UPATECO
UNIVERSIDAD PROVINCIAL
ADMINISTRACIÓN • TECNOLOGÍA • OFICIOS

Diplomatura en CIBERPATRULLAJE APLICADA A LA SEGURIDAD PÚBLICA E INVESTIGACIÓN PENAL

DENOMINACIÓN DEL PROYECTO:

"Diplomatura en Ciberpatrullaje, aplicada a la Seguridad Pública e Investigación penal"

1. CERTIFICACIÓN A OTORGAR:
"Diplomado/a en Ciberpatrullaje, aplicada a la Seguridad Pública e Investigación Penal"

2. DURACIÓN: 24 semanas (6 meses)

3. CARGA HORARIA:

- **Horas reloj totales:** 312, duración 6 meses (3oct25, al 31mzo26)

4. RESPONSABLE:

Lic. Emilio Tomás Albornoz, *"Responsable de Proyectos Formativos en Seguridad." UPATECO – Universidad Provincial de la Administración, Tecnología y Oficios*

5. FUNDAMENTACIÓN

a. **Necesidad de formación integral para múltiples actores en seguridad y justicia.** El creciente avance de las tecnologías digitales ha generado un entorno delictivo complejo que trasciende el ámbito exclusivo de las fuerzas policiales. Por ello, la demanda formativa incluye a un conjunto amplio de profesionales vinculados al combate del ciberdelito: agentes de fuerzas de seguridad, operadores judiciales, fiscales, abogados especializados, técnicos en informática forense y otros especialistas que intervienen en la prevención, persecución y abordaje legal de los delitos digitales. Esta diversidad de perfiles requiere una formación interdisciplinaria y actualizada que permita a todos los actores comprender las dinámicas del ciberespacio, aplicar herramientas técnicas y jurídicas, y coordinar acciones dentro del marco legal vigente. La diplomatura está diseñada para fortalecer las capacidades de estas diversas personas, asegurando una respuesta integral, colaborativa y eficaz frente a las amenazas digitales que impactan en la seguridad pública y la administración de justicia.
b. **Reforzamiento del trabajo articulado y colaboración interinstitucional.** En el actual contexto, si bien muchas instituciones desarrollan esfuerzos conjuntos para combatir el ciberdelito, persiste la necesidad de consolidar estas prácticas mediante la capacitación especializada que armonice protocolos, mejore el flujo de información y fomente estándares comunes interoperables, tanto a nivel local como federal. La diplomatura no solo facilita este proceso mediante una formación que integra aspectos técnicos, legales y estratégicos, sino que

también promueve la creación de redes profesionales interdisciplinarias, fortaleciendo la cooperación operativa y judicial que resulta imprescindible para enfrentar eficazmente las conductas delictivas en el ciberespacio y proteger los derechos fundamentales.

c. **Formación interdisciplinaria para actores diversos.** El fenómeno del ciberdelito involucra múltiples dimensiones (tecnológica, jurídica, criminológica, psicológica, social), por lo cual no puede ser abordado desde una sola disciplina o sector. El ciberpatrullaje, como práctica técnica y estratégica, exige la colaboración articulada entre agentes policiales, personal del sistema penitenciario, operadores judiciales, fiscales, técnicos en informática forense, analistas de inteligencia, analista en análisis criminal y profesionales en seguridad pública, seguridad privada. Por esta razón, la diplomatura ha sido concebida con una lógica formativa inclusiva, que incorpora saberes de distintas áreas del conocimiento para que todos los participantes —desde sus respectivos roles— puedan interpretar adecuadamente las dinámicas criminales en el entorno digital, articular procedimientos entre instituciones y operar con marcos comunes de referencia técnica y legal. Esta articulación fortalece no solo la eficacia en la prevención e investigación del delito, sino también la transparencia y el respeto por los derechos fundamentales.
d. **Ausencia de instancias formativas técnico-operativas especializadas.** A pesar de la creciente demanda de formación en temas relacionados con ciberdelito, OSINT, análisis digital y herramientas tecnológicas aplicadas, la mayoría de las propuestas disponibles en el país están orientadas al ámbito académico, jurídico o de ciberseguridad informática, con escasa atención a las necesidades concretas del personal operativo de seguridad pública y otros actores implicados en estas investigaciones. Esta situación genera una brecha entre los conocimientos teóricos y la práctica profesional cotidiana, donde los agentes y profesionales enfrentan situaciones reales que requieren respuestas rápidas, fundamentadas y técnicamente adecuadas. La presente diplomatura fue diseñada para cubrir ese vacío, brindando una formación aplicada, con foco en la operatividad, el análisis de casos reales, la utilización de herramientas OSINT, y el trabajo con laboratorios de simulación. Esto permite que los egresados se desempeñen con competencia técnica en su entorno laboral inmediato, garantizando así una respuesta efectiva y actualizada frente a la criminalidad digital.
e. **Evolución del delito organizado y reconfiguración de las redes criminales.** Las organizaciones criminales han adoptado con rapidez los recursos digitales para expandir sus actividades ilícitas: grooming, trata de personas, tráfico de estupefacientes, contrabando, fraudes financieros, captación de menores, acoso, extorsión y otros delitos complejos. Estas organizaciones utilizan métodos sofisticados para encubrir su identidad, dispersar la evidencia digital, operar desde jurisdicciones extranjeras o emplear monedas virtuales no rastreables. La respuesta estatal tradicional resulta insuficiente ante esta realidad. Por ello, es indispensable que las fuerzas de seguridad y los

operadores judiciales estén capacitados para intervenir en estos nuevos escenarios, comprender la lógica criminal en redes digitales y anticiparse con medidas preventivas y estrategias de detección temprana. Esta diplomatura contribuye a desarrollar una perspectiva criminológica actualizada sobre el uso del ciberespacio por parte de redes delictivas complejas, permitiendo a los profesionales diseñar y ejecutar intervenciones efectivas que fortalezcan la seguridad y justicia.

f. **Demanda creciente por parte de las instituciones de seguridad y justicia.** En los últimos años se ha incrementado significativamente la demanda institucional de capacitación en temas de ciberdelito, análisis de redes sociales, rastreo de criptoactivos, y metodologías OSINT. Esta necesidad surge tanto de las fuerzas policiales como de organismos judiciales y ministerios públicos, que identifican una creciente presencia de delitos cometidos a través de internet, así como la aparición de nuevas modalidades de criminalidad que requieren ser comprendidas desde una lógica digital. Esta diplomatura responde a esa demanda, articulando contenidos técnicos, legales y operativos, en una modalidad virtual que facilita el acceso federal, la autogestión del tiempo y la formación de equipos interdisciplinarios. Al mismo tiempo, se configura como una herramienta estratégica para promover la profesionalización sostenida y la actualización constante frente a un panorama criminal dinámico y en expansión.
g. **Transformación digital institucional y fortalecimiento organizacional.** Más allá de la capacitación individual, la diplomatura contribuye al proceso de transformación digital institucional, promoviendo el desarrollo de protocolos, mejores prácticas y estrategias que fortalezcan la capacidad operativa y de investigación en las fuerzas de seguridad y órganos judiciales, promoviendo una cultura organizacional adaptada a la nueva realidad digital. Esta transformación implica incorporar nuevas tecnologías, metodologías de trabajo colaborativas y marcos normativos actualizados que permitan responder con agilidad y eficacia a las amenazas cibernéticas. De esta forma, el programa apoya no solo a los profesionales participantes sino que tiene un impacto positivo en la modernización integral del sistema de seguridad y justicia.

6. JUSTIFICACIÓN

a. **Demanda operativa real:** la diplomatura responde a la demanda real y creciente de personal de fuerzas de policial, fuerzas de seguridad, servicios penitenciarios y operadores judiciales que enfrentan delitos digitales para los cuales no poseen formación técnica y jurídica especializada.

b. **Vacíos formativos locales:** se busca cubrir los vacíos formativos existentes en la región, especialmente en la zona NOA y otras zonas, contribuyendo a equilibrar la capacidad institucional frente al ciberdelito**.**

c. **Aporte a la política pública:** el programa aporta a la construcción de políticas públicas integrales y protocolos estandarizados que regulan el ciberpatrullaje y la investigación digital.

d. **Flexibilidad andragógica:** la modalidad virtual y modular facilita el acceso a la capacitación, permitiendo la autogestión del tiempo, conciliación laboral y alcance federal.

e. **Transferencia inmediata de conocimientos:** la diplomatura garantiza la transferencia inmediata de conocimientos y habilidades aplicables en el entorno laboral, fortaleciendo la seguridad pública y la justicia en contextos digitales complejos.

7. OBJETIVOS

7.1. General:

Brindar una formación técnico-jurídica y operativa especializada en ciberpatrullaje, ciberinvestigación y análisis de delitos en entornos digitales, orientada a profesionales y agentes de fuerzas policiales, fuerzas de seguridad, ministerios públicos, poder judicial, abogados, técnicos informáticos y otros actores del sistema de seguridad y justicia, que les permita actuar con competencia profesional, ética y legal en la prevención, investigación y persecución del ciberdelito.

