Máster Título Propio
Derecho Penal Informático

tech global university

Máster Título Propio
Derecho Penal Informático

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: **www.techtitute.com/derecho/master/master-derecho-penal-informatico**

Índice

01
Presentación del programa
pág. 4

02
¿Por qué estudiar en TECH?
pág. 8

03
Plan de estudios
pág. 12

04
Objetivos docentes
pág. 26

05
Metodología de estudio
pág. 30

06
Titulación
pág. 40

01

Presentación del programa

El Derecho Penal Informático se ha convertido en una disciplina crucial en un mundo cada vez más interconectado, donde los delitos cibernéticos se presentan como una amenaza creciente para individuos y organizaciones. Según un nuevo informe de la Organización de las Naciones Unidas, los ciberataques han aumentado un 45% durante los últimos años. Este hecho pone de manifiesto la necesidad de que los profesionales adquieran competencias avanzadas para afrontar los desafíos jurídicos del entorno digital. Por este motivo, TECH ha creado una pionera titulación universitaria focalizada en las herramientas más modernas para prevenir conductas delictivas. A su vez, se basa en un cómodo formato 100% online que permite al alumnado establecer sus propios horarios y ritmo de estudio.

Con este programa universitario 100% online, dominarás el marco normativo que regula los delitos informáticos y actuarás de forma eficaz en litigios relacionados con la protección de datos confidenciales"

En la actualidad, el Derecho Penal Informático juega un papel fundamental en la regulación de las actividades digitales y la protección de la seguridad de las personas. En este sentido, durante la última década se han producido un notable aumento de delitos como el robo de datos, fraudes electrónicos o el acceso no autorizado a sistemas informáticos. De ahí la importancia de que los expertos cuenten con una comprensión integral para aplicar eficazmente la normativa penal vigente en el ámbito digital. Asimismo, deben estar capacitados para identificar brechas legales, proponer reformas y garantizar la protección de los derechos fundamentales frente a nuevas amenazas tecnológicas.

En este contexto, TECH presenta un vanguardista Máster Título Propio Derecho Penal Informático. Diseñado por especialistas de renombre en esta área, el plan de estudios ahondará en cuestiones que van desde el uso de medios electrónicos en la Administración de Justicia hasta la regulación penal de delitos informáticos contra la propiedad intelectual.

También, los materiales didácticos profundizarán en el manejo de redes sociales y ofrecerán técnicas avanzadas de ciberseguridad para la protección de infraestructuras digitales. Gracias a esto, los egresados obtendrán una comprensión holística sobre las implicaciones jurídicas del cibercrimen y actuar con solvencia en entornos tecnológicos complejos.

Por otra parte, este plan de estudios se imparte mediante una modalidad 100% online, que permite a los alumnos planificar sus propios horarios de estudio. Además, los profesionales disfrutarán de una gran variedad de recursos multimedia destinados a fomentar una enseñanza dinámica y natural. Para acceder al Campus Virtual, lo único que necesitarán los es un dispositivo con acceso a Internet (sirviendo incluso su propio móvil). En adición, TECH emplea su disruptiva metodología *Relearning* para garantizar una asimilación natural de los conceptos esenciales del temario.

Este **Máster Título Propio en Derecho Penal Informático** contiene el programa universitario más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Derecho Penal Informático
- 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
- 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

Manejarás las técnicas más sofisticadas de prevención, detección y persecución del ciberdelito desde una perspectiva jurídica sólida"

El vanguardista método Relearning de TECH te permitirá aprender con menos esfuerzo y más rendimiento. ¡Inscríbete ahora!"

Profundizarás en la evolución comparada del Derecho Penal Informático en distintos ordenamientos jurídicos.

Fomentarás el análisis crítico de los desafíos éticos, sociales y normativos vinculados a la criminalidad digital.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito del Derecho Penal Informático, que vierten en este programa 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 un estudio inmersivo programado para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el alumno 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.

02

¿Por qué estudiar en TECH?

TECH es la mayor Universidad digital del mundo. Con un impresionante catálogo de más de 14.000 programas universitarios, disponibles en 11 idiomas, se posiciona como líder en empleabilidad, con una tasa de inserción laboral del 99%. Además, cuenta con un enorme claustro de más de 6.000 profesores de máximo prestigio internacional.

Estudia en la mayor universidad digital del mundo y asegura tu éxito profesional. El futuro empieza en TECH"

La mejor universidad online del mundo según FORBES

La prestigiosa revista Forbes, especializada en negocios y finanzas, ha destacado a TECH como «la mejor universidad online del mundo». Así lo han hecho constar recientemente en un artículo de su edición digital en el que se hacen eco del caso de éxito de esta institución, «gracias a la oferta académica que ofrece, la selección de su personal docente, y un método de aprendizaje innovador orientado a formar a los profesionales del futuro».

El mejor claustro docente top internacional

El claustro docente de TECH está integrado por más de 6.000 profesores de máximo prestigio internacional. Catedráticos, investigadores y altos ejecutivos de multinacionales, entre los cuales se destacan Isaiah Covington, entrenador de rendimiento de los Boston Celtics; Magda Romanska, investigadora principal de MetaLAB de Harvard; Ignacio Wistumba, presidente del departamento de patología molecular traslacional del MD Anderson Cancer Center; o D.W Pine, director creativo de la revista TIME, entre otros.

La mayor universidad digital del mundo

TECH es la mayor universidad digital del mundo. Somos la mayor institución educativa, con el mejor y más amplio catálogo educativo digital, cien por cien online y abarcando la gran mayoría de áreas de conocimiento. Ofrecemos el mayor número de titulaciones propias, titulaciones oficiales de posgrado y de grado universitario del mundo. En total, más de 14.000 títulos universitarios, en once idiomas distintos, que nos convierten en la mayor institución educativa del mundo.

Los planes de estudio más completos del panorama universitario

TECH ofrece los planes de estudio más completos del panorama universitario, con temarios que abarcan conceptos fundamentales y, al mismo tiempo, los principales avances científicos en sus áreas científicas específicas. Asimismo, estos programas son actualizados continuamente para garantizar al alumnado la vanguardia académica y las competencias profesionales más demandadas. De esta forma, los títulos de la universidad proporcionan a sus egresados una significativa ventaja para impulsar sus carreras hacia el éxito.

Un método de aprendizaje único

TECH es la primera universidad que emplea el *Relearning* en todas sus titulaciones. Se trata de la mejor metodología de aprendizaje online, acreditada con certificaciones internacionales de calidad docente, dispuestas por agencias educativas de prestigio. Además, este disruptivo modelo académico se complementa con el "Método del Caso", configurando así una estrategia de docencia online única. También en ella se implementan recursos didácticos innovadores entre los que destacan vídeos en detalle, infografías y resúmenes interactivos.

La universidad online oficial de la NBA

TECH es la universidad online oficial de la NBA. Gracias a un acuerdo con la mayor liga de baloncesto, ofrece a sus alumnos programas universitarios exclusivos, así como una gran variedad de recursos educativos centrados en el negocio de la liga y otras áreas de la industria del deporte. Cada programa tiene un currículo de diseño único y cuenta con oradores invitados de excepción: profesionales con una distinguida trayectoria deportiva que ofrecerán su experiencia en los temas más relevantes.

Líderes en empleabilidad

TECH ha conseguido convertirse en la universidad líder en empleabilidad. El 99% de sus alumnos obtienen trabajo en el campo académico que ha estudiado, antes de completar un año luego de finalizar cualquiera de los programas de la universidad. Una cifra similar consigue mejorar su carrera profesional de forma inmediata. Todo ello gracias a una metodología de estudio que basa su eficacia en la adquisición de competencias prácticas, totalmente necesarias para el desarrollo profesional.

