UPATECO
UNIVERSIDAD PROVINCIAL
ADMINISTRACIÓN • TECNOLOGÍA • OFICIOS

Diplomatura Universitaria en INFORMÁTICA FORENSE Y CIBERSEGURIDAD

“Diplomatura Universitaria en Informática Forense y Ciberseguridad”

1. CERTIFICACIÓN A OTORGAR:
“Diplomado/a Universitario/a en Informática Forense y Ciberseguridad”

2. DURACIÓN: 24 semanas (6 meses)

3. CARGA HORARIA:

- **Horas reloj totales:** 240, duración 6 meses.

4. RESPONSABLE: Académico / Responsable de la Gestión Integral de la Diplomatura:
Lic. Prof. Emilio Tomás Albornoz. Responsable del diseño de planificación general, coordinación institucional, supervisión académica, seguimiento del desarrollo curricular y articulación con las políticas académicas de la institución.

- ✓ **Coordinador de Contenidos y Desarrollo Curricular: Prto. Tec. Marcelo Rubén Romero.** Facilita a la actualización y coherencia de los contenidos formativos y acompañamiento del cuerpo de formadores.
- ✓ **Tutor:** tendrá a cargo la diseño, adminsitración y puesta a punto de los sistemas de la UPATecO para el desarrollo de la diplomatura, autogestión, gestión, Zoop, Moodle, soporte de comunicación centralizada con alumnos, otras.
- ✓ **Equipo formador:** Integrado por profesionales especializados en Informática Forense, Ciberseguridad, Derecho Digital, Redes, Sistemas, Análisis de Incidentes y disciplinas afines, con formación académica y experiencia profesional acreditable en los campos vinculados a la presente diplomatura.

5. FUNDAMENTACIÓN
a. Transformación del entorno digital y aumento del riesgo cibernético
El crecimiento sostenido de la digitalización en los ámbitos públicos y privados ha ampliado significativamente la superficie de exposición a riesgos tecnológicos. Las organizaciones enfrentan amenazas cada vez más complejas, como ransomware, ataques distribuidos, filtración de datos e intrusiones persistentes. Este escenario exige profesionales capaces no solo de prevenir incidentes, sino también de analizarlos, comprender su origen y actuar de manera técnica y fundamentada frente a eventos de seguridad.
b. Crecimiento del cibercrimen y necesidad de capacidades forenses
El cibercrimen se ha consolidado como una problemática estructural que impacta tanto a instituciones como a individuos. Fraudes digitales, accesos indebidos, delitos contra la integridad de las personas y ataques a infraestructuras críticas requieren de abordajes especializados. En este contexto, la informática forense

adquiere un rol central, permitiendo la identificación, preservación y análisis de evidencia digital conforme a metodologías válidas y reconocidas, contribuyendo tanto a la investigación como a la toma de decisiones.

c. Necesidad de articulación entre lo técnico y lo legal

La intervención en incidentes de seguridad y en procesos de investigación digital implica comprender no solo los aspectos técnicos, sino también el marco legal que regula la obtención y tratamiento de la evidencia. En Argentina, normativas como la Ley de Protección de Datos Personales y la legislación sobre delitos informáticos establecen límites y condiciones que deben ser respetados. Por ello, resulta fundamental formar profesionales capaces de actuar con criterio técnico y respaldo jurídico, garantizando la validez de sus intervenciones.

d. Brecha de formación especializada en informática forense y ciberseguridad aplicada

A pesar del aumento de la demanda, la oferta formativa existente presenta, en muchos casos, un enfoque generalista en seguridad informática, con escasa profundización en prácticas forenses, análisis de evidencia digital y respuesta a incidentes. Asimismo, se observa una distancia entre la formación teórica y las necesidades operativas reales. Esta diplomatura busca reducir esa brecha, ofreciendo un trayecto formativo aplicado, centrado en el uso de herramientas, análisis de casos y desarrollo de habilidades prácticas.

e. Demanda del sector público y privado

Diversos organismos del Estado, fuerzas de seguridad, ámbitos judiciales y organizaciones privadas requieren actualmente perfiles técnicos capaces de intervenir en incidentes de seguridad, analizar evidencia digital y colaborar en procesos investigativos. A su vez, sectores como el financiero, tecnológico y de servicios enfrentan exigencias crecientes en materia de protección de la información. Esta diplomatura responde a esa demanda, aportando formación específica orientada a contextos reales de aplicación.

f. Evolución tecnológica y nuevas formas de ataque

El avance de tecnologías como la computación en la nube, dispositivos móviles, Internet de las Cosas y sistemas distribuidos introduce nuevas vulnerabilidades y desafíos en materia de seguridad. Los actores maliciosos emplean técnicas cada vez más sofisticadas, lo que requiere profesionales actualizados, capaces de comprender estas dinámicas y analizar evidencias en entornos diversos. La formación propuesta incorpora estos escenarios, abordando tanto los aspectos técnicos como su impacto en la investigación digital.

g. Enfoque práctico y orientado a la intervención profesional

La presente diplomatura se estructura sobre un enfoque aplicado, priorizando el desarrollo de competencias operativas a través de laboratorios, análisis de casos y uso de herramientas especializadas. Se busca que los cursantes no solo adquieran conocimientos teóricos, sino que puedan aplicarlos en situaciones concretas, fortaleciendo su desempeño en ámbitos laborales vinculados a la seguridad y la investigación digital.

h. Pertinencia territorial e institucional

En el contexto actual, tanto a nivel provincial como nacional, existe una necesidad creciente de fortalecer capacidades en ciberseguridad e investigación digital dentro de organismos públicos, instituciones judiciales y organizaciones privadas. La presente propuesta formativa contribuye a ese objetivo, promoviendo la profesionalización de recursos humanos y el desarrollo de competencias alineadas a las necesidades reales del entorno institucional y productivo.