7.2. Específicos:

a. Desarrollar habilidades avanzadas para el uso de herramientas OSINT y técnicas de investigación en fuentes abiertas, redes sociales y entornos digitales complejos.

b. Capacitar en el reconocimiento y análisis de conductas delictivas digitales vinculadas a grooming, trata de personas, estafas, narcotráfico, contrabando y otros fenómenos emergentes.

c. Actualizar sobre el marco legal nacional e internacional que regula el ciberpatrullaje, la cadena de custodia y la admisibilidad de evidencia digital.

d. Formar en el manejo de software libre y profesional para análisis forense, rastreo de criptoactivos y navegación segura en Deep Web y Dark Web.

e. Promover la articulación interinstitucional entre áreas policiales, judiciales y fiscales para un abordaje integral y coordinado del delito digital.

f. Desarrollar capacidades para el diseño y ejecución de acciones operativas y estrategias preventivas en ciberpatrullaje, con enfoque en gestión del riesgo y anticipación.

g. Fortalecer competencias para la elaboración, ejecución y evaluación de planes de intervención y monitoreo digital, basados en procedimientos estandarizados y evidencias verificables

8. MÓDULOS

MÓD	NOMBRE DEL MÓDULO	DURACIÓN	HS RELOJ SEMANAL	TOTAL HS RELOJ	CONDICIÓN
1	**Conceptos, Contexto y Marco Legal del Ciberpatrullaje**: Delitos Digitales y Normativa Aplicada	Bimestre	5	40	Promocionable
2	**Técnicas OSINT y Herramientas Prácticas para Investigación en Fuentes Abiertas**	Trimestre	4	48	Promocionable
3	**Investigación Digital Avanzada**: Criptoactivos, Dark Web y Análisis Forense Básico	Semestre	3	72	Promocionable
4	**Coordinación Operativa Interinstitucional y Prácticas Éticas en Ciberpatrullaje**	Trimestre	4	48	Promocionable
5	**Laboratorio de Simulaciones Integradas y Análisis de Casos Reales**	Semestre	3	72	Promocionable
6	**Trabajo Final Integrador:** Proyecto Aplicado de Ciberpatrullaje	Bimestre	4	32	Certificable
			Total de horas reloj de la Diplomatura:	**312**	

9. CONTENIDOS

MÓDULO 1: Conceptos, Contexto y Marco Legal del Ciberpatrullaje: Delitos Digitales y Normativa Aplicada

a. **Síntesis explicativa**. Este módulo brinda una base fundamental para comprender el ciberpatrullaje desde una perspectiva integral que combina el análisis del ciberespacio, las principales tipologías delictivas digitales y el marco legal vigente que regula la actuación en este ámbito. Se procura que los participantes logren interiorizar la complejidad del entorno digital como espacio social y delictual, distingan las características de los delitos emergentes y comprendan el contexto normativo y ético aplicable a la investigación y prevención. Este conocimiento es esencial para que profesionales de fuerzas policiales, fiscales, judiciales, técnicos e informáticos puedan actuar con rigor, eficiencia y respeto a los derechos humanos en la gestión y abordaje de incidentes en entornos digitales.

b. Contenidos

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
1	Introducción al ciberespacio: definición, evolución histórica de Internet; arquitectura y capas (Web superficial, Deep Web, Dark Web). Características y funciones principales.	Foro presentación con consignas sobre percepción personal del ciberespacio; cuestionario diagnóstico inicial sobre conceptos básicos, con feedback devolutivo.
2	Actores en el ciberespacio: usuarios legítimos e ilegítimos; ciberdelincuentes y colectivos delictivos; análisis de roles y motivaciones.	Lectura guiada de material oficial; elaboración individual de mapa conceptual sobre actores en el ciberespacio.
3	Conceptualización del ciberdelito: definición, características, clasificación; delitos tradicionales y emergentes; ciberdelito transnacional.	Foro de discusión sobre casos emblemáticos; elaboración colaborativa de un documento resumen de las tipologías delictivas digitales.
4	Tipologías delictivas digitales: estafas, grooming, trata, ciberacoso, fraudes informáticos, delitos asociados a criptoactivos; análisis de impacto local, nacional e internacional.	Estudio de caso práctico; cuestionario temático sobre tipos de delitos digitales, con feedback devolutivo.
Parcial 1	Evaluación parcial 1: abarca semanas 1 a 4.	Evaluación en línea a través de cuestionarios integrados y participación en foros evaluativos.
5	Introducción al ciberpatrullaje: definición, objetivos, tipos (preventivo, reactivo, proactivo); diferencias entre monitoreo en fuentes abiertas y técnicas encubiertas.	Análisis y desarrollo grupal de un caso de patrullaje OSINT; entrega de conclusiones preliminares en foro. Con feedback devolutivo.
6	Valor estratégico del ciberpatrullaje: importancia en seguridad pública y justicia; vinculación con investigación preventiva y operativa; desafíos operativos.	Foro de debate sobre relevancia del ciberpatrullaje en la actualidad; lectura y reflexión crítica. Con feedback devolutivo.
7	Marco jurídico nacional: Constitución Nacional y derechos fundamentales en entornos digitales; Ley de Protección de Datos Personales; legislación penal y procesal aplicable al ciberdelito.	Elaboración de cuadro comparativo sobre normativas; participación en foro temático sobre derechos digitales y legales.

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
8	Ética y procedimiento en ciberpatrullaje: principios éticos (proporcionalidad, razonabilidad, respeto a derechos humanos); cadena de custodia digital y protocolos para preservación y presentación de evidencias digitales; introducción a normativas internacionales básicas.	Simulación de redacción de acta para cadena de custodia digital; ensayo breve reflexivo sobre dilemas éticos; evaluación online parcial 2. Con feedback devolutivo.
Parcial 2	Evaluación parcial 2: abarca semanas 5 a 8.	Evaluación en línea integradora con preguntas de análisis normativo, ético y operacional; revisión participativa de actividades entregadas.

c. Competencias sugeridas. Este módulo propicia que los participantes adquieran una comprensión sólida del ciberespacio y sus dinámicas delictivas, en combinación con un marco legal y ético actualizado, fortaleciendo así la capacidad crítica y operacional para abordar eficazmente situaciones en ámbitos digitales. La adquisición de estas competencias es clave para consolidar la base conceptual y normativa que sustentará la aplicación práctica y estratégica en etapas posteriores de la diplomatura, fomentando una actuación profesional, ética y ajustada a la legalidad.

Objetivos de Aprendizaje	Competencias Esperadas	Instrumentos de Evaluación
• Comprender la estructura y características del ciberespacio como entorno	• Reconoce las distintas capas del ciberespacio y roles de actores que intervienen en él	• Cuestionarios interactivos y participación en foros
• Comprender las tipologías y características del ciberdelito	• Identifica y clasifica los principales delitos digitales y su impacto en la seguridad pública	• Mapa conceptual colaborativo y evaluaciones escritas
• Conocer los fundamentos, alcance y modalidades del ciberpatrullaje	• Analiza y distingue tipos de patrullaje digital y su aplicación práctica en contextos reales	• Análisis de casos prácticos y entrega de planes
• Comprender el marco legal vigente y los límites éticos en ciberpatrullaje	• Aplica principios legales, éticos y normativos en investigaciones digitales y preservación de evidencia	• Debate, ensayo reflexivo y actividades prácticas

d. Bibliografía de referencia.

1. Archivo Amarillo. Cada Capa de INTERNET. 2025. https://youtu.be/8CwHN-10wSs
2. INCIBE. 2024. Episodio 1: Ciberdelincuencia - En clave segura. https://youtu.be/ldHK9BF6ND0
3. Ministerio de Seguridad de la Nación. (2024). *Resolución 428/2024 sobre ciberpatrullaje en fuentes abiertas*. URL https://www.boletinoficial.gob.ar/detalleAviso/primera/294737/20240402
4. CELS-Centro de estudios Legales y Sociales. Sobre el Proyecto de Protocolo de Ciberpatrullaje". Año 2020. Disponible https://www.cels.org.ar/web/wp-content/uploads/2020/04/CELS-sobre-protocolo-ciberpatrullaje.pdf
5. Video "Ciberpatrullaje y su Marco Constitucional" — Charla del abogado constitucionalista Oscar Blando (2025). Disponible https://www.youtube.com/watch?v=0u0jgjM7zfY
6. Guía Oficial con marco normativo, tipologías de ciberdelitos y lineamientos vigentes para seguridad pública. Año 2023. Disponible https://www.mseg.gba.gov.ar/areas/Vucetich/MANUALES%20DE%20MATERIAS%202022/MANUAL%20Cibercrimen%20y%20delitos%20informáticos.pdf
7. Moconomy - Economía y finanzas. La verdad sobre la ciberseguridad | Documental gratuito. 2024. https://youtu.be/3FVG_1kNBXA
8. Jhonsec IT. 2025. Conceptos básicos de Ciberseguridad | Ciberseguridad desde cero. https://youtu.be/poPWzt75a8c
9. Cjfasociados. Ciberseguridad al límite ¿sabrías reconocer un caso de grooming o un intento de phishing?. 2025. https://youtu.be/CNHaJRSsbR4
10. FIAP. ¿Qué es … ciberpatrullaje?. https://youtu.be/0fXVnfYtJSA
11. RevistaSemana. ¿Qué es el ciberpatrullaje?. https://youtu.be/Etmp9UM9_OE
12. Fundación Vía Libre. No es ciberpatrullaje, es inteligencia. https://youtu.be/V1tv2_tsEVU
13. ADC - Asociación por los Derechos Civiles. Webinar: "Ciberpatrullaje: Seguridad y privacidad". https://youtu.be/bXT5_HBHyH4
14. Viejo Libertario. ECONOMISTA LIBERAL ANUNCIÓ LAS MAYORES MEDIDAS DE MILEI POST ELECCIONES. 2025. https://youtu.be/BS1hylPTBCs

MÓDULO 2: Técnicas OSINT y Herramientas Prácticas para investigación en Fuentes Abiertas

a. Síntesis explicativa: este módulo capacita a los participantes en el manejo integral y práctico de técnicas OSINT (Open Source Intelligence) para la búsqueda, recolección, análisis y validación de información disponible en fuentes abiertas. Se enfatiza el aprendizaje y dominio de herramientas gratuitas y profesionales para monitorear redes sociales, blogs, foros y plataformas digitales, con un enfoque aplicado a la prevención, detección y análisis del ciberdelito. El objetivo es que los estudiantes desarrollen habilidades para construir productos de investigaciónes útiles y confiables que aporten a la seguridad pública y procesos judiciales, integrando aspectos técnicos, éticos y legales en el uso de fuentes abiertas.

b. Contenidos

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
1	Introducción a OSINT: Concepto, evolución y aplicaciones; marco legal en el uso de fuentes abiertas; fases del ciclo	Cuestionario sobre ciclo OSINT; foro de discusión inicial sobre

