ISEIE
ISEIE INNOVATION SCHOOL

BROCHURE

DIPLOMADO EN DERECHO DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD

DERECHO

www.iseie.com

ÍNDICE DEL DIPLOMADO

DIPLOMADO EN DERECHO DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD

En un entorno global altamente digitalizado, donde los datos personales circulan de forma constante y las amenazas cibernéticas se multiplican, la protección de la información se ha convertido en un derecho fundamental y una prioridad estratégica para empresas, instituciones públicas y profesionales del derecho y la tecnología. Nuestro Diplomado en Derecho de Protección de Datos y Ciberseguridad proporciona un abordaje integral, técnico y jurídico sobre los principales marcos normativos, responsabilidades legales y mecanismos de cumplimiento vinculados al tratamiento seguro y ético de los datos personales y la defensa frente a riesgos cibernéticos. Este programa responde a la creciente demanda de especialistas capaces de garantizar el cumplimiento normativo, prevenir incidentes de seguridad y responder eficazmente ante situaciones de crisis digital

ISEIE INNOVATION SCHOOL

POR QUÉ REALIZAR UN DIPLOMADO

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 DIPLOMADO

A Interpretar y aplicar la normativa nacional e internacional en materia de protección de datos (como el GDPR) y ciberseguridad.

B Ejercer funciones de cumplimiento, auditoría, supervisión y gestión de riesgos en organizaciones que traten datos personales. Diseñar políticas internas y programas de cumplimiento adaptados a diferentes contextos organizacionales.

C Responder eficazmente a brechas de seguridad, auditorías o inspecciones por parte de autoridades de control. Asesorar legalmente en temas complejos como transferencia internacional de datos, uso de inteligencia artificial o contratos con terceros.

D Comprender el marco sancionador y la jurisprudencia vigente sobre privacidad, cibercrimen y delitos informáticos. Contribuir a la construcción de una cultura organizacional ética y responsable, centrada en la seguridad de la información y la defensa de los derechos digitales.

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 diplomado en derecho, 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

Abogados/as, juristas y asesores legales interesados en especializarse en derecho digital y privacidad.

Delegados de Protección de Datos (DPO/DPD) o responsables de cumplimiento normativo en el sector público y privado.

Profesionales de TI y ciberseguridad que deseen comprender la regulación aplicable y asumir roles de responsabilidad.

Funcionarios públicos, responsables de tratamiento de datos, reguladores o auditores.

Académicos, investigadores y consultores que trabajan con tecnologías emergentes, big data, nteligencia artificial o servicios digitales.

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 DIPLOMADO

A Una vez que haya completado satisfactoriamente todos los módulos del diplomado, 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.

DIPLOMADO EN DERECHO DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD

MÓDULO 1: FUNDAMENTOS Y MARCO LEGAL DE LA PROTECCIÓN DE DATOS

1.1 Introducción a la protección de datos personales
1.1.1 Concepto y definiciones básicas
1.1.2 Tipos de datos personales
1.1.3 Importancia de la protección de datos
1.1.4 Derechos de los titulares de datos
1.1.5 Riesgos y amenazas a la privacidad
1.2 Marco jurídico internacional de protección de datos
1.2.1 Convenios y tratados internacionales
1.2.2 Normativas de la Unión Europea (GDPR)
1.2.3 Legislación en América Latina y otras regiones
1.2.4 Estándares internacionales y recomendaciones
1.2.5 Retos en la armonización legal
1.3 Legislación nacional sobre protección de datos
1.3.1 Leyes y regulaciones nacionales principales
1.3.2 Autoridades de control y supervisión
1.3.3 Procedimientos de cumplimiento y sanciones
1.3.4 Derechos y obligaciones en el contexto local
1.3.5 Casos prácticos y jurisprudencia
1.4 Principios rectores de la protección de datos
1.4.1 Licitud, lealtad y transparencia
1.4.2 Minimización y calidad de datos
1.4.3 Limitación del plazo de conservación
1.4.4 Integridad y confidencialidad
1.4.5 Responsabilidad proactiva
1.5 Derechos de los titulares de datos
1.5.1 Derecho de acceso
1.5.2 Derecho a la rectificación y cancelación
1.5.3 Derecho a la portabilidad
1.5.4 Derecho de oposición
1.5.5 Derechos en el entorno digital
1.6 Obligaciones de los responsables y encargados del tratamiento
1.6.1 Definición y roles
1.6.2 Registro de actividades de tratamiento
1.6.3 Evaluaciones de impacto de privacidad
1.6.4 Medidas técnicas y organizativas
1.6.5 Notificación de brechas de seguridad
1.7 Transferencia internacional de datos
1.7.1 Normativas aplicables
1.7.2 Mecanismos de transferencia
1.7.3 Garantías y excepciones
1.7.4 Riesgos asociados
1.7.5 Supervisión y control