6. JUSTIFICACIÓN

La presente Diplomatura se justifica en la necesidad de ofrecer un trayecto formativo especializado, coherente y aplicable, que responda a las demandas actuales en materia de ciberseguridad e informática forense, articulando de manera equilibrada los componentes técnicos, metodológicos y legales.

El diseño curricular de la propuesta, estructurado en **24 semanas y 240 horas reloj**, permite un desarrollo progresivo de competencias, evitando enfoques fragmentados o meramente teóricos, y favoreciendo la construcción de aprendizajes significativos con orientación práctica.

La organización en módulos secuenciales responde a una lógica formativa que parte de los fundamentos y el marco legal, avanza hacia la comprensión de sistemas, amenazas y vulnerabilidades, y culmina en el abordaje de metodologías forenses, análisis de evidencia digital y respuesta a incidentes, garantizando coherencia pedagógica a lo largo de todo el trayecto.

Asimismo, la modalidad e-learning combinada, con alternancia entre instancias sincrónicas y asincrónicas, permite compatibilizar la formación con la actividad laboral de los cursantes, promoviendo la autonomía, la continuidad del aprendizaje y el desarrollo de habilidades prácticas mediante el uso de entornos virtuales, laboratorios y actividades guiadas.

El enfoque aplicado de la diplomatura, centrado en el uso de herramientas, análisis de casos y producción de informes técnicos, favorece la transferencia directa de los conocimientos al ámbito profesional, fortaleciendo el desempeño en contextos reales de intervención.

En este sentido, la propuesta no solo responde a una demanda formativa existente, sino que se orienta a la generación de capacidades concretas en los participantes, contribuyendo al fortalecimiento institucional en ámbitos vinculados a la seguridad, la justicia y la gestión de la información.

7. OBJETIVOS

7.1. General:

Brindar formación universitaria especializada y aplicada en ciberseguridad e informática forense, orientada al desarrollo de competencias técnicas, metodológicas y legales para la adquisición, preservación, análisis e interpretación de evidencia digital, así como para la respuesta a incidentes, con criterios éticos, trazabilidad y apego al marco normativo vigente.

7.2. Específicos:

a. Desarrollar fundamentos sólidos de ciberseguridad, amenazas, vulnerabilidades y gestión básica del riesgo, orientados a escenarios reales de investigación y respuesta.
b. Capacitar en la identificación, recolección, preservación y documentación de evidencia digital, incluyendo control de integridad y criterios de trazabilidad.
c. Formar en metodologías de informática forense aplicables al análisis de sistemas y dispositivos, con enfoque en artefactos, correlación y línea de tiempo.
d. Integrar el análisis de redes y eventos de seguridad para detectar actividad maliciosa, extraer indicadores y construir hallazgos verificables.
e. Comprender técnicas, tácticas y procedimientos habituales de actores maliciosos, con fines de interpretación forense, análisis defensivo y fortalecimiento de capacidades de respuesta.
f. Incorporar procesos de respuesta a incidentes articulados con preservación de evidencia y comunicación técnica adecuada.
g. Elaborar informes técnicos y periciales estructurados, claros y consistentes, adecuados a destinatarios técnicos y no técnicos, defendibles metodológicamente.

8. DESTINATARIOS

La Diplomatura Universitaria en Ciberseguridad e Informática Forense está destinada a:

- Integrantes de fuerzas de seguridad, organismos públicos y áreas de investigación administrativa o penal.
- Profesionales y técnicos que se desempeñen en áreas de tecnología de la información, seguridad informática, auditoría, cumplimiento, control interno o gestión de riesgos.
- Integrantes de equipos de respuesta a incidentes, áreas de sistemas, centros de monitoreo o unidades de análisis digital.
- Profesionales del ámbito jurídico, judicial o pericial que requieran incorporar competencias técnicas vinculadas al tratamiento de evidencia digital.
- Personas interesadas-público en general- en adquirir formación universitaria especializada en ciberseguridad e informática forense, con orientación práctica y aplicada.

Se recomienda que los/as postulantes cuenten con conocimientos básicos de informática, uso de sistemas operativos y navegación en entornos digitales, a fin de facilitar el seguimiento de los módulos técnicos de la diplomatura.

9. REQUISITOS DE ADMISIÓN

Para la inscripción a la Diplomatura se deberá contar con:

- Poseer título de nivel secundario completo.

10. MÓDULOS Y PLAN DE ESTUDIOS

La Diplomatura se organiza en nueve (9) módulos, desarrollados de manera progresiva, integrando contenidos teóricos y prácticos, con un Trabajo Final Integrador obligatorio.