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
	OSINT: definición de objetivos, planificación, recolección, análisis y difusión.	aplicaciones prácticas y legales en OSINT.
2	Herramientas básicas de recolección OSINT: buscadores avanzados, metadatos, análisis de dominios y direcciones IP, verificación de fuentes; automatización básica de búsquedas.	Ejercicio práctico guiado con Google Dorks; entrega de pasos y resultados en foro; retroalimentación grupal. Con feedback devolutivo del formador.
3	Análisis de redes sociales para inteligencia: identificación y análisis de perfiles, detección de perfiles falsos, seguimiento de hashtags, minería de datos en Facebook, Instagram, TikTok, Telegram, X y foros.	Elaboración de informe grupal sobre perfiles sospechosos detectados; análisis crítico con evidencias.
4	Técnicas de integración y análisis correlacional de datos OSINT: construcción de mapas de vínculos y redes, identificación de patrones; uso básico de plataformas como Maltego CE y SpiderFoot.	Taller de construcción de mapas y redes con Maltego CE; entrega de gráficos y reportes de análisis. Con feedback devolutivo del formador.
5	Validación y corroboración de información: técnicas de verificación cruzada, análisis crítico de fuentes, resguardo de la calidad de la información.	Análisis y corrección de casos prácticos de verificación; presentación de resultados en foro.
6	Elaboración y presentación de productos de investigación OSINT: formatos estándar, documentación y reporte; aspectos legales y éticos en presentación de informes.	Redacción y entrega de reporte OSINT de investigación guiada; autoevaluación y con feedback devolutivo del formador.
Parcial 1	Evaluación parcial 1: abarca semanas 1 a 6.	Prueba en línea tipo test y entrega de informe integrado; participación en foro evaluativo.
7	Herramientas OSINT avanzadas: automatización de búsquedas con software como SpiderFoot, recon-ng, Shodan; correlación y análisis de información automatizada.	Taller práctico con SpiderFoot y Shodan; entrega de capturas y análisis; discusión grupal.
8	Técnicas avanzadas en análisis de redes sociales y plataformas digitales: minería de datos con Maltego avanzado, análisis profundo de vínculos y comunidades digitales.	Ejercicios avanzados con Maltego CE; informe detallado sobre comunidades digitales y sus relaciones.
9	Validación avanzada y gestión de riesgos: detección de desinformación, manejo de	Análisis de casos complejos de desinformación; elaboración de

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
	información sensible y riesgo operativo en la recolección y análisis de datos.	estrategias para mitigación; debate virtual.
10	Integración de OSINT en operativos de ciberpatrullaje: aplicación práctica en casos reales; coordinación con actores operativos y judiciales; presentación de resultados.	Simulación grupal de operación OSINT; entrega de producto final con análisis y recomendaciones, feedback devolutivo del formador.
11	Ética, legalidad y privacidad en inteligencia de fuentes abiertas: límites éticos, responsabilidad profesional, privacidad y derechos humanos en la recolección de información.	Ensayo reflexivo sobre dilemas éticos en OSINT; foro de debate con análisis crítico de casos reales.
12	Proyecto final práctico OSINT: diseño y ejecución de una investigación OSINT integral basada en un caso simulado o real, aplicando todas las técnicas, herramientas y criterios éticos y legales estudiados.	Entrega y presentación del proyecto final en plataforma; defensa oral sincrónica o asincrónica ante el formador.
Parcial 2	Evaluación parcial 2: abarca semanas 7 a 12.	Evaluación práctica integradora; revisión y retroalimentación del proyecto final; participación en foro reflexivo.

c. Competencias sugeridas. Este módulo impulsa el desarrollo de competencias técnicas, analíticas y éticas en la aplicación de OSINT, permitiendo a los participantes extraer, interpretar y validar información de fuentes abiertas con rigurosidad profesional. Las habilidades adquiridas son fundamentales para la generación de investigación confiable, que apoye la prevención e investigación del delito digital en un marco legal y respetuoso de derechos. El dominio de herramientas avanzadas y la comprensión crítica del contexto ético potencian la capacidad de respuesta frente a amenazas digitales crecientes.

Objetivos de Aprendizaje	Competencias Esperadas	Instrumentos de Evaluación
• Comprender y aplicar el ciclo OSINT en investigaciones de fuentes abiertas	• Implementa todas las fases del ciclo OSINT con comprensión técnica y legal	• Cuestionarios, trabajos prácticos y participación en foros
• Utilizar herramientas básicas y avanzadas de OSINT para recolección y análisis	• Domina el uso de software OSINT (Google Dorks, Maltego, SpiderFoot, Shodan) para obtener y analizar información	• Talleres prácticos con entregas, informes y análisis

Objetivos de Aprendizaje	Competencias Esperadas	Instrumentos de Evaluación
• Analizar y validar información en redes sociales y otras plataformas digitales	• Identifica perfiles sospechosos, verifica fuentes y mitiga riesgos de desinformación	• Informes grupales, mapas conceptuales y debates críticos
• Elaborar productos de investigación aplicables para seguridad y justicia	• Produce y presenta informes OSINT claros, documentados y fundamentados, respetando marco ético y legal	• Producción y defensa del proyecto final práctico del módulo; evaluaciones integradoras
• Aplicar principios éticos y legales en la gestión de inteligencia de fuentes abiertas	• Reconoce la importancia de la privacidad, ética y normativa en la recopilación y uso de datos	• Ensayos reflexivos y participación en foros sobre ética y legalidad

d. Bibliografía de referencia

1. Seisdedos, C., & Aguilera, V. (2021). Open Source INTelligence (OSINT): investigar personas e identidades en Internet. España. Disponible en: https://odint.net/libros-osint/ Estudio actualizado que adapta OSINT al contexto iberoamericano, incluyendo procesos, privacidad y herramientas específicas).
2. Seguridad Cero Academy. (2024). Curso OSINT Automático: Uso de SpiderFoot [Blog y tutorial]. Perú. Disponible en: https://academy.seguridadcero.com.pe/blog/osint-automatico-spiderfoot (Guía práctica y técnica sobre uso avanzado de SpiderFoot para la automatización de investigaciones OSINT).
3. TheGoodHacker. (2022). Maltego – Tutorial de inteligencia y reconocimiento en fuentes abiertas [Video]. España. Disponible en YouTube: https://youtu.be/tV33-2VNhj8 (Video didáctico para utilización efectiva de Maltego en análisis de redes y vínculos).
4. Iforense. (2017). Aplicación de OSINT en informática forense: herramientas y metodología. Disponible en: https://es.scribd.com/document/472880241/OSINT (Documentación especializada que vincula OSINT con análisis forense para la recolección y verificación de evidencia digital).
5. Rega. Spiderfoot (OSINT) introducción de redes y servicios. 2024. https://youtu.be/hr1StF-lu0I

MÓDULO 3: Investigación Digital Avanzada: Criptoactivos, Dark Web y Análisis Forense Básico

a. Síntesis explicativa: este módulo brinda una formación avanzada y aplicada en el análisis y rastreo de criptoactivos, la exploración y monitoreo de la Dark Web, y los fundamentos del análisis forense digital básico. Se abordan las tecnologías

blockchain, los mecanismos de anonimización en redes anónimas, y el uso de herramientas para la recolección, preservación y análisis de evidencias digitales. Los participantes desarrollarán competencias para investigar delitos complejos que emplean tecnologías avanzadas, con una visión integral que combina aspectos técnicos, legales y operativos, garantizando la validez jurídica y la ética profesional en cada actuación. La duración semestral permite una profundización progresiva con énfasis en ejercicios prácticos y casos reales, distribuida en dos parciales.

b. Contenidos

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
1	Introducción a criptoactivos: definición, tecnologías blockchain, concepto de ledger distribuido; tipos de criptomonedas (Bitcoin, Ethereum, Monero, etc.); usos lícitos e ilícitos en el contexto digital.	Infografía grupal sobre ecosistema blockchain y criptoactivos; cuestionario básico diagnóstico.
2	Funcionamiento de transacciones en blockchain: wallets, exchanges, direcciones; trazabilidad, técnicas de anonimización; riesgos asociados y regulaciones vigentes.	Ejercicio práctico de seguimiento de una transacción simple en blockchain utilizando exploradores públicos. Con feedback devolutivo del formador.
3	Herramientas y técnicas para análisis y rastreo de criptoactivos: introducción al uso de Chainalysis, CipherTrace y otras; análisis de patrones sospechosos; detección de flujos ilícitos.	Taller guiado sobre análisis de transacciones sospechosas con herramientas simuladas; entrega de reporte preliminar.
4	Arquitectura y características de la Dark Web y Deep Web: diferencias con la web superficial; redes anónimas (TOR, I2P); modelos y dinámicas criminales en estos espacios; riesgos y protocolos de seguridad para investigadores.	Exploración virtual controlada de la Dark Web (entorno simulado, sin acceso ilícito o interacción con delincuentes); foro de seguridad digital y aspectos éticos asociados. Con feedback devolutivo del formador.
5	Técnicas de monitoreo y patrullaje en la Dark Web: identificación de foros, marketplaces, y comunidades; inteligencia operativa en entornos anónimos; gestión de identidad e infiltración digital segura.	Estudio de caso sobre un foro delictivo en Dark Web; entrega de análisis de inteligencia y riesgo. Con feedback devolutivo del formador.
6	Preservación y cadena de custodia de evidencias digitales en entornos complejos: protocolos específicos para criptoactivos y Dark Web;	Simulación formal de cadena de custodia para evidencia digital capturada en entorno darknet; entrega de acta formal.