1.8 Procedimientos y sanciones en materia de protección de datos
1.8.1 Inspecciones y auditorías
1.8.2 Procedimientos sancionadores
1.8.3 Tipos de infracciones y multas
1.8.4 Recursos y defensa jurídica
1.8.5 Casos emblemáticos
1.9 Gobernanza y cultura organizacional en protección de datos
1.9.1 Políticas internas y formación
1.9.2 Designación de Delegados de Protección de Datos (DPD)
1.9.3 Auditorías internas y externas
1.9.4 Gestión del riesgo y compliance
1.9.5 Conciencia y ética empresarial
1.10 Tendencias y futuro en la protección de datos
1.10.1 Innovaciones tecnológicas y desafíos
1.10.2 Impacto de la inteligencia artificial
1.10.3 Protección de datos en el internet de las cosas (IoT)
1.10.4 Regulación emergente y jurisprudencia
1.10.5 Desarrollo global y cooperación internacional

MÓDULO 2: FUNDAMENTOS Y MARCO LEGAL DE LA CIBERSEGURIDAD

2.1 Introducción a la ciberseguridad
2.1.1 Conceptos y definiciones clave
2.1.2 Amenazas y vulnerabilidades comunes
2.1.3 Principios básicos de ciberseguridad
2.1.4 Ciberseguridad y protección de datos
2.1.5 Panorama global de la ciberseguridad
2.2 Marco normativo internacional en ciberseguridad
2.2.1 Convenciones internacionales relevantes (Budapest, etc.)
2.2.2 Estándares y certificaciones internacionales
2.2.3 Cooperación internacional y alianzas
2.2.4 Protección crítica de infraestructuras
2.2.5 Retos para países en desarrollo
2.3 Legislación nacional en ciberseguridad
2.3.1 Leyes específicas y regulaciones generales
2.3.2 Autoridades y organismos competentes
2.3.3 Estrategias nacionales de ciberseguridad
2.3.4 Responsabilidades legales y sanciones
2.3.5 Casos de aplicación práctica

2.4 Cibercrimen y delitos informáticos
2.4.1 Tipos de ciberdelitos
2.4.2 Marco legal penal y sanciones
2.4.3 Procedimientos de investigación y persecución
2.4.4 Cooperación judicial internacional
2.4.5 Prevención y sensibilización
2.5 Gestión de incidentes de ciberseguridad
2.5.1 Detección y respuesta a incidentes
2.5.2 Planes de contingencia y continuidad del negocio
2.5.3 Comunicación y notificación de incidentes
2.5.4 Roles y responsabilidades internas
2.5.5 Análisis post-incidente y aprendizaje
2.6 Seguridad en redes y sistemas de información
2.6.1 Arquitectura segura y diseño de sistemas
2.6.2 Control de accesos y autenticación
2.6.3 Protección de datos en tránsito y almacenamiento
2.6.4 Criptografía aplicada
2.6.5 Auditorías y pruebas de penetración
2.7 Ciberseguridad en entornos corporativos
2.7.1 Políticas y normativas internas
2.7.2 Formación y concienciación del personal
2.7.3 Gestión de riesgos y compliance
2.7.4 Herramientas y tecnologías de defensa
2.7.5 Evaluación y mejora continua
2.8 Seguridad en la nube y nuevas tecnologías
2.8.1 Riesgos específicos en entornos cloud
2.8.2 Modelos de responsabilidad compartida
2.8.3 Protección de datos y cumplimiento normativo
2.8.4 Seguridad en IoT y dispositivos móviles
2.8.5 Tecnologías emergentes y desafíos
2.9 Ética y privacidad en ciberseguridad
2.9.1 Principios éticos aplicados
2.9.2 Protección de la privacidad y datos personales
2.9.3 Dilemas éticos y casos de estudio
2.9.4 Transparencia y confianza
2.9.5 Responsabilidad social corporativa
2.10 Futuro y tendencias en ciberseguridad
2.10.1 Inteligencia artificial y automatización
2.10.2 Seguridad en el 5G y más allá
2.10.3 Nuevos modelos de amenaza
2.10.4 Regulación y gobernanza global
2.10.5 Innovación y resiliencia

