ISEIE
ISEIE INNOVATION SCHOOL

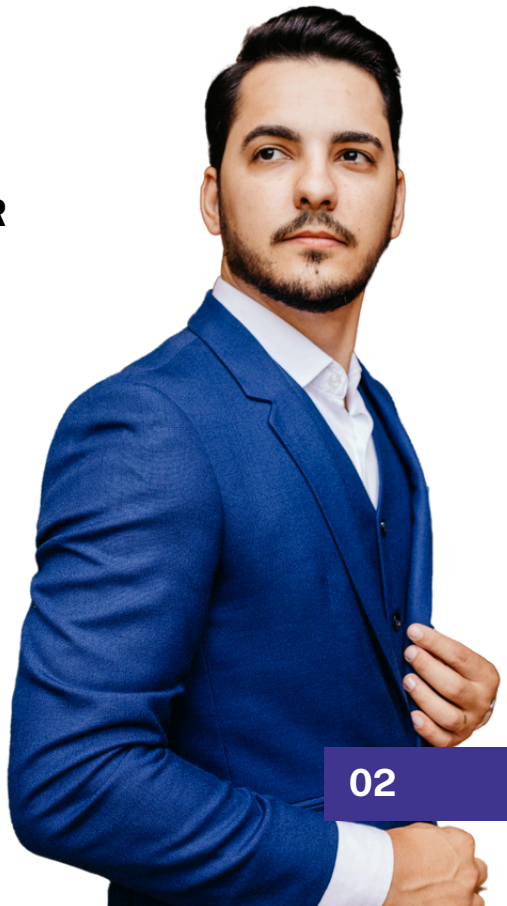
BROCHURE

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y DELITOS INFORMÁTICOS

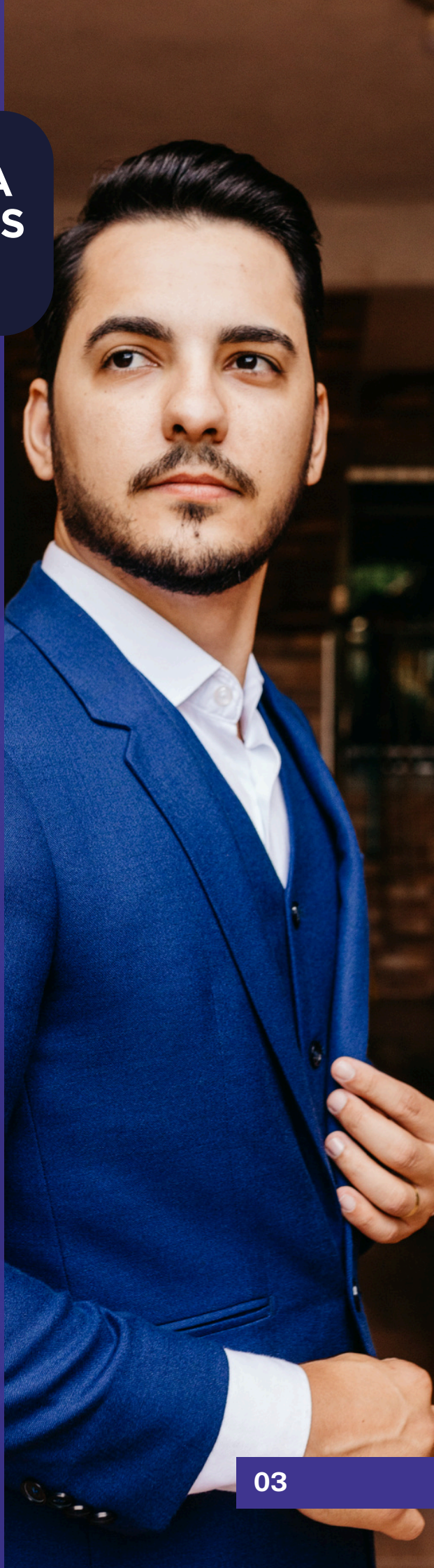
DERECHO

www.iseie.com

ÍNDICE DEL MÁSTER



MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y DELITOS INFORMÁTICOS



En una era cada vez más digitalizada, los riesgos asociados al uso de tecnologías de la información y la comunicación se han convertido en una preocupación central para gobiernos, empresas, instituciones y ciudadanos. El ciberespacio, si bien ofrece oportunidades sin precedentes, también representa un escenario de alta exposición a amenazas, vulneraciones de privacidad, fraudes, espionaje digital y delitos de nueva generación.