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
	documentación y admisibilidad en procesos judiciales.	
7	Introducción al análisis forense digital básico: principios, objetivos, tipos de evidencia digital; herramientas de adquisición y preservación.	Cuadro comparativo sobre tipos de evidencias digitales y técnicas forenses; cuestionario de conceptos básicos.
8	Herramientas forenses gratuitas y profesionales: Autopsy, FTK Imager, EnCase (visión general); uso básico para captura y análisis de datos en dispositivos electrónicos.	Taller práctico básico con Autopsy: análisis de imagen forense; entrega de informe parcial de hallazgos. Con feedback devolutivo del formador.
9	Análisis de metadatos en archivos digitales (documentos, imágenes, vídeos); técnicas de verificación y detección de manipulación.	Práctica de extracción y análisis de metadatos en archivos reales; presentación de resultados en foro. Con feedback devolutivo del formador.
10	Técnicas de análisis de logs y rastreo de actividades en sistemas operativos y redes; introducción al análisis de evidencias en dispositivos móviles. Redacción de Informes, contenidos y detalles.	Ejercicio guiado de análisis de logs con herramientas básicas; entrega de informe de correlación.
11	Elaboración de informes forenses digitales: estructura, validez jurídica, presentación de resultados técnicos de forma comprensible para audiencia no técnica. ***Taller de redacción técnica y narrativa forense integrado***.	***Redacción y revisión de informe forense***; simulación de presentación ante audiencia judicial. Con feedback devolutivo del formador.
12	Caso integrador parcial 1: investigación combinada de flujo de criptoactivos, análisis en Dark Web y peritaje básico forense en dispositivo; integración de hallazgos y elaboración de informe conjunto.	Presentación grupal del caso integrador; entrega de informe final con sustentación. Con feedback devolutivo del formador.
Parcial 1	Evaluación parcial 1: abarca semanas 1 a 12.	Evaluación teórico-práctica y presentación del caso integrador.
13	Herramientas avanzadas para rastreo y análisis de criptoactivos: análisis cruzado, inteligencia financiera, detección de evasión y lavado en blockchain.	Taller avanzado con Chainalysis (simulado); entrega de reportes sobre casos complejos. Con feedback devolutivo del formador.

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
14	Técnicas para anonimización, contraataques digitales y protección de la identidad en Dark Web; estrategias de infiltración y resguardo corporativo para investigadores.	Simulación de técnicas de anonimización y protección; foro de debate sobre riesgos y mitigación.
15	Aspectos legales internacionales y nacionales en investigación de criptoactivos y Dark Web (compliance, normativas, tratados).	Análisis documental y debate en foro sobre marco legal vigente y desafíos regulatorios.
16	Análisis forense avanzado: creación y manejo de imágenes forenses, recuperación de datos eliminados, análisis de fragmentos y artefactos digitales.	Práctica avanzada con Autopsy o FTK Imager; entrega de análisis detallado. Con feedback devolutivo del formador.
17	Análisis de datos de dispositivos móviles y aplicaciones: extracción, análisis y reportes básicos.	Taller de extracción y análisis de datos de dispositivo móvil (simulación).
18	Integración de sistemas OSINT con análisis forense y blockchain para investigaciones complejas; técnicas de correlación y análisis estratégico.	Estudio de caso con integración de tecnologías OSINT, forense y blockchain; reporte colaborativo.
19	Presentación de productos de investigación y evidencia forense digital ante tribunales: normativas y metodologías para la transmisión clara y comprensible.	Simulación de audiencia judicial; presentación oral y defensa de informe técnico. Con feedback devolutivo del formador.
20	Identificación y gestión de riesgos éticos en investigación digital avanzada: análisis de normativas nacionales e internacionales de privacidad y protección de datos personales aplicables al entorno digital: principios rectores, derechos de los titulares y obligaciones de los operadores en ciberpatrullaje y procesamiento de información, con foco en la Ley 25.326 y equivalentes internacionales como GDPR.	Ensayo crítico y debate en foro sobre dilemas éticos; análisis de casos reales y simulados. Dilemas.
21	Buenas prácticas y protocolos de seguridad para investigadores digitales en ambientes complejos; prevención de riesgos operativos.	Elaboración de protocolo de seguridad personal y operativo; foro de revisión crítica.

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
22	Taller integrador final: plan de investigación digital avanzada combinando análisis de criptoactivos, monitoreo Dark Web y análisis forense; roles, cronogramas y metodología.	Desarrollo grupal y entrega de plan de investigación; feedback del formador.
23	Ejecución simulada del plan integrador con levantamiento, análisis y reporte de evidencias digitales.	Simulación en plataforma Moodle y Zoom; entrega de resultados y registro de actividades.
24	Revisión y presentación final del proyecto integrador; feedback y cierre del módulo con análisis de lecciones aprendidas.	Presentación sincrónica del informe final; evaluación integradora; foro de cierre y autoevaluación.
Parcial 2	Evaluación parcial 2: abarca semanas 13 a 24.	Evaluación práctica y presentación integradora del proyecto final.

c. Competencias sugeridas. Este módulo busca que los participantes desarrollen competencias especializadas para investigar delitos digitales complejos que involucran tecnologías avanzadas como criptoactivos y redes anónimas. Al dominar técnicas de análisis forense básico junto con herramientas para rastrear transacciones digitales y monitorear la Dark Web, los cursantes estarán capacitados para aportar pruebas jurídicas sólidas y realizar investigaciones integrales y éticas. La formación prolongada permite integrar conocimientos técnicos, legales y operativos para una respuesta profesional y efectiva frente a la criminalidad digital sofisticada.

Objetivos de Aprendizaje	Competencias Esperadas	Instrumentos de Evaluación
• Comprender funcionamiento y usos de criptoactivos y blockchain	• Explica y analiza flujos y transacciones en entornos blockchain, identificando usos ilícitos y legales.	• Infografías, reportes prácticos y cuestionarios.
• Aplicar técnicas para rastreo y análisis de transacciones digitales	• Usa herramientas técnicas para seguimiento y análisis de criptotransacciones y patrones sospechosos.	• Talleres, análisis de casos y reportes con herramientas especializadas.
• Analizar y patrullar la Dark Web y redes anónimas	• Reconoce dinámicas criminales en la Dark Web y aplica técnicas seguras de monitoreo e infiltración.	• Simulaciones, foros de discusión, y trabajos prácticos.

Objetivos de Aprendizaje	Competencias Esperadas	Instrumentos de Evaluación
• Implementar análisis forense digital básico en dispositivos y archivos	• Realiza adquisición, preservación y análisis de pruebas digitales manejando software forense básico.	• Talleres prácticos, elaboración de informes y presentaciones.
• Elaborar informes técnico-legales para presentación en procesos judiciales	• Redacta informes forenses comprensibles y válidos jurídicamente para audiencias técnicas y no técnicas.	• Informes escritos, simposios técnicos y simulaciones orales.
• Integrar conocimientos técnicos con aspectos éticos y legales para investigaciones sólidas	• Aplica principios éticos y legales en investigaciones, respetando derechos y normas, y asegurando la cadena de custodia.	• Ensayos reflexivos, debates y evaluaciones integradas.

d. Bibliografía de referencia

1. Balthasar, T. (2022). Blockchain Forensics: Detecting Illicit Financial Flows (Edición en español). Manual técnico sobre rastreo de criptoactivos en investigaciones criminales, adaptado para hispanohablantes. Disponible para descarga gratuita en repositorios académicos o mediante solicitud institucional. (Puedo ayudarte a buscar repositorios específicos si lo deseas).
2. Secretos Prohibidos del Internet | Iceberg de la Dark Web. 2025. https://youtu.be/VXqsjo8dE-o
3. Horizon. Tecnología del futuro. La Internet Oscura | Dentro de la Dark Web. 2025. Diponible: https://youtu.be/RXLbH4aX0FM
4. Informática forense y más. 2023. Herramientas de Análisis Forense Digital: FTK Imager y Autopsy. https://youtu.be/zncyUGEn-_I
5. Redes Plus. 2024. Primeros pasos con FTK IMAGER - Análisis Forense Digital. https://youtu.be/6OUQcL_8XXA
6. Piensa luego siente. 2024. ¿Qué son los metadatos y como funcionan? https://youtu.be/ekjDI42OrNs
7. Los videos de ITSecure. Año 2024. La importancia de los logs en los sistemas de información. https://youtu.be/_xfvDpzehxw
8. Hackavis. Forense Digital Desde Cero: fundamentos y Casos Reales de Cibercrimen. 2025. https://youtu.be/2s9JyChjUnA
9. Duriva. 2023. ESTA ES LA IMPORTANCIA DE HACER UN ANÁLISIS FORENSE A UN DISPOSITIVO CELULAR. https://youtu.be/-qYQN5oBirM
   Hackavis. 2025. Autopsy Forense Digital: tutorial Completo Paso a Paso (Caso Real Incluido). https://youtu.be/gWclBdzBzDM
10. Hixec. 2023. Necesitas APRENDER ANONIMATO, DEEP WEB Y DARK WEB | Curso Ciberseguridad Y Privacidad. https://youtu.be/mgo1CRBaooo?t=80
11. Colabro. Blockchain y Derecho 11/10. Año 2023. https://youtu.be/_KI7Ag3Ca6E
12. ECFORENSICS. Peritaje y Seguridad Informática. El poder de la Investigación Abierta. 2025. https://youtu.be/um__o70fHQU

MÓDULO 4: Coordinación Operativa Interinstitucional y Prácticas Éticas en Ciberpatrullaje

a. Síntesis explicativa: este módulo aborda las habilidades y conocimientos necesarios para integrar y coordinar operaciones de ciberpatrullaje entre diferentes instituciones y organismos de seguridad, justicia y administración pública. Se profundiza en la planificación operativa, establecimiento de protocolos de comunicación seguros y eficientes, y en la aplicación rigurosa de principios éticos y legales para garantizar el respeto a derechos fundamentales y la correcta gestión de la evidencia digital. La formación está orientada a desarrollar capacidades para liderar o participar en equipos interdisciplinarios con enfoque colaborativo, asegurando que las prácticas de ciberpatrullaje se realicen dentro de marcos operativos integrados, efectivos y con alta responsabilidad social.

b. Contenidos

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
1	Introducción a la coordinación interinstitucional: actores clave en el sistema de seguridad y justicia; funciones y competencias; importancia del trabajo colaborativo y multidisciplinario.	Foro presentación y reflexión sobre experiencias previas en trabajo interinstitucional; cuestionario inicial.
2	Mecanismos y protocolos de intercambio de información: interoperabilidad tecnológica, seguridad en la transmisión, uso de canales cifrados y sistemas seguros.	Análisis de casos prácticos de intercambio seguro; simulación virtual de transmisión de información. Con feedback devolutivo del formador.
3	Planificación operativa de acciones conjuntas: definición de objetivos, roles, cronogramas y asignación de recursos; gestión de riesgos y toma de decisiones en equipo.	Elaboración grupal de un plan operativo simulado; entrega y retroalimentación en foro colaborativo.
4	Protocolos de actuación ética en ciberpatrullaje: lineamientos para garantizar proporcionalidad, privacidad, confidencialidad y respeto a derechos humanos.	Debate virtual sobre dilemas éticos con análisis de casos reales; redacción individual de reflexión ética. Con feedback devolutivo del formador.
5	Normativas y legislación aplicables a la coordinación operativa: cumplimiento de regulaciones, marco legal y sanciones por incumplimiento; análisis de jurisprudencia relevante.	Estudio de jurisprudencia y normativa; foro crítico sobre impacto legal en la actuación práctica.

