Diplomado Internacional en Cibercriminología y Seguridad Digital

Estructura informativa y alcance técnico del contenido formativo

Dirección Académica:	Coordinación Académica de Criminología	**Modalidad y Fecha de Inicio:**	Online / 06 de agosto de 2026
Fecha de Emisión:	15 de Julio de 2026	**Código de Registro:**	CPLV-VIT-DICSD2026-001

1. Resumen Ejecutivo del Programa

El Diplomado Internacional en Cibercriminología y Seguridad Digital es un programa especializado de alto nivel académico, diseñado para profesionales del derecho, la seguridad, la criminalistica, la criminología y la tecnología que deseen adquirir competencias avanzadas para comprender, investigar y combatir el fenómeno del cibercrimen en todas sus dimensiones.

En un mundo donde las amenazas digitales evolucionan con una rapidez sin precedentes, este diplomado proporciona las herramientas conceptuales, técnicas y jurídicas necesarias para responder de manera eficiente, ética y fundamentada a los desafíos que plantea la delincuencia en el ciberespacio.

El programa combina rigor académico con aplicación práctica, integrando casos reales, simulaciones, laboratorios virtuales y la participación de expertos nacionales e internacionales. Está organizado en seis módulos progresivos que cubren desde los fundamentos de la cibercriminología hasta la formulación de políticas públicas integrales en ciberseguridad.

2. Perfil del Participante y Competencias

El diplomado está dirigido a:

- Abogados, fiscales y jueces que intervienen en procesos relacionados con el cibercrimen.
- Investigadores policiales, agentes de inteligencia y funcionarios de seguridad del Estado.
- Profesionales de ciberseguridad, analistas forenses digitales e ingenieros de sistemas.
- Académicos, investigadores y consultores en criminología, derecho penal y seguridad.
- Funcionarios públicos responsables de políticas de seguridad digital e infraestructuras críticas.

Al finalizar el Diplomado habrá desarrollado las siguientes competencias:

- Analítica: identificar, clasificar y perfilar comportamientos delictivos en el ciberespacio.
- Jurídica: aplicar el marco legal nacional e internacional vigente en materia de cibercrimen.
- Técnica: utilizar herramientas y metodologías de investigación digital forense y OSINT.
- Ética: tomar decisiones fundamentadas que respeten los derechos fundamentales y la privacidad.
- Estratégica: diseñar e implementar políticas públicas integrales de ciberseguridad.
- Colaborativa: participar en redes de cooperación internacional contra el cibercrimen

3. Contenido Programático Temático

El diplomado se estructura en 6 módulos de 4 semanas cada uno, con una carga total de 180 horas académicas distribuidas en 24 semanas de formación.

Módulo	Título	Capítulos base	Horas
Módulo 1	**Fundamentos de la Cibercriminología y el Entorno Digital**	Capítulos 1 y 2	**30 h**
Módulo 2	**Perfilación Criminal Digital y Análisis Conductual**	Capítulos 3 y 4	**30 h**
Módulo 3	**Ética, Legalidad y Jurisdicción en el Ciberespacio**	Capítulos 5 y 6	**30 h**
Módulo 4	**Cooperación Internacional y Evidencia Digital**	Capítulos 7 al 10	**30 h**
Módulo 5	**Gobernanza Global, Ciberguerra y Delitos Emergentes**	Capítulos 11 al 13	**30 h**
Módulo 6	**Políticas Públicas Integrales en Cibercriminología**	Capítulo 14	**30 h**
TOTAL	**6 módulos · 14 Capítulos · 24 Semanas**	Capítulos 1 al 14	**180 h**

MÓDULO 1	Fundamentos de la Cibercriminología y el Entorno Digital

□ Duración	Horas	Nivel	Unidades
4 semanas	30 h	Básico–Intermedio	6 unidades

Descripción del Módulo

Este módulo sienta las bases conceptuales, históricas y teóricas de la cibercriminología, estableciendo el marco analítico para comprender el fenómeno del cibercrimen desde una perspectiva multidisciplinar. Se analiza el ciberespacio como nuevo escenario criminal y las formas emergentes de delincuencia digital.