Google Partner
PREMIER 2024

NBA
Universidad online oficial de la **NBA**

4.9/5
★★★★★
★ global score

99%
Garantía de máxima empleabilidad

Google Partner Premier

El gigante tecnológico norteamericano ha otorgado a TECH la insignia Google Partner Premier. Este galardón, solo al alcance del 3% de las empresas del mundo, pone en valor la experiencia eficaz, flexible y adaptada que esta universidad proporciona al alumno. El reconocimiento no solo acredita el máximo rigor, rendimiento e inversión en las infraestructuras digitales de TECH, sino que también sitúa a esta universidad como una de las compañías tecnológicas más punteras del mundo.

La universidad mejor valorada por sus alumnos

Los alumnos han posicionado a TECH como la universidad mejor valorada del mundo en los principales portales de opinión, destacando su calificación más alta de 4,9 sobre 5, obtenida a partir de más de 1.000 reseñas. Estos resultados consolidan a TECH como la institución universitaria de referencia a nivel internacional, reflejando la excelencia y el impacto positivo de su modelo educativo.

03

Plan de estudios

Este programa universitario se complementa con un novedoso itinerario académico que abordará temas clave del Derecho Penal Informático. Por lo tanto, se profundizará en ciberseguridad, proporcionando conocimientos sobre la protección de sistemas y datos frente a ciberataques. Además, se analizará la criminalidad informática, con énfasis en los tipos de delitos cibernéticos y las estrategias de prevención. También se tratará la prueba digital, garantizando la correcta recolección y validez de las evidencias en procesos legales. Este enfoque integral permitirá a los profesionales desarrollar competencias avanzadas para enfrentar los retos legales del entorno digital de manera efectiva.

Valorarás la admisibilidad, legalidad y cadena de custodia de evidencias digitales en una variedad de procedimientos judiciales"

Módulo 1. Derecho Informático

1.1. Introducción al derecho Informático
- 1.1.1. Introducción
- 1.1.2. Definición
- 1.1.3. Origen y evolución
- 1.1.4. El derecho informático y las demás ramas del Derecho

1.2. El Derecho Informático en la Administración de Justicia
- 1.2.1. Introducción
- 1.2.2. Normativa aplicable
- 1.2.3. Ámbito de aplicación
- 1.2.4. Definiciones

1.3. Uso de los medios electrónicos en la Administración de Justicia
- 1.3.1. Introducción
- 1.3.2. Derechos de los ciudadanos en sus relaciones con la Administración de Justicia
- 1.3.3. Derechos y deberes de los profesionales de la justicia en sus relaciones con la Administración de Justicia por medios electrónicos
- 1.3.4. Utilización obligatoria de los medios electrónicos en la tramitación de los procedimientos electrónicos judiciales

1.4. Sede judicial electrónica
- 1.4.1. Características y clases
- 1.4.2. Contenido y servicios
- 1.4.3. Reglas especiales de responsabilidad
- 1.4.4. Punto de acceso general

1.5. Identificación y autenticación. Disposiciones comunes
- 1.5.1. Formas
- 1.5.2. Personas jurídicas y entidades sin personalidad jurídica
- 1.5.3. Firma electrónica
- 1.5.4. Sustitución y habilitación entre profesionales

1.6. Identificación electrónica de los órganos judiciales y autenticación del ejercicio de su competencia
- 1.6.1. Identificación de las sedes judiciales electrónicas
- 1.6.2. Sistemas de firma electrónica
  - 1.6.2.1. Actuación judicial automatizada
  - 1.6.2.2. Sello electrónico
- 1.6.3. Firma electrónica de los operadores jurídicos

1.7. Interoperabilidad. Acreditación y representación
- 1.7.1. Introducción
- 1.7.2. Identificación y autenticación
  - 1.7.2.1. Por medio de certificados electrónicos
  - 1.7.2.2. Por funcionario público
- 1.7.3. Intercambio electrónico de datos en entornos cerrados de comunicación

1.8. Tramitación electrónica de los procedimientos judiciales
- 1.8.1. Criterios para la gestión electrónica
- 1.8.2. Expediente judicial electrónico
  - 1.8.2.1. Expediente
  - 1.8.2.2. Documento
  - 1.8.2.3. Copias
  - 1.8.2.4. Archivo electrónico

1.9. Registro de escritos, comunicaciones y notificaciones electrónicas
- 1.9.1. Registro judicial electrónico
  - 1.9.1.1. Funcionamiento
  - 1.9.1.2. Cómputo de plazos
  - 1.9.1.3. Apoderamientos *apud* acta
- 1.9.2. Comunicaciones y notificaciones electrónicas
  - 1.9.2.1. Comunicaciones electrónicas
  - 1.9.2.2. Práctica de actos de comunicación por medios electrónicos
  - 1.9.2.3. Comunicación edictal electrónica

1.10. Tramitación electrónica
- 1.10.1. Iniciación del procedimiento
- 1.10.2. Tramitación del procedimiento
- 1.10.3. Presentación de documentos
- 1.10.4. Copias
- 1.10.5. Acreditación de la representación procesal
- 1.10.6. Acceso de las partes a la información sobre el estado de tramitación
- 1.10.7. Actuación judicial automatizada
- 1.10.8. Subsanación de actos procesales

Módulo 2. Tratamiento de datos personales en el ámbito Penal

2.1. Tratamiento de los datos personales de las personas físicas a nivel europeo
- 2.1.1. Introducción
- 2.1.2. Principios
- 2.1.3. Derechos del interesado
  - 2.1.3.1. Transparencia y modalidades
  - 2.1.3.2. Información y acceso a los datos personales
  - 2.1.3.3. Rectificación y supresión
  - 2.1.3.4. Derecho de oposición y decisiones individuales automatizadas
  - 2.1.3.5. Limitaciones

2.2. Protección de datos personales en el ámbito Penal
- 2.2.1. Introducción
- 2.2.2. Principios y licitud del tratamiento
- 2.2.3. Ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad

2.3. Derechos de las personas
- 2.3.1. Régimen general
  - 2.3.1.1. Condiciones
  - 2.3.1.2. Información
  - 2.3.1.3. Derechos
  - 2.3.1.4. Restricciones a los derechos
  - 2.3.1.5. Ejercicio de los derechos
- 2.3.2. Régimen especial

2.4. Responsable y encargado de tratamiento
- 2.4.1. Obligaciones generales
- 2.4.2. Seguridad de los datos personales
- 2.4.3. Delegado de protección de datos
  - 2.4.3.1. Designación
  - 2.4.3.2. Posición
  - 2.4.3.3. Funciones

2.5. Transferencia de datos
- 2.5.1. Principios generales
- 2.5.2. Decisión de adecuación
- 2.5.3. Garantías apropiadas
- 2.5.4. Excepciones para situaciones específicas
- 2.5.5. Transferencias directas

2.6. Autoridades de protección de datos
- 2.6.1. Introducción
- 2.6.2. Autoridades de protección de dato
- 2.6.3. Funciones
- 2.6.4. Potestades
- 2.6.5. Asistencia

2.7. Reclamaciones
- 2.7.1. Régimen aplicable
- 2.7.2. Derecho a indemnización
- 2.7.2.1. Sector público
- 2.7.2.2. Sector privado
- 2.7.3. Tutela judicial efectiva

2.8. Régimen sancionador
- 2.8.1. Sujetos responsables
- 2.8.2. Concurso de normas
- 2.8.3. Infracciones
  - 2.8.3.1. Infracciones muy graves
  - 2.8.3.2. Infracciones graves
  - 2.8.3.3. Infracciones leves

2.8.4. Régimen jurídico
2.8.5. Sanciones
2.8.6. Prescripción
2.8.7. Caducidad del procedimiento
2.8.8. Procedimiento administrativo sancionador

2.9. Disposiciones adicionales de la legislación aplicable
2.9.1. Introducción
2.9.2. Regímenes específicos
2.9.3. Intercambio de datos dentro de la Unión Europea
2.9.4. Acuerdos internacionales en el ámbito de la cooperación judicial en materia Penal y de la cooperación policial
2.9.5. Ficheros y Registros de Población de las Administraciones Públicas
2.9.6. Otras disposiciones
2.9.7. Protección de datos de carácter personal en la Administración de Justicia