Malla Curricular – Organización del dictado-Duración y Carga Horaria reloj

Módulo	Denominación del Módulo	Duración (en semanas)	Dictado (en la semanas N°)	Carga horaria reloj
M1	Fundamentos de Ciberseguridad, Evidencia Digital y Marco Legal	2 semanas	Sem 1y2	16 hs
M2	Arquitectura de Sistemas, Redes y Trazabilidad Digital	3 semanas	Sem 3,4y5	24 hs
M3	Amenazas, Vulnerabilidades y Hacking Ético orientado a DFIR	3 semanas	Sem 6,7y8	24 hs
M4	Metodologías de Informática Forense y Cadena de Custodia	3 semanas	Sem 9,10y11	24 hs
M5	Adquisición y Preservación de Evidencia Digital	3 semanas	Sem 12,13y14	32 hs
M6	Análisis Forense de Sistemas (Windows / Linux)	4 semanas	Sem 15,16, 17y18	40 hs
M7	Forense de Redes, Malware y Análisis de Incidentes	2 semanas	Sem 19y20	24 hs
M8	Respuesta a Incidentes, Gestión de Crisis y CSIRT	2 semanas	Sem 21y22	20 hs
M9	Trabajo Final Integrador (TFI)	2 semanas (final) + desarrollo transversal	Sem 23y24	36 hs
			Total: 24 semanas	**240**

ACLARACIÓN PEDAGÓGICA

La estructura curricular se organiza en módulos secuenciales, evitando el dictado simultáneo de contenidos, a fin de garantizar la progresión del aprendizaje, la coherencia metodológica y la consolidación de competencias en cada etapa del trayecto formativo.

El Trabajo Final Integrador (TFI) se desarrolla de manera intensiva en las últimas semanas, con instancias de orientación y seguimiento progresivo a lo largo de la diplomatura.

ORGANIZACIÓN SEMANAL DEL CURSADO

Esquema general

El cursado se desarrolla de manera semanal, con actividades los días:

- **Viernes:** de 16:00 a 18.45 hs

- **Sábado:** de 09:00 a 11.45 hs

Modalidad de cursado

La diplomatura adopta una modalidad **e-learning combinada**, organizada bajo un esquema de alternancia semanal:

Semana SINCRÓNICA

- Clases en vivo a través de Zoom
- Desarrollo de contenidos teóricos
- Resolución guiada de casos
- Demostraciones prácticas

Distribución:

- Viernes: desarrollo conceptual, más introducción práctica
- Sábado: profundización, más práctica guiada

Semana ASINCRÓNICA

- Materiales estructurados en plataforma Moodle o video clases complementaria
- Actividades prácticas y laboratorios
- Foros de discusión y análisis de casos
- Evaluaciones parciales y entregas

Enfoque:

- Trabajo autónomo guiado
- Aplicación práctica de contenidos
- Seguimiento docente y retroalimentación

CRITERIO PEDAGÓGICO

Ambas instancias (sincrónicas y asincrónicas) poseen igual valor académico, integrándose como parte del proceso formativo continuo y permitiendo:

- Consolidar aprendizajes,
- Favorecer la autonomía del cursante,
- Compatibilizar estudio y actividad laboral,
- Y sostener un ritmo progresivo de formación.

MÓDULO 1. FUNDAMENTOS DE CIBERSEGURIDAD, EVIDENCIA DIGITAL Y MARCO LEGAL

a. Síntesis explicativa. Este módulo introduce los fundamentos esenciales de la ciberseguridad con orientación específica a la informática forense, estableciendo las bases conceptuales, técnicas y legales necesarias para el abordaje de incidentes que involucren evidencia digital.

Se desarrollan los principios de seguridad de la información, el análisis básico del riesgo y el reconocimiento de amenazas, integrando desde el inicio la noción de evidencia digital, su carácter volátil y la importancia de su correcta preservación. Asimismo, se aborda el marco normativo argentino e internacional aplicable, junto con los principios éticos que regulan la intervención profesional.

El módulo se orienta a que el cursante comprenda el rol de la ciberseguridad en contextos de investigación, incorporando una mirada inicial sobre la trazabilidad digital y la necesidad de actuar conforme a criterios técnicos y legales, sentando las bases para el desarrollo del enfoque DFIR en los módulos posteriores.

b. Contenidos

N°	Contenidos a desarrollar	Actividad sugerida
1	Introducción a la ciberseguridad. Principios de la seguridad de la información (Confidencialidad, Integridad, Disponibilidad). Conceptos de riesgo, amenaza y vulnerabilidad. Panorama actual de amenazas: ransomware, phishing, ataques DDoS, amenazas persistentes avanzadas (APT).	Foro de presentación y diagnóstico. Análisis guiado de un caso simple para identificar tipo de amenaza y posibles impactos.
2	Marco legal argentino: Ley 25.326 (Protección de Datos Personales), Ley 26.388 (Delitos Informáticos), Ley 27.078 (Argentina Digital). Marco internacional: GDPR, Convenio de Budapest, estándares ISO 27001 y 27037. Ética profesional: límites de la intervención técnica, uso responsable de herramientas y tratamiento de la información.	Análisis de caso con implicancias legales. Elaboración de cuadro comparativo normativo. Debate guiado sobre ética profesional en ciberseguridad.