MÓDULO 3: GESTIÓN DE LA PROTECCIÓN DE DATOS Y CUMPLIMIENTO NORMATIVO

3.1 Programas de cumplimiento en protección de datos
3.1.1 Diseño e implementación de programas
3.1.2 Políticas internas y manuales
3.1.3 Capacitación y formación continua
3.1.4 Seguimiento y auditoría
3.1.5 Mejora continua y actualizaciones
3.2 Delegado de Protección de Datos (DPD)
3.2.1 Funciones y responsabilidades
3.2.2 Perfil y competencias requeridas
3.2.3 Designación y comunicación a autoridades
3.2.4 Apoyo y coordinación interna
3.2.5 Buenas prácticas y casos
3.3 Evaluaciones de Impacto en Protección de Datos (EIPD)
3.3.1 Metodología y requisitos legales
3.3.2 Identificación y análisis de riesgos
3.3.3 Medidas mitigadoras
3.3.4 Documentación y seguimiento
3.3.5 Casos prácticos
3.4 Contratos y cláusulas en tratamiento de datos
3.4.1 Contratos con proveedores y encargados
3.4.2 Cláusulas obligatorias
3.4.3 Supervisión y control contractual
3.4.4 Subcontratación y responsabilidad
3.4.5 Modelos y plantillas

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

3.5 Registro de actividades y documentación
3.5.1 Requisitos normativos
3.5.2 Herramientas y sistemas de gestión
3.5.3 Conservación y acceso
3.5.4 Control interno
3.5.5 Auditorías internas
3.6 Notificación y gestión de brechas de seguridad
3.6.1 Definición y tipos de brechas
3.6.2 Procedimientos de notificación
3.6.3 Comunicación con afectados y autoridades
3.6.4 Medidas correctivas
3.6.5 Prevención futura
3.7 Supervisión y sanciones por incumplimiento
3.7.1 Autoridades de control y sus competencias
3.7.2 Procedimientos sancionadores
3.7.3 Tipos de infracciones
3.7.4 Recursos y defensa jurídica
3.7.5 Análisis de casos relevantes
3.8 Herramientas tecnológicas para la protección de datos
3.8.1 Sistemas de gestión de privacidad
3.8.2 Software de monitoreo y auditoría
3.8.3 Encriptación y seguridad
3.8.4 Evaluación continua
3.8.5 Integración con sistemas