2.10. Modificaciones legislativas
2.10.1. Introducción
2.10.2. Ley General Penitenciaria
2.10.3. Estatuto Orgánico del Ministerio Fiscal
2.10.4. Ley Orgánica del Poder Judicial
2.10.5. Ley de protección de datos y garantía de los derechos digitales
2.10.6. Ley Orgánica sobre la utilización de los datos del registro de nombres de pasajeros en relación con los delitos de terrorismo y delitos graves
2.10.7. Ley contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte
2.10.8. Ley de Seguridad Privada
2.10.9. Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial

Módulo 3. Redes Sociales y delitos informáticos

3.1. Delitos informáticos. Introducción
3.1.1. Delitos informáticos y derecho a la intimidad
3.1.2. Conceptos básicos
3.1.3. Ámbito en el que puede darse un delito informático
3.1.4. Red social y conducta delictiva

3.2. Redes sociales: WhatsApp
3.2.1. Introducción
3.2.2. Origen y evolución
3.2.3. Funcionalidad
3.2.4. Conductas delictivas a través de WhatsApp
3.2.5. Otras redes sociales de mensajería instantánea: Telegram

3.3. Redes sociales: Facebook
3.3.1. Introducción
3.3.2. Origen y evolución
3.3.3. Funcionalidad
3.3.4. Conductas delictivas a través de Facebook

3.4. Redes sociales: Instagram
3.4.1. Introducción
3.4.2. Origen y evolución
3.4.3. Funcionalidad
3.4.4. Conductas delictivas a través de Instagram

3.5. Redes sociales: Twitter
3.5.1. Introducción
3.5.2. Origen y evolución
3.5.3. Funcionalidad
3.5.4. Conductas delictivas a través de Twitter

3.6. Redes sociales: Tik Tok
3.6.1. Introducción
3.6.2. Origen y evolución
3.6.3. Funcionalidad
3.6.4. Conductas delictivas a través de Tik Tok

3.7. Redes sociales: YouTube y Twitch
3.7.1. Introducción
3.7.2. Origen y evolución
3.7.3. Funcionalidad
3.7.4. Conductas delictivas a través de YouTube y Twitch

3.8. Redes sociales: Pinterest
- 3.8.1. Introducción
- 3.8.2. Origen y evolución
- 3.8.3. Funcionalidad
- 3.8.4. Conductas delictivas a través de Pinterest

3.9. Redes sociales: LinkedIn
- 3.9.1. Introducción
- 3.9.2. Origen y evolución
- 3.9.3. Funcionalidad
- 3.9.4. Conductas delictivas a través de LinkedIn

3.10. Redes sociales: Tinder
- 3.10.1. Introducción
- 3.10.2. Origen y evolución
- 3.10.3. Funcionalidad
- 3.10.4. Conductas delictivas a través de Tinder
- 3.10.5. Otras redes sociales de citas en línea

Módulo 4. Delitos informáticos contra el patrimonio

4.1. Introducción de los delitos informáticos contra el patrimonio
- 4.1.1. Introducción
- 4.1.2. Delitos contra el patrimonio
- 4.1.3. Clases de delitos informáticos contra el patrimonio
- 4.1.4. Bien jurídico protegido
- 4.1.5. Sujetos activos
- 4.1.6. Sujetos pasivos

4.2. Estafa
- 4.2.1. Introducción
- 4.2.2. Regulación
- 4.2.3. Bien jurídico protegido
- 4.2.4. Sujetos del delito
- 4.2.5. Exenciones

4.3. Estafa informática I
- 4.3.1. El delito de estafa
- 4.3.2. El engaño
  - 4.3.2.1. En el tipo básico
  - 4.3.2.2. En la estafa informática
- 4.3.3. Modalidades de estafa informática
- 4.3.4. Delito de estafa en el ámbito bancario

4.4. Estafa informática II
- 4.4.1. Concursos de leyes y concurso de delitos. Introducción
- 4.4.2. Concursos de delito de estafa con otros delitos
  - 4.4.2.1. Concurso de delito de estafa con delito de falsificación de tarjetas de crédito
  - 4.4.2.2. Concurso de delito de estafa con delito de falsedad en documento oficial o mercantil
  - 4.4.2.3. Concurso del delito de estafa con delito de insolvencia punible
  - 4.4.2.4. Concurso del delito de estafa con delito de apropiación indebida
- 4.4.3. Estafa impropia

4.5. *Phishing*
- 4.5.1. Introducción
- 4.5.2. El *phishing* y el delito de blanqueo de capitales imprudentes
- 4.5.3. Elemento subjetivo en los supuestos de *phishing*
- 4.5.4. *Phishing* en el ámbito internacional

4.6. Estafa telefónica
- 4.6.1. Introducción
- 4.6.2. Conducta delictiva
- 4.6.3. Sujetos del delito
- 4.6.4. Prevención

4.7. Robo y hurto
- 4.7.1. Introducción
- 4.7.2. Normativa vigente
- 4.7.3. Robos y hurtos en la era digital
- 4.7.4. Robos y hurtos a través de la red

4.8. Las defraudaciones de fluido eléctrico y análogas
- 4.8.1. Introducción
- 4.8.2. Evolución normativa
- 4.8.3. Bien jurídico protegido
- 4.8.4. Fórmulas específicas

4.9. Daños informáticos I
- 4.9.1. Introducción
- 4.9.2. Bien jurídico protegido
- 4.9.3. Acción del delito

4.10. Daños informáticos II
- 4.10.1. Delitos de daños informáticos con penas agravadas
- 4.10.2. Irrupción en el funcionamiento de un sistema informático ajeno
- 4.10.3. Producción, adquisición o ayuda a terceros
- 4.10.4. Responsabilidad penal de las personas jurídicas

Módulo 5. Delitos informáticos contra las personas físicas

5.1. Introducción de los delitos informáticos contra las personas físicas
- 5.1.1. Introducción
- 5.1.2. Bien jurídico protegido
- 5.1.3. Características
- 5.1.4. Clases de delitos informáticos contra las personas físicas

5.2. Delitos contra la intimidad I
- 5.2.1. Introducción
- 5.2.2. Tipo básico
- 5.2.2.1. Delitos de descubrimiento y revelación de secretos
- 5.2.3. Subtipos agravados
- 5.2.4. Relaciones concursales
- 5.2.4.1. Entre el artículo 197.6 y el artículo 171.2 del Código Penal
- 5.2.4.2. Entre los delitos de allanamiento de morada y revelación de secretos
- 5.2.4.3. Entre el artículo 197.2 y el artículo 417.2 del Código Penal

5.3. Delitos contra la intimidad II
- 5.3.1. *Sexting*
- 5.3.2. Delito de acceso ilegal a sistemas informáticos
- 5.3.3. Delito de abuso de dispositivos

5.4. Delitos contra la intimidad III
- 5.4.1. Agravaciones
- 5.4.2. Responsabilidad penal de las personas jurídicas
- 5.4.3. Requisito de perseguibilidad y perdón del ofendido

5.5. *Stalking* I
- 5.5.1. Introducción
- 5.5.2. Bien jurídico protegido
- 5.5.3. Sujetos activo y pasivo
- 5.5.4. Elementos determinantes

5.6. *Stalking* II
- 5.6.1. Concurso del delito de acoso con otros tipos penales
- 5.6.2. Requisito para perseguir el delito de *stalking*
- 5.6.3. Subtipos agravados
- 5.6.4. Ciberacoso y *cyberbullying*

5.7. *Child grooming*
- 5.7.1. Delito de ciberacoso sexual de menores
- 5.7.2. Conductas ilícitas
- 5.7.3. Relaciones concursales
  - 5.7.3.1. Prostitución de menores
  - 5.7.3.2. Agresión sexual

5.8. Pornografía infantil
- 5.8.1. Introducción
- 5.8.2. Bien jurídico protegido
- 5.8.3. Conducta típica
- 5.8.4. Conductas agravadas

