Máster Título Propio
Derecho Penal Informático

tech global university

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

Los entornos digitales han adquirido una complejidad cada vez mayor en el ámbito judicial. La rápida evolución de la tecnología, acompañada de la aparición de redes sociales como Tik Tok o mercados como el de las criptomonedas, ha propiciado que juristas de todos los ámbitos deban adquirir unas competencias elevadas en ciberseguridad, pruebas digitales, peritajes informáticos y Derecho Penal Informático. Esta coyuntura ha motivado, precisamente, la creación de esta titulación, que profundiza en todas las cuestiones mencionadas y las amplía bajo el prisma de la jurisdicción y metodología legal más actual. Una oportunidad académica única para profundizar en el Derecho Penal Informático a través de un contenido multimedia de alta calidad, en un formato completamente online, dinámico y flexible.

Defínete como un jurista experto en Derecho Penal Informático gracias a un Máster Título Propio que recoge los preceptos legales más rigurosos y vigentes en la materia"

El campo del Derecho Penal Informático es uno de los que más oportunidades ofrece ahora mismo. El tratamiento de datos personales en la red, los delitos informáticos contra la propiedad intelectual o la proliferación de *malware* de todo tipo ha hecho que la demanda de profesionales del Derecho dedicados al ámbito digital se multiplique.

De hecho, las amenazas que pueden encontrarse en las redes o internet son varias. *Stalking*, *phishing*, *grooming* o estafas de diversa índole son solo algunos ejemplos de delitos comunes en internet, para los que los juristas deben estar preparados. Dada su naturaleza digital y tecnológica, su evolución es constante, lo que exige que los profesionales involucrados tengan un alto nivel de competencias tanto para detectar dichos delitos como para interpretarlos correctamente dentro del orden jurídico vigente.

Ante esta situación, TECH ha elaborado un Máster Título Propio en Derecho Penal Informático que recopila la casuística y jurisprudencia en derecho informático y delitos telemáticos de la manera más rigurosa. Con un enfoque siempre dirigido hacia la propia práctica legal, el alumno encontrará multitud de temas que van desde la tramitación electrónica a los delitos informáticos más comunes, ciberseguridad, servicios de peritaje y comparativa de la normativa entre los principales países europeos y americanos.

Por tanto, se trata de una oportunidad académica inigualable para posicionarse como un especialista en la materia, apoyándose en numerosos análisis de casos reales, desgranados hasta el más mínimo detalle. El formato de la titulación en sí es 100% online, lo que permite una flexibilidad inusitada, pues no existen ni clases presenciales ni horarios prefijados.

Esto implica que todo el contenido se puede descargar desde cualquier dispositivo con conexión a internet, pudiendo estudiarlo y almacenarlo en la *tablet*, ordenador o *smartphone* de referencia del propio alumno. Así, se puede compaginar la propia labor lectiva con las responsabilidades profesionales o laborales más exigentes.

Este **Máster Título Propio en Derecho Penal Informático** contiene el programa educativo 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 está concebido recogen una información 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

Tendrás la libertad necesaria para acceder al Campus Virtual las 24 horas del día, siendo tú quien dictamine el ritmo de estudio”

Proyecta tu carrera hacia el ámbito jurídico de mayor relevancia presente y futura, preparándote con solvencia para los retos del mañana”

Profundiza en los perfiles delictivos más comunes en el ámbito penal informático: hackers, crackers, phreakers y lammers.

Examina la documentación más detallada acerca de las pruebas digitales y su valor probatorio en procesos judiciales.

El programa incluye, en su cuadro docente, a profesionales del sector 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, contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.

02

Objetivos

Debido a que el ámbito informático evoluciona a un ritmo vertiginoso, el objetivo principal de este programa es ofrecerle al jurista las herramientas competenciales y documentación técnica de mayor importancia actualmente. De este modo, podrá adaptarse a las diferentes situaciones o evoluciones que puedan darse en materia de delitos informáticos, accediendo a una guía de referencia de gran calado que impulsará su trayectoria profesional.

