

Máster de Formación Permanente

Protección de Datos





Máster de Formación Permanente Protección de Datos

- » Modalidad: **online**
- » Duración: **7 meses**
- » Titulación: **TECH Universidad Tecnológica**
- » Acreditación: **60 ECTS**
- » Horario: **a tu ritmo**
- » Exámenes: **online**

Acceso web: www.techtitute.com/derecho/master/master-proteccion-datos

Índice

01

Presentación

pág. 4

02

Objetivos

pág. 8

03

Competencias

pág. 14

04

Estructura y contenido

pág. 18

05

Metodología

pág. 28

06

Titulación

pág. 36

01

Presentación

La protección de datos es un elemento central en las empresas de la actualidad. Las autoridades europeas son conscientes de ello y han impuesto la obligatoriedad de designar un responsable de protección de datos en cada compañía, tal y como expresa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, que regula el tratamiento que realizan personas, empresas u organizaciones de los datos personales relacionados con personas en la Unión Europea. Esta titulación, por tanto, ofrece a sus alumnos los conocimientos para convertirse en un especialista en protección de datos y poder, así, ocupar el puesto de responsable en las numerosas empresas que requieren un experto en la materia. Todo ello con la metodología más vanguardista y en formato totalmente online.





“

Las empresas buscan abogados capaces de defenderlas en asuntos relacionados con la Protección de Datos, por lo que tu cualificación superior será un plus para acceder a un mercado laboral altamente competitivo”

Proteger y salvaguardar la información confidencial y personal de la entidad, los trabajadores, colaboradores y clientes pueden salvar a las compañías de tener que enfrentarse a procedimientos legales en los que tendrían mucho que perder. Por ello, las compañías, en la actualidad, deben contar con responsables de protección de datos que sean capaces de cumplir con las normativas vigentes, así como con equipos de abogados que les asesoren para llevar a cabo dichas tareas de manera precisa. Sin duda, el papel del abogado es fundamental en este tipo de actuaciones y su especialización en las normativas nacionales e internacionales sobre protección de datos será fundamental para su crecimiento profesional, habilitándole para gestionar y aplicar dichos reglamentos y, sobre todo, abriéndole las puertas a un mercado laboral de alta remuneración, en el que será considerado como uno de los profesionales más capacitados de la compañía. Pero, además, los abogados con este tipo de especialización tendrán la cualificación necesaria para defender a sus compañías o clientes con éxito en los tribunales, en los casos relacionados en que se puedan ver involucrados.

Para alcanzar estos objetivos, TECH propone la realización de un programa de primer nivel, en el que se ofrece una visión integral y multidisciplinar de la materia, no solo abarcando las cuestiones tradicionales objeto de estudio en el ámbito del derecho de protección de datos, como es el análisis de la normativa aplicable, la prestación del consentimiento, los derechos digitales o el régimen sancionatorio, sino abordando también otras materias vinculadas con la protección de datos, como las relativas a la protección penal o la protección de datos en el sector público.

De esta manera, este Máster de Formación Permanente le servirá al alumnado para profundizar en el estudio del régimen jurídico de la protección de datos, complementando el conocimiento teórico con cuestiones prácticas, innovadoras y de actualidad que se requieren en un profesional vinculado con la protección de datos y que demanda el mercado laboral. Un programa 100% online que será un gran valor añadido en su CV y que marcará la distancia con el resto de los abogados con dicha especialidad.

Este **Máster de Formación Permanente en Protección de Datos** contiene el programa más completo y actualizado del mercado. Sus características más destacadas son:

- ♦ El desarrollo de casos prácticos presentados por expertos Protección de Datos
- ♦ Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que están concebidos recogen una información científica y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- ♦ Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- ♦ Su especial hincapié en metodologías innovadoras Protección de Datos
- ♦ Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- ♦ La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet



Conocer en profundidad la normativa sobre protección de datos te situará como uno de los profesionales más importantes de tu empresa”



Las empresas buscan profesionales como tú para asesorarlas ante posibles conflictos sobre protección de datos. Así que no pierdas la oportunidad de estudiar este Máster de Formación Permanente y destacar en el sector”

Incluye como editores de material a profesionales pertenecientes al ámbito de Protección de Datos, que vierten en esta capacitación la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextual, es decir, un entorno simulado que proporcionará una capacitación inmersiva programada para entrenarse ante situaciones reales.

El diseño de este programa se centra en el aprendizaje basado en problemas, mediante el cual el profesional deberá tratar de resolver las distintas situaciones de práctica profesional que se le planteen a lo largo del curso académico. Para ello, el profesional contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos Protección de Datos, y con gran experiencia.

Las regulaciones actuales sobre protección de datos han promovido una nueva oportunidad laboral en el ámbito del derecho. Especialízate en este campo y aumenta tu competitividad y opciones de empleabilidad.

Con estrategias de aprendizaje centradas en la práctica, esta capacitación te permitirá aprender de manera real e inmediata.



02

Objetivos

El objetivo de esta capacitación es conseguir que nuestro alumnado aprenda de forma estimulante y atractiva, de manera que el interés en el estudio no decaiga durante el tiempo de trabajo. De esta manera, TECH impulsa de forma real la consecución de los objetivos de aprendizaje y con ellos, tu crecimiento profesional.



“

Conviértete en un abogado especializado en protección de datos y da servicio a múltiples empresas que precisan de asesoramiento en este campo”