5.9. Amenazas
- 5.9.1. Introducción
- 5.9.2. El delito de amenazas
- 5.9.3. Amenazas en las redes sociales
- 5.9.4. Situaciones típicas
- 5.9.5. Jurisprudencia

5.10. Injurias y calumnias
- 5.10.1. Introducción
- 5.10.2. Tipificación penal
- 5.10.3. Injurias en Internet
  - 5.10.3.1. Consecuencias
- 5.10.4. Calumnias en Internet
  - 5.10.4.1. Consecuencias

Módulo 6. Delitos informáticos contra la propiedad intelectual, industrial y comercial

6.1. Propiedad intelectual. Introducción
- 6.1.1. Introducción
- 6.1.2. Derechos de autor
- 6.1.3. Sujetos
- 6.1.4. Objeto
- 6.1.5. Contenido
  - 6.1.5.1. Derecho moral
  - 6.1.5.2. Derechos de explotación
  - 6.1.5.3. Otros derechos

6.2. Programas de ordenador
- 6.2.1. Régimen jurídico
- 6.2.2. Objeto de la protección
- 6.2.3. Titularidad de los derechos
- 6.2.4. Duración de la protección
- 6.2.5. Contenido de los derechos de explotación
- 6.2.6. Límites a los derechos de explotación
- 6.2.7. Protección registral
- 6.2.8. Infracción de los derechos
- 6.2.9. Medidas de protección
- 6.2.10. Salvaguardia de aplicación de otras disposiciones legales

6.3. Protección de los derechos de la propiedad intelectual
- 6.3.1. Acciones y procedimientos
  - 6.3.1.1. Acciones y medidas cautelares urgentes
  - 6.3.1.2. Cese de la actividad ilícita
  - 6.3.1.3. Indemnización
  - 6.3.1.4. Medidas cautelares
  - 6.3.1.5. Procedimiento
  - 6.3.1.6. Causas criminales
- 6.3.2. Registro de la propiedad Intelectual
- 6.3.3. Símbolos o indicaciones de la reserva de derechos

6.4. Delitos informáticos contra la propiedad intelectual
- 6.4.1. Introducción
- 6.4.2. Delitos contra la propiedad intelectual
- 6.4.3. Sanciones penales
- 6.4.4. La propiedad intelectual y su penalidad en el ámbito digital
- 6.4.5. Casos reales. Jurisprudencia

6.5. Propiedad industrial: patentes
- 6.5.1. Introducción
- 6.5.2. Patentabilidad
- 6.5.3. Derecho a la patente
- 6.5.4. Designación de inventor
- 6.5.5. Invenciones realizadas en el marco de una relación de empleo o de servicios
- 6.5.6. Acciones por violación del Derecho de patente

6.6. Propiedad industrial: marcas
- 6.6.1. Introducción
- 6.6.2. Concepto de marca
- 6.6.3. Prohibiciones de registro
  - 6.6.3.1. Prohibiciones absolutas
  - 6.6.3.2. Prohibiciones relativas
- 6.6.4. Contenido del derecho de marca
- 6.6.5. Acciones por violación del Derecho de marca

6.7. Delitos informáticos contra la propiedad industrial
- 6.7.1. Introducción
- 6.7.2. Delitos contra la propiedad industrial
- 6.7.3. Sanciones penales
- 6.7.4. La propiedad intelectual y su penalidad en el ámbito digital
- 6.7.5. Casos reales. Jurisprudencia

6.8. Comercio electrónico en el mercado interior
- 6.8.1. Introducción
- 6.8.2. Principios
  - 6.8.2.1. Régimen de establecimiento y de información
  - 6.8.2.2. Comunicaciones comerciales
  - 6.8.2.3. Contratos por vía electrónica
  - 6.8.2.4. Responsabilidad de los prestadores de servicios intermediarios
- 6.8.3. Aplicación

6.9. Servicios de la sociedad de la información y de comercio electrónico
- 6.9.1. Prestación de servicios de la sociedad de la información
  - 6.9.1.1. Principios de libre prestación de servicios
  - 6.9.1.2. Obligaciones y régimen de responsabilidad
    - 6.9.1.2.1. Obligaciones
    - 6.9.1.2.2. Régimen de responsabilidad
  - 6.9.1.3. Códigos de conducta
- 6.9.2. Comunicaciones comerciales por vía electrónica
- 6.9.3. Contratación por vía electrónica

6.10. Delitos informáticos contra el mercado y los consumidores
- 6.10.1. Introducción
- 6.10.2. Delitos contra el mercado y los consumidores
- 6.10.3. Sanciones penales
- 6.10.4. El mercado y los consumidores y su penalidad en el ámbito digital
- 6.10.5. Casos reales. Jurisprudencia

Módulo 7. Posibles perfiles en el ámbito Penal Informático

7.1. Perfiles en el ámbito penal informático. Introducción
- 7.1.1. Introducción
- 7.1.2. Origen
- 7.1.3. Evolución
- 7.1.4. Sujetos activos
- 7.1.5. Sujetos pasivos
- 7.1.6. *Malware*

7.2. *Hacker*
- 7.2.1. Introducción
- 7.2.2. Definición
- 7.2.3. Historia
- 7.2.4. Clasificación de los *hackers*
  - 7.2.4.1. *Hacker* de sombrero blanco
  - 7.2.4.2. *Hacker* de sombrero negro
  - 7.2.4.3. *Hacker* de sombrero gris
  - 7.2.4.4. *Hacker* de sombrero azul
  - 7.2.4.5. *Hacker* de sombrero dorado
  - 7.2.4.6. *Hacker* de sombrero rojo

7.3. *Cracker*
- 7.3.1. Introducción
- 7.3.2. Definición
- 7.3.3. Tipos de *crackers*
- 7.3.4. Ataques informáticos
- 7.3.5. Hackers y *crackers*

7.4. *Phreakers*
- 7.4.1. Introducción
- 7.4.2. Definición
- 7.4.3. Origen
- 7.4.4. Actividad
- 7.4.5. Técnicas de procedimiento

7.5. *Lammers*, gurús y otros perfiles
- 7.5.1. Introducción
- 7.5.2. *Lammers*
- 7.5.3. Gurús
- 7.5.4. *Newbie*
- 7.5.5. Bucaneros
- 7.5.6. *Trashing*

7.6. Sujetos pasivos en el ámbito Penal Informático
- 7.6.1. Introducción
- 7.6.2. Personas físicas
- 7.6.3. Personas jurídicas
- 7.6.4. Entidades sin personalidad jurídica

7.7. *Malware:* troyanos, virus y gusanos
- 7.7.1. *Malware:* Programa malicioso
- 7.7.2. Características
- 7.7.3. Troyano
- 7.7.4. Virus
- 7.7.5. Gusano

7.8. *Malware: spam, hoax y adware*
- 7.8.1. Introducción
- 7.8.2. *Spam*
- 7.8.3. *Hoax*
- 7.8.4. *Adware*

7.9. *Malware: spyware, botnets* y *keylogger*
- 7.9.1. Introducción
- 7.9.2. *Spyware*
- 7.9.3. *Botnets*
- 7.9.4. *Keylogger*

7.10. Reconocimiento, prevención y reporte de programas maliciosos
- 7.10.1. Introducción
- 7.10.2. Prevención
- 7.10.3. Reconocimiento
- 7.10.4. Denuncia

Módulo 8. Ciberseguridad y criminalidad informática

8.1. Ciberseguridad. Introducción
- 8.1.1. ¿Qué es la ciberseguridad?
- 8.1.2. Dominios de ciberseguridad
- 8.1.3. Mitos sobre ciberseguridad
- 8.1.4. Ciber amenazas más comunes

8.2. Ciberseguridad: *hardware* y *software*
- 8.2.1. Introducción
- 8.2.2. *Hardware*
  - 8.2.2.1. Clases y funciones
- 8.2.3. *Software*
  - 8.2.3.1. Clases y funciones

8.3. Ciberseguridad en la Unión Europea
- 8.3.1. Introducción
- 8.3.2. Estrategia de ciberseguridad de la Unión Europea
  - 8.3.2.1. Comisión Europea
  - 8.3.2.2. Servicio Europeo de Acción Exterior