c. Competencias sugeridas

Objetivos de aprendizaje	Competencias esperadas	Instrumentos de evaluación
Comprender los fundamentos de la ciberseguridad en relación con la evidencia digital	Identifica amenazas y reconoce posibles fuentes de evidencia digital en distintos escenarios	Cuestionario + análisis de caso
Reconocer el carácter volátil y sensible de la evidencia digital	Distingue tipos de evidencia y aplica criterios básicos de preservación inicial	Actividad práctica guiada
Conocer el marco legal aplicable a la ciberseguridad y la evidencia digital	Interpreta situaciones básicas conforme a normativa vigente	Análisis de caso
Reconocer los límites éticos y legales de la intervención técnica	Evalúa escenarios considerando responsabilidad profesional	Debate guiado

d. Bibliografía de referencia

- Ley 25.326 – Protección de los Datos Personales. InfoLEG. https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm
- Ley 26.388 – Delitos Informáticos. InfoLEG. https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=141790
- Ley 27.078 – Argentina Digital. InfoLEG. https://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm
- Council of Europe. Convention on Cybercrime (Budapest Convention). https://rm.coe.int/1680081561
- ISO/IEC 27001: Information Security Management Systems – Overview. https://www.iso.org/isoiec-27001-information-security.html
- ISO/IEC 27002: Information Security Controls. https://www.iso.org/standard/75652.html
- ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/standard/44381.html
- NIST Special Publication 800-61 Rev. 2. Computer Security Incident Handling Guide. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- RFC 3227 – Guidelines for Evidence Collection and Archiving. https://datatracker.ietf.org/doc/html/rfc3227
- Reglamento (UE) 2016/679 – General Data Protection Regulation (GDPR). https://www.legislation.gov.uk/eur/2016/679/contents
- NIST Cybersecurity Framework (CSF 2.0) https://www.nist.gov/cyberframework
- **Convenio de Budapest** https://rm.coe.int/16802fa403
- **AAIP – Guías oficiales Argentina** https://www.argentina.gob.ar/aaip

MÓDULO 2. ARQUITECTURA DE SISTEMAS, REDES Y TRAZABILIDAD DIGITAL

a. **Síntesis explicativa.** Este módulo profundiza en la comprensión técnica de la arquitectura de sistemas operativos, redes de computadoras y protocolos de comunicación, incorporando una perspectiva orientada a la trazabilidad digital. Los cursantes aprenderán cómo funcionan los componentes de la infraestructura tecnológica, sus vulnerabilidades inherentes, y los principales mecanismos de protección y monitoreo. Este conocimiento resulta fundamental para comprender vectores de ataque, interpretar eventos de seguridad, y sostener hallazgos técnicos con evidencias verificables (registros del sistema, trazas de red y telemetría disponible), aportando bases sólidas para los módulos posteriores de análisis forense y respuesta a incidentes.

b. Contenidos

	Contenidos a desarrollar	Actividad sugerida
1	**Arquitectura de sistemas operativos:** estructura general de Windows, Linux y macOS; gestión de procesos, memoria y sistema de archivos; registro del sistema (Windows Registry, logs de Linux); permisos y control de acceso. **Trazabilidad en SO:** noción de registro/auditoría, consistencia temporal básica de eventos (fecha/hora) y preservación inicial de registros.	Laboratorio práctico: exploración de estructura de directorios y logs en máquina virtual Linux (búsqueda y lectura guiada de registros). Entrega breve: "hallazgo + evidencia" (captura del log o extracto relevante + explicación).
2	**Fundamentos de redes:** modelo OSI y TCP/IP; direccionamiento IP (IPv4, IPv6, subnetting); protocolos fundamentales (HTTP/HTTPS, DNS, FTP, SSH, SMTP); arquitecturas de red (LAN, WAN, VPN).	Ejercicio de subnetting y configuración básica de red en entorno simulado. Cuestionario aplicado: "protocolo/puerto → evidencia esperable en logs/tráfico".
3	**Análisis de tráfico de red:** captura de paquetes con Wireshark; filtros BPF; identificación de protocolos; detección de anomalías en tráfico de red. **Trazabilidad en red:** 5-tupla (origen/destino/puertos/protocolo), tiempos de sesión y relación DNS ↔ conexión.	Práctica guiada: captura y análisis de tráfico HTTP/HTTPS con Wireshark. Entrega: filtros utilizados + identificación de 3 hallazgos (con evidencia en capturas).
4	**Infraestructura de seguridad:** firewalls, IDS/IPS, proxies; segmentación de red y DMZ; VPN y túneles seguros; arquitectura de defensa en profundidad. **Virtualización y cloud computing:** conceptos de virtualización (hypervisors tipo 1 y 2); contenedores (Docker, Kubernetes); modelos de cloud (IaaS, PaaS, SaaS); desafíos de seguridad y trazabilidad en entornos virtualizados y cloud.	Análisis de caso: diseño de arquitectura de red segura para una organización mediana (defensa en profundidad + segmentación + puntos de monitoreo). Quiz breve de virtualización/cloud y foro de debate: "riesgos y registros mínimos a exigir".

c. Competencias sugeridas

Objetivos de aprendizaje	Competencias esperadas	Instrumentos de evaluación
Comprender la estructura básica de sistemas operativos y redes	Reconoce componentes de sistemas y redes relevantes para el análisis digital	Actividad práctica + cuestionario

Identificar fuentes de información digital en sistemas y redes	Localiza registros, logs y artefactos digitales en distintos entornos	Ejercicio guiado
Interpretar eventos básicos en sistemas y comunicaciones	Analiza registros simples y relaciona eventos en una secuencia lógica	Análisis de caso
Introducir el concepto de trazabilidad digital	Aplica criterios básicos de correlación de eventos en un entorno controlado	Práctica de correlación simple

d. Bibliografía de referencia

- Tanenbaum, A. Redes de computadoras (6ta edición). Pearson Education.
- Silberschatz, A., Galvin, P. & Gagne, G. Fundamentos de Sistemas Operativos (9na edición). Wiley.
- Sanders, C. Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems (3rd ed.). No Starch Press.
- NIST. SP 800-42: Guideline on Network Security Testing. https://csrc.nist.gov/pubs/sp/800/42/final
- Cisco Networking Basics (curso abierto – material estable) https://skillsforall.com/course/networking-basics
- Introducción a redes (INET / Educ.ar – Argentina) https://www.educ.ar/recursos/150147/redes-informaticas
- NIST SP 800-61 (gestión de incidentes – para conexión con DFIR) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Microsoft Learn – Conceptos de Windows (oficial y estable) https://learn.microsoft.com/es-es/windows/
- Linux Foundation – Intoducción (material abierto) https://training.linuxfoundation.org/resources/open-source-guides/
- Video: Wireshark Tutorial para principiantes – Análisis de tráfico de red. YouTube. https://www.youtube.com/watch?v=TkCSr30UojM