Nuestro Máster en Derecho de la Ciberseguridad y Delitos Informáticos ofrece una formación especializada, interdisciplinaria y actualizada que combina el estudio del derecho digital con los fundamentos técnicos y normativos de la seguridad informática. A lo largo del programa, se abordan los principales marcos jurídicos, nacionales e internacionales, así como la tipología de los delitos informáticos, las estrategias legales de prevención, la gestión de la ciberseguridad en infraestructuras críticas y las respuestas forenses ante incidentes.

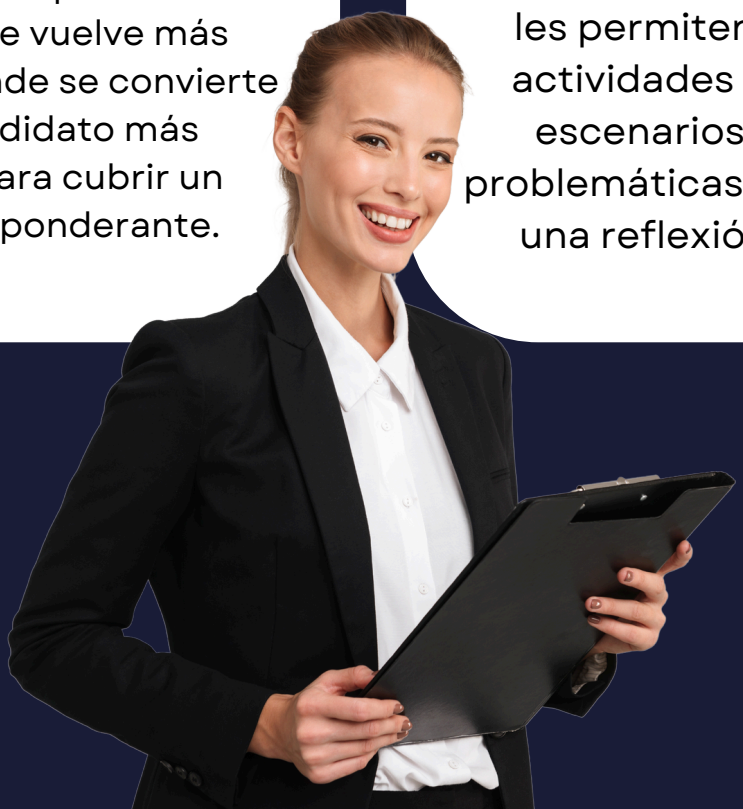
Desde la protección de datos hasta la regulación de nuevas tecnologías como el blockchain o la inteligencia artificial, este máster prepara a profesionales capaces de enfrentar los desafíos jurídicos más complejos en el entorno digital contemporáneo.

ISEIE INNOVATION SCHOOL

POR QUÉ REALIZAR UN MÁSTER

Un diplomado supone una especialización en un rubro específico, se eleva el conocimiento y nivel académico de la persona, convirtiéndola en un elemento fundamental dentro de un esquema de trabajo; su trascendencia radica en el desarrollo de competencias adicionales que adquiere, su proceso formativo se vuelve más sólido y por ende se convierte en un candidato más atractivo para cubrir un puesto preponderante.

Esta metodología de estudio implica una responsabilidad especial para el estudiante, ya que el nivel de exigencia es mayor y la batería de asignaturas es más compleja, los catedráticos asumen que están frente a profesionistas competentes, con un cúmulo de competencias firmes que les permiten desarrollar actividades que simulan escenarios reales con problemáticas que inducen a una reflexión profunda.



OBJETIVOS

A partir del uso generalizado de sistemas informáticos y muy especialmente con la utilización de las redes masivas, comenzaron a surgir controversias jurídicas que no se prestaban a soluciones clásicas. Las dificultades son, esencialmente, la caracterización jurídica de los hechos que suceden en Internet, la determinación del lugar donde se producen (ley aplicable y tribunal competente) y del tiempo en que suceden (en los casos en que éste sea un elemento de configuración).