8.4. Agencia Europea para la Ciberseguridad
- 8.4.1. Regulación
- 8.4.2. Estructura y organización
- 8.4.3. Política de ciberseguridad
- 8.4.4. Criptografía
- 8.4.5. Amenazas cibernéticas
- 8.4.6. Gestión de crisis cibernéticas

8.5. Ciberseguridad en España
- 8.5.1. Introducción
- 8.5.2. Consejo Nacional de Ciberseguridad
- 8.5.3. Estrategia Nacional de Ciberseguridad
  - 8.5.3.1. El ciberespacio como espacio común global
  - 8.5.3.2. Las amenazas y desafíos en el ciberespacio
  - 8.5.3.3. Propósitos, principios y objetivos para la ciberseguridad
  - 8.5.3.4. Líneas de acción y medidas
  - 8.5.3.5. La ciberseguridad en el Sistema de Seguridad Nacional

8.6. Foro nacional de Ciberseguridad
- 8.6.1. Origen
- 8.6.2. Funciones
- 8.6.3. Naturaleza jurídica
- 8.6.4. Misión, visión y valores
- 8.6.5. Composición

8.7. Peritaje Informático
- 8.7.1. Introducción
- 8.7.2. Perito informático
- 8.7.3. Metodología
  - 8.7.3.1. Análisis inicial de la situación
  - 8.7.3.2. Investigación y realización del informe
  - 8.7.3.3. Defensa del informe

8.8. Servicios de peritaje informático I
- 8.8.1. Autenticidad e integridad de páginas web y redes sociales
- 8.8.2. Autenticidad e integridad de ficheros de audio
- 8.8.3. Autenticidad e integridad de ficheros de vídeo
- 8.8.4. Cumplimiento o incumplimiento de contrato en desarrollo de proyectos informáticos y sistemas ERP
- 8.8.5. Análisis forense y peritaje informático de teléfonos móviles
- 8.8.6. Conversaciones de WhatsApp
- 8.8.7. Autenticidad e integridad de correos electrónicos y sus adjuntos
- 8.8.8. Suplantación de identidad, *phishing* y estafa del CEO
- 8.8.9. Criptomonedas

8.9. Servicios de peritaje informático II
- 8.9.1. Sistema de nube o *cloud*
- 8.9.2. Ordenadores y discos duros
- 8.9.3. Tasaciones o valoraciones económicas de proyectos o activos informáticos
- 8.9.4. Redacción de informe contra pericial informático
- 8.9.5. Auditoría de sistemas informáticos contables para cumplimiento con la ley antifraude
- 8.9.6. Asesoría tecnológica a empresas
- 8.9.7. Ciberseguridad y *pentesting*

8.10. Criminalidad informática
- 8.10.1. Introducción
- 8.10.2. Fiscal de Sala de criminalidad informática y secciones
- 8.10.3. Grupo de Delitos Telemáticos de la Guardia Civil
- 8.10.4. Brigada de Investigación Tecnológica de la Policía Nacional

Módulo 9. La prueba digital y sus implicaciones en los principios penales

9.1. Introducción de la prueba digital
- 9.1.1. Concepto
- 9.1.2. Medios de prueba en los procesos judiciales
  - 9.1.2.1. Interrogatorio de las partes
  - 9.1.2.2. Documentos públicos y privados
  - 9.1.2.3. Dictámenes periciales
  - 9.1.2.4. Reconocimiento judicial
  - 9.1.2.5. Interrogatorio de testigos
  - 9.1.2.6. Medios de reproducción de la palabra, el sonido y la imagen
  - 9.1.2.7. Instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase
- 9.1.3. Prueba digital

9.2. Proposición y admisión de la prueba digital
- 9.2.1. Proposición y admisión de la prueba digital en la norma procesal civil
- 9.2.2. Proposición y admisión de la prueba digital en la norma procesal Penal
- 9.2.3. Proposición y admisión de la prueba digital en la norma procesal contencioso-administrativa
- 9.2.4. Proposición y admisión de la prueba digital en la norma procesal social

9.3. Valor probatorio de las pruebas en formato digital I
- 9.3.1. Valor probatorio de la prueba digital en el orden civil
  - 9.3.1.1. Correos electrónicos
  - 9.3.1.2. Justificante de presentación a través de LexNET
  - 9.3.1.3. “Pantallazo” con un listado de correos electrónicos
  - 9.3.1.4. Cuestionario electrónico

9.4. Valor probatorio de las pruebas en formato digital II
- 9.4.1. Valor probatorio de la prueba digital en el orden Penal
  - 9.4.1.1. Grabaciones realizadas por cámaras de videovigilancia
  - 9.4.1.2. Documentos electrónicos. Cadena de custodia
  - 9.4.1.3. Grabaciones con cámara oculta
  - 9.4.1.4. Mensajes realizados a través de WhatsApp

9.5. Valor probatorio de las pruebas en formato digital III
- 9.5.1. Valor probatorio de la prueba digital en el orden contencioso-administrativo
  - 9.5.1.1. Necesidad de pericial informática cuando se impugna la prueba digital
- 9.5.2. Valor probatorio de la prueba digital en el orden social
  - 9.5.2.1. Mensajes a través de WhatsApp
  - 9.5.2.2. Correos electrónicos
  - 9.5.2.3. Videovigilancia
  - 9.5.2.4. Medios de grabación

9.6. Pruebas obtenidas vulnerando derechos fundamentales I
- 9.6.1. Introducción
- 9.6.2. Análisis jurisprudencial
  - 9.6.2.1. Grabación de conversaciones aportadas por uno de los interlocutores
  - 9.6.2.2. Pruebas obtenidas vulnerando derechos fundamentales

9.7. Pruebas obtenidas vulnerando derechos fundamentales II
- 9.7.1. Posible ilicitud de la prueba digital por vulnerar derechos fundamentales en el orden civil
  - 9.7.1.1. Nulidad de los informes de detectives privados que recojan información de dispositivos GPS colocados en el coche de un tercero
  - 9.7.1.2. Validez de una conversación entre padre e hijo aportada en una modificación de medidas sin consentimiento del padre
  - 9.7.1.3. Ilicitud de conversación de WhatsApp entre madre e hija aportada por la madre en una modificación de medidas
  - 9.7.1.4. Licitud de correos electrónicos entre los representantes de las partes en el orden civil
  - 9.7.1.5. Artículo 287 de la LEC y licitud de faxes intercambiados entre letrados
  - 9.7.1.6. Licitud de conversación telefónica grabada sin consentimiento

9.8. Problemática jurídica de la prueba digital y sus implicaciones en los principios penales I
- 9.8.1. Concepto y características de la prueba digital en el proceso penal
- 9.8.2. Obtención de la evidencia digital y su conversión en prueba digital
- 9.8.2.1. Normativa internacional
- 9.8.2.2. La importancia de la pericial informática

9.9. Problemática jurídica de la prueba digital y sus implicaciones en los principios penales II
- 9.9.1. Problemática asociada a la incorporación al proceso de la prueba digital y su incidencia sobre los principios penales
  - 9.9.1.1. Referencia a la vulneración de derechos fundamentales
- 9.9.2. Infracción de la cadena de custodia de las evidencias digitales
- 9.9.3. Errores en la valoración de las pruebas digitales por parte de los Tribunales de Justicia

9.10. Juicios en línea
- 9.10.1. Introducción
- 9.10.2. Tramitación electrónica de los procedimientos judiciales
  - 9.10.2.1.Disposiciones comunes e inicio del procedimiento
  - 9.10.2.2.Tramitación orientada al dato
- 9.10.3. Actos y servicios no presenciales
- 9.10.4. Resumen
- 9.10.5. Bibliografía

Módulo 10. Delitos informáticos en el Derecho comparado

10.1. Delitos informáticos en la Unión Europea
- 10.1.1. Introducción
- 10.1.2. Directivas de seguridad en las redes y sistemas de información de la Unión
  - 10.1.2.1. Directiva 2016/1148
  - 10.1.2.2. Orientación general sobre la nueva directiva
- 10.1.3. Reglamento de Ciberseguridad de la UE