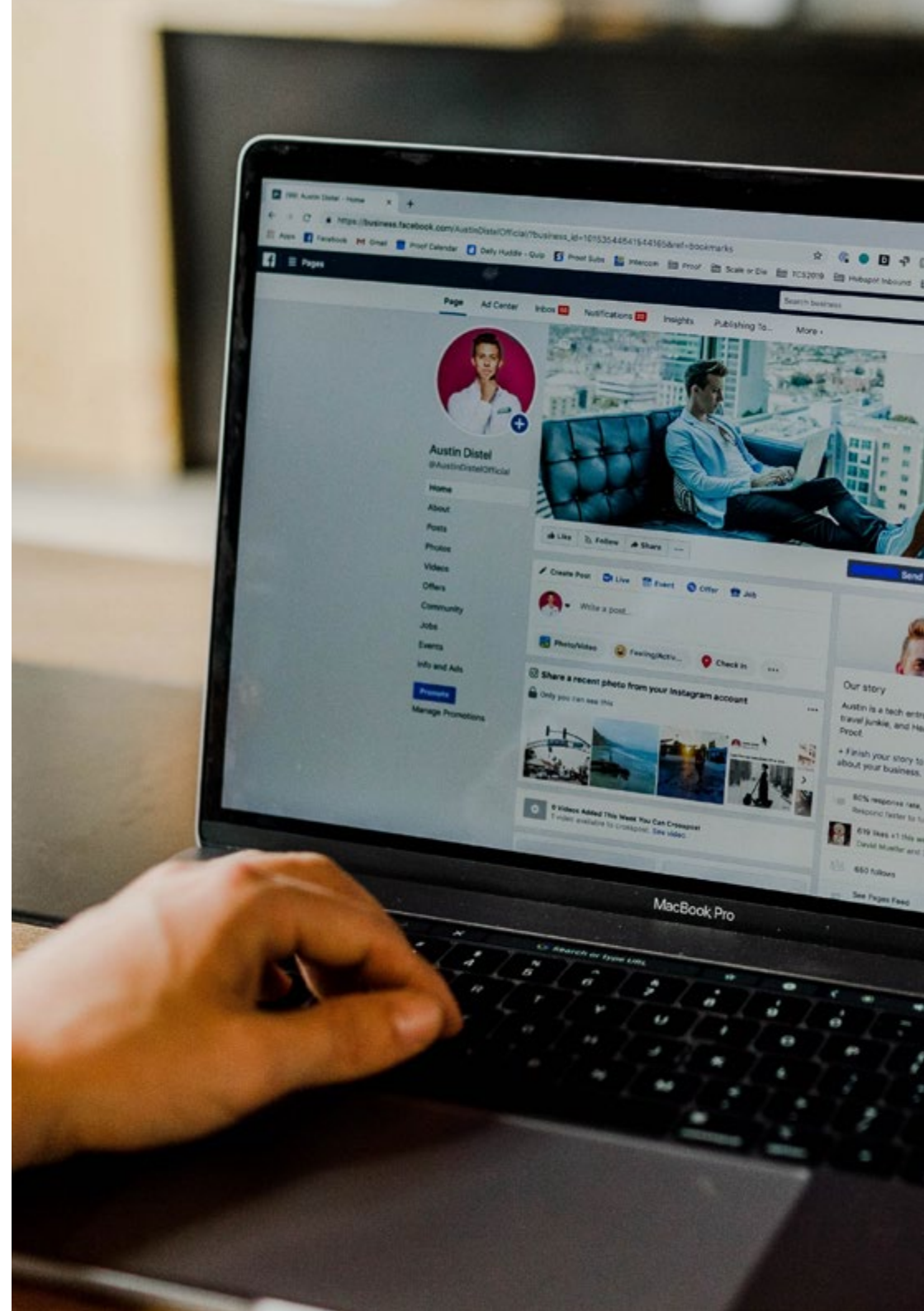


Objetivos generales

- ◆ Adquirir los conocimientos y técnicas imprescindibles para la asunción y organización de las responsabilidades organizativas de una oficina
- ◆ Aprender a liderar y dirigir proyectos de menor o mayor intensidad y complejidad, Gestionar de manera fluida y dirigir con acierto en todas las áreas en que esta acción se realiza

“

Nuestro objetivo es sencillo: impulsarte hacia el dominio de todos los aspectos de esta cuestión”





Objetivos específicos

Módulo 1. Marco normativo de protección de datos y la prestación del consentimiento

- ◆ Detallar el marco normativo
- ◆ Identificar los distintos problemas en la obtención del consentimiento en este ámbito

Módulo 2. La protección de datos en el sector público

- ◆ Analizar la normativa de protección de datos desde el ámbito público
- ◆ Conocer la estructura institucional en materia de protección de datos: órganos, competencias, procedimientos
- ◆ Delegar la protección de datos: relevancia de esta figura como garante del cumplimiento de la normativa por las administraciones públicas y de los derechos de los interesados
- ◆ Conocer las reglas especiales para el tratamiento de los datos en las Administraciones Públicas
- ◆ Conocer la regulación sectorial

Módulo 3. Un estudio sobre los datos de salud como categoría especial de datos personales

- ◆ Obtener la capacidad necesaria para abordar las cuestiones en torno a la salud, identificando las principales problemáticas
- ◆ Identificar los datos de salud, con especial incidencia en los datos sensibles o especiales
- ◆ Adquirir la habilidad necesaria en el análisis del tratamiento de los datos de salud
- ◆ Interrelacionar los datos de salud con la investigación científica o biomédica
- ◆ Aprender el tratamiento de los datos de salud en tiempos de pandemia

Módulo 4. Los derechos de las personas en materia de protección de datos

- ♦ Detallar el régimen jurídico de los derechos y libertades reconocidos en los principales instrumentos de protección de datos a las personas interesadas en el entorno Big data
- ♦ Ahondar en el fenómeno de transformación social y jurídica del Big data y su incidencia en los derechos fundamentales a través de su progresión temporal y jurídica
- ♦ Profundizar en el análisis y comprensión del derecho de supresión (derecho al olvido) y detallar las claves para su ejercicio procesal
- ♦ Dominar la terminología jurídica aplicable, diferenciar entre figuras jurídicas afines y discernir el método jurídico más idóneo para la protección de los derechos del interesado en el caso concreto
- ♦ Identificar los puntos débiles de la regulación actual y los retos jurídicos en la materia para poder adelantarse a contextos futuros

Módulo 5. El régimen de responsabilidad civil y sancionatoria

- ♦ Ampliar conocimiento en el régimen jurídico del sistema de responsabilidad civil en materia de protección de datos
- ♦ Profundizar en las características especiales de la acción de reclamación y ser capaz de redactar la misma
- ♦ Detallar las peculiaridades de los prestadores de servicios de la sociedad de la información como sujetos responsables en materia de protección de datos
- ♦ Distinguir la terminología sancionatoria tanto del RGPD, como de la LOPDGDD
- ♦ Profundiza en las distintas infracciones y los sujetos responsables de las mismas para poder iniciar un procedimiento sancionador

Módulo 6. La protección de datos personales y las garantías de los derechos digitales en relación a las TICs en la sociedad de la información

- ♦ Consolidar los principales aspectos referentes a la protección de datos personales en relación con las nuevas tecnologías de la información y comunicación
- ♦ Determinar los conflictos jurídicos que se plantean en torno a la protección de datos en relación con la persona y la salud, así como en el ámbito civil y empresarial
- ♦ Profundizar en los diferentes aspectos que se originan en relación con la información falsa, inteligencia artificial y el derecho de información
- ♦ Abordar las cuestiones que inciden en el ámbito de la genética y la salud, así como los avances en relación con la protección del menor
- ♦ Establecer e identificar los efectos y consecuencias que se producen en relación a la protección de datos personales y las personas fallecidas

Módulo 7. Protección penal de los datos

- ♦ Examinar el régimen jurídico del sistema de responsabilidad penal en materia de protección de datos
- ♦ Detallar las infracciones penales en el ámbito de los datos permitiendo identificarlas de forma correcta
- ♦ Ahondar en el régimen de la responsabilidad penal de las personas jurídicas permitiendo detectar las infracciones, modo de actuar y su fin preventivo
- ♦ Distinguir la interrelación entre el proceso penal en materia de datos y las tecnologías
- ♦ Profundizar en el proceso penal, límites y garantías, en el tratamiento de datos

Módulo 8. Los modelos de *compliance*. Un enfoque práctico de la protección de datos en las empresas

- ♦ Examinar el marco jurídico de los modelos de *compliance* en España, partiendo de la evolución histórica de estas figuras
- ♦ Ahondar, desde una perspectiva práctica, el funcionamiento y los principales elementos de los modelos de *compliance*
- ♦ Adquirir una comprensión de la finalidad de los modelos de *compliance*, con el objetivo de contextualizar de manera adecuada todas las medidas que los integran, enfatizando el papel del *compliance* como forma de generar confianza en terceros
- ♦ Profundizar en la problemática actual en los modelos de *compliance* relativa a la protección de datos

Módulo 9. La protección de datos en Europa: presente y futuro desde la perspectiva del derecho internacional privado

- ♦ Detallar el sistema de protección de datos internacional en Europa
- ♦ Especializarse en la interconexión entre los diversos instrumentos normativos
- ♦ Determinar la competencia judicial internacional en los diversos conflictos transfronterizos sobre protección de datos
- ♦ Determinar la ley aplicable para los diversos conflictos transfronterizos sobre protección de datos
- ♦ Detallar la problemática particular del derecho internacional privado en relación con la protección de datos
- ♦ Reflexionar sobre la importancia del acercamiento entre las conexiones utilizadas para la determinación de la competencia judicial internacional y la ley aplicable en los diversos conflictos internacionales sobre la protección de datos