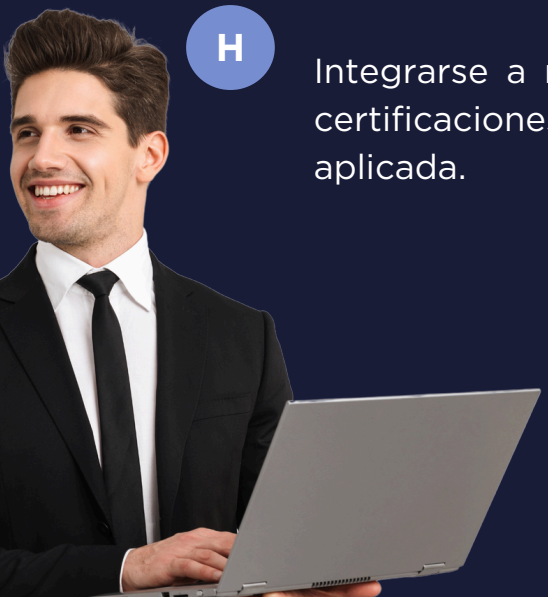
Así surgen dos puntos fundamentales a considerar: el dictado de nuevas normas específicas y la reinterpretación de las normas existentes para ser aplicadas a las nuevas situaciones.

Nuestro diplomado permite comprender los problemas han surgido en todas las ramas del derecho: cuestiones de responsabilidad civil (violación de la propiedad intelectual, relación entre marca y nombre de dominio, responsabilidad de los administradores de redes y de los programadores),

alcanzarás un conocimiento exhaustivo de los derechos que existen y la manera de solucionar las controversias surgidas y podrás estudiar el marco legal nacional e internacional existente

PARA QUÉ TE PREPARA EL MÁSTER

- **A** Aplicar modelos de mediación y técnicas avanzadas de resolución de conflictos en diferentes ámbitos profesionales.
- **B** Intervenir como mediador/a profesional en procesos voluntarios o institucionales, respetando principios éticos y marcos jurídicos vigentes.
- **C** Diseñar e implementar programas de mediación institucional o comunitaria, evaluando su impacto y sostenibilidad.
- **D** Gestionar conflictos complejos con perspectiva interdisciplinaria, integrando dimensiones psicológicas, culturales y sociales.
- **E** Dominar el marco normativo nacional e internacional que regula la mediación y otros métodos ADR.
- **F** Fomentar una cultura del diálogo y la paz, promoviendo la mediación como herramienta de transformación social y de fortalecimiento institucional.
- **G** Explorar las innovaciones tecnológicas y digitales aplicadas a la mediación, incluyendo plataformas de e-mediation, justicia digital e inteligencia artificial.
- **H** Integrarse a redes profesionales de mediación, accediendo a certificaciones, oportunidades laborales e investigación aplicada.



DISEÑO Y CONTENIDO

01

Para el diseño del Plan de estudios de este curso, ISEIE Innovation School ha seguido las directrices del equipo docente, el cual ha sido el encargado de seleccionar la información con la que posteriormente se ha constituido el plan de estudio.

02

De esta forma, el profesional que acceda al programa encontrará el contenido más vanguardista y exhaustivo relacionado con el uso de procesos innovadores y altamente eficaces, conforme a las necesidades y problemáticas actuales.

Buscando la integración de conocimientos académicos y de formación profesional, en un ambiente competitivo y globalizado. Todo ello a través de cada uno de sus módulos de estudio presentado en un cómodo y accesible formato 100% online.

03

El empleo de la metodología Relearning en el desarrollo de este programa te permitirá fortalecer y enriquecer tus conocimientos y hacer que perduren en el tiempo a base de una reiteración de contenidos.

04

REQUISITOS DE POSTULACIÓN

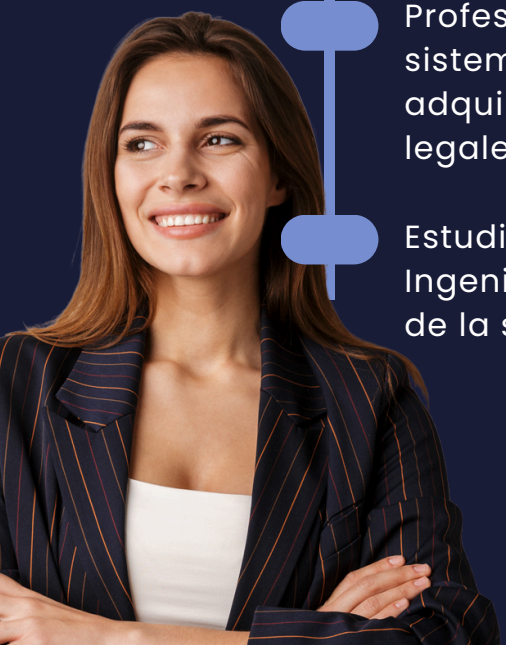
Para postular a nuestro máster, debes cumplir con los siguientes requisitos:

- **Documento de identidad**
- **Correo electrónico**
- **Curriculum Vitae**

Si eres estudiante, conocimientos equivalentes en el área del diplomado al que estas postulando.

A QUIÉN ESTÁ DIRIGIDO

- Juristas, abogados/as, fiscales y jueces que deseen especializarse en derecho digital, cibercriminalidad y delitos informáticos.
- Funcionarios públicos, miembros de cuerpos de seguridad y responsables de políticas públicas relacionados con justicia, defensa, privacidad o ciberseguridad.
- Consultores legales, auditores de TI y profesionales de compliance que operan en sectores regulados o con alto riesgo tecnológico.
- Profesionales de ciberseguridad, administradores de sistemas y técnicos en informática que busquen adquirir una comprensión sólida de los aspectos legales y éticos del entorno digital.
- Estudiantes de posgrado en Derecho, Informática, Ingeniería o Ciencias Políticas interesados en el futuro de la seguridad jurídica digital.



TITULACIÓN PROPIA

Al concluir el curso, los participantes serán galardonados con una titulación propia otorgada por ISEIE Innovation School. Esta titulación se encuentra respaldada por una certificación que equivale a 4 créditos ECTS (European Credit Transfer and Accumulation System) y representa un total de 100 horas de dedicación al estudio.

Esta titulación no solo enriquecerá su imagen y credibilidad ante potenciales clientes, sino que reforzara significativamente su perfil profesional en el ámbito laboral. Al presentar esta certificación, podrá demostrar de manera concreta y verificable su nivel de conocimiento y competencia en el área temática del curso.

Esto resultará en un aumento de su empleabilidad, al hacerle destacar entre otros candidatos resaltando su compromiso con la mejora continua y el desarrollo profesional.

TRABAJO FINAL DEL MÁSTER

A Una vez que haya completado satisfactoriamente todos los módulos del máster, deberá llevar a cabo un trabajo final en el cual deberá aplicar y demostrar los conocimientos que ha adquirido a lo largo del programa.

B Este trabajo final suele ser una oportunidad para poner en práctica lo que ha aprendido y mostrar su comprensión y habilidades en el tema.

C Puede tomar la forma de un proyecto, un informe, una presentación u otra tarea específica, dependiendo del contenido del curso y sus objetivos. Recuerde seguir las instrucciones proporcionadas y consultar con su instructor o profesor si tiene alguna pregunta sobre cómo abordar el trabajo final.

CONTENIDO MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y DELITOS INFORMÁTICOS

MÓDULO 1: FUNDAMENTOS DE CIBERSEGURIDAD Y DERECHO DIGITAL

1.1 Conceptos básicos de ciberseguridad
1.2 Historia y evolución del derecho digital
1.3 Marco normativo internacional y nacional
1.4 Principios jurídicos aplicados a la ciberseguridad
1.5 Tipos de amenazas y vulnerabilidades digitales
1.6 Protección de datos personales y privacidad
1.7 Seguridad de la información
1.8 Gobernanza y políticas públicas en ciberseguridad
1.9 Responsabilidad civil y penal en el entorno digital
1.10 Ética y derechos humanos en el ciberespacio

MÓDULO 2: DELITOS INFORMÁTICOS Y MARCO LEGAL

2.1 Tipología de delitos informáticos
2.2 Legislación penal nacional e internacional
2.3 Delitos contra la privacidad y datos personales
2.4 Fraude y estafa digital
2.5 Acceso indebido y ataques cibernéticos
2.6 Delitos relacionados con la propiedad intelectual digital
2.7 Ciberterrorismo y ciberguerra
2.8 Cooperación internacional en la persecución de delitos informáticos
2.9 Procedimientos de investigación penal digital
2.10 Casos emblemáticos y jurisprudencia