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
6	Gestión de crisis y contingencias operativas: protocolos para incidentes imprevistos, comunicación de emergencias, y manejo de conflictos interinstitucionales.	Simulación de caso de crisis con roles interinstitucionales; evaluación formativa con feedback.
Parcial 1	Evaluación parcial 1: abarca semanas 1 a 6.	Evaluación en línea mediante cuestionarios, análisis de casos y participación en foros.
7	Prácticas avanzadas de coordinación: integración de equipos de diferentes agencias, planificación conjunta de operaciones y seguimiento de acciones.	Taller práctico de simulación de operación coordinada; entrega de informe y presentación en foro. Con feedback devolutivo del formador.
8	Sistemas de información compartida: plataformas colaborativas, bases de datos conjuntas y uso de tecnologías para intercambio ágil y seguro de información.	Ejercicio práctico con sistemas simulado de gestión compartida; reporte de experiencia y mejoras propuestas.
9	Evaluación y control de la calidad operativa: indicadores de desempeño, auditorías internas y monitoreo de resultados para mejora continua.	Desarrollo de indicadores para caso hipotético; evaluación grupal y discusión crítica.
10	Ética profesional en la gestión interinstitucional: responsabilidad, transparencia, rendición de cuentas y códigos de conducta aplicables en ciberpatrullaje.	Redacción y presentación de un código de ética aplicado a coordinadores y equipos multidisciplinarios.
11	Prevención de corrupción y manejo de conflictos de interés: identificación, políticas preventivas y protocolos de acción en entornos digitales y multidisciplinarios.	Debate y análisis de casos prácticos; elaboración de propuesta de políticas preventivas. Con feedback devolutivo del formador.
12	Proyecto integrador final: planificación completa de una operación de ciberpatrullaje con roles, protocolos, gestión ética y legal, y seguimiento post-operativo.	Presentación sincrónica grupal del proyecto; entrega de documentación integral; retroalimentación final.
Parcial 2	Evaluación parcial 2: abarca semanas 7 a 12.	Evaluación integradora incluyendo defensa del proyecto final, cuestionarios y participación en foro.

c. Competencias sugeridas. Este módulo busca desarrollar en los participantes habilidades para gestionar y coordinar eficazmente operaciones de ciberpatrullaje en entornos interinstitucionales, garantizando una actuación ética, legal y colaborativa. La capacidad para planificar, comunicar de forma segura, resolver conflictos y promover la transparencia es fundamental para el éxito de las acciones conjuntas y para reforzar la confianza en el sistema de seguridad pública y justicia. También se enfatiza la adopción de prácticas profesionales éticas y responsables que protejan derechos y legitimen las intervenciones digitales.

Objetivos de Aprendizaje	Competencias Esperadas	Instrumentos de Evaluación
• Comprender la estructura y actores de la coordinación	• Identifica y describe funciones y competencias de instituciones de seguridad y justicia en ciberpatrullaje	• Cuestionarios y participación en foros
• Aplicar protocolos y mecanismos seguros de comunicación	• Implementa prácticas seguras y eficientes para el intercambio interinstitucional de información	• Simulaciones y análisis de casos
• Diseñar y ejecutar planes operativos coordinados	• Elabora planes que integran roles, responsabilidades y gestión de riesgos en equipos multidisciplinarios	• Elaboración y presentación de planes operativos
• Aplicar principios éticos y legales en la coordinación	• Identifica y resuelve dilemas éticos y legales respetando derechos y normativa vigente	• Debates, ensayos reflexivos y evaluación de participación
• Gestionar crisis y conflictos interinstitucionales	• Ejecuta protocolos de gestión de crisis y maneja conflictos interinstitucionales con eficacia y ética	• Simulaciones grupales y evaluación formativa
• Implementar sistemas de evaluación y mejora continua	• Diseña indicadores y aplica auditorías internas para optimizar la calidad operativa	• Desarrollo de indicadores y participación en discusiones

d. Bibliografía de referencia

1. Ministerio Público Fiscal (2022). *Manual de coordinación interinstitucional en investigaciones digitales*. Disponible en sitio oficial institucional.
2. UNODC (2021). *Interagency Cooperation for Cybercrime Investigations*. Recuperado de https://www.unodc.org
3. INTERPOL (2022). *Best Practices for International Cooperation in Cybercrime*. Disponible en línea.
4. González, R. (2023). *Ética aplicada a la seguridad pública en entornos digitales*. Editorial Universitaria.

5. Profe Sang. Encriptación (Cifrado) Simétrica y Asimétrica. Expciación fácil. https://youtu.be/wDpqrasDmxM
6. Cámara Argentina de Comercio y Servicios. Arquitectura del comercio internacional digital: tecnologías,interoperabilidad,seguridad y confianza. 2025. https://youtu.be/d1b4syNsFl4
7. Red de Herramientas Entre Mujeres. #ClicSeguroEnRED 23 de Julio 2025. Protocolo del Defensor. El CiberPatrullaje. https://youtu.be/G6ACUIjkI1E

MÓDULO 5: Laboratorio de Simulaciones Integradas y Análisis de Casos Reales

a. Síntesis explicativa: este módulo tiene como objetivo consolidar los conocimientos y habilidades adquiridos en los módulos anteriores mediante la realización de simulaciones prácticas integradas y el análisis detallado de casos reales. Los participantes tendrán la oportunidad de aplicar técnicas de ciberpatrullaje, OSINT, análisis forense básico, rastreo de criptoactivos y coordinación interinstitucional en escenarios simulados que reproducen situaciones habituales y complejas en la investigación digital. Se enfatiza el desarrollo de competencias operativas, éticas, analíticas y de toma de decisiones, con una visión interdisciplinaria y colaborativa, buscando asegurar una transferencia directa de la formación al ámbito profesional.

b. Contenidos

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
1	Introducción al laboratorio: presentación de objetivos, metodología y recursos; roles y responsabilidades de los participantes; normas de seguridad y confidencialidad digital.	Sesión sincrónica de inducción + foro de presentación y compromiso de confidencialidad.
2	Diseño de escenarios de simulación: elaboración y análisis de casos adaptados a delitos digitales frecuentes (grooming, estafas, trata, narcotráfico digital). Actualización Tecnológica y tendencias emergentes.	Análisis grupal y propuesta de escenarios; entrega de plan de simulación. Con feedback devolutivo del formador.
3	Simulación 1: Ciberpatrullaje OSINT en redes sociales y fuentes abiertas; detección de perfiles falsos y vigilancia digital.	Ejecución práctica en entorno simulado; entrega de informe preliminar; retroalimentación del formador. Con feedback devolutivo del formador.
4	Simulación 2: análisis forense básico: adquisición y preservación de evidencia digital en dispositivos	Taller práctico de extracción y análisis de evidencias; entrega de

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
	electrónicos; aplicación de protocolos de cadena de custodia.	reporte forense parcial. Con feedback devolutivo del formador.
5	Simulación 3: rastreo y análisis de criptoactivos en operaciones ilícitas; uso de herramientas prácticas de seguimiento en blockchain.	Ejercicio guiado de mapeo y análisis de transacciones sospechosas; presentación de resultados.
6	Simulación 4: navegación y monitoreo seguro en la Dark Web; infiltración y recolección de información en entornos anónimos; manejo de riesgos operativos.	Simulación controlada en Dark Web; análisis de inteligencia y entrega de reporte. Con feedback devolutivo del formador.
Parcial 1	Evaluación parcial 1: integra las simulaciones y análisis realizados en semanas 1 a 6.	Evaluación práctica en línea: cuestionarios, entrega de informes y participación en foros de retroalimentación.
7	Coordinación operativa en equipos interinstitucionales: planificación, comunicación segura y gestión de información en escenarios simulados.	Ejercicio grupal de planificación coordinada; elaboración de protocolos de comunicación y seguridad; entrega de plan.
8	Simulación 5: investigación de casos complejos combinados (OSINT + Dark Web + análisis forense); integración de múltiples fuentes de evidencia y técnicas de análisis.	Desarrollo de caso complejo; entrega parcial de informe y discusión grupal.
9	Simulación 6: análisis de inteligencia digital para la toma de decisiones estratégicas y operativas; elaboración de planes de acción basados en resultados de simulación.	Taller de diseño de planes de intervención; presentación de estrategias defensivas y preventivas.
10	Simulación 7: redacción de Informes, contenidos y detalles. Presentación y defensa de informes técnicos y jurídicos ante audiencias simuladas; rol del analista y operadores en la exposición de pruebas digitales.	***Simulación de audiencia; presentación oral y defensa de informes;*** retroalimentación y evaluación formativa. Con feedback devolutivo del formador.
11	Evaluación y mejora continua: técnicas para la gestión de la calidad en investigaciones digitales; análisis crítico de las simulaciones realizadas; aprendizajes y ajustes para casos reales.	Análisis crítico y autoevaluación; entrega de informe integrador sobre mejoras y aprendizajes.