MÓDULO 3. AMENAZAS, VULNERABILIDADES Y HACKING ÉTICO ORIENTADO A DFIR

a. Síntesis explicativa. Este módulo aborda el estudio de amenazas, vulnerabilidades y técnicas utilizadas por actores maliciosos, con el propósito de comprender cómo se originan los incidentes de seguridad y qué tipo de evidencias digitales generan.

Se introduce el hacking ético en un enfoque estrictamente formativo y controlado, orientado a la comprensión del comportamiento del atacante y su relación con la

trazabilidad digital. Se analizan técnicas básicas de reconocimiento, explotación inicial y post-explotación a nivel conceptual, vinculándolas con marcos de referencia como MITRE ATT&CK.
El módulo se orienta a que el cursante pueda interpretar eventos desde la perspectiva del atacante, identificar vectores de ingreso y comprender las huellas que estos dejan en los sistemas, sentando bases para el análisis forense y la respuesta a incidentes en los módulos posteriores.

b. Contenidos

N°	Contenidos a desarrollar	Actividad sugerida
1	Introducción a amenazas y vulnerabilidades. Tipos de atacantes. Ciclo de ataque. Conceptos de reconocimiento (OSINT básico). Introducción a MITRE ATT&CK.	Análisis de un caso real de ataque. Identificación de fases del ataque.
2	Técnicas básicas de explotación (enfoque conceptual). Introducción a OWASP Top 10. Concepto de post-explotación. Relación entre técnicas de ataque y evidencia generada.	Actividad guiada: vincular técnicas de ataque con posibles evidencias digitales.
3	Introducción a herramientas (visión general): escaneo, reconocimiento y análisis. Generación de indicadores de compromiso (IOCs). Relación ataque–detección–evidencia.	Ejercicio práctico: identificación de IOCs en un escenario simulado.

c. Competencias sugeridas

Objetivos de aprendizaje	Competencias esperadas	Instrumentos de evaluación
Comprender las principales amenazas y vectores de ataque	Identifica tipos de ataques y sus etapas	Cuestionario, más análisis de caso
Interpretar técnicas básicas utilizadas por atacantes	Relaciona técnicas con posibles evidencias digitales	Actividad práctica
Introducir el uso de marcos como MITRE ATT&CK	Ubica técnicas dentro de un modelo estructurado de ataque	Ejercicio guiado
Reconocer indicadores de compromiso (IOCs)	Identifica señales básicas de compromiso en sistemas y redes	Práctica aplicada

d. Bibliografía de referencia

- OWASP Foundation. OWASP Top 10 – The Ten Most Critical Web Application Security Risks. https://owasp.org/www-project-top-ten/
- MITRE. ATT&CK Framework. https://attack.mitre.org/

- INCIBE – Amenazas y ciberseguridad (España, contenido accesible) https://www.incibe.es/ciudadania/amenazas
- CISA – Cybersecurity Resources (EE.UU.) https://www.cisa.gov/cybersecurity muy actualizado y práctico
- SANS – Introducción a amenazas (artículos abiertos) https://www.sans.org/white-papers/
- NIST. National Vulnerability Database (NVD). https://nvd.nist.gov/
- NIST. SP 800-61 Rev. 2 – Computer Security Incident Handling Guide. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- Scarfone, K., Grance, T. Computer Security Incident Handling Guide. NIST Special Publication. https://csrc.nist.gov/pubs/sp/800/61/r2/final
- EC-Council. Hacking Ético – Conceptos y Metodologías (material introductorio). https://www.eccouncil.org/ethical-hacking/

MÓDULO 4. METODOLOGÍAS DE INFORMÁTICA FORENSE Y CADENA DE CUSTODIA

a. Síntesis explicativa. Este módulo desarrolla las metodologías fundamentales de la informática forense, orientadas a la correcta identificación, recolección, preservación y análisis de la evidencia digital, conforme a estándares y buenas prácticas reconocidas a nivel internacional.

Se abordan modelos metodológicos como NIST, ISO y RFC aplicados al proceso forense, junto con la implementación práctica de la cadena de custodia como elemento clave para garantizar la integridad, autenticidad y validez de la evidencia.