Contenidos Temáticos

- 1.1 Concepto y Definición de la Cibercriminología
- 1.2 Evolución Histórica de la Cibercriminología
- 1.3 Diferencias entre Criminología Tradicional y Cibercriminología
- 1.4 Tipologías del Cibercrimen
- 1.5 Principales Teorías Aplicadas: Oportunidad, Control Social, Neutralización y Subculturas
- 2.1 El Ciberespacio como Nuevo Escenario Criminal
- 2.2 Nuevas Formas de Criminalidad: Phishing, Ransomware, Ciberacoso, Grooming, Deepfakes
- 2.3 Factores de Riesgo en el Ciberespacio
- 2.4 Victimología Digital
- 2.5 El Rol de la Tecnología en la Evolución del Crimen

Objetivos de Aprendizaje

1. Comprender los fundamentos conceptuales y teóricos de la cibercriminología.
2. Identificar las principales tipologías del cibercrimen y sus características.
3. Analizar el ciberespacio como escenario criminal diferenciado.
4. Aplicar las teorías criminológicas clásicas al contexto digital.
5. Reconocer los factores de riesgo y las dinámicas de victimización digital.

Recursos y Materiales

- Lecturas especializadas en Cibercriminología
- Bases de datos de casos reales (anonimizados)
- Videos de expertos internacionales
- Plataformas de simulación de escenarios digitales

MÓDULO 2	Perfilación Criminal Digital y Análisis Conductual

Duración	Horas	Nivel	Unidades
4 semanas	30 h	Intermedio	6 unidades

Descripción del Módulo

Este módulo aborda las técnicas especializadas de perfilación criminal aplicadas al ciberespacio, incluyendo el análisis del comportamiento de ciberdelincuentes, sus tipologías, las herramientas digitales forenses y la inteligencia conductual aplicada a investigaciones digitales.

Contenidos Temáticos

- 3.1 Concepto de Perfilación Criminal Digital
- 3.2 La Psicología del Ciberdelincuente
- 3.3 Tipologías de Ciberdelincuentes
- 3.4 Técnicas de Perfilación en el Ámbito Digital: Modus Operandi, Firma Digital, Comportamiento en Línea
- 3.5 Análisis de Metadatos y Huella Digital
- 3.6 Perfilación basada en Machine Learning
- 3.7 Indicadores de Perfilación Digital
- 4.1 Análisis del Comportamiento de Usuarios y Entidades (UEBA)
- 4.2 Inteligencia de Fuentes Abiertas (OSINT) y Redes Sociales (SOCMINT)
- 4.3 Procesamiento de Lenguaje Natural y Estilometría
- 4.4 Técnicas Forenses Conductuales y Psicología Digital
- 4.5 Análisis Visual de Anomalías de Comportamiento

Objetivos de Aprendizaje

6. Dominar las técnicas de perfilación criminal aplicadas al entorno digital.
7. Identificar tipologías y patrones conductuales de ciberdelincuentes.
8. Aplicar herramientas de OSINT y SOCMINT en investigaciones digitales.
9. Interpretar metadatos y rastros digitales con fines investigativos.
10. Integrar técnicas de machine learning en la detección de comportamientos anómalos.

Recursos y Materiales

- Software OSINT (Maltego, Shodan)
- Laboratorios virtuales de análisis de metadatos
- Casos prácticos de ciberinvestigación
- Tutoriales sobre herramientas de UEBA

MÓDULO 3	Ética, Legalidad y Jurisdicción en el Ciberespacio

⏱ Duración	📚 Horas	🎯 Nivel	📖 Unidades
4 semanas	30 h	Intermedio–Avanzado	7 unidades

Descripción del Módulo

Este módulo examina los desafíos éticos y jurídicos que plantea la perfilación criminal digital y la investigación en el ciberespacio, así como los problemas de jurisdicción y territorialidad que surgen cuando los delitos transcienden fronteras nacionales.

Contenidos Temáticos

- 5.1 Privacidad y Protección de Datos Personales
- 5.2 Sesgos Algorítmicos, Presunción de Inocencia y Discriminación
- 5.3 Consentimiento y Transparencia en la Recolección de Datos
- 5.4 El Conflicto entre Seguridad y Derechos Fundamentales
- 5.5 Más Seguridad vs. Más Libertad: Un Dilema
- 5.6 Cooperación Internacional y Mecanismos Jurídicos
- 6.1 Jurisdicción Universal y Principio de Territorialidad
- 6.2 Jurisdicción Basada en la Nacionalidad y Protección de Nacionales
- 6.3 Jurisdicción por Ubicuidad y Principio de Subsidiariedad
- 6.4 Retos en la Cooperación Internacional

Objetivos de Aprendizaje

11. Analizar los dilemas éticos en la investigación y perfilación digital.

12. Aplicar el marco normativo de protección de datos personales.
13. Identificar los conflictos entre seguridad pública y derechos fundamentales.
14. Comprender los principios de jurisdicción aplicables al ciberdelito.
15. Evaluar los mecanismos de cooperación internacional en materia penal digital.

