

# Diplomatura en Seguridad Digital, Inteligencia Artificial y Normativas en el Ciberespacio

---

## Información General

---

**Fecha de inicio:** 22/09/2026

**Frecuencia:** Semanal

**Carga horaria por clase:** 120 min

## Presentación

---

La diplomatura en sí está diseñada para abordar principios de la Inteligencia Artificial, Protección de Datos Personales, Seguridad de la Información y la Gestión de Riesgos. Actualmente podemos distinguir los siguientes especialistas: Inteligencia Artificial Ciberseguridad Aspectos Normativos Sin embargo, en esta era digital, existe una brecha entre IA, Ciber espacio y Derecho, esta brecha es el resultado de diferencias profundas en formación, lenguaje y objetivos entre ambos mundos. La disociación entre tecnología y derecho no es sostenible en un mundo donde algoritmos deciden sobre libertad, seguridad y economía. Los "traductores" entre ambos mundos serán tan críticos como los propios desarrolladores o legisladores. La próxima frontera no está en crear más IA o leyes, sino en profesionales que las hagan coexistir.

## Objetivos Generales

---

Formar profesionales capaces de integrar conocimientos técnicos, jurídicos y estratégicos para intervenir con solvencia en escenarios institucionales vinculados al ciberespacio, la inteligencia artificial y la protección de datos, promoviendo una gobernanza digital efectiva y resiliente.

## Objetivos Específicos

---

- Identificar riesgos operativos y normativos en el ciberespacio, reconociendo actores, infraestructuras críticas y vectores de amenaza en contextos institucionales.
- Analizar marcos jurídicos nacionales e internacionales, con énfasis en el GDPR (General Data Protection Regulation) y sus implicancias operativas, especialmente en el tratamiento de datos personales sensibles y la obligación de designar un DPO (Data Protection Officer) en organismos públicos o actividades de monitoreo sistemático.
- Diseñar estrategias institucionales de defensa digital y gobernanza, integrando equipos técnico-jurídicos para la gestión de crisis, la preservación de evidencia digital y la protección de derechos fundamentales.
- Evaluar escenarios donde la designación de un DPO (Data Protection Officer) es legalmente exigible, considerando el tipo de datos tratados, el volumen de procesamiento y la naturaleza de las actividades institucionales.

## Destinatarios

---

- Personal operativo o de gestión en organismos públicos o privados del ámbito tecnológico, jurídico o de seguridad informática.

- Funcionarios y equipos técnicos que requieran fortalecer la articulación entre marcos normativos y herramientas tecnológicas en contextos institucionales, especialmente en escenarios donde se evalúe, implemente o supervise el uso de sistemas de inteligencia artificial.
- Profesionales de las ciencias jurídicas, técnicas o sociales que requieran en adquirir competencias aplicadas en materia de ciberseguridad, inteligencia artificial y gobernanza digital, incluyendo el análisis ético, normativo y estratégico de algoritmos utilizados en procesos institucionales.

## Requisitos Previos

---

- Poseer antecedentes laborales en las áreas de “Gestión de Tecnologías y/o Legales de empresas tecnológicas”
- Título de nivel superior no universitario y/o título universitario o formación profesional equivalente.

## Plan de Estudios

---

### Módulo 1: Módulo 1: Introducción al Ciberespacio y la Seguridad Digital

- Clase 1: El ciberespacio como dominio estratégico: actores, infraestructuras críticas, forensia digital y OSINT aplicado a contextos institucionales
- Clase 2: Protección de datos personales (Ley 25.326), gobernanza de datos e Inteligencia Artificial como herramienta estratégica y operativa

### Módulo 2: MÓDULO 2 — Ciberseguridad: conceptos y actores

- Clase 3: Ciberseguridad en el sector privado: grandes empresas, PYMES y ciudadanía. Incentivos económicos, regulatorios y reputacionales. Casos de estudio argentinos
- Clase 4: Ciberseguridad en el Estado argentino: Defensa Nacional, Ministerio Público, Seguridad Interior y DNCS. Diferencias con el sector privado y obligaciones normativas específicas

### Módulo 3: MÓDULO 3 — Ciberseguridad jurídica y normativa

- Clase 5: Marco internacional de ciberseguridad: Manual de Tallinn 2.0, Convenio de Budapest, aplicación práctica y posición de Argentina frente a estos instrumentos
- Clase 6: Marco regional y nacional: estrategias OEA y MERCOSUR, normativa ONTI, Estrategia Nacional de Ciberseguridad 2023 y arquitectura institucional argentina

### Módulo 4: MÓDULO 4 — Infraestructura tecnológica: Laboratorio I

- Clase 7: Laboratorio de redes: arquitectura de red segura con VirtualBox y Amazon AWS. Configuración de router, firewall (iptables), servidor web (Apache) y DNS (BIND9)
- Clase 8: Laboratorio de ataque: ejecución de ataque Man in the Middle, captura de tráfico con Wireshark, seguridad en redes IT/OT, análisis del caso STUXNET y diseño de esquemas de contingencia

### Módulo 5: MÓDULO 5 — Inteligencia Artificial: conceptos y casos aplicados

- Clase 9: IA en investigaciones penales, justicia y salud: sistemas de scoring predictivo,

reconocimiento facial, sesgos algorítmicos y casos de discriminación automatizada