El módulo se enfoca en la correcta documentación de los procedimientos, la elaboración de registros técnicos y la comprensión del rol del perito en contextos judiciales y administrativos, preparando al cursante para intervenir de manera estructurada, trazable y defendible en procesos de investigación digital.

b. Contenidos

	Contenidos a desarrollar	Actividad sugerida
1	**Introducción a la informática forense:** definición y alcance; tipos de investigaciones forenses digitales; fases del proceso forense. Principios fundamentales: integridad, autenticidad, trazabilidad y reproducibilidad.	Foro de discusión: análisis de distintos tipos de casos forenses (penales, administrativos, corporativos). Cuestionario introductorio sobre principios forenses.
2	**Metodologías y estándares forenses:** guías y buenas prácticas (NIST SP 800-86, ISO/IEC 27037, RFC 3227). Modelos de proceso forense. Rol del perito informático y responsabilidades profesionales.	Análisis comparativo de metodologías forenses. Actividad práctica: identificación de etapas del

		proceso forense en un caso propuesto.
3	**Cadena de custodia:** concepto y finalidad; procedimientos de identificación, rotulación, registro y resguardo de evidencia digital; documentación asociada (actas, formularios, bitácoras). Custodia en entornos físicos y digitales.	Simulación guiada: confección de actas y registros de cadena de custodia a partir de un escenario planteado. Entrega de documentación completa.
4	**Admisibilidad y presentación de la evidencia:** validez técnica y legal; control de integridad (hashing); preservación de la evidencia durante el análisis; errores frecuentes y riesgos de invalidación. Introducción a la elaboración de informes forenses.	Análisis de casos reales donde la evidencia fue cuestionada. Actividad aplicada: detección de fallas metodológicas y propuesta de corrección.

c. Competencias sugeridas

Objetivos de aprendizaje	Competencias esperadas	Instrumentos de evaluación
Comprender el proceso metodológico de la informática forense	Aplica las fases del proceso forense en escenarios simulados	Análisis de caso
Reconocer la importancia de la cadena de custodia	Registra y documenta correctamente la manipulación de evidencia	Práctica guiada
Aplicar criterios de preservación de evidencia digital	Identifica riesgos de alteración y aplica medidas básicas de resguardo	Ejercicio práctico
Elaborar documentación técnica forense	Produce informes básicos con estructura adecuada	Informe técnico

d. Bibliografía de referencia

- NIST. SP 800-86 – Guide to Integrating Forensic Techniques into Incident Response. https://csrc.nist.gov/publications/detail/sp/800-86/final
- ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/standard/44381.html
- RFC 3227. Guidelines for Evidence Collection and Archiving. https://datatracker.ietf.org/doc/html/rfc3227
- Europol – Digital Forensics (recursos abiertos) https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime
- Guías de evidencia digital (Argentina – Ministerio Público / judicial)

MÓDULO 5. ADQUISICIÓN Y PRESERVACIÓN DE EVIDENCIA DIGITAL

a. **Síntesis explicativa.** Este módulo aborda los procedimientos técnicos para la adquisición y preservación de evidencia digital, aplicando los principios metodológicos desarrollados previamente y orientándose a la práctica operativa en distintos entornos.

Se desarrollan técnicas de obtención de evidencia en medios de almacenamiento, memoria volátil y sistemas en funcionamiento, priorizando la integridad, trazabilidad y no alteración de la información. Asimismo, se introducen herramientas y procedimientos básicos utilizados en la práctica forense.

El módulo se enfoca en la correcta ejecución de procesos de adquisición, la identificación de fuentes de evidencia y la aplicación de criterios de resguardo, preparando al cursante para intervenir de manera controlada en escenarios reales de recolección de datos.

b. **Contenidos.**

	Contenidos a desarrollar	Actividad sugerida
1	**Principios de adquisición forense:** objetivos de la adquisición; tipos de evidencia digital (volátil y no volátil); estrategias de adquisición según escenario; preservación de la escena digital. **Integridad de la evidencia:** funciones hash (MD5, SHA-1, SHA-256); verificación y documentación de integridad.	Análisis guiado de escenarios de adquisición (sistema encendido vs. apagado). Ejercicio práctico de cálculo y verificación de hashes sobre archivos de muestra.
2	**Adquisición de medios de almacenamiento:** imágenes bit a bit; adquisición lógica y física; formatos de imagen forense (RAW, E01); herramientas de adquisición (dd, Guymager, FTK Imager u otras). Uso de write blockers.	Práctica de laboratorio: creación de una imagen forense de un medio de almacenamiento. Entrega: registro del procedimiento, herramienta utilizada y valores hash obtenidos.
3	**Adquisición de evidencia volátil:** memoria RAM, procesos activos, conexiones de red y estado del sistema. Orden de volatilidad. Herramientas para captura de memoria. Riesgos y limitaciones de la adquisición en sistemas en funcionamiento.	Simulación guiada: identificación de información volátil relevante en un sistema en ejecución. Actividad práctica de captura de memoria (dataset o entorno controlado) con documentación básica.

4	**Adquisición en entornos específicos:** nociones de adquisición forense en dispositivos móviles (enfoque procedimental); adquisición y preservación en entornos virtualizados y cloud computing; responsabilidades compartidas y trazabilidad. **Resguardo y almacenamiento de evidencia:** rotulación, embalaje, almacenamiento seguro y control de acceso.	Análisis de caso: estrategia de adquisición en un incidente que involucra dispositivos móviles y servicios en la nube. Elaboración de un plan de adquisición y preservación acorde al escenario.