Recursos y Materiales

- Reglamento RGPD y legislaciones comparadas
- Jurisprudencia del TJUE y CEDH
- Convenio de Budapest sobre Cibercrimen
- Bases de datos jurídicas especializadas

MÓDULO 4	Cooperación Internacional y Evidencia Digital

⏱ Duración	📚 Horas	🎯 Nivel	📖 Unidades
4 semanas	30 h	Avanzado	8 unidades

Descripción del Módulo

Este módulo profundiza en los marcos de cooperación técnica y jurídica internacional para combatir el ciberdelito, incluyendo el análisis de tratados bilaterales, la asistencia jurídica mutua, las obligaciones de los proveedores de servicios digitales y los estándares internacionales de evidencia digital.

Contenidos Temáticos

- 7.1 Cooperación Técnica Internacional contra el Ciberdelito
- 7.2 Alianzas Público-Privadas en Ciberseguridad
- 8.1 Asistencia Jurídica Mutua (MLAT) y Tratados Bilaterales
- 8.2 Barreras para el Intercambio de Evidencia Digital Transfronteriza
- 9.1 Tipos de Proveedores de Servicios Digitales
- 9.2 Obligaciones de Conservación y Retención de Datos
- 9.3 Resistencia, Desafíos y Buenas Prácticas
- 9.4 Perspectiva Legal y Derechos Fundamentales
- 10.1 Cadena de Custodia en la Evidencia Digital
- 10.2 Características de la Evidencia Digital
- 10.3 Etapas de la Cadena de Custodia
- 10.4 Estándares Internacionales de Admisibilidad Probatoria
- 10.5 Desafíos en Países en Desarrollo

Objetivos de Aprendizaje

16. Gestionar procesos de cooperación técnica y jurídica internacional en cibercrimen.
17. Evaluar el rol de los proveedores de servicios digitales en las investigaciones.
18. Aplicar los estándares de cadena de custodia para evidencia digital.
19. Analizar los tratados y mecanismos de asistencia jurídica mutua.
20. Identificar buenas prácticas en el intercambio de evidencia digital transfronteriza.

Recursos y Materiales

- Normas ISO/IEC 27037 sobre evidencia digital
- Guías del Consejo de Europa
- Modelos de solicitudes MLAT
- Estudio comparado de legislaciones de retención de datos

MÓDULO 5	Gobernanza Global, Ciberguerra y Delitos Emergentes

⏳ Duración	📑 Horas	🎯 Nivel	📖 Unidades
4 semanas	30 h	Avanzado	9 unidades

Descripción del Módulo

Este módulo examina los modelos de gobernanza global del ciberespacio, los retos criminológicos emergentes vinculados a la inteligencia artificial, el metaverso y el ransomware como servicio, así como la ciberguerra, el terrorismo digital y las amenazas híbridas a la seguridad nacional.

Contenidos Temáticos

- 11.1 Modelos de Gobernanza Global: Multilateral, Multistakeholder e Híbrido
- 11.2 Actores Clave en la Gobernanza Global
- 11.3 Desafíos Globales: Ciberconflictos, Ciberarmas y Falta de Capacidades
- 11.4 Hacia una Gobernanza Ética y Colaborativa
- 12.1 Delitos asistidos por IA: nuevas tipologías
- 12.2 Ransomware como Servicio (RaaS)
- 12.3 Ciberdelitos en el Metaverso
- 12.4 Explotación Sexual Infantil facilitada por tecnología
- 12.5 Retos Criminológicos Emergentes: Despersonalización, Transnacionalidad, Delincuencia Organizada Digital
- 13.1 ¿Qué es la Ciberguerra?
- 13.2 Terrorismo Digital y Actores Híbridos
- 13.3 Desinformación y Guerra Cognitiva

- 13.4 Problemas Jurídicos y Éticos de la Ciberguerra

Objetivos de Aprendizaje

21. Comprender los modelos de gobernanza global del ciberespacio.
22. Identificar y analizar las nuevas tipologías de ciberdelitos emergentes.
23. Analizar la ciberguerra y el terrorismo digital como amenazas a la seguridad nacional.
24. Evaluar el impacto de la IA y el metaverso en la criminalidad digital.
25. Proponer respuestas estratégicas frente a amenazas híbridas y desinformación.