Módulo 10. Evaluaciones de impacto y gestión de la seguridad de la información

- ♦ Detallar el proceso de gestión de los riesgos en materia de protección de datos
- ♦ Ahondar en las distintas etapas de un análisis de riesgos: identificación, análisis, evaluación y tratamiento
- ♦ Profundizar en las diferencias entre un análisis de riesgos y una evaluación de impacto
- ♦ Dominar cómo se realiza una evaluación de impacto
- ♦ Ahondar la relación que existe entre el derecho y la ciberseguridad
- ♦ Distinguir los conceptos principales de seguridad de la información
- ♦ Detallar los roles existentes en las entidades públicas y privadas que realizan funciones de seguridad
- ♦ Especializarse con el concepto gobierno de seguridad de la información
- ♦ Examinar las sinergias existentes entre seguridad y privacidad
- ♦ Profundizar cómo se estructura un equipo de respuesta ante incidentes de seguridad y la importancia de cumplir con los aspectos legales asociados a estos procesos
- ♦ Saber el proceso de auditoría de sistemas de gestión y la cadena de custodia informática

03

Competencias

Nuestro programa se ha diseñado para conseguir de manera específica, que los alumnos terminen la capacitación con la capacidad real de aplicar los conocimientos adquiridos. Estas nuevas competencias te llevarán hacia una capacidad de trabajo mucho mayor y darán a tu CV un nuevo valor de competitividad, imprescindible en el mercado laboral actual.

anal

A

Analytics

IMAGES

NEWS

Google Analytics - Mobile

https://www.google.com

“

Incorpora a tu capacitación las competencias necesarias para trabajar en el ámbito de la protección de datos con seguridad y solvencia”

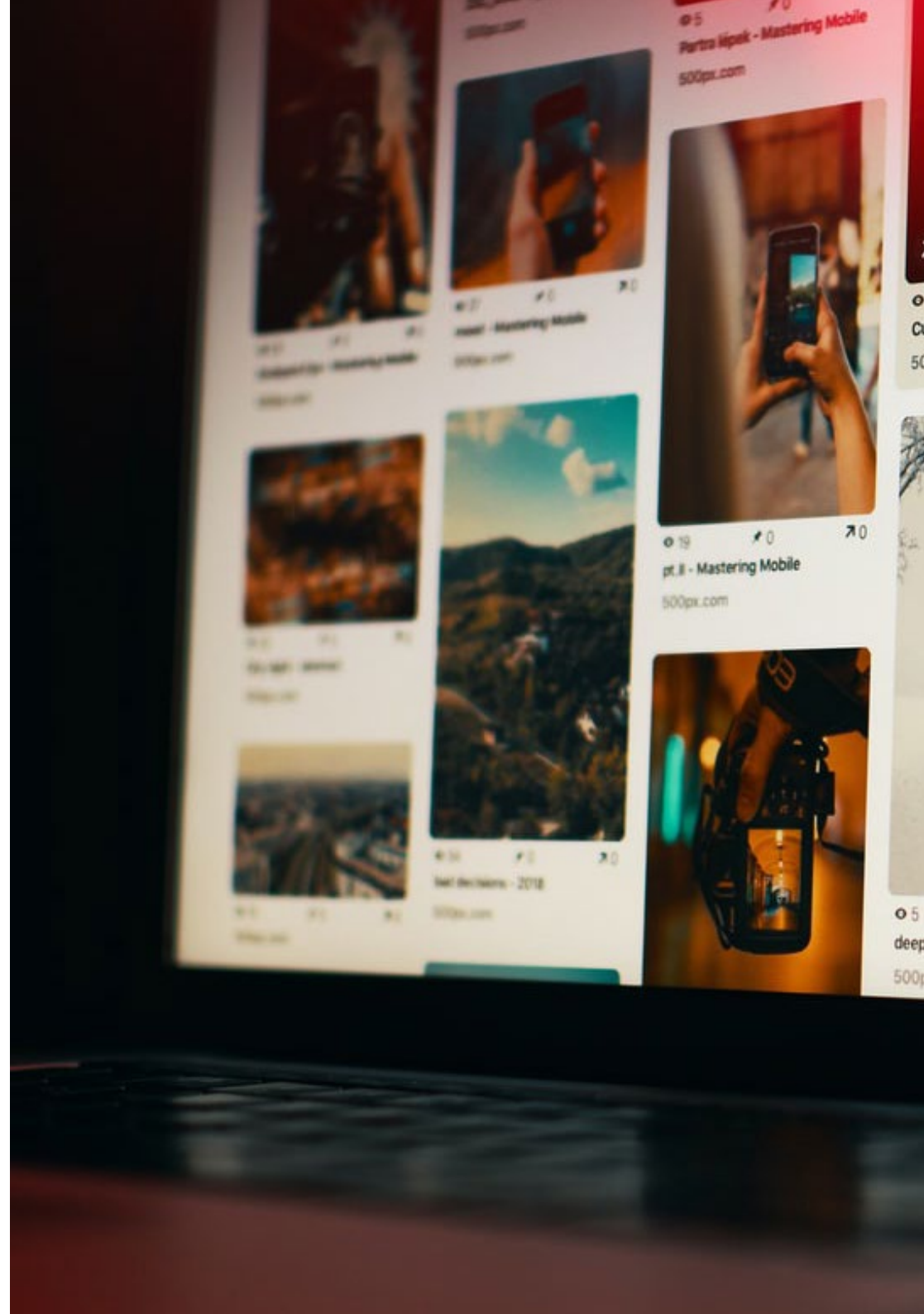


Competencias generales

- Aplicar los conocimientos de protección de datos en el ejercicio de sus respectivas profesiones
- Poder aplicar de forma sistematizada los procesos de protección de datos
- Explicar la problemática existente en el área de la protección de datos
- Actuar con seguridad en la resolución de estos conflictos
- Aportar la seguridad de una praxis correcta en el terreno de la protección de datos

“

La calidad de un programa desarrollado para ser una herramienta útil y accesible, a tu alcance”





Competencias específicas

- ♦ Moverse dentro del marco normativo de protección de datos y prestación del consentimiento
- ♦ Reconocer las características concretas de la protección de datos en el sector público
- ♦ Adaptarse al especial campo de la salud en los derechos de protección de datos
- ♦ Conocer los derechos de las personas en materia de protección de datos
- ♦ Explicar el régimen de responsabilidad civil y sancionatoria
- ♦ Usar las garantías de protección de datos en el entorno de las TICs
- ♦ Explicar la protección penal aplicable en el entorno del uso de datos
- ♦ Utilizar los modelos de *compliance*
- ♦ Reconocer el pasado y el futuro previsible en Europa en cuanto a la protección de datos

04

Estructura y contenido

El temario del Máster de Formación Permanente se configura como un completísimo recorrido a través de todos y cada uno de los conocimientos necesarios para comprender y asumir las formas de trabajo de este campo. Con un planteamiento centrado en la aplicación práctica que le permitirá crecer como profesional desde el primer momento de la capacitación.