Lidera los departamentos jurídicos de delitos informáticos en prestigiosos bufetes o instituciones gracias a este Máster Título Propio"

Objetivos generales

- Adquirir los conocimientos jurídicos ofrecidos por la jurisprudencia
- Identificar los posibles ciberdelincuentes existentes en la actualidad
- Profundizar en los derechos existentes en materia de legislación informática
- Consolidar conocimientos acerca de los servicios de peritaje informático existentes

Avanza con decisión hacia un futuro profesional prometedor, donde destacarás por tu capacidad de adaptación y celeridad a la hora de resolver complejos casos informáticos"

Objetivos específicos

Módulo 1. Derecho Informático

- Distinguir el derecho informático de otras ramas del derecho
- Profundizar en la Administración Judicial electrónica
- Apreciar el uso de los medios electrónicos en la Administración de Justicia
- Indagar en la tramitación electrónica de los procedimientos judiciales

Módulo 2. Tratamiento de datos personales en el ámbito penal

- Identificar la regulación vigente en el ámbito europeo sobre el tratamiento de los datos personales de las personas físicas
- Reconocer la protección de los datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales
- Identificar los derechos reconocidos a las personas
- Visualizar las situaciones especiales

Módulo 3. Redes sociales y delitos informáticos

- Relacionar los delitos informáticos con el derecho a la intimidad
- Reconocer la existencia de distintas redes sociales
- Identificar las redes sociales más utilizadas por los usuarios
- Profundizar en las conductas delictivas más significativas dentro de cada red social

Módulo 4. Delitos informáticos contra el patrimonio

- Identificar los delitos que pueden tener lugar en el ámbito de la informática
- Reconocer las conductas delictivas
- Indagar en la tipificación penal de los supuestos de hecho
- Detectar el bien jurídico protegido de los diferentes tipos delictivos

Módulo 5. Delitos informáticos contra las personas físicas

- Identificar los diferentes delitos en el ámbito informático contra las personas físicas
- Reconocer las sanciones aparejadas a dichos delitos
- Diferenciar las diversas situaciones típicas
- Distinguir los concursos de leyes y delitos que pueden darse en la práctica jurídica

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

- Reconocer la normativa que regula la propiedad intelectual e industrial, así como el comercio electrónico
- Enumerar los delitos contra la propiedad intelectual, industrial y comercial
- Observar las penas aparejadas a los delitos conforme al Código Penal vigente
- Observar el incremento de delitos informáticos en relación con la propiedad intelectual, industrial y contra el mercado y los consumidores
- Comprender la postura jurisprudencial, a través de la visualización de casos reales

Módulo 7. Posibles perfiles en el ámbito penal informático

- Reconocer las características que posee cada uno de ellos
- Diferenciar los distintos programas maliciosos más comunes en la actualidad
- Profundizar en las diferentes consecuencias de cada *malware*
- Analizar las pautas para la prevención, reconocimiento y denuncia

Módulo 8. Ciberseguridad y criminalidad informática

- Identificar el ámbito de la ciberseguridad
- Reconocer la actuación de la Unión Europea
- Profundizar en la Estrategia de Ciberseguridad de España
- Señalar distintos organismos públicos encargados de luchar contra los delitos informáticos

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

- Reconocer los delitos existentes contra la intimidad que pueden tener lugar dentro del ámbito informático
- Diferenciar las distintas relaciones concursales existentes
- Analizar los medios de prueba
- Visualizar las ventajas y desventajas de la celebración de juicios en línea

Módulo 10. Delitos informáticos en el derecho comparado

- Señalar los instrumentos normativos de los que dispone la Unión Europea en cuanto a la lucha contra los delitos informáticos
- Apreciar la existencia de los delitos informáticos en diferentes países
- Reconocer la legislación de cada uno de tales países
- Comparar los regímenes existentes en cada uno de los Estados a estudiar

03

Competencias

Las competencias necesarias para destacar en el ámbito jurídico del Derecho Penal Informático son múltiples, siendo especialmente relevante la capacidad de adaptación del jurista ante todo tipo de requerimientos o delitos. Desde ciberacoso a estafas mediante *phishing,* la casuística es enorme, por lo que esta titulación incide también no solo en las propias habilidades prácticas relacionadas con el área del derecho, sino en las necesarias competencias transversales para distinguirse como un profesional eficaz y resolutivo.