10.2. Delitos informáticos en el derecho comparado: Portugal
- 10.2.1. Introducción
- 10.2.2. Normativa reguladora vigente
- 10.2.3. Clases de delitos informáticos
- 10.2.4. Sanciones

10.3. Delitos informáticos en el derecho comparado: Francia
- 10.3.1. Introducción
- 10.3.2. Normativa reguladora vigente
- 10.3.3. Clases de delitos informáticos
- 10.3.4. Sanciones

10.4. Delitos informáticos en el derecho comparado: Italia
- 10.4.1. Introducción
- 10.4.2. Normativa reguladora vigente
- 10.4.3. Clases de delitos informáticos
- 10.4.4. Sanciones

10.5. Delitos informáticos en el derecho comparado: Grecia
- 10.5.1. Introducción
- 10.5.2. Normativa reguladora vigente
- 10.5.3. Clases de delitos informáticos
- 10.5.4. Sanciones

10.6. Delitos informáticos en el derecho comparado: Alemania
- 10.6.1. Introducción
- 10.6.2. Normativa reguladora vigente
- 10.6.3. Clases de delitos informáticos
- 10.6.4. Sanciones

10.7. Delitos informáticos en el derecho comparado: Reino Unido
- 10.7.1. Introducción
- 10.7.2. Normativa reguladora vigente
- 10.7.3. Clases de delitos informáticos
- 10.7.4. Sanciones

10.8. Delitos informáticos en el derecho comparado: Estados Unidos
- 10.8.1. Introducción
- 10.8.2. Normativa reguladora vigente
- 10.8.3. Clases de delitos informáticos
- 10.8.4. Sanciones

10.9. Delitos informáticos en el derecho comparado: México
- 10.9.1. Introducción
- 10.9.2. Normativa reguladora vigente
- 10.9.3. Clases de delitos informáticos
- 10.9.4. Sanciones

10.10. Delitos informáticos en el derecho comparado: Argentina
- 10.10.1. Introducción
- 10.10.2. Normativa reguladora vigente
- 10.10.3. Clases de delitos informáticos
- 10.10.4. Sanciones

"Obtendrás destrezas para contrastar sistemas jurídicos en materia de delitos informáticos y extraer las mejores prácticas normativas"

04

Objetivos docentes

Esta titulación universitaria ofrece a los profesionales una comprensión integral del Derecho Informático y sus diversas ramas. A través de un enfoque práctico, los profesionales desarrollarán competencias esenciales para abordar casos relacionados con delitos cibernéticos; así como para gestionar la seguridad de los datos y la privacidad en entornos digitales. Además, los profesionales manejarán los principales medios electrónicos en la Administración de Justicia. De esta forma, los expertos aplicarán con minuciosidad las normativas y procedimientos legales en el contexto digital. Así, estarán mejor preparados para enfrentar los retos legales que plantea la evolución tecnológica.

Evaluarás el valor probatorio de la evidencia digital en los distintos órdenes jurisdiccionales"

Objetivos generales

- Analizar el marco jurídico internacional aplicable a los delitos informáticos y su evolución en el contexto digital
- Identificar y clasificar las distintas tipologías de ciberdelitos, incluyendo aquellos que afectan a las personas, al patrimonio y a la seguridad pública
- Comprender los principios y normas del Derecho Penal aplicables a las conductas ilícitas cometidas mediante el uso de tecnologías de la información
- Estudiar el tratamiento jurídico de la prueba digital, su obtención, validez, cadena de custodia y límites constitucionales
- Examinar las garantías procesales frente a la criminalidad informática, con especial atención a la tutela judicial efectiva y a los derechos fundamentales
- Profundizar en las implicaciones del tratamiento de datos personales en el ámbito Penal, así como su vinculación con los derechos de privacidad y protección de la información
- Adquirir conocimientos prácticos sobre la detección, prevención y persecución de delitos informáticos en colaboración con cuerpos de seguridad, peritos y autoridades judiciales
- Promover una reflexión crítica sobre los desafíos éticos y legales que plantea la transformación digital tanto de la criminalidad como de la Justicia Pena

Objetivos específicos

Módulo 1. Derecho Informático

- Analizar los fundamentos del Derecho Informático y su interacción con otras ramas jurídicas
- Comprender la evolución normativa aplicable al uso de medios electrónicos en la Administración de Justicia

Módulo 2. Tratamiento de datos personales en el ámbito Penal

- Examinar el marco jurídico europeo y nacional sobre protección de datos en procesos penales
- Abordar el régimen sancionador y las implicaciones legales de las transferencias internacionales de datos

Módulo 3. Redes sociales y delitos informáticos

- Reconocer las principales tipologías de delitos cometidos a través de redes sociales
- Ahondar en las implicaciones jurídicas del uso delictivo de plataformas como WhatsApp, Instagram o TikTok

Módulo 4. Delitos informáticos contra el patrimonio

- Interpretar la normativa penal sobre estafas informáticas, fraudes electrónicos y *phishing* con precisión
- Distinguir los elementos objetivos y subjetivos de los delitos patrimoniales cometidos en entornos digitales

Módulo 5. Delitos informáticos contra las personas físicas

- Identificar los delitos informáticos que atentan contra la intimidad, integridad o libertad individual
- Profundizar en la aplicación del Código Penal en casos de amenazas y calumnias en línea

Módulo 6. Delitos informáticos contra la propiedad intelectual, industrial y comercial

- Estudiar la protección Penal de los derechos de autor, patentes y marcas en el entorno digital
- Establecer el marco normativo sobre el comercio electrónico y su vinculación con delitos informáticos

Módulo 7. Posibles perfiles en el ámbito Penal Informático

- Describir las tipologías de actores delictivos en el ciberespacio con énfasis en los *hackers*
- Profundizar en el uso y detección de *malware* como herramienta delictiva esencial

Módulo 8. Ciberseguridad y criminalidad informática

- Comprender el marco normativo de la ciberseguridad a nivel nacional y europeo
- Ser capaz de identificar las principales amenazas cibernéticas y analizar sus implicaciones penales

Módulo 9. La prueba digital y sus implicaciones en los principios penales

- Estudiar la admisibilidad y validez de la prueba digital en los distintos órdenes jurisdiccionales
- Analizar la cadena de custodia y el principio de legalidad en la valoración de la evidencia digital

Módulo 10. Delitos informáticos en el Derecho comparado

- Ahondar en las diferencias legislativas en materia de ciberdelitos entre distintos países
- Comparar las sanciones aplicables en el ámbito Penal Informático en múltiples jurisdicciones

05

Metodología de estudio

TECH es la primera universidad en el mundo que combina la metodología de los ***case studies*** con el ***Relearning***, un sistema de aprendizaje 100% online basado en la reiteración dirigida.

Esta disruptiva estrategia pedagógica ha sido concebida para ofrecer a los profesionales la oportunidad de actualizar conocimientos y desarrollar competencias de un modo intensivo y riguroso. Un modelo de aprendizaje que coloca al estudiante en el centro del proceso académico y le otorga todo el protagonismo, adaptándose a sus necesidades y dejando de lado las metodologías más convencionales.

TECH te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"

El alumno: la prioridad de todos los programas de TECH

En la metodología de estudios de TECH el alumno es el protagonista absoluto. Las herramientas pedagógicas de cada programa han sido seleccionadas teniendo en cuenta las demandas de tiempo, disponibilidad y rigor académico que, a día de hoy, no solo exigen los estudiantes sino los puestos más competitivos del mercado.

Con el modelo educativo asincrónico de TECH, es el alumno quien elige el tiempo que destina al estudio, cómo decide establecer sus rutinas y todo ello desde la comodidad del dispositivo electrónico de su preferencia. El alumno no tendrá que asistir a clases en vivo, a las que muchas veces no podrá acudir. Las actividades de aprendizaje las realizará cuando le venga bien. Siempre podrá decidir cuándo y desde dónde estudiar.