- Clase 10: IA en la administración pública argentina, ética algorítmica, manipulación digital (Cambridge Analytica, deepfakes) y principios de diseño ético de sistemas de IA

### **Módulo 6: MÓDULO 6 — Inteligencia Artificial: marcos jurídicos y normativos**

- Clase 11: Constitucionalismo y IA: derechos fundamentales frente a sistemas algorítmicos. Principios INTERPOL-UNICRI para el uso ético de la IA en seguridad y justicia
- Clase 12: AI Act europeo: cuatro categorías de riesgo, obligaciones para sistemas de alto riesgo, regulación comparada (EE.UU., LATAM, Argentina) y responsabilidad jurídica cuando la IA produce daños

### **Módulo 7: MÓDULO 7 — Inteligencia Artificial: Laboratorio II**

- Clase 13: Laboratorio de Machine Learning: tipos de modelos, primer clasificador en Google Colabs (Python/scikit-learn), análisis de sesgo algorítmico en dataset de crédito
- Clase 14: Laboratorio de IA generativa: visión por computadora, NLP y análisis de sentimiento, modelos fundacionales, técnicas de prompting avanzado e implicancias legales de las alucinaciones

### **Módulo 8: MÓDULO 8 — Ciberespacio: conceptos y normativa**

- Clase 15: Criptomonedas y contratos inteligentes: marco regulatorio argentino (CNV, BCRA, AFIP), blockchain y privacidad, tensión entre inmutabilidad y derecho al olvido
- Clase 16: Normativa argentina de ciberseguridad: Ley 26.388 de delitos informáticos, evidencia digital, cadena de custodia y actuación de la UFECI en investigaciones cibernéticas

### **Módulo 9: MÓDULO 9 — Ciberespacio: área técnica y simulación de crisis**

- Clase 17: Simulación de ataque coordinado tipo ransomware con equipos técnico, jurídico y de dirección: gestión de crisis en tiempo real, notificaciones obligatorias y decisiones bajo presión
- Clase 18: SOC y CSIRT: diferencias, roles y complementariedad. ISO 27001:2022, NIST SP 800-61 y estándares internacionales de respuesta a incidentes aplicados al caso simulado

### **Módulo 10: MÓDULO 10 — Gobernanza, riesgo, cumplimiento y certificaciones**

- Clase 19: Gobernanza de datos, figura del DPO (GDPR), PCI DSS y marcos GRC (COBIT 2019, ISO 31000). Integración con la Estrategia Nacional de Ciberseguridad 2023
- Clase 20: Certificaciones profesionales del ecosistema: CISSP, CISM, CRISC, DPO certificado y CompTIA Security+. Mapa de carrera en ciberseguridad y derecho digital post-diplomatura

### **Módulo 11: MÓDULO 11 — Diseño colaborativo y cierre del programa**

- Clase 21: Taller integrador: diseño colaborativo de estrategia institucional de ciberseguridad sobre caso ficticio. Equipos interdisciplinarios con roles técnico, jurídico,

## GRC y comunicación

- Clase 22: Evaluación técnico-operativa grupal ante tribunal, orientación final para la defensa del TFI y cierre formal del programa con entrega de diplomas de participación

## Módulo 12: TFI — Trabajo Final Integrador

- Clase 23: Defensa oral individual ante tribunal (modalidad virtual): presentación de 8 a 10 minutos del Trabajo Final Integrador seguida de preguntas del tribunal evaluador
- Clase 24: Devolución oral del tribunal con calificación final y orientaciones para el desarrollo profesional post-diplomatura. Emisión del diploma universitario oficial

## Bibliografía

- Ciberseguridad y Seguridad de la Información NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.04162018> Schmitt, M. N. (Ed.) (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2.ª ed.). Cambridge University Press. Consejo de Europa (2001). Convenio sobre la Ciberdelincuencia (Convenio de Budapest). Serie de Tratados Europeos N.º 185. Estrasburgo. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. International Organization for Standardization.
- Inteligencia Artificial: ética, regulación y aplicaciones Russell, S. & Norvig, P. (2021). Inteligencia Artificial: Un enfoque moderno (4.ª ed.). Pearson. Cath, C. (2018). Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges. Philosophical Transactions of the Royal Society A, 376(2133). <https://doi.org/10.1098/rsta.2018.0080> Floridi, L. et al. (2018). AI4People — An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, 28(4), 689–707. INTERPOL – UNICRI (2019). Towards Responsible AI Innovation: A Practical Guide for Law Enforcement. United Nations Interregional Crime and Justice Research Institute. Unión Europea (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de IA). Diario Oficial de la Unión Europea, L 2024/1689.
- Protección de datos personales y privacidad Unión Europea (2016). Reglamento General de Protección de Datos — RGPD (Reglamento 2016/679 del Parlamento Europeo y del Consejo). Diario Oficial de la Unión Europea. Argentina (2000). Ley 25.326 de Protección de los Datos Personales. Boletín Oficial de la República Argentina. Solove, D. J. (2008). Understanding Privacy. Harvard University Press. Agencia de la Unión Europea para la Ciberseguridad — ENISA (2022). Threat Landscape 2022. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu>
- Gobernanza digital, derecho internacional y GRC ISACA (2018). COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association. OEA – Comité Interamericano contra el Terrorismo (2021). Estrategia Interamericana para Proteger la Infraestructura Crítica. Organización de los Estados Americanos. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