MÓDULO 4: CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS Y EMPRESAS
4.1 Identificación de infraestructuras críticas
4.1.1 Concepto y clasificación
4.1.2 Importancia estratégica
4.1.3 Regulaciones aplicables
4.1.4 Riesgos y amenazas
4.1.5 Estudios de caso
4.2 Gestión de riesgos y evaluación de vulnerabilidades
4.2.1 Metodologías de análisis
4.2.2 Herramientas de evaluación
4.2.3 Identificación de activos críticos
4.2.4 Análisis de amenazas
4.2.5 Gestión de vulnerabilidades
4.3 Implementación de controles y medidas de seguridad
4.3.1 Controles técnicos
4.3.2 Controles organizacionales
4.3.3 Controles físicos
4.3.4 Sistemas de detección y prevención
4.3.5 Mejores prácticas
4.4 Respuesta ante incidentes y gestión de crisis
4.4.1 Procedimientos y protocolos
4.4.2 Equipos de respuesta rápida
4.4.3 Comunicación interna y externa
4.4.4 Recuperación y continuidad
4.4.5 Evaluación post-incidente
4.5 Ciberseguridad en el sector financiero
4.5.1 Regulaciones específicas
4.5.2 Riesgos y amenazas comunes
4.5.3 Protección de datos financieros
4.5.4 Auditorías y cumplimiento
4.5.5 Tecnologías aplicadas
4.6 Protección en sectores de salud y educación
4.6.1 Datos sensibles y su protección
4.6.2 Normativas aplicables
4.6.3 Buenas prácticas sectoriales
4.6.4 Gestión de incidentes
4.6.5 Retos y oportunidades
4.7 Seguridad en tecnologías emergentes
4.7.1 IoT y dispositivos conectados
4.7.2 Inteligencia artificial y machine learning
4.7.3 Blockchain y seguridad
4.7.4 Computación en la nube
4.7.5 Retos legales y técnicos
4.8 Normativas y estándares internacionales
4.8.1 ISO/IEC 27001 y familia
4.8.2 NIST Cybersecurity Framework
4.8.3 GDPR y ciberseguridad
4.8.4 Leyes nacionales y su alineación
4.8.5 Certificaciones y auditorías
4.9 Formación y capacitación en ciberseguridad
4.9.1 Programas educativos
4.9.2 Certificaciones profesionales
4.9.3 Talleres y simulacros
4.9.4 Cultura organizacional
4.9.5 Actualización continua
4.10 Futuro y tendencias en ciberseguridad empresarial
4.10.1 Automatización y AI en seguridad
4.10.2 Nuevos vectores de ataque
4.10.3 Estrategias de defensa avanzadas
4.10.4 Colaboración y compartición de información
4.10.5 Evolución normativa

MÓDULO 5: PROTECCIÓN DE DATOS EN NUEVAS TECNOLOGÍAS Y ENTORNOS DIGITALES

5.1 Protección de datos en inteligencia artificial
5.1.1 Datos utilizados por IA
5.1.2 Transparencia y explicabilidad
5.1.3 Regulación y responsabilidad
5.1.4 Riesgos de discriminación
5.1.5 Buenas prácticas
5.2 Privacidad y datos en Internet de las cosas (IoT)
5.2.1 Tipos de dispositivos IoT
5.2.2 Riesgos para la privacidad
5.2.3 Regulación específica
5.2.4 Seguridad en IoT
5.2.5 Ejemplos prácticos
5.3 Protección en redes sociales y plataformas digitales
5.3.1 Manejo de datos personales
5.3.2 Consentimiento y términos de uso
5.3.3 Riesgos de exposición y filtraciones
5.3.4 Políticas de privacidad
5.3.5 Casos destacados
5.4 Regulación del big data y análisis masivo de datos
5.4.1 Conceptos y aplicaciones
5.4.2 Impacto en la privacidad
5.4.3 Legislación aplicable
5.4.4 Técnicas de anonimización
5.4.5 Buenas prácticas y ética
5.5 Protección de datos en comercio electrónico
5.5.1 Datos sensibles y transacciones
5.5.2 Seguridad en pagos electrónicos
5.5.3 Derechos del consumidor digital
5.5.4 Políticas de privacidad y cookies
5.5.5 Incidentes y reclamaciones
5.6 Protección de datos en salud digital
5.6.1 Datos personales y sensibles en salud
5.6.2 Regulación y estándares internacionales
5.6.3 Consentimiento informado
5.6.4 Seguridad y confidencialidad
5.6.5 Telemedicina y protección de datos
5.7 Privacidad y protección en aplicaciones móviles
5.7.1 Permisos y accesos a datos
5.7.2 Evaluación de riesgos
5.7.3 Regulación y buenas prácticas
5.7.4 Protección del usuario
5.7.5 Casos de análisis
5.8 Protección en sistemas de reconocimiento biométrico
5.8.1 Tipos de biometría
5.8.2 Riesgos y vulnerabilidades
5.8.3 Legislación y regulación
5.8.4 Consentimiento y uso responsable
5.8.5 Ejemplos y casos prácticos
5.9 Uso ético de datos y tecnologías digitales
5.9.1 Principios éticos
5.9.2 Transparencia y responsabilidad
5.9.3 Impacto social y cultural
5.9.4 Buenas prácticas empresariales
5.9.5 Casos de estudio
5.10 Desafíos futuros en protección de datos digitales
5.10.1 Nuevas tecnologías emergentes
5.10.2 Adaptación normativa
5.10.3 Colaboración internacional
5.10.4 Educación y concienciación
5.10.5 Innovación responsable