“

Un temario completo centrado en la adquisición de conocimientos y su conversión en habilidades reales, creado para impulsarte hacia la excelencia”

Módulo 1. Marco normativo de protección de datos y la prestación del consentimiento

- 1.1. Evolución histórica del derecho de protección de datos en España
 - 1.1.1. Artículo 18.4 CE
 - 1.1.2. LOTRAD
 - 1.1.3. LOPDCP 1999
 - 1.1.3.1. Vigente normativa LOPDGDD
- 1.2. El Derecho de protección de datos como derecho fundamental
 - 1.2.1. Delimitación
 - 1.2.2. Contenido esencial
 - 1.2.2.1. Distinción con derecho al honor e intimidad
- 1.3. El reglamento general de protección de datos de la UE
 - 1.3.1. Jerarquía en el sistema de fuentes
 - 1.3.2. Estructura del Reglamento
 - 1.3.3. Distinción con normativa de sociedad de la información
- 1.4. La normativa de civil española de protección de datos
 - 1.4.1. LOPDGDD
 - 1.4.2. Contenido Esencial de la LOPDGDD
 - 1.4.3. Los derechos digitales
- 1.5. Introducción a la prestación del consentimiento en el ámbito de la protección de datos
- 1.6. El consentimiento como base legítima para el tratamiento de datos personales
 - 1.6.1. Consentimiento libre
 - 1.6.2. Consentimiento informado
 - 1.6.3. Consentimiento específico
 - 1.6.4. Consentimiento inequívoco

Módulo 2. La protección de datos en el sector público

- 2.1. El marco europeo y español de la protección de datos
 - 2.1.1. Contexto normativo
 - 2.1.2. Marco europeo de la protección de datos
 - 2.1.3. El impacto de la regulación europea en España
- 2.2. Estructura institucional de protección de datos y supervisión de la actividad de las administraciones públicas
 - 2.2.1. Organización administrativa española: La AEPD y las autoridades autonómicas de protección de datos
 - 2.2.2. Competencia y ámbito de actuación en el control a las Administraciones Públicas
 - 2.2.3. Las Autoridades autonómicas
- 2.3. Estructura institucional impuesta por el RGPD
 - 2.3.1. Cuestiones generales
 - 2.3.2. La comisión
 - 2.3.3. El comité europeo de protección de datos
- 2.4. Los delegados de protección de datos en el sector público
 - 2.4.1. La exigencia de DPO en el sector público
 - 2.4.2. Funciones del DPO
 - 2.4.3. Requisitos, posibilidades y tipos de DPO en el sector público
- 2.5. Actividad administrativa y protección de datos I
 - 2.5.1. Cuestiones generales
 - 2.5.2. Incidencia en el ámbito procedimental
 - 2.5.3. Incidencia en la transparencia y acceso a la información
- 2.6. Actividad administrativa y protección de datos II
 - 2.6.1. Protección de datos en los procedimientos electrónicos
 - 2.6.2. Protección de datos y gestión de personal
 - 2.6.3. Archivos, investigación histórica estadística y científica
- 2.7. Las sanciones administrativas en materia de protección de datos
 - 2.7.1. La tipología de sanciones. Especial posición de las Administraciones Públicas
 - 2.7.2. El procedimiento sancionador
 - 2.7.3. Órganos competentes

- 2.8. Tutela jurisdiccional de la protección de datos en el RGPD
 - 2.8.1. El acceso a la jurisdicción. Aspectos procedimentales
 - 2.8.2. Derecho de indemnización
 - 2.8.3. Recursos frente a la autoridad de control y frente a las resoluciones del Comité
- 2.9. Regulación sectorial I
 - 2.9.1. Protección de datos en materia sanitaria
 - 2.9.2. Protección de datos en materia educativa
 - 2.9.3. Protección de datos en materia de servicios sociales
- 2.10. Regulación sectorial II
 - 2.10.1. Protección de datos en el sector de las telecomunicaciones
 - 2.10.2. Transparencia y protección de datos
 - 2.10.3. Protección de datos en la contratación del sector público

Módulo 3. Un estudio sobre los datos de salud como categoría especial de datos personales

- 3.1. Concepto de salud
 - 3.1.1. Concepto de salud. El derecho a la salud como derecho fundamental
 - 3.1.2. Concepto de salud global
 - 3.1.3. De un sistema tradicional de salud a la llamada "salud digital"
- 3.2. Bioética. Salud. Datos personales
 - 3.2.1. Bioética y los principios que la informa
 - 3.2.2. Bioética y salud
 - 3.2.3. Bioética y datos personales
- 3.3. Derecho de los pacientes en el entorno de los datos personales
 - 3.3.1. Derechos de los pacientes: sanos y enfermos
 - 3.3.2. Pacientes y datos personales
 - 3.3.3. Autonomía de la voluntad, datos personales y pacientes
- 3.4. Salud. Investigación biomédica. Protección de los datos personales
 - 3.4.1. Investigación científica e investigación biomédica y salud
 - 3.4.2. Investigación científica e investigación biomédica y datos personales
 - 3.4.3. Normativa de interés

- 3.5. Datos relativos a la salud. Categorías especiales de datos
 - 3.5.1. Marco conceptual
 - 3.5.2. Marco legislativo
 - 3.5.3. Los datos sensibles o protegidos como modalidad de derechos personales
- 3.6. Datos genéticos
 - 3.6.1. Marco conceptual
 - 3.6.2. Marco legislativo
 - 3.6.3. Datos genéticos y datos personales. Principales disquisiciones doctrinales y prácticas. Derecho a la información genética versus el derecho a no saber
- 3.7. Datos biométricos
 - 3.7.1. Marco conceptual
 - 3.7.2. Marco legislativo
 - 3.7.3. Datos biométricos y datos personales. Principales disquisiciones doctrinales y prácticas
- 3.8. Tratamiento de la categoría de datos especiales o sensibles
 - 3.8.1. Principios básicos del tratamiento de los datos especiales
 - 3.8.2. Derechos de las personas en sede de tratamiento de datos sensibles en salud
 - 3.8.3. La cuestión de la elaboración de perfiles
- 3.9. Protección de los datos sanitarios
 - 3.9.1. Protección de datos sanitarios. Notas que la informan
 - 3.9.2. La historia clínica. Su incidencia en el tratamiento de los datos personales de salud
 - 3.9.3. El consentimiento informado. Su incidencia en el tratamiento de los datos personales de salud
- 3.10. Tratamiento de los datos de la salud en tiempos de pandemia
 - 3.10.1. Salud global y tratamiento de datos personales
 - 3.10.2. Tratamiento de los datos de salud y los derechos de los pacientes en tiempos de pandemia
 - 3.10.3. Estudio legislativo. Análisis de la Orden SND/297/2020, de 27 de marzo por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19

Módulo 4. Los derechos de las personas en materia de protección de datos

- 4.1. La protección de los derechos y libertades en el Big data
 - 4.1.1. Cuestiones preliminares
 - 4.1.2. El Big data como punto de partida
 - 4.1.3. La respuesta del Derecho al nuevo escenario
- 4.2. El derecho a la protección de datos
 - 4.2.1. La privacidad como objeto de protección
 - 4.2.2. Evolución normativa y jurisprudencial
 - 4.2.3. Nuevo marco europeo de protección de datos
- 4.3. Los derechos del interesado I: principios generales
 - 4.3.1. Derecho de acceso
 - 4.3.2. Información y transparencia
 - 4.3.3. Derecho a la limitación del tratamiento
- 4.4. Los derechos del interesado II: principios generales
 - 4.4.1. Derecho a la portabilidad de los datos
 - 4.4.2. Decisiones automatizadas y elaboración de perfiles
 - 4.4.3. Privacidad desde el diseño
- 4.5. Los derechos del interesado III: el derecho al olvido
 - 4.5.1. El caso Google como *leading case*
 - 4.5.2. Evolución jurisprudencial
 - 4.5.3. Marco legal actual
- 4.6. Los derechos del interesado IV: el derecho de supresión
 - 4.6.1. Concepto y naturaleza jurídica
 - 4.6.2. Objeto y contenido
 - 4.6.3. Sujetos y titularidad
- 4.7. Los derechos del interesado V: los derechos arco
 - 4.7.1. Cancelación
 - 4.7.2. Oposición
 - 4.7.3. Rectificación
- 4.8. Los derechos del interesado VI: los derechos digitales
 - 4.8.1. Cuestiones preliminares
 - 4.8.2. Derechos y libertades de la era digital
 - 4.8.3. Garantías jurídicas de los derechos digitales