Las competencias que perfeccionarás en esta titulación te convertirán en la punta de lanza ante todo caso judicial relacionado con el Derecho Penal Informático"

Competencias generales

- Aplicar los preceptos del Código Penal vigente
- Desenvolverse con eficacia ante casos jurídicos que impliquen delitos informáticos
- Analizar casuísticas informáticas complejas, que involucren distintos tipos de delito o delincuentes

Perfeccionarás tus competencias en el ámbito internacional a través de una enseñanza intensiva en rol geoestratégico que deben asumir los juristas más avanzados"

Competencias específicas

- Identificar el derecho informático
- Diferenciar las sanciones previstas para los delitos informáticos
- Diferenciar las distintas infracciones existentes en materia de tratamiento de datos personales
- Determinar todos los posibles sujetos intervinientes en delitos informáticos contra el patrimonio
- Analizar la prueba digital dentro de los distintos órdenes jurisdiccionales
- Aplicar la normativa vigente sobre el tratamiento de los datos personales en la rama penal

04

Estructura y contenido

Todo el contenido ofrecido en este Máster Título Propio se ha elaborado basándose en la actualidad más rigurosa del Derecho Penal Informático. De esta forma, se obtiene una contextualización práctica necesaria para cada tema tratado, ofrecida a través de múltiples videos en detalles, análisis de casos y ejemplos reales, resúmenes interactivos y más material multimedia de gran calidad. Todo ello habilita una experiencia académica mucho más efectiva, sin tener que invertir numerosas horas de estudio en material puramente teórico.

Benefíciate de la metodología pedagógica del Relearning, en la que TECH es pionera, para avanzar durante todo el programa con paso firme y decidido"

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. Introducción
- 1.4.2. Normativa
- 1.4.3. Características y clases
- 1.4.4. Contenido y servicios
- 1.4.5. Reglas especiales de responsabilidad
- 1.4.6. 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 d 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. *Childgrooming*
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

Al descargarte todo el contenido del Campus Virtual tendrás acceso a una guía de referencia imprescindible en el Derecho Penal Informático”

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 tomasen decisiones y emitiesen 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

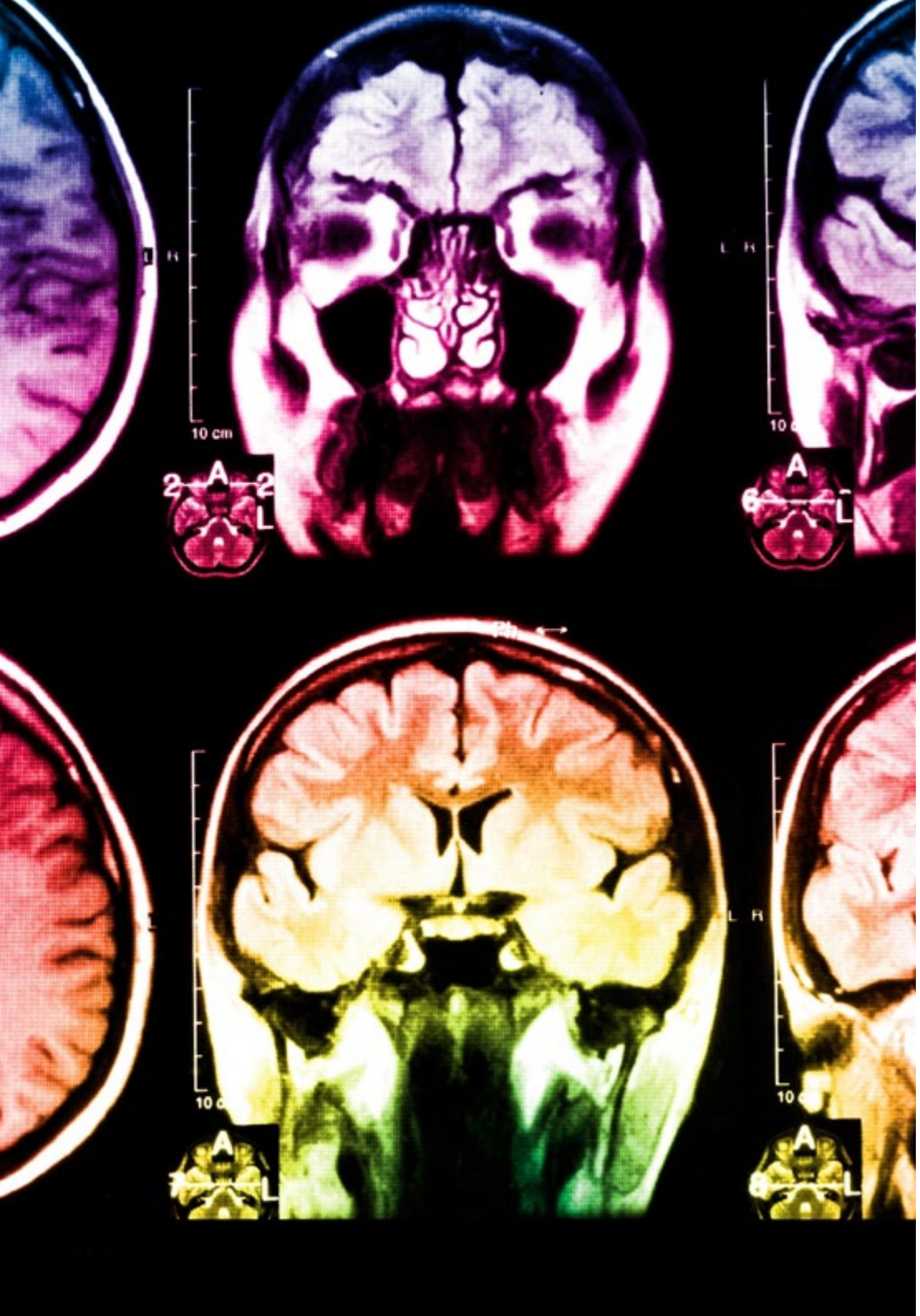
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina 8 elementos didácticos diferentes en cada lección.