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
12	Cierre del primer trimestre: consolidación de competencias prácticas; revisión final y asesorías personalizadas para el parcial 2.	Tutorías individuales y grupales; sesiones Q&A; planificación del trabajo para segunda parte del módulo. Con feedback devolutivo del formador.
13	Simulación 8: nuevos escenarios y actualización tecnológica en ciberpatrullaje; análisis de casos emergentes y tendencias delictivas digitales.	Desarrollo de casos nuevos; entrega y discusión en foros sobre innovaciones y tendencias.
14	Simulación 9: integración avanzada de análisis OSINT y forense en ambientes complejos; coordinación con escenarios reales y ficticios.	Ejecución de investigación integrada; entrega de reportes combinados; retroalimentación detallada. Con feedback devolutivo del formador.
15	Simulación 10: manejo de crisis digitales y respuesta ante incidentes cibernéticos en entornos organizacionales; estrategias de mitigación y comunicación.	Ejercicio de crisis simulada; plan y presentación de respuesta; evaluación grupal.
16	Simulación 11: auditoría y control de procesos en investigaciones digitales; diseño de indicadores de desempeño y evaluación de calidad.	Desarrollo de indicadores; evaluación de procesos; reporte de auditoría simulada.
17	Simulación 12: entrenamiento en habilidades blandas para el trabajo interdisciplinario: comunicación efectiva, negociación y liderazgo en contextos de seguridad y justicia digital.	Taller de habilidades blandas; role-playing; entrega de reflexión personal y grupal.
18	Simulación 13: elaboración de protocolos operativos y éticos de intervención; actualización normativa y adaptación a cambios tecnológicos. Redacción de informes.	***Redacción colaborativa de protocolos***; foro para revisión y aprobación por pares. Con feedback devolutivo del formador.
19	Simulación 14: análisis integrador de caso complejo con enfoque interdisciplinario y multi-agencial; coordinación de recursos y manejo de información crítica.	Trabajo grupal complejo; presentación y retroalimentación detallada.
20	Simulación 15: presentación y defensa ante audiencias mixtas (judiciales y	Simulación de audiencia avanzada; exposición, preguntas y defensa de informes.

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
	operativas); manejo de interrogatorios y pruebas digitales.	
21	Evaluación de la gestión ética y profesional en las simulaciones: reflexión crítica, identificación de buenas prácticas y áreas de mejora.	Ensayo reflexivo; debate en foro; entrega de Con feedback devolutivo del formador. informe de autoevaluación.
22	Planificación y ejecución final de simulación integradora: consolidación de aprendizajes en caso de investigación digital completa. Redacción de Informes, contenidos y detalles	Simulación integradora final de módulo; ***entrega de informe global*** y presentación oral.
23	Presentación final del proyecto integrador: defensa frente a tribunal docente; feedback y recomendaciones para la práctica profesional.	Defensa sincrónica ante tribunal; participación en sesión de feedback.
24	Cierre del módulo: evaluación final integradora; autoevaluación y plan de desarrollo profesional continuo.	Evaluación integradora online; entrega de plan de desarrollo personal; foro de cierre y despedida.
Parcial 2	Evaluación parcial 2: abarca semanas 13 a 24.	Evaluación práctica integradora con entrega final de proyectos, presentaciones y participación en foros.

c. Competencias sugeridas. Este módulo se orienta a que los participantes apliquen de manera integrada y autónoma todas las técnicas, herramientas y conocimientos adquiridos en contextos simulados que reflejan la complejidad del ambiente profesional real. El desarrollo de competencias en análisis crítico, toma de decisiones, trabajo colaborativo y gestión ética garantiza que los estudiantes estén preparados para enfrentar situaciones diversas y complejas en la investigación digital, fortaleciendo su impacto profesional y la eficiencia institucional.

Objetivos de Aprendizaje	Competencias Esperadas	Instrumentos de Evaluación
• Aplicar técnicas integradas de investigación digital en escenarios simulados	• Ejecuta patrullajes, análisis forense, OSINT y rastreos en entornos controlados con rigor y precisión	• Evaluación continua en simulaciones y entrega de informes

Objetivos de Aprendizaje	Competencias Esperadas	Instrumentos de Evaluación
• Coordinar equipos multidisciplinarios en operaciones conjuntas	• Planifica y gestiona la colaboración interinstitucional eficiente y ética	• Informes grupales, simulaciones y debates
• Elaborar y presentar informes técnicos y jurídicos claros y documentados	• Redacta y defiende productos de inteligencia y peritajes comprensibles para audiencias judiciales y operativas	• Presentaciones orales, informes escritos y evaluaciones
• Analizar críticamente resultados de investigaciones simuladas y proponer mejoras	• Evalúa procesos, detecta errores u omisiones y recomienda acciones correctivas	• Autoevaluación, análisis crítico y debates grupales
• Aplicar principios éticos y legales en la conducción de investigaciones digitales	• Conduce actividades profesionales respetando derechos humanos, legalidad y buenas prácticas	• Ensayos reflexivos, análisis de casos y participación en foros

d. Bibliografía de referencia

1. UNIR- la universidad en internet. La práctica de la Informática Forense | UNIR OPENCLASS. https://youtu.be/VKVu3_SLqwM
2. ESCOBAR, RODOLFO. Interrogatorio a perito en informática forense. 2023. https://youtu.be/_znHlCY0cZQ
3. Hackavis. Forense Digital Desde Cero: Fundamentos y Casos Reales de Cibercrimen. 2024. https://youtu.be/2s9JyChjUnA
4. David Pereira. Secretos para detectar perfiles falsos en Redes Sociales. 2023. https://youtu.be/0Jd32fgarp0
5. Ciberseguridad Comprensible. Descubre su identidad secreta. #maltego #OSINT #investigacion . https://youtu.be/fwAwxvpaXpM
6. Laura García Prado. Cómo investigar y verificar con OSINT Datos en Facebook. Módulos 1 y 2. Año 2025. https://youtu.be/T_3xCaW0WGo
7. David Pereira. Descubre cómo recopilar toda la Información de Alguien. Año 2024. https://youtu.be/hEt0B5ugJIw
8. Cyberhill-Security. Forense de Criptomonedas: Herramientas y Técnicas para Rastrear Bitcoins a Través del Blockchain. 2023. https://youtu.be/vpr0l56apoA
9. The Wild Project. Entrando en la DARK WEB en directo con un HACKER (Mercados Ilegales, Sicarios, Secretos empresas...). 2025. https://youtu.be/dtbFPVxYhPk
10. Ciencia por la Verdad. Ciberseguridad: Del OSINT hasta la DarkWeb. 2024. https://youtu.be/8uqxcTf8GOM
11. María Aperador | Criminología y Ciberseguridad. El año de los CIBERATAQUES Tendencias en Ciberseguridad 2025. https://youtu.be/EKwJT7e0ILQ
12. IMMUNE Technology Institute. Webinar | De la Amenaza a la Acción: Taller de Gestión de Incidentes Cibernéticos. 2025. https://youtu.be/bMPCLPA3sKc

13. Ministerio Público Fiscal (2022). *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital. URL https://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf*
14. INTERPOL (2022). *Cybercrime Simulation Exercises: Best Practices Manual*. Disponible en línea. https://www.interpol.int/en
15. UNODC (2021). *Manual de prácticas simuladas para el combate al ciberdelito*. PDF disponible en: https://www.unodc.org
16. Ministerio Público Fiscal de Argentina (2023). *Guía de cadena de custodia digital y presentación de pruebas*.

MÓDULO 6: Trabajo Final Integrador: Proyecto Aplicado de Ciberpatrullaje

a. Síntesis explicativa: este módulo final tiene como objetivo principal que los participantes integren y apliquen de manera práctica todos los conocimientos, habilidades y competencias adquiridas a lo largo de la diplomatura, mediante la elaboración, desarrollo, presentación y defensa de un proyecto aplicado de ciberpatrullaje. El trabajo final debe evidenciar la capacidad de diseñar y ejecutar una estrategia o investigación integral en un caso real o simulado, combinando técnicas OSINT, análisis forense digital, rastreo de criptoactivos, monitoreo en redes sociales y coordinación interinstitucional, siempre bajo el marco legal y ético. El módulo propicia el trabajo colaborativo en grupos de hasta tres integrantes, el desarrollo de habilidades de comunicación profesional y argumentación fundamentada para la presentación ante jurado evaluador.

b. Contenidos

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
1	**Introducción al Trabajo Final Integrador** (TFI): objetivos, metodología y expectativas; presentación de criterios y formato de evaluación; orientación para la elección del tema y delimitación del problema.	Sesión sincrónica de inducción; foro de consultas e inquietudes; entrega de guías y rúbricas de evaluación del TFI.
2	**Diseño del proyecto**: formulación de objetivos específicos, selección de técnicas y herramientas aplicables; planificación de recursos y cronograma; definición de roles y responsabilidades en equipo.	Tutorías en grupos; foro para presentación de anteproyectos y retroalimentación colaborativa. Con feedback devolutivo del formador.

Semana	Contenidos a desarrollar	Actividad sugerida en Moodle
3	**Revisión y validación del diseño del proyecto**: ajustes metodológicos, identificación de posibles dificultades y estrategias para superarlas; normas para preservación de la cadena de custodia digital.	Entrega formal del anteproyecto; feedback personalizado por formadores; foro de discusión sobre mejoras y ajustes necesarios.
4	**Desarrollo inicial**: recopilación de información, aplicación de técnicas OSINT, inicio del análisis forense digital y monitoreo en fuentes abiertas; articulación con marcos legales y éticos.	Reuniones de seguimiento; entrega parcial de avances; actividades prácticas individuales y grupales con supervisión docente.
5	**Desarrollo avanzado**: integración de análisis de criptoactivos, rastreo en redes anónimas (Dark Web), análisis de perfiles digitales y coordinación interinstitucional según el caso abordado.	Talleres prácticos y ejercicios integradores; entrega de informes parciales; sesiones de asesoría técnica y jurídica.
6	**Consolidación del proyecto**: elaboración del informe final escrito, preparación de materiales complementarios (mapas, gráficos, reportes de evidencia) y diseño de la presentación en video.	Entrega del borrador final; retroalimentación para perfeccionamiento; taller de comunicación y producción audiovisual para la defensa. Con feedback devolutivo del formador.
7	**Preparación para la presentación y defensa**: coaching para exposición oral, manejo de preguntas, argumentación fundamentada; refinamiento de la síntesis y aspectos comunicativos del video.	Simulaciones de defensa grupal; revisión y ajustes finales; foro de intercambio de experiencias y recomendaciones.
8	**Presentación y defensa formal del TFI**: presentación en video grupal (hasta 3 integrantes) donde se expone y defiende el proyecto ante el jurado evaluador; foro de preguntas y respuestas; cierre y evaluaciones.	***Entrega del video; evaluación según rúbrica***; participación en sesión de defensa sincrónica o asincrónica; retroalimentación final. Con feedback devolutivo del formador.

c. Competencias sugeridas. Este módulo busca que los estudiantes integren y desplieguen de manera profesional y rigurosa todos los conocimientos y habilidades adquiridos durante la diplomatura. Se pretende que desarrollen competencias para planificar, ejecutar y presentar proyectos complejos de ciberpatrullaje, manejando aspectos técnicos, legales, éticos y comunicativos con alta calidad. Además, se fortalece la capacidad de trabajo colaborativo, síntesis y

defensa argumentativa, habilidades fundamentales para la práctica profesional en entornos interinstitucionales y judiciales.