"En TECH NO tendrás clases en directo (a las que luego nunca puedes asistir)"

Los planes de estudios más exhaustivos a nivel internacional

TECH se caracteriza por ofrecer los itinerarios académicos más completos del entorno universitario. Esta exhaustividad se logra a través de la creación de temarios que no solo abarcan los conocimientos esenciales, sino también las innovaciones más recientes en cada área.

Al estar en constante actualización, estos programas permiten que los estudiantes se mantengan al día con los cambios del mercado y adquieran las habilidades más valoradas por los empleadores. De esta manera, quienes finalizan sus estudios en TECH reciben una preparación integral que les proporciona una ventaja competitiva notable para avanzar en sus carreras.

Y además, podrán hacerlo desde cualquier dispositivo, pc, tableta o smartphone.

> *El modelo de TECH es asincrónico, de modo que te permite estudiar con tu pc, tableta o tu smartphone donde quieras, cuando quieras y durante el tiempo que quieras"*

Case studies o Método del caso

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

Con este modelo de enseñanza es el propio alumno quien va construyendo su competencia profesional a través de estrategias como el *Learning by doing* o el *Design Thinking*, utilizadas por otras instituciones de renombre como Yale o Stanford.

Este método, orientado a la acción, será aplicado a lo largo de todo el itinerario académico que el alumno emprenda junto a TECH. De ese modo se enfrentará a múltiples situaciones reales y deberá integrar conocimientos, investigar, argumentar y defender sus ideas y decisiones. Todo ello con la premisa de responder al cuestionamiento de cómo actuaría al posicionarse frente a eventos específicos de complejidad en su labor cotidiana.

Método *Relearning*

En TECH los *case studies* son potenciados con el mejor método de enseñanza 100% online: el *Relearning*.

Este método rompe con las técnicas tradicionales de enseñanza para poner al alumno en el centro de la ecuación, proveyéndole del mejor contenido en diferentes formatos. De esta forma, consigue repasar y reiterar los conceptos clave de cada materia y aprender a aplicarlos en un entorno real.

En esta misma línea, y de acuerdo a múltiples investigaciones científicas, la reiteración es la mejor manera de aprender. Por eso, TECH ofrece entre 8 y 16 repeticiones de cada concepto clave dentro de una misma lección, presentada de una manera diferente, con el objetivo de asegurar que el conocimiento sea completamente afianzado durante el proceso de estudio.

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

Un Campus Virtual 100% online con los mejores recursos didácticos

Para aplicar su metodología de forma eficaz, TECH se centra en proveer a los egresados de materiales didácticos en diferentes formatos: textos, vídeos interactivos, ilustraciones y mapas de conocimiento, entre otros. Todos ellos, diseñados por profesores cualificados que centran el trabajo en combinar casos reales con la resolución de situaciones complejas mediante simulación, el estudio de contextos aplicados a cada carrera profesional y el aprendizaje basado en la reiteración, a través de audios, presentaciones, animaciones, imágenes, etc.

Y es que las últimas evidencias científicas en el ámbito de las Neurociencias apuntan a la importancia de tener en cuenta el lugar y el contexto donde se accede a los contenidos antes de iniciar un nuevo aprendizaje. Poder ajustar esas variables de una manera personalizada favorece que las personas puedan recordar y almacenar en el hipocampo los conocimientos para retenerlos a largo plazo. Se trata de un modelo denominado *Neurocognitive context-dependent e-learning* que es aplicado de manera consciente en esta titulación universitaria.

Por otro lado, también en aras de favorecer al máximo el contacto mentor-alumno, se proporciona un amplio abanico de posibilidades de comunicación, tanto en tiempo real como en diferido (mensajería interna, foros de discusión, servicio de atención telefónica, email de contacto con secretaría técnica, chat y videoconferencia).

Asimismo, este completísimo Campus Virtual permitirá que el alumnado de TECH organice sus horarios de estudio de acuerdo con su disponibilidad personal o sus obligaciones laborales. De esa manera tendrá un control global de los contenidos académicos y sus herramientas didácticas, puestas en función de su acelerada actualización profesional.

"La modalidad de estudios online de este programa te permitirá organizar tu tiempo y tu ritmo de aprendizaje, adaptándolo a tus horarios"

La eficacia del método se justifica con cuatro logros fundamentales:

1. Los alumnos que siguen este método no solo consiguen la asimilación de conceptos, sino un desarrollo de su capacidad mental, mediante ejercicios de evaluación de situaciones reales y aplicación de conocimientos.
2. El aprendizaje se concreta de una manera sólida en capacidades prácticas que permiten al alumno una mejor integración en el mundo real.
3. Se consigue una asimilación más sencilla y eficiente de las ideas y conceptos, gracias al planteamiento de situaciones que han surgido de la realidad.
4. La sensación de eficiencia del esfuerzo invertido se convierte en un estímulo muy importante para el alumnado, que se traduce en un interés mayor en los aprendizajes y un incremento del tiempo dedicado a trabajar en el curso.

La metodología universitaria mejor valorada por sus alumnos

Los resultados de este innovador modelo académico son constatables en los niveles de satisfacción global de los egresados de TECH.

La valoración de los estudiantes sobre la calidad docente, calidad de los materiales, estructura del curso y sus objetivos es excelente. No en valde, la institución se convirtió en la universidad mejor valorada por sus alumnos según el índice global score, obteniendo un 4,9 de 5.

Accede a los contenidos de estudio desde cualquier dispositivo con conexión a Internet (ordenador, tablet, smartphone) gracias a que TECH está al día de la vanguardia tecnológica y pedagógica.

Podrás aprender con las ventajas del acceso a entornos simulados de aprendizaje y el planteamiento de aprendizaje por observación, esto es, Learning from an expert.

Así, en este programa estarán disponibles los mejores materiales educativos, preparados a conciencia:

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 que creará nuestra manera de trabajo online, con las técnicas más novedosas que nos permiten ofrecerte una gran calidad, en cada una de las piezas que pondremos a tu servicio.

Prácticas de habilidades y competencias

Realizarás 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.