c. Competencias sugeridas

Objetivos de aprendizaje	Competencias esperadas	Instrumentos de evaluación
Comprender los principios de adquisición de evidencia digital	Distingue tipos de evidencia y aplica criterios de adquisición	Cuestionario + práctica
Aplicar procedimientos básicos de recolección de evidencia	Ejecuta procesos de adquisición en entornos controlados	Práctica guiada
Reconocer la importancia de la integridad de la evidencia	Aplica técnicas de verificación mediante hashing	Ejercicio práctico
Evaluar escenarios de adquisición en sistemas activos	Toma decisiones básicas en situaciones de adquisición en vivo	Análisis de caso

d. Bibliografía de referencia

- RFC 3227 – Evidence Collection and Archiving https://www.rfc-editor.org/rfc/rfc3227
- Guía básica de evidencia digital – INCIBE (España) https://www.incibe.es/ciudadania/blog/evidencias-digitales accesible y clara para alumnos
- NIST – Digital Forensics (portal actualizado) https://www.nist.gov/itl/ssd/software-quality-group/digital-forensics
- NIST SP 800-61 (gestión de incidentes) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Guías de buenas prácticas en ciberseguridad – INCIBE https://www.incibe.es/protege-tu-empresa
- Documentación Autopsy (herramienta forense open source) https://www.autopsy.com/documentation/

MÓDULO 6. ANÁLISIS FORENSE DE SISTEMAS (WINDOWS / LINUX)

a. Síntesis explicativa. Este módulo desarrolla las técnicas de análisis forense aplicadas a sistemas operativos, con foco en la identificación, interpretación y correlación de artefactos digitales relevantes para la reconstrucción de eventos. Se abordan en profundidad los sistemas Windows y Linux, priorizando el análisis de registros, configuraciones, actividad de usuarios y mecanismos de persistencia, utilizando herramientas y metodologías propias del análisis forense. El módulo se orienta a que el cursante pueda reconstruir secuencias de actividad a partir de evidencia digital, aplicando criterios de interpretación y correlación temporal, constituyendo el eje central del análisis forense dentro del proceso DFIR.

b. Contenidos

N°	Contenidos a desarrollar	Actividad sugerida
1	Introducción al análisis forense de sistemas. Tipos de artefactos digitales. Sistemas de archivos (NTFS, EXT). Introducción a herramientas de análisis forense.	Reconocimiento guiado de estructura de sistema. Identificación de artefactos básicos.
2	Análisis forense en Windows: registro (Registry), eventos del sistema (Event Logs), archivos Prefetch, accesos directos (LNK), historial de actividad.	Práctica guiada: identificación de actividad del usuario en sistema Windows.
3	Análisis forense en Linux: logs del sistema, autenticación, actividad de usuarios, procesos, persistencia básica.	Ejercicio práctico: análisis de logs en entorno Linux.
4	Correlación de eventos. Construcción de línea de tiempo (timeline). Introducción a herramientas como Plaso / Timesketch. Interpretación de eventos.	Actividad integradora: reconstrucción de un escenario a partir de múltiples artefactos.

d. Competencias sugeridas

Objetivos de aprendizaje	Competencias esperadas	Instrumentos de evaluación
Comprender el análisis forense de sistemas operativos	Identifica artefactos relevantes en distintos sistemas	Práctica guiada
Analizar registros y actividad en sistemas Windows	Interpreta eventos y reconstruye acciones del usuario	Ejercicio práctico

Analizar registros en sistemas Linux	Identifica actividad y posibles indicadores de compromiso	Actividad práctica
Aplicar correlación temporal de eventos	Construye líneas de tiempo coherentes a partir de evidencia	Caso integrador

d. Bibliografía de referencia

- NIST – Digital Forensics (portal actualizado) https://www.nist.gov/itl/ssd/software-quality-group/digital-forensics
- Documentación Autopsy (herramienta forense) https://www.autopsy.com/documentation/
- Microsoft Learn – Eventos y sistema Windows (oficial) https://learn.microsoft.com/es-es/windows/security/
- Linux Logs – Introducción (Linux Foundation) https://training.linuxfoundation.org/resources/open-source-guides/
- Timesketch (herramienta de timeline) https://timesketch.org
- Plaso (log2timeline) https://plaso.readthedocs.io

MÓDULO 7. FORENSE DE REDES, MALWARE Y ANÁLISIS DE INCIDENTES

a. Síntesis explicativa. Este módulo aborda el análisis forense aplicado a redes y el estudio básico de malware, con el objetivo de identificar, interpretar y correlacionar evidencias digitales vinculadas a incidentes de seguridad.

Se desarrollan técnicas de análisis de tráfico de red, interpretación de registros y detección de patrones asociados a actividades maliciosas. Asimismo, se introduce el análisis funcional de malware desde una perspectiva forense, orientada a comprender su comportamiento y las evidencias que genera, sin profundizar en ingeniería inversa avanzada.

El módulo se orienta a que el cursante pueda analizar eventos en redes, identificar indicadores de compromiso (IOCs) y comprender la dinámica de los incidentes, integrando la información obtenida con el análisis de sistemas realizado en módulos anteriores.

b. Contenidos

	Contenidos a desarrollar	Actividad sugerida
1	**Forense de redes – fundamentos:** conceptos de tráfico de red; tipos de captura (PCAP); puntos de captura; preservación de tráfico como evidencia digital. Protocolos y servicios relevantes para el análisis forense.	Análisis guiado de un archivo PCAP: identificación de protocolos, hosts y sesiones. Actividad práctica de reconocimiento de tráfico normal vs. anómalo.
2	**Análisis de tráfico y detección de intrusiones:** análisis detallado de PCAP; correlación de tráfico con eventos;	Práctica de laboratorio: análisis de un PCAP con indicadores de actividad sospechosa. Entrega

	herramientas de análisis (Wireshark, NetworkMiner u otras). Introducción a IDS/IPS (Snort, Suricata) y su valor forense.	de evidencias seleccionadas y breve descripción de hallazgos.
3	**Introducción al análisis de malware:** conceptos y tipos de malware; ciclo de vida; análisis estático básico (hashes, strings, metadatos); análisis dinámico controlado (comportamiento). Generación de indicadores de compromiso (IOCs).	Ejercicio práctico: análisis básico de una muestra de malware (dataset controlado). Identificación de IOCs y elaboración de una ficha técnica simple.
4	**Análisis de incidentes:** integración de evidencias de red, sistemas y malware; clasificación de incidentes; reconstrucción del incidente; lecciones aprendidas. Relación con procesos de respuesta a incidentes y preservación de evidencia.	Caso integrador: análisis de un incidente simulado con múltiples fuentes de evidencia. Elaboración de un informe técnico de incidente con hallazgos e indicadores.