- 4.9. El ejercicio de los derechos
 - 4.9.1. Cuestiones procesales
 - 4.9.2. Sujetos activos
 - 4.9.3. Sujetos pasivos
- 4.10. Límites y limitaciones de los derechos
 - 4.10.1. Cuestiones generales
 - 4.10.2. Colisión de derechos
 - 4.10.3. El papel de la jurisprudencia

Módulo 5. El régimen de responsabilidad civil y sancionatoria

- 5.1. El derecho de resarcimiento
 - 5.1.1. Notas preliminares del derecho de resarcimiento
 - 5.1.2. Protección uniforme del derecho de datos
 - 5.1.3. Regulación, principios y características del específico sistema de responsabilidad en materia de protección de datos
- 5.2. Sujetos responsables
 - 5.2.1. Delimitación
 - 5.2.2. Pluralidad de sujetos
 - 5.2.3. Los IPS como sujetos responsables en el tratamiento de datos personales
- 5.3. El régimen de responsabilidad civil en materia de protección de datos
 - 5.3.1. Responsabilidad directa y extracontractual
 - 5.3.2. Responsabilidad subjetiva y solidaria
 - 5.3.3. Reparación integral del daño
- 5.4. La acción de reclamación
 - 5.4.1. Regulación y legitimación
 - 5.4.2. Tribunales competentes
 - 5.4.3. Especial referencia a la acción colectiva
- 5.5. Régimen de infracciones en el RGPD I
 - 5.5.1. Delimitación del ámbito de aplicación
 - 5.5.2. Sujetos responsables
 - 5.5.3. Entidades sancionatorias
- 5.6. Régimen de infracciones en el RGPD II
 - 5.6.1. Regulación
 - 5.6.2. Infracciones
 - 5.6.3. Infracciones con multa agravada

- 5.7. Régimen de sanciones en el RGPD
 - 5.7.1. Tipología de sanciones
 - 5.7.2. Multas administrativas
 - 5.7.3. Multas coercitivas
- 5.8. La derogada LOPD
 - 5.8.1. Breve referencia al régimen sancionador
 - 5.8.2. Infracciones
 - 5.8.3. Sanciones
- 5.9. El régimen sancionador de la LOPDGDD I
 - 5.9.1. Cuestiones generales
 - 5.9.2. Infracciones muy graves
 - 5.9.3. Infracciones graves
- 5.10. El régimen sancionador de la LOPDGDD II
 - 5.10.1. Infracciones leves
 - 5.10.2. Prescripción de infracciones
 - 5.10.3. Sanciones
- 6.6. Protección de datos personales en el ámbito de la contratación electrónica de seguros de salud
 - 6.6.1. Relaciones contractuales en relación con la salud y la protección de datos personales
 - 6.6.2. El caso de personas portadoras de VIH/SIDA
- 6.7. Protección de datos personales, inteligencia artificial y responsabilidad civil
 - 6.7.1. La protección de datos personales y robótica
 - 6.7.2. La responsabilidad civil e inteligencia artificial
- 6.8. Protección de datos personales y secretos empresariales
 - 6.8.1. Los secretos empresariales
 - 6.8.2. La protección de datos personales, prestación del consentimiento y confidencialidad
- 6.9. Protección de datos personales e información falsa
 - 6.9.1. Derecho de información y protección de datos personales
 - 6.9.2. Inteligencia artificial y veracidad
- 6.10. Protección de datos personales de personas fallecidas en el entorno tecnológico
 - 6.10.1. Límites de acceso a los datos personales de personas fallecidas
 - 6.10.2. Acceso a los contenidos gestionados por prestadores de servicios de la sociedad de la información

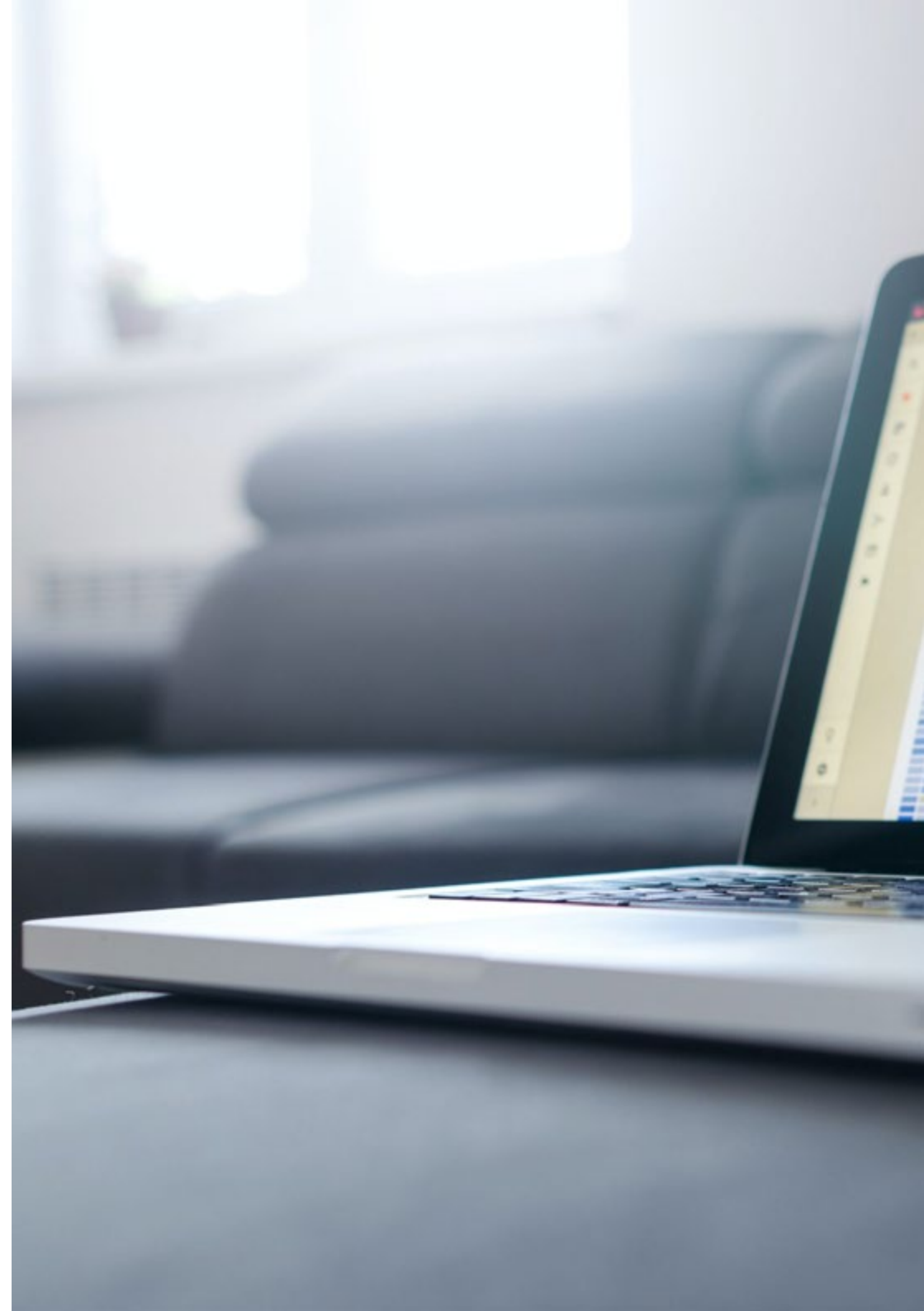
Módulo 6. La protección de datos personales y las garantías de los derechos digitales en relación a las TICs en la sociedad de la información