MÓDULO 3: PROTECCIÓN DE DATOS Y PRIVACIDAD

3.1 Legislación sobre protección de datos
3.2 Derechos de los titulares de datos
3.3 Obligaciones de responsables y encargados del tratamiento
3.4 Transferencia internacional de datos
3.5 Medidas técnicas y organizativas de seguridad
3.6 Evaluaciones de impacto en protección de datos
3.7 Notificación y gestión de brechas de seguridad
3.8 Autoridades de control y supervisión
3.9 Responsabilidad por incumplimiento
3.10 Tendencias y desafíos futuros

MÓDULO 4: INVESTIGACIÓN Y PERSECUCIÓN DE DELITOS INFORMÁTICOS

4.1 Técnicas y herramientas forenses digitales
4.2 Recolección y preservación de evidencia digital
4.3 Cadena de custodia y validez probatoria
4.4 Investigación criminal informática
4.5 Colaboración entre autoridades nacionales e internacionales
4.6 Procedimientos judiciales y procesales
4.7 Derechos de las víctimas y protección de testigos
4.8 Estrategias de litigación en delitos informáticos
4.9 Análisis de casos y sentencias
4.10 Desarrollo de protocolos y buenas prácticas

MÓDULO 5: SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS Y SISTEMAS DE INFORMACIÓN

5.1 Concepto y clasificación de infraestructuras críticas
5.2 Normativa aplicable a infraestructuras críticas
5.3 Gestión de riesgos y vulnerabilidades
5.4 Medidas de protección y control de accesos
5.5 Respuesta y gestión de incidentes
5.6 Continuidad y recuperación de negocios
5.7 Evaluación y auditoría de seguridad

5.8 Seguridad en sistemas de control industrial
5.9 Protección en redes y telecomunicaciones
5.10 Casos prácticos y estudios de impacto

MÓDULO 6: CONTRATOS Y REGULACIÓN EN CIBERSEGURIDAD

6.1 Contratos tecnológicos y acuerdos de nivel de servicio (SLA)
6.2 Responsabilidad contractual y garantías
6.3 Cláusulas de confidencialidad y protección de información
6.4 Contratos de outsourcing y seguridad
6.5 Regulación de proveedores y terceros
6.6 Cumplimiento normativo y auditorías contractuales
6.7 Contratos en servicios cloud y almacenamiento de datos
6.8 Aspectos legales de licencias y software
6.9 Contratos de respuesta a incidentes y contingencias
6.10 Jurisprudencia y análisis de casos

MÓDULO 7: ÉTICA, GOBERNANZA Y POLÍTICAS PÚBLICAS EN CIBERSEGURIDAD

7.1 Principios éticos en ciberseguridad
7.2 Gobernanza corporativa y responsabilidad social
7.3 Políticas públicas y estrategias nacionales
7.4 Participación ciudadana y educación en ciberseguridad
7.5 Protección de derechos fundamentales en el ciberespacio
7.6 Transparencia y rendición de cuentas
7.7 Innovación responsable y tecnologías emergentes
7.8 Colaboración público-privada
7.9 Estándares y certificaciones internacionales
7.10 Retos y perspectivas globales

MÓDULO 8: NUEVAS TECNOLOGÍAS Y DESAFÍOS JURÍDICOS EN CIBERSEGURIDAD

8.1 Inteligencia artificial y seguridad informática
8.2 Blockchain y seguridad de la información
8.3 Internet de las cosas (IoT) y riesgos asociados
8.4 Computación en la nube y desafíos legales
8.5 Seguridad en dispositivos móviles y redes inalámbricas
8.6 Ciberseguridad en el sector financiero y bancario
8.7 Protección frente a amenazas avanzadas y persistentes
8.8 Regulación y desafíos de la criptografía
8.9 Impacto de la tecnología 5G en la seguridad digital
8.10 Futuro y tendencias en derecho y ciberseguridad

MÓDULO 9: TRABAJO FINAL MÁSTER

Nota: El contenido del programa académico puede estar sometido a ligeras modificaciones, en función de las actualizaciones o de las mejoras efectuadas.

ISEIE
ISEIE INNOVATION SCHOOL

CONTÁCTANOS

+34 960 25 47 46

Av. Aragón 30, 5. 46021 Valencia.

www.iseie.com