos		8	0

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
BLOQUE I: Derecho Constitucional y Ciberseguridad	0.5	Primera semana
BLOQUE II.- Consecuencias administrativas de los retos planteados por la ciberseguridad	0.5	Segunda semana
BLOQUE III: Derecho Penal y ciberseguridad	0.5	Tercera semana
BLOQUE IV: Consecuencias jurídicas del big data en la empresa	0.5	Cuarta semana
BLOQUE V: Derecho Internacional Privado y Ciberseguridad	0.5	Quinta semana
Entrega final de trabajos, pruebas y corrección	0.5	Sexta semana

7. Evaluación

Instrumento / Procedimiento	Peso primera convocatoria	Peso segunda convocatoria
Evaluación sumativa, que incluye pruebas parciales individuales y prueba final	30%	30%
Realización de trabajos, proyectos, resolución de problemas y casos	60%	60%
Participación en foros y otros medios participativos	10%	10%

Criterios / Comentarios a la evaluación
• **Convocatoria ordinaria:** La evaluación continua se realizará a través de la resolución de las distintas actividades (casos prácticos, test, comentarios, resúmenes, etc.) propuestos en clase en las fechas indicadas por cada Profesor. En su corrección se tendrán en cuenta los siguientes criterios: correcto planteamiento de la solución, estructura, calidad, uso debido del lenguaje, redacción, interpretación hermenéutica de la norma, capacidad crítica y claridad en la exposición. Las prácticas sólo se valorarán de forma continua cuando el alumno las haya hecho y entregado en el plazo fijado por el profesor a lo largo del semestre. No se podrán, por tanto, entregar con posterioridad • **Convocatoria extraordinaria:** En segunda convocatoria ordinaria serán evaluables las actividades indicadas por cada profesor, semejantes a los de la primera convocatoria, con los requisitos expuestos para la primera convocatoria respecto a la utilización de legislación, y fuentes de información físicas o tecnológicas. La simple tenencia de dichos dispositivos así como de apuntes, libros, carpetas o materiales diversos no autorizados durante las pruebas de evaluación, supondrá la retirada inmediata del examen, su expulsión del mismo y su calificación como suspenso, comunicándose la incidencia a la Autoridad Académica del Centro para que realice las actuaciones previstas en las Pautas de Actuación en los Supuestos de Plagio, Copia o Fraude en Exámenes o Pruebas de Evaluación, aprobadas por la Comisión Permanente del Consejo de Gobierno de 29 de enero de 2015.

9. Consideraciones / Comentarios adicionales