- 6.1. Protección de datos personales y recursos humanos
 - 6.1.1. La protección de datos personales en relación a los recursos humanos
 - 6.1.2. Gestión de la información y derechos digitales
- 6.2. Protección de datos personales y mediación electrónica
 - 6.2.1. La mediación electrónica y protección de datos personales
 - 6.2.2. Cuestiones referentes a las garantías en el procedimiento de mediación
- 6.3. Protección de datos personales y redes sociales
 - 6.3.1. Datos personales y redes sociales
 - 6.3.2. La prestación del consentimiento y sus efectos
- 6.4. Protección de datos personales en aplicaciones móviles de diagnóstico de enfermedades
 - 6.4.1. Protección de datos personales e investigación biomédica
 - 6.4.2. Menores y aplicaciones móviles de diagnóstico de enfermedades
- 6.5. Protección de datos personales en relación a la identidad y expresión de género
 - 6.5.1. Protección de datos personales en relación con la identidad
 - 6.5.2. Protección de datos personales y la expresión de género

Módulo 7. Protección penal de los datos

- 7.1. Marco jurídico actual
 - 7.1.1. En el derecho de la Unión
 - 7.1.2. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo y su trasposición mediante el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
 - 7.1.3. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
 - 7.1.4. Tratamiento de datos de naturaleza penal en RGPD y LO 3/2018
- 7.2. La protección de datos en el derecho penal español
 - 7.2.1. Delitos tecnológicos y cibercrimitos
 - 7.2.2. Delitos ciber-económicos
 - 7.2.3. Delitos ciberintrusivos
 - 7.2.4. Cybersec

- 7.3. Cuestiones generales de la instrucción I
 - 7.3.1. La denuncia y la querrela
 - 7.3.2. Solicitud de diligencias
 - 7.3.3. La prueba
 - 7.3.4. El escrito de conclusiones provisionales
- 7.4. Cuestiones generales de la instrucción II
 - 7.4.1. El proceso de investigación tecnológica
 - 7.4.2. Evidencias digitales
 - 7.4.3. El informe pericial
 - 7.4.4. Régimen de recursos
- 7.5. Descubrimiento y revelación de secretos. Art. 197 del Código Penal
 - 7.5.1. Cuestiones generales
 - 7.5.2. Bien jurídico protegido
 - 7.5.3. Subtipos agravados
 - 7.5.4. Cuestiones penológicas
- 7.6. Daños informáticos. Art. 264 del Código Penal
 - 7.6.1. Cuestiones generales
 - 7.6.2. Bien jurídico protegido
 - 7.6.3. Subtipos agravados
 - 7.6.4. Cuestiones penológicas
- 7.7. Responsabilidad penal de las personas jurídicas
 - 7.7.1. Ámbito de aplicación
 - 7.7.2. El debido control para la prevención de delitos en la empresa
 - 7.7.3. Circunstancias modificativas de la RPPJ
 - 7.7.4. Medidas cautelares y cuestiones penológicas
- 7.8. Cuestiones procesales de los medios tecnológicos II. Art. 588 bis LECrim
 - 7.8.1. Principios rectores, solicitud de autorización judicial y resolución judicial
 - 7.8.2. Secreto, duración, solicitud de prórroga y control de la medida
 - 7.8.3. Afectación de terceras personas y utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales
 - 7.8.4. Cese de la medida y destrucción de registros





- 7.9. Cuestiones procesales en la persecución penal de los delitos tecnológicos III
 - 7.9.1. La interceptación de las comunicaciones telefónicas y telemáticas
 - 7.9.2. Acceso de las partes a las grabaciones
 - 7.9.3. Incorporación al proceso de datos electrónicos de tráfico o asociados
 - 7.9.4. Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad
- 7.10. Cuestiones procesales en la persecución penal de los delitos tecnológicos IV
 - 7.10.1. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos
 - 7.10.2. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización
 - 7.10.3. Registro de dispositivos de almacenamiento masivo de la información
 - 7.10.4. Registro remoto sobre equipos informáticos

Módulo 8. Los modelos de *compliance*. Un enfoque práctico de la protección de datos en las empresas

- 8.1. Introducción al *compliance*. Finalidad e importancia
 - 8.1.1. Introducción a los modelos de *compliance*
 - 8.1.2. Naturaleza y objetivos de los modelos de *compliance*
 - 8.1.3. Riesgos normativos. La protección de datos como objeto de los modelos de *compliance*
 - 8.1.4. Situación actual en las empresas españolas
- 8.2. Antecedentes históricos y evolución del *compliance*
 - 8.2.1. Antecedentes históricos. Derecho estadounidense
 - 8.2.2. Normativa sobre *compliance* y su evolución
 - 8.2.3. *Soft law* y estandarización
- 8.3. Modelos de *compliance*: normativa y requisitos generales
 - 8.3.1. Normativa española de referencia
 - 8.3.2. Estándares internacionales y nacionales
 - 8.3.3. Principios y requisitos generales de los modelos de *compliance*

- 8.4. Elementos de los modelos de *compliance* I: bases del modelo
 - 8.4.1. Análisis de riesgos normativos: penales y administrativos
 - 8.4.2. Medidas de mitigación del riesgo
 - 8.4.2.1. Protocolos sobre toma de decisiones en la empresa
 - 8.4.2.2. Modelos de gestión de los recursos financieros
 - 8.4.2.3. Medidas específicas de mitigación del riesgo
- 8.5. Elementos de los modelos de *compliance* II: garantías de cumplimiento
 - 8.5.1. Régimen sancionador de infracciones
 - 8.5.2. Canales de denuncias y otras vías de comunicación
 - 8.5.3. Directiva (UE) 2019/1937
- 8.6. Elementos de los modelos de *compliance* III: investigaciones internas
 - 8.6.1. Requisitos de las investigaciones internas
 - 8.6.2. Garantías de los trabajadores. Jurisprudencia relevante
 - 8.6.3. Procedimiento sancionador
- 8.7. Elementos de los modelos de *compliance* IV: difusión del modelo
 - 8.7.1. Papel de la alta dirección: contexto de la organización y liderazgo
 - 8.7.2. Comunicación interna de las medidas que integran el modelo
 - 8.7.3. Formación a empleados
- 8.8. Elementos de los modelos de *compliance* V: supervisión
 - 8.8.1. Órgano de control. Similitudes y diferencias con DPD
 - 8.8.2. Modelo de supervisión
 - 8.8.3. Estructura de las tres líneas de defensa: convivencia con la auditoría interna
- 8.9. Modelos de *compliance* como garantía frente a terceros
 - 8.9.1. Deber de diligencia con terceros en el Derecho español
 - 8.9.2. Códigos de conducta en materia de protección de datos
 - 8.9.3. Cláusulas contractuales con terceros
 - 8.9.4. Certificaciones y su valor probatorio
- 8.10. Consideraciones prácticas sobre los modelos de *compliance*
 - 8.10.1. Incidencia sectorial de los modelos de *compliance*
 - 8.10.2. Confidencialidad de los datos en sentido amplio. Ley 1/2019, de 20 de febrero, de Secretos Empresariales
 - 8.10.3. Ciberseguridad y *compliance*. Norma ISO 27.0001 y sistemas de gestión de la seguridad de la información