Objetivos de Aprendizaje	Competencias Esperadas	Instrumentos de Evaluación
• Diseñar un proyecto integrador aplicando metodologías y técnicas aprendidas	• Formula un plan integral y articulado para un caso real o simulado de ciberpatrullaje	• Evaluación del anteproyecto y entregas parciales
• Desarrollar un análisis técnico y operativo que utilice herramientas OSINT, forenses y monitoreo	• Aplica técnicas combinadas con rigurosidad y creatividad para evidenciar e interpretar datos digitales	• Seguimiento y evaluación continua de avances y entregas
• Elaborar informe final y materiales de apoyo para la defensa profesional	• Redacta documentos claros, coherentes y fundamentados que respalden el proyecto	• Revisión del informe final y materiales audiovisuales
• Presentar y defender oralmente el proyecto con fundamentos técnicos y legales	• Expone y argumenta con claridad, demostrando dominio del tema y capacidad de respuesta a preguntas	• Evaluación de la presentación y defensa según rúbrica, ante el formador.
• Trabajar efectivamente en equipo colaborativo y multidisciplinario	• Coordina tareas, roles y trabajo grupal para alcanzar objetivos comunes con respeto y compromiso	• Observación de dinámica de grupo y evaluación del trabajo final

d. Bibliografía de referencia

1. Ministerio Público Fiscal (2022). *Guía para la elaboración y presentación de informes periciales digitales*. Disponible en sitio oficial institucional.
2. INTERPOL (2023). *Manual de diseño y evaluación de estrategias integradas de ciberpatrullaje*. Disponible en línea.
3. UNODC (2022). *Métodos y buenas prácticas para la investigación digital aplicada*. Recuperado de https://www.unodc.org
4. Video: “Cómo preparar y presentar un informe OSINT profesional”. Disponible en YouTube: https://youtu.be/8n0qpl44vTg
5. Martínez, S. (2023). *Ciberinteligencia aplicada: de la teoría a la práctica*. Editorial Académica.

10. Destinatario

La diplomatura está diseñada para profesionales y agentes que cuenten con título secundario completo y se desempeñen en:

- Fuerzas Policiales
- Fuerzas de Seguridad

- Servicio Penitenciario
- Poder Judicial
- Ministerios Públicos Fiscales
- Otras áreas vinculadas a la investigación criminal, seguridad pública, seguridad privada, actividad particular vinculada con los objetivos.

También podrán acceder personas externas a estas instituciones, siempre que acrediten la necesidad de formación en la temática, mediante:

- Entrevista previa, y/o
- Análisis de Currículum Vitae, y/o
- Carta de presentación institucional

La Universidad Provincial de la Administración, Tecnología y Oficios (UPATecO) se reserva el derecho de admisión, basado en criterios de pertinencia, trayectoria y adecuación del perfil del postulante al objetivo formativo de la diplomatura.

11. Requisitos de admisión

Para postularse a la diplomatura, los interesados deben cumplir con:

- Acreditación de título secundario completo o constancia de título en trámite.
- Presentar carta de presentación institucional, firmada por la autoridad competente, que certifique el desempeño laboral en áreas relacionadas (fuerzas policiales, de seguridad, servicio penitenciario, fiscalías, juzgados u organismos afines) o, en caso contrario, una nota personal justificando la necesidad formativa.
- Remitir fotocopia del DNI y fotografía digitalizada actualizada.

La Universidad se reserva el derecho de admisión conforme a la evaluación de estos requisitos y, en su caso, a una entrevista previa, todo ello conforme a cupo se fije oportunamente.

12. Perfil de los formadores

Módulo	Perfil del formador
01. **Conceptos, Contexto y Marco Legal del Ciberpatrullaje**: Delitos Digitales y Normativa Aplicada	Fiscal o auxiliar penal especializados; o Especialista en derecho penal digital o en criminología con experiencia en ciberpatrullaje, normativa digital y docencia.
02. Técnicas OSINT y Herramientas Prácticas para investigación en Fuentes Abiertas	Analista OSINT certificado o experto en inteligencia digital con experiencia práctica en uso de herramientas OSINT en investigaciones. Con experiencia actualizada.

Módulo	Perfil del formador
03. **Investigación Digital Avanzada**: Criptoactivos, Dark Web y Análisis Forense Básico	Especialista en blockchain, criptoactivos y análisis forense digital con trayectoria en investigación de delitos informáticos complejos, con experiencia actualizada
04. Coordinación Operativa Interinstitucional y Prácticas Éticas en Ciberpatrullaje	Profesional con experiencia en gestión y coordinación interinstitucional en seguridad pública o justicia, con conocimientos legales y éticos, vinculado a la temática.
05. Laboratorio de Simulaciones Integradas y Análisis de Casos Reales	Formador con experiencia en prácticas intensivas de simulación, evaluación de competencias digitales y manejo de entornos virtuales.
06. **Trabajo Final Integrador**: Proyecto Aplicado de Ciberpatrullaje	Coordinador académico o profesional senior con experiencia en metodologías de proyectos integradores y evaluación multidisciplinaria.

13. COMPETENCIAS ADQUIRIDAS

Al finalizar la Diplomatura, los estudiantes habrán desarrollado un conjunto integral de competencias técnicas, jurídicas, operativas y éticas, que les permitirán desempeñarse laboralmente con eficacia en el ámbito del ciberpatrullaje y la investigación digital aplicada a la seguridad pública y la justicia.

Conocimientos

- Comprenden el ciberespacio como entorno social, tecnológico y criminal, y las dinámicas específicas que en él se desarrollan.
- Reconocen las principales tipologías de ciberdelito, incluyendo fenómenos emergentes, así como la normativa nacional e internacional vigente y los procedimientos legales asociados.
- Dominan las bases y aplicaciones de herramientas OSINT, análisis forense digital y tecnologías emergentes como criptoactivos, Deep Web y Dark Web.

Habilidades generales y específicas

- Ejecutan ciberpatrullajes efectivos en fuentes abiertas y redes sociales utilizando herramientas OSINT (software de inteligencia de código abierto y profesional).
- Documentan y preservan adecuadamente evidencias digitales, asegurando el respeto de la cadena de custodia.
- Elaboran reportes e informes de inteligencia claros, fundamentados y adaptados a requerimientos judiciales y policiales.

- Integran técnicas avanzadas de análisis forense, rastreo de criptoactivos y monitoreo en ecosistemas digitales en operaciones interinstitucionales coordinadas.
- Aplican protocolos de coordinación operativa y respetan los límites éticos y legales en la gestión de investigaciones digitales.

Actitudes y valores

- Actúan con profesionalismo ético, respetando los derechos humanos y la intimidad en entornos digitales.
- Mantienen una actitud proactiva, colaborativa e interdisciplinaria, fomentando el trabajo en equipo y el intercambio de conocimientos.
- Valoran y promueven el aprendizaje continuo, la innovación tecnológica y la mejora permanente para afrontar los retos del ciberdelito.

14. METODOLOGÍA

14.1 Modalidad e-learning sincrónica y asincrónica. La Diplomatura se desarrolla en modalidad e-learning combinando:

- Encuentro semanal hibrida, combinado con clase grabadas y sincrónicos en vivo por plataforma Zoom, con actividades de intercambio, tutorías, debates y simulaciones.
- Actividad asincrónica en la plataforma educativa Moodle 5.0 (UPATecO), donde los estudiantes acceden a grabaciones, documentos, foros, cuestionarios y ejercicios prácticos.

Esta combinación permite:

- Alcance federal garantizado, con flexibilidad horaria adaptada a estudiantes activos profesionalmente.
- Acceso permanente y diferido al 100% del material audiovisual.
- Uso de recursos interactivos que favorecen la participación activa y la retroalimentación continua de formadores y tutores.
- Cuidado del bienestar laboral y personal, facilitando el estudio desde el lugar de residencia.

14.2 Modelo andragógico modular. El diseño curricular se basa en un modelo andragógico enfocado en adultos con carga laboral y responsabilidades:

- Modularidad: contenidos organizados en 6 módulos independientes, con posibilidad de cursarse consecutivamente o en bloques.
- Enfoque por competencias: cada módulo desarrolla conocimientos, habilidades y actitudes aplicables directamente al trabajo profesional en seguridad pública.
- Horizontalidad: fomentamos relaciones formador-estudiante basadas en el diálogo, la experiencia previa y la participación activa.
- Aprendizaje significativo: promovemos la reflexión crítica, el análisis contextualizado y la autogestión del proceso formativo.

14.3 Certificación por competencias

- Cada módulo cuenta con evaluaciones diseñadas para evidenciar el desarrollo de competencias técnicas, jurídicas, éticas y estratégicas.
- Las actividades incluyen laboratorios prácticos, elaboración de informes, ejercicios OSINT, simulaciones integradas y trabajos grupales.
- La acreditación final se obtiene tras la aprobación de todas las instancias y la defensa exitosa del Trabajo Final Integrador (TFI).