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.

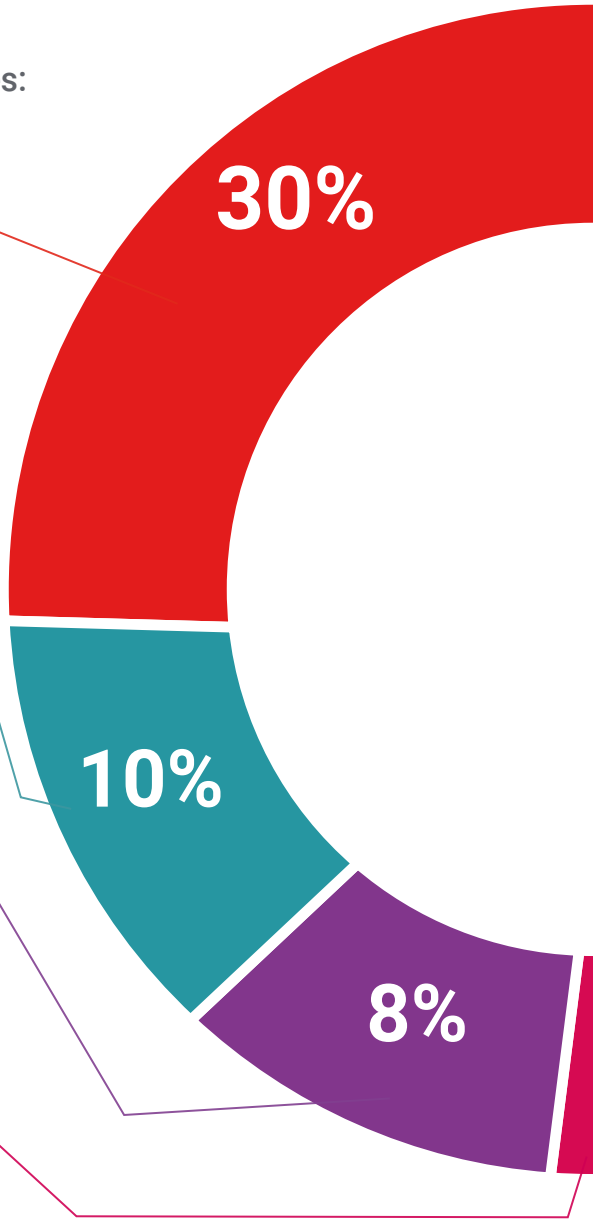
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