Recursos y Materiales

- Informes ENISA, Europol y Interpol
- Doctrinas de ciberguerra de la OTAN
- Investigaciones sobre ransomware y RaaS
- Plataformas de threat intelligence (TI)

MÓDULO 6	Políticas Públicas Integrales en Cibercriminología y Ciberseguridad

Duración	Horas	Nivel	Unidades
4 semanas	30 h	Avanzado–Estratégico	4 unidades

Descripción del Módulo

El módulo de cierre integra todos los conocimientos adquiridos para la formulación de propuestas de políticas públicas integrales en cibercriminología y ciberseguridad. Los participantes desarrollarán propuestas concretas, aplicadas y fundamentadas para contextos institucionales reales.

Contenidos Temáticos

- 14.1 Principios Rectores para una Política Pública en Ciberseguridad
- 14.2 Diagnóstico de Capacidades Institucionales
- 14.3 Diseño e Implementación de Estrategias Nacionales de Ciberseguridad
- 14.4 Propuesta de Política Pública Integral: metodología y estructura
- 14.5 Evaluación, Monitoreo y Métricas de Impacto
- 14.6 Comunicación pública y rendición de cuentas en ciberseguridad
- Proyecto Final Integrador: Presentación ante panel de expertos

Objetivos de Aprendizaje

26. Diseñar políticas públicas integrales en cibercriminología y ciberseguridad.
27. Aplicar metodologías de formulación e implementación de estrategias nacionales.

28. Evaluar capacidades institucionales y brechas de seguridad.
29. Desarrollar métricas e indicadores de seguimiento de políticas.
30. Presentar y defender propuestas ante actores institucionales y académicos.

Recursos y Materiales

- Marcos estratégicos nacionales (España, México, Colombia, UE)
- Herramientas de diseño de políticas públicas (OCDE, BID)
- Rúbricas y plantillas para el proyecto final
- Panel de expertos externos evaluadores

Metodología de Enseñanza

El diplomado adopta una metodología activa, combinando los siguientes enfoques pedagógicos:

Clases magistrales online (sincrónicas)	Exposición de contenidos por docentes y expertos invitados con participación activa de los estudiantes.
Aprendizaje Basado en Casos (ABCs)	Análisis de casos reales anonimizados de cibercrimen internacional para aplicar los conocimientos teóricos.
Laboratorios y Simulaciones	Uso de entornos virtuales para practicar herramientas OSINT, análisis de metadatos y cadena de custodia.
Debates y Foros Académicos	Espacios estructurados de debate sobre dilemas éticos, jurídicos y estratégicos del ciberespacio.
Trabajo Colaborativo	Proyectos en equipo multidisciplinar que replican la dinámica real de equipos de ciberinvestigación.
Proyecto Final Integrador	Cada participante desarrollará un artículo científico susceptible de ser publicado en la revista institucional.

Sistema de Evaluación General

La evaluación del diplomado combina instrumentos formativos y sumativos distribuidos a lo largo del programa:

Instrumento de Evaluación	Peso (%)	Momento
Evaluaciones por módulo (6 × 100%)	**60%**	A lo largo del programa
Participación en foros y debates	**10%**	Continua
Proyecto Final Integrador	**25%**	Módulo 6 – Semana 24
Autoevaluación y coevaluación	**5%**	Al cierre de cada módulo

Nota mínima de aprobación: 70/100

Los participantes que aprueben todos los módulos y el Proyecto Final recibirán el Diploma en formación especializada en Cibercriminología y Seguridad Digital.

Requisitos de Egreso y Certificación

- Asistencia mínima del 75% a sesiones sincrónicas de cada módulo.
- Aprobación de todos los instrumentos de evaluación de los 6 módulos.
- Entrega del Articulo Cientifico.
- Cumplimiento del Reglamento Académico del Diplomado.

La certificación otorgada acredita al participante como especialista en Cibercriminología y Seguridad Digital, con competencias reconocidas para desempeñarse en investigación de cibercrimen, asesoría jurídica en materia digital, análisis de inteligencia cibernética y formulación de políticas públicas de seguridad digital.