15. Autogestión.

El costo total de la Diplomatura será determinado por la Universidad Provincial de la Administración, Tecnología y Oficios (UPATecO) mediante Resolución Rectoral. Esta información se comunicará a los interesados durante los procesos de promoción e inscripción.

16. Evaluación y acreditación

Asistencia virtual:

- Se exige un mínimo del 60% de asistencia a clases sincrónicas a través de Zoom; igual o más revisión de clases grabadas disponibles en Moodle de los que no pudieron asistir, con trazabilidad en plataforma.

Trabajos Prácticos (TP):

- Para la aprobación de los módulos promocionales es obligatorio aprobar el 100% de los trabajos prácticos.
- En los módulos con condición certificable, se debe aprobar al menos el 60% de las actividades evaluativas.

Trabajo Final Integrador (TFI):

- Entrega de anteproyecto: individual o grupal (máximo tres estudiantes); se realizará a partir del último mes del primer bimestre y se presentará a través de la plataforma Moodle.
- Entrega y defensa del proyecto final: una vez aprobados todos los módulos, los estudiantes presentarán y defenderán mediante un video grabado, donde desarrollarán conforme rúbrica de evaluación, tiempo y demás condiciones del formador evaluador disponga su defensa de su TFI. Con el informe de aprobación del formador, el estudiante habrá cumplimentado las exigencias académicas necesaria para su certificación como Diplomado.
- La acreditación final de la Diplomatura se otorga al cumplir con todos los requisitos de asistencia, evaluaciones parciales, trabajos prácticos y defensa exitosa del TFI.

17. RÚBRICAS Y PONDERACIONES SUGERIDAS

17.1. Ponderación general:

- **Trabajos prácticos (TP):** 40%
- **Parciales (2):** 30% (15% cada uno)
- **Trabajo Final Integrador (TFI):** 30%

- **Asistencia mínima obligatoria:** requisito habilitante (no pondera, pero condiciona la regularidad).

17.2. Rúbrica para Trabajos Prácticos (TP) – 40%

	Promocionado		Certificable	Libre
Criterio	**Excelente (10-9)**	**Muy bueno/ Bueno (8-7)**	**Suficiente (6.99-6)**	**Insuficiente (<6)**
Comprensión conceptual	Domina conceptos y los aplica críticamente	Aplica conceptos, con leves imprecisiones	Identifica conceptos, pero con errores	Desconoce o confunde conceptos
Aplicación práctica	Resoluciones completas, creativas y ajustadas al caso	Resoluciones correctas, aunque estándar	Parcialmente correctas, faltan elementos clave	Inadecuadas o irrelevantes
Rigor metodológico	Uso de fuentes confiables, citación correcta, orden lógico	Fuentes adecuadas pero citación parcial	Fuentes limitadas, citación incompleta	Sin fuentes o metodológicamente inválido
Presentación y redacción	Clara, estructurada, sin errores	Clara, con algunos errores menores	Comprensible con dificultad, errores notables	Poco clara, desordenada o con errores graves

17.3. Rúbrica para Parciales (2x15%) – 30%

	PROMOCIONADO		Certificable	Libre
Criterio	**Excelente (10-9)**	**Muy bueno/ Bueno (8-7)**	**Suficiente (6.99-6)**	**Insuficiente (<6)**
Dominio de contenidos	Respuestas precisas, completas y argumentadas	Correctas con leves omisiones	Parcialmente correctas, con vacíos relevantes	Incorrectas o irrelevantes
Capacidad analítica	Relaciona marcos teóricos y casos prácticos	Relaciona parcialmente, con limitaciones	Escasa vinculación teoría–práctica	No logra relacionar teoría y práctica
Claridad y estructura	Muy clara, ordenada y coherente	Clara, con alguna desorganización	Comprensible con dificultad	Confusa, incoherente o ilegible

17.4. Rúbrica para Trabajo Final Integrador (TFI) – 30%

	Excelente (10-9)		Muy bueno/ Bueno (8-7)	Suficiente (6.99-6)
Criterio	**Excelente (10-9)**	**Muy bueno/ Bueno (8-7)**	**Suficiente (6.99-6)**	**Insuficiente (<6)**
Relevancia y pertinencia del tema	Tema original, altamente pertinente al campo	Tema pertinente, con menor originalidad	Tema básico, limitado en alcance	Tema poco pertinente o irrelevante

Metodología aplicada	Correcta, consistente, justificada	Correcta, con justificación parcial	Incompleta, justificación insuficiente	Inadecuada o ausente
Análisis crítico y aportes	Profundo, aporta soluciones o reflexiones novedosas	Correcto, con aportes limitados	Descriptivo más que analítico	Superficial, sin aporte real
Estructura y presentación escrita	Cumple normas académicas, impecable	Cumple en general, con fallas menores	Cumple parcialmente, errores frecuentes	No cumple normas, deficiente
Defensa oral	Sólida, clara, argumentada, responde preguntas con solvencia	Clara, responde con solvencia parcial	Responde con dificultad, discurso débil	No responde, exposición deficiente

18. Requisitos técnicos y privacidad

18.1. Requisitos técnicos mínimos para cursado:

- **Dispositivo:** PC o notebook con procesador mínimo i5 / Ryzen 3 o equivalente, 8 GB RAM, disco SSD recomendado.
- **Conectividad:** Internet estable ≥ 10 Mbps de bajada y 2 Mbps de subida.
- **Software:**
  - ✓ Navegador actualizado (Chrome, Firefox, Edge).
  - ✓ Paquete ofimático (LibreOffice/MS Office).
  - ✓ Acceso a Moodle (plataforma de cursado) y Zoom (clases sincrónicas).
  - ✓ Antivirus actualizado.
- **Periféricos:** Cámara web y micrófono funcionales para clases y defensa del TFI.
- **Almacenamiento:** Al menos 5 GB libres para descargas de materiales/datasets.

18.2. Política de grabaciones (Zoom/Moodle)

- Todas las clases sincrónicas se graban y se suben a Moodle en un plazo de 48 h.
- El acceso es exclusivo para estudiantes inscriptos, no transferible.
- Está prohibida la descarga, reproducción o difusión no autorizada de las grabaciones.
- Las grabaciones se mantienen disponibles hasta 60 días posteriores a la finalización de la cursada.

18.3. Privacidad y tratamiento de datos (Ley 25.326)

- Los datos personales de los alumnos se recolectan con fines estrictamente académicos y administrativos.
- Se garantiza:
  - ✓ **Confidencialidad** de la información.
  - ✓ **Acceso restringido** solo a personal docente/administrativo.

- ✓ **Derecho de acceso, rectificación y supresión** de los datos por parte del estudiante.
- ✓ Eliminación de los datos sensibles y grabaciones transcurridos los plazos académicos y legales.

- En las prácticas y TP se utilizan **datasets sintéticos** o datos públicos, evitando exposición de información personal real.

19. RECURSOS

- Plataformas tecnológicas: Moodle 5.0 para gestión académica y Zoom ilimitado versión 6.4.12 para clases sincrónicas, con soporte técnico institucional permanente.
- Material didáctico: bibliografía digitalizada, guías de práctica, grabaciones de clases, foros participativos, cuestionarios y recursos multimedia especializados.
- Tutorías y gestión pedagógica: acompañamiento constante para resolver dudas, asesorías personalizadas y coordinación de actividades académicas.
- Equipo docente especializado: formadores con experiencia en cibercrimen, derecho penal digital, OSINT, análisis forense y coordinación interinstitucional, contratados mediante convenio de servicio institucional.

20. EVALUACIÓN DE IMPLEMENTACIÓN Y RESULTADOS. Se establece un sistema integral de evaluación continua en cuatro niveles, garantizando la calidad y pertinencia de la Diplomatura:

A. Evaluación del proceso de aprendizaje:

- Calidad y atención del servicio brindado por tutores y formadores.
- Actualización y relevancia de contenidos, materiales y recursos.
- Efectividad y pertinencia de las actividades, trabajos prácticos y evaluaciones.

B. Evaluación curricular:

- Cumplimiento y coherencia con los objetivos y competencias previstas en el plan.
- Ajuste y adecuación de módulos y contenidos a los perfiles profesionales de egreso.

C. Evaluación tecnológica:

- Accesibilidad, funcionalidad y estabilidad de la plataforma Moodle.
- Competencias TIC de estudiantes y formadores para el uso eficiente de las herramientas digitales.
- Satisfacción con las plataformas de videoconferencia y soporte técnico.

D. Evaluación de impacto:

- Aplicación efectiva de los conocimientos y competencias adquiridos en el ejercicio laboral.
- Aporte tangible al fortalecimiento del servicio público o institucional en materia de seguridad digital.

- Identificación y planificación de futuras necesidades de actualización, innovación o ajuste del plan formativo.

Los resultados de estos procesos se utilizarán para la mejora continua de la Diplomatura.

21. ANTECEDENTES CONSULTADOS

- Interpol. (2022). *Cybercrime simulation exercises: Best practices manual*. INTERPOL.
- Ministerio de Seguridad de la Nación. (2024, 28 de mayo). *Resolución n.° 428/2024 sobre ciberpatrullaje en fuentes abiertas*. Boletín Oficial de la República Argentina.
- Naciones Unidas Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2020). *Manual sobre la investigación de delitos cibernéticos*.
- Naciones Unidas Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2021). *Manual de pruebas electrónicas para fiscales*.
- Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). *Conceptualizing Cybercrime: Definitions, typologies and taxonomies*. Forensic Sciences, 2(2), 379–398.
- Europol. (2022). *Cryptocurrencies and crime: Investigations and prevention*.
- Chainalysis. (2023). *Crypto Crime Report*. Chainalysis Blog.
- Ministerio Público Fiscal de Argentina. (2022). *Guía de coordinación interinstitucional en investigaciones digitales*.
- Diario Judicial. (2024). *Ciberpatrullaje para la seguridad: nuevas directivas (Resolución 428/2024)*.
- Camacho, L. (2024). *Ciberpatrullaje en Argentina: análisis crítico de la Resolución 428/2024*. Observatorio Legislativo CELE.
- Otros.