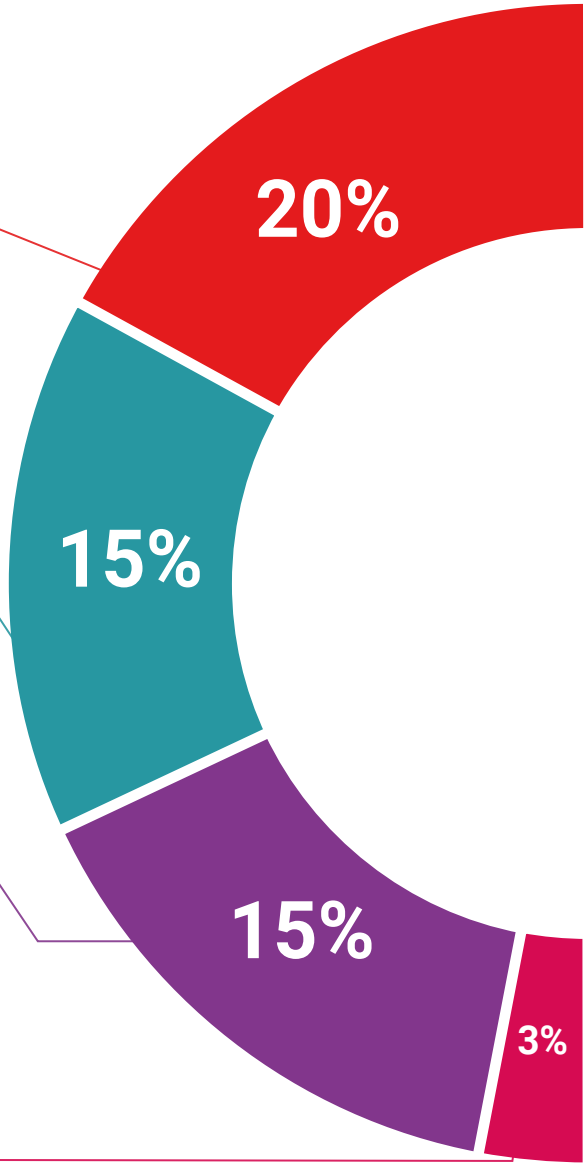
Resúmenes interactivos

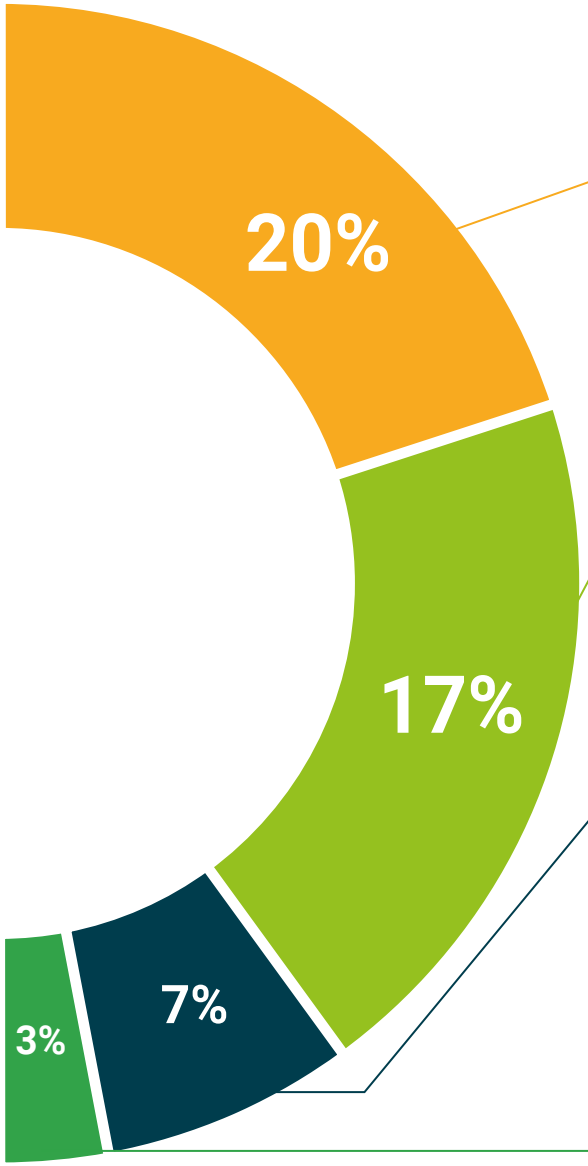
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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

Lecturas complementarias

Artículos recientes, documentos de consenso, guías internacionales... En nuestra biblioteca virtual tendrás acceso a todo lo que necesitas para completar tu capacitación.





Case Studies

Completarás una selección de los mejores *case studies* de la materia. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Testing & Retesting

Evaluamos y reevaluamos periódicamente tu conocimiento a lo largo del programa. Lo hacemos sobre 3 de los 4 niveles de la Pirámide de Miller.

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 nuestras futuras decisiones difíciles.

Guías rápidas de actuación

TECH ofrece los contenidos más relevantes del curso en forma de fichas o guías rápidas de actuación. Una manera sintética, práctica y eficaz de ayudar al estudiante a progresar en su aprendizaje.

06

Titulación

El Máster Título Propio en Derecho Penal Informático garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Máster Propio expedido por TECH Global University.

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

Este programa te permitirá obtener el título propio de **Máster en Derecho Penal Informático** avalado por **TECH Global University**, la mayor Universidad digital del mundo.

TECH Global University, es una Universidad Oficial Europea reconocida públicamente por el Gobierno de Andorra (***boletín oficial***). Andorra forma parte del Espacio Europeo de Educación Superior (EEES) desde 2003. El EEES es una iniciativa promovida por la Unión Europea que tiene como objetivo organizar el marco formativo internacional y armonizar los sistemas de educación superior de los países miembros de este espacio. El proyecto promueve unos valores comunes, la implementación de herramientas conjuntas y fortaleciendo sus mecanismos de garantía de calidad para potenciar la colaboración y movilidad entre estudiantes, investigadores y académicos.

Este título propio de **TECH Global University**, es un programa europeo de formación continua y actualización profesional que garantiza la adquisición de las competencias en su área de conocimiento, confiriendo un alto valor curricular al estudiante que supere el programa.

Título: **Máster Título Propio en Derecho Penal Informático**

Modalidad: **online**

Duración: **12 meses**

Acreditación: **60 ECTS**

tech global university

D/Dña _____, con documento de identificación _____ ha superado con éxito y obtenido el título de:

Máster Título Propio en Derecho Penal Informático

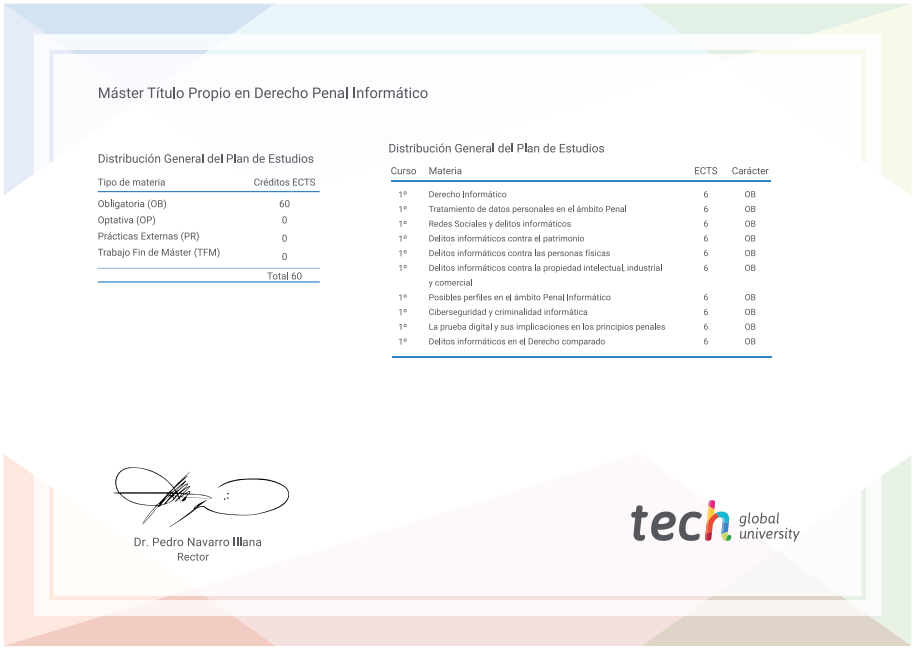
Se trata de un título propio de 1.800 horas de duración equivalente a 60 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Global University es una universidad reconocida oficialmente por el Gobierno de Andorra el 31 de enero de 2024, que pertenece al Espacio Europeo de Educación Superior (EEES).

En Andorra la Vella, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos



Máster Título Propio en Derecho Penal Informático

Distribución General del Plan de Estudios

Tipo de materia	Créditos ECTS
Obligatoria (OB)	60
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
	Total 60

Distribución General del Plan de Estudios

Curso	Materia	ECTS	Carácter
1º	Derecho Informático	6	OB
1º	Tratamiento de datos personales en el ámbito Penal	6	OB
1º	Redes Sociales y delitos informáticos	6	OB
1º	Delitos informáticos contra el patrimonio	6	OB
1º	Delitos informáticos contra las personas físicas	6	OB
1º	Delitos informáticos contra la propiedad intelectual, industrial y comercial	6	OB
1º	Posibles perfiles en el ámbito Penal Informático	6	OB
1º	Ciberseguridad y criminalidad informática	6	OB
1º	La prueba digital y sus implicaciones en los principios penales	6	OB
1º	Delitos informáticos en el Derecho comparado	6	OB

Dr. Pedro Navarro Illana
Rector

tech global university

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

Máster Título Propio
Derecho Penal Informático

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster Título Propio
Derecho Penal Informático

tech global university