MÓDULO 6: ASPECTOS PROCESALES Y JURISPRUDENCIA EN PROTECCIÓN DE DATOS Y CIBERSEGURIDAD

6.1 Procedimientos administrativos en protección de datos
6.1.1 Presentación de denuncias
6.1.2 Inspecciones y auditorías
6.1.3 Resolución de reclamaciones
6.1.4 Sanciones administrativas
6.1.5 Recursos y apelaciones
6.2 Jurisdicción y competencia en materia de datos y ciberseguridad
6.2.1 Competencia territorial
6.2.2 Competencia material
6.2.3 Jurisdicción internacional
6.2.4 Casos de conflictos jurisdiccionales
6.2.5 Coordinación interinstitucional
6.3 Procedimientos penales relacionados con ciberdelitos
6.3.1 Tipos de ciberdelitos penales
6.3.2 Investigación y recolección de pruebas
6.3.3 Cooperación internacional
6.3.4 Procesos judiciales
6.3.5 Ejecución de sentencias
6.4 Pruebas digitales y cadena de custodia

6.4.1 Obtención y preservación de evidencia
6.4.2 Autenticidad y validez legal
6.4.3 Técnicas forenses digitales
6.4.4 Cadena de custodia
6.4.5 Presentación en juicio
6.5 Jurisprudencia relevante en protección de datos
6.5.1 Sentencias nacionales destacadas
6.5.2 Decisiones de tribunales internacionales
6.5.3 Interpretaciones normativas
6.5.4 Análisis de precedentes
6.5.5 Impacto en la legislación
6.6 Recursos judiciales y administrativos
6.6.1 Tipos de recursos
6.6.2 Procedimientos y plazos
6.6.3 Defensa y representación legal
6.6.4 Recursos especiales
6.6.5 Estrategias procesales
6.7 Mediación y arbitraje en conflictos de datos y ciberseguridad
6.7.1 Alternativas al proceso judicial
6.7.2 Procedimientos y reglas
6.7.3 Conveniencia y limitaciones
6.7.4 Casos de éxito
6.7.5 Integración con otros mecanismos
6.8 Responsabilidad civil y penal en protección de datos
6.8.1 Elementos de la responsabilidad civil
6.8.2 Daños y perjuicios
6.8.3 Responsabilidad penal aplicable
6.8.4 Casos prácticos
6.8.5 Medidas de reparación
6.9 Protección internacional y cooperación jurídica
6.9.1 Convenios y tratados
6.9.2 Mecanismos de cooperación
6.9.3 Intercambio de información
6.9.4 Coordinación en investigaciones
6.9.5 Desafíos y oportunidades
6.10 Tendencias jurisprudenciales y desarrollo normativo
6.10.1 Evolución de la jurisprudencia
6.10.2 Impacto en futuras leyes
6.10.3 Áreas emergentes de litigio
6.10.4 Rol de tribunales internacionales
6.10.5 Retos y perspectivas

MÓDULO 7: TRABAJO FINAL DIPLOMADO

ISEIE
ISEIE INNOVATION SCHOOL

CONTÁCTANOS

+34 960 25 47 46

Av. Aragón 30, 5. 46021 Valencia.

www.iseie.com