Módulo 9. La protección de datos en Europa: presente y futuro desde la perspectiva del derecho internacional privado

- 9.1. Protección de derechos en Europa
 - 9.1.1. Derechos de privacidad
 - 9.1.2. Derechos de la personalidad
 - 9.1.3. Protección de datos
- 9.2. Fuentes europeas
 - 9.2.1. Directiva 95/46/EC
 - 9.2.2. Reglamento (UE) N.º 2016/679
 - 9.2.3. Propuesta de reglamento sobre *ePrivacy*
- 9.3. La competencia judicial internacional en conflictos transfronterizos
 - 9.3.1. Generalidades
 - 9.3.2. Reglamento Bruselas Ibis (UE) N.º 1215/2012
 - 9.3.3. Reglamento (UE) N.º 106/679
 - 9.3.4. Normas nacionales
- 9.4. La ley aplicable en conflictos transfronterizos
 - 9.4.1. Obligaciones contractuales. Reglamento Roma I 598/2010
 - 9.4.2. Obligaciones extracontractuales
 - 9.4.3. Directiva 2000/31/EC relativa a los servicios de la sociedad de la información
- 9.5. Relaciones internacionales entre los proveedores de redes sociales y los potenciales usuarios
 - 9.5.1. Los acuerdos de elección de foro en las condiciones generales de contratación
 - 9.5.2. Los acuerdos de elección del derecho aplicable en las condiciones generales de contratación
 - 9.5.3. La ley aplicable a la protección de datos
 - 9.5.4. Usuarios potenciales
- 9.6. Relaciones entre los usuarios de las redes sociales
 - 9.6.1. La conexión entre *lex fori* y *lex loci delicti*
 - 9.6.2. Convergencia empírica
- 9.7. La jurisprudencia Europea (TJUE y TEDH)
 - 9.7.1. VKI vs. Amazon
 - 9.7.2. Grecia vs. Nikiforidis
 - 9.7.3. Stylianou vs. Cyprus

- 9.8. *Big Data* y el derecho internacional privado
 - 9.8.1. Implicaciones jurídicas internacionales
 - 9.8.2. La protección legal del algoritmo y la base de datos
 - 9.8.3. Relaciones contractuales
 - 9.8.4. Relaciones laborales
- 9.9. El derecho al olvido
 - 9.9.1. Europa
 - 9.9.2. EEUU
 - 9.9.3. Convergencia
- 9.10. Hacia una síntesis
 - 9.10.1. El acercamiento entre la competencia judicial internacional y las normas de conflicto
 - 9.10.2. Conexiones
 - 9.10.3. La búsqueda de la neutralidad

Módulo 10. Evaluaciones de impacto y gestión de la seguridad de la información

- 10.1. Análisis y gestión de riesgos de los tratamientos de datos personales
 - 10.1.1. Conceptos generales de la gestión de riesgos
 - 10.1.2. *Privacy by Design* y riesgo
 - 10.1.3. Aproximación a la ISO 31000 de gestión de riesgos
- 10.2. Fundamentos de las Evaluaciones de Impacto (EIPD)
 - 10.2.1. Origen de las EIPD
 - 10.2.2. Necesidad y alcance de las EIPD
 - 10.2.3. Metodologías
- 10.3. Las EIPD en el reglamento general de protección de datos
 - 10.3.1. Regulación
 - 10.3.2. El principio de responsabilidad activa
 - 10.3.3. Las guías de la agencia española de protección de datos
- 10.4. Análisis previo y tratamientos donde es necesario realizar una EIPD
 - 10.4.1. Sujetos obligados a realizar una EIPD
 - 10.4.2. Evaluación de la necesidad y proporcionalidad
 - 10.4.3. El informe de necesidad

- 10.5. Aspectos prácticos de la realización de una EIPD
- 10.6. Introducción a la seguridad de la información
 - 10.6.1. Derecho y ciberseguridad
 - 10.6.2. Conceptos básicos
 - 10.6.3. Roles y responsabilidades
- 10.7. Dominios principales
 - 10.7.1. Introducción de gobierno de seguridad de la información
 - 10.7.2. Estratégico
 - 10.7.3. *Compliance*
 - 10.7.4. Gestión de riesgos
 - 10.7.5. Operación
- 10.8. Convergencia entre seguridad y privacidad
 - 10.8.1. Introducción a los marcos de gestión
 - 10.8.2. ISO/IEC 27001 y esquema nacional de seguridad
 - 10.8.3. ISO/IEC 27701 y RGPD-LOPD GDD
- 10.9. Respuesta a incidentes de seguridad
 - 10.9.1. Introducción a la continuidad de negocio
 - 10.9.2. Equipos de respuesta ante incidentes de seguridad
 - 10.9.3. Implicaciones legales
- 10.10. Principios básicos de auditoría y cadena de custodia de la prueba digital
 - 10.10.1. Proceso de auditoría (ISO 19011)
 - 10.10.2. La evidencia digital y sus implicaciones legales
 - 10.10.3. Ejemplos de sentencias



Aprovecha la oportunidad para conocer los últimos avances en esta materia para aplicarla a tu práctica diaria

05

Metodología

Este programa de capacitación ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de un modo de aprendizaje de forma cíclica: ***el Relearning***.

Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine***.



“

Descubre el Relearning, un sistema que abandona el aprendizaje lineal convencional para llevarte a través de sistemas cíclicos de enseñanza: una forma de aprender que ha demostrado su enorme eficacia, especialmente en las materias que requieren memorización”

Estudio de Caso para contextualizar todo el contenido

Nuestro programa ofrece un método revolucionario de desarrollo de habilidades y conocimientos. Nuestro objetivo es afianzar competencias en un contexto cambiante, competitivo y de alta exigencia.

“

Con TECH podrás experimentar una forma de aprender que está moviendo los cimientos de las universidades tradicionales de todo el mundo”



Accederás a un sistema de aprendizaje basado en la reiteración, con una enseñanza natural y progresiva a lo largo de todo el temario.



El alumno aprenderá, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales.

Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0, que propone los retos y decisiones más exigentes en este campo, ya sea en el ámbito nacional o internacional. Gracias a esta metodología se impulsa el crecimiento personal y profesional, dando un paso decisivo para conseguir el éxito. El método del caso, técnica que sienta las bases de este contenido, garantiza que se sigue la realidad económica, social y profesional más vigente.

“ *Nuestro programa te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera* ”

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de negocios del mundo desde que éstas existen. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, el método del caso consistió en presentarles situaciones complejas reales para que tomaran decisiones y emitieran juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Ante una determinada situación, ¿qué debería hacer un profesional? Esta es la pregunta a la que nos enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del curso, los estudiantes se enfrentarán a múltiples casos reales. Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

Relearning Methodology

TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina 8 elementos didácticos diferentes en cada lección.

Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

En 2019, obtuvimos los mejores resultados de aprendizaje de todas las universidades online en español en el mundo.

En TECH aprenderás con una metodología vanguardista concebida para capacitar a los directivos del futuro. Este método, a la vanguardia pedagógica mundial, se denomina Relearning.

Nuestra universidad es la única en habla hispana licenciada para emplear este exitoso método. En 2019, hemos conseguido mejorar los niveles de satisfacción global de nuestros alumnos (calidad docente, calidad de los materiales, estructura del curso, objetivos...) con respecto a los indicadores de la mejor universidad online en español.



En nuestro programa, el aprendizaje no es un proceso lineal, sino que sucede en espiral (aprender, desaprender, olvidar y reaprender). Por eso, combinamos cada uno de estos elementos de forma concéntrica. Con esta metodología se han capacitado más de 650.000 graduados universitarios con un éxito sin precedentes en ámbitos tan distintos como la bioquímica, la genética, la cirugía, el derecho internacional, las habilidades directivas, las ciencias del deporte, la filosofía, el derecho, la ingeniería, el periodismo, la historia o los mercados e instrumentos financieros. Todo ello en un entorno de alta exigencia, con un alumnado universitario de un perfil socioeconómico alto y una media de edad de 43,5 años.

El Relearning te permitirá aprender con menos esfuerzo y más rendimiento, implicándote más en tu capacitación, desarrollando el espíritu crítico, la defensa de argumentos y el contraste de opiniones: una ecuación directa al éxito.

A partir de la última evidencia científica en el ámbito de la neurociencia, no solo sabemos organizar la información, las ideas, las imágenes y los recuerdos, sino que sabemos que el lugar y el contexto donde hemos aprendido algo es fundamental para que seamos capaces de recordarlo y almacenarlo en el hipocampo, para retenerlo en nuestra memoria a largo plazo.

De esta manera, y en lo que se denomina Neurocognitive context-dependent e-learning, los diferentes elementos de nuestro programa están conectados con el contexto donde el participante desarrolla su práctica profesional.



Este programa ofrece los mejores materiales educativos, preparados a conciencia para los profesionales:



Material de estudio

Todos los contenidos didácticos son creados por los especialistas que van a impartir el curso, específicamente para él, de manera que el desarrollo didáctico sea realmente específico y concreto.

Estos contenidos son aplicados después al formato audiovisual, para crear el método de trabajo online de TECH. Todo ello, con las técnicas más novedosas que ofrecen piezas de gran calidad en todos y cada uno los materiales que se ponen a disposición del alumno.



Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos.

El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.



Prácticas de habilidades y competencias

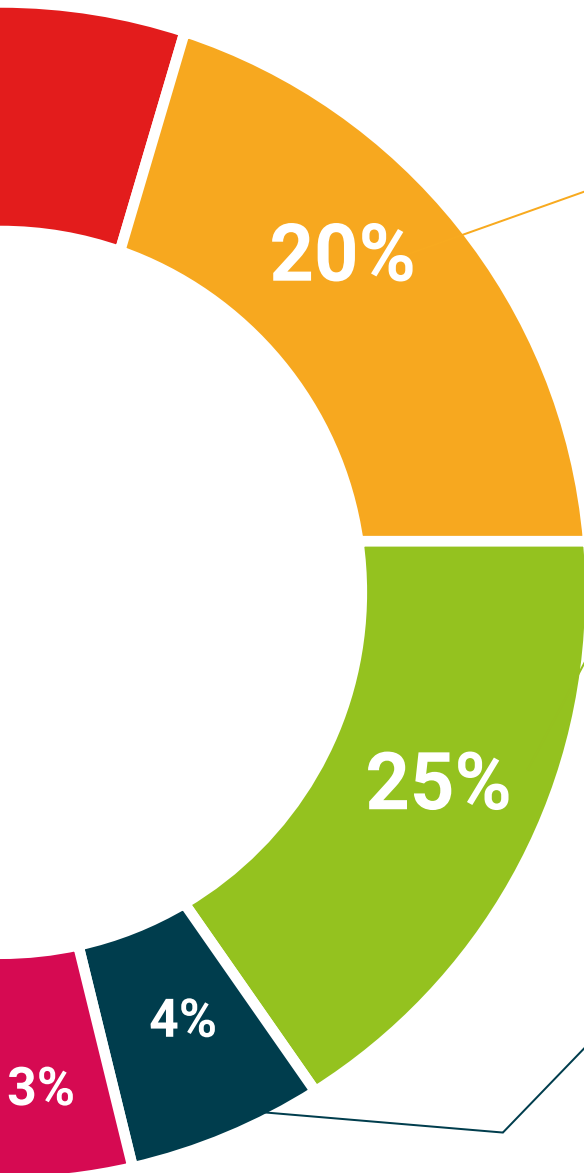
Realizarán actividades de desarrollo de competencias y habilidades específicas en cada área temática. Prácticas y dinámicas para adquirir y desarrollar las destrezas y habilidades que un especialista precisa desarrollar en el marco de la globalización que vivimos.



Lecturas complementarias

Artículos recientes, documentos de consenso y guías internacionales, entre otros. En la biblioteca virtual de TECH el estudiante tendrá acceso a todo lo que necesita para completar su capacitación.





Case studies

Completarán una selección de los mejores casos de estudio elegidos expresamente para esta titulación. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.



Resúmenes interactivos

El equipo de TECH presenta los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audios, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

Este exclusivo sistema educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".



Testing & Retesting

Se evalúan y reevalúan periódicamente los conocimientos del alumno a lo largo del programa, mediante actividades y ejercicios evaluativos y autoevaluativos para que, de esta manera, el estudiante compruebe cómo va consiguiendo sus metas.



06

Titulación

Este programa en Protección de Datos garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Máster de Formación Permanente expedido por TECH Universidad Tecnológica.



“

Supera con éxito este programa y recibe tu titulación universitaria sin desplazamientos ni farragosos trámites”

Este programa te permitirá obtener el título de **Máster de Formación Permanente en Protección de Datos** emitido por TECH Universidad Tecnológica.

TECH Universidad Tecnológica, es una Universidad española oficial, que forma parte del Espacio Europeo de Educación Superior (EEES). Con un enfoque centrado en la excelencia académica y la calidad universitaria a través de la tecnología.

Este título propio contribuye de forma relevante al desarrollo de la educación continua y actualización del profesional, garantizándole la adquisición de las competencias en su área de conocimiento y aportándole un alto valor curricular universitario a su formación. Es 100% válido en todas las Oposiciones, Carrera Profesional y Bolsas de Trabajo de cualquier Comunidad Autónoma española.

Además, el riguroso sistema de garantía de calidad de TECH asegura que cada título otorgado cumpla con los más altos estándares académicos, brindándole al egresado la confianza y la credibilidad que necesita para destacarse en su carrera profesional.

Título: **Máster de Formación Permanente en Protección de Datos**

Modalidad: **100% Online**

Duración: **7 meses**

Créditos: **60 ECTS**



*Apostilla de La Haya. En caso de que el alumno solicite que su título en papel recabe la Apostilla de La Haya, TECH EDUCATION realizará las gestiones oportunas para su obtención, con un coste adicional.



Máster de Formación Permanente Protección de Datos

- » Modalidad: online
- » Duración: 7 meses
- » Titulación: TECH Universidad Tecnológica
- » Acreditación: 60 ECTS
- » Horario: a tu ritmo
- » Exámenes: online

Máster de Formación Permanente

Protección de Datos