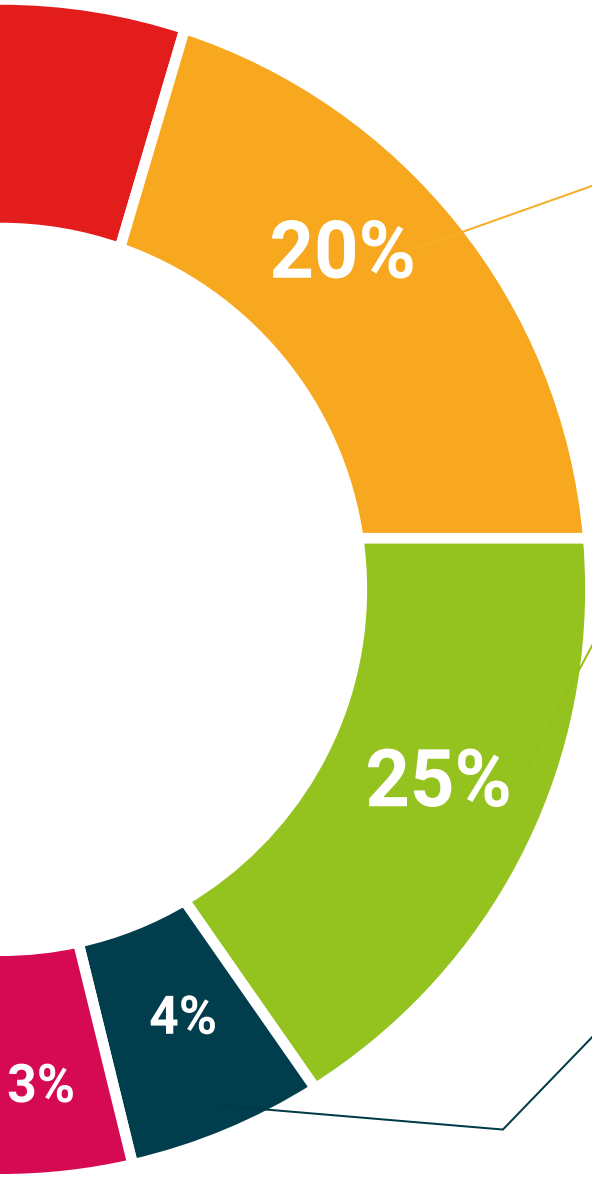
Prácticas de habilidades y competencias

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

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

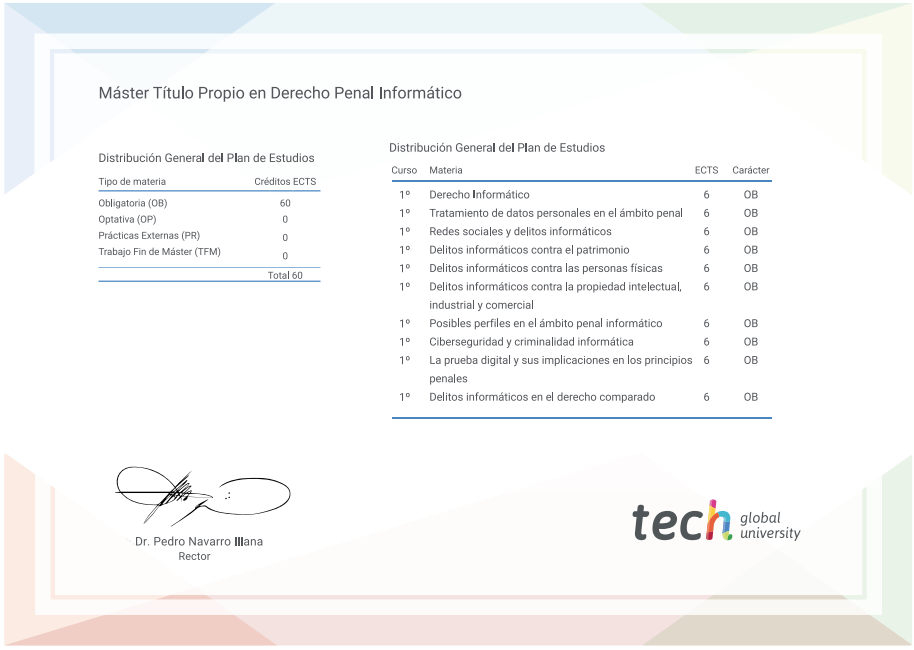
Se trata de un título propio de 1.800 horas de duración equivalente a 60 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

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.

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**

Máster Título Propio
Derecho Penal Informático

tech global university