c. Competencias sugeridas

Objetivos de aprendizaje	Competencias esperadas	Instrumentos de evaluación
Comprender el análisis forense de redes	Interpreta tráfico básico y reconoce patrones de comunicación	Práctica guiada
Identificar actividad sospechosa en redes	Detecta comportamientos anómalos en tráfico digital	Ejercicio práctico
Comprender el comportamiento básico del malware	Reconoce tipos de malware y sus efectos en sistemas	Análisis de caso
Integrar información de red y sistema	Relaciona eventos para identificar indicadores de compromiso (IOCs)	Caso integrador

d. Bibliografía de referencia

- Wireshark Documentation (oficial) https://www.wireshark.org/docs/
- CISA – Malware Analysis Resources https://www.cisa.gov/malware-analysis
- MITRE ATT&CK (técnicas y comportamiento) https://attack.mitre.org
- NetworkMiner (herramienta y documentación) https://www.netresec.com/?page=NetworkMiner
- SANS – Papers sobre análisis de tráfico y malware https://www.sans.org/white-papers/
- NIST – Cybersecurity Framework https://www.nist.gov/cyberframework

MÓDULO 8. RESPUESTA A INCIDENTES, GESTIÓN DE CRISIS Y CSIRT

a. Síntesis explicativa. Este módulo aborda la respuesta a incidentes de seguridad desde una perspectiva técnica y operativa, integrando los conocimientos adquiridos en análisis forense, redes y sistemas.

Se desarrollan las fases del proceso de respuesta a incidentes, incluyendo detección, contención, erradicación y recuperación, con énfasis en la preservación de la evidencia digital durante todo el proceso. Asimismo, se introduce el funcionamiento de equipos CSIRT y la gestión básica de incidentes en entornos organizacionales.

El módulo se orienta a que el cursante pueda intervenir en escenarios de incidentes de seguridad, aplicando criterios técnicos, metodológicos y de trazabilidad, integrando análisis, documentación y toma de decisiones en contextos reales.

b. Contenidos

	Contenidos a desarrollar	Actividad sugerida
1	**Introducción a la respuesta a incidentes:** definición y tipos de incidentes; ciclo de vida de la respuesta a incidentes; roles y responsabilidades. Detección y análisis inicial del incidente. Importancia de la preservación de evidencia durante la respuesta.	Análisis guiado de distintos tipos de incidentes (ransomware, acceso no autorizado, fuga de información). Cuestionario aplicado sobre fases y roles en la respuesta a incidentes.
2	**Gestión del incidente:** contención, erradicación y recuperación. Registro de acciones y decisiones. Coordinación con áreas técnicas, legales y de gestión. Comunicación interna y externa durante el incidente. Gestión de crisis y toma de decisiones bajo presión.	Caso práctico: definición de acciones de contención y recuperación ante un incidente simulado. Elaboración de un registro de acciones y decisiones adoptadas.
3	**Equipos CSIRT:** concepto, funciones y modelos de CSIRT. Políticas y procedimientos de respuesta a incidentes (IRP). Lecciones aprendidas y mejora continua. Integración de la respuesta a incidentes con el análisis forense posterior.	Actividad integradora: diseño básico de un procedimiento de respuesta a incidentes (IRP) y estructura mínima de un CSIRT para una organización tipo. Debate guiado sobre lecciones aprendidas.

c. Competencias sugeridas

Objetivos de aprendizaje	Competencias esperadas	Instrumentos de evaluación
Comprender el proceso de respuesta a incidentes	Identifica fases y acciones en un incidente	Análisis de caso

Aplicar criterios de intervención técnica	Ejecuta acciones básicas de contención y análisis	Simulación práctica
Preservar evidencia durante la respuesta	Aplica criterios de resguardo en escenarios dinámicos	Ejercicio guiado
Integrar conocimientos previos en un incidente	Relaciona información de sistemas, red y malware	Caso integrador

d. Bibliografía de referencia

- NIST SP 800-61 Rev. 2 – Incident Handling Guide, estandar mundical en IR: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- CISA – Incident Response Resources, actual y práctico: https://www.cisa.gov/incident-response
- FIRST – CSIRT Guidelines https://www.first.org/resources/guides
- ENISA – Incident Response Guidelines (Europa) https://www.enisa.europa.eu
- NIST Cybersecurity Framework (CSF 2.0) https://www.nist.gov/cyberframework
- ENISA. Good Practice Guide for Incident Management. https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
- FIRST. CSIRT Services Framework. https://www.first.org/standards/frameworks/csirt-services-framework
- ISO/IEC 27035. Information security incident management. https://www.iso.org/standard/60803.html

MÓDULO 9. TRABAJO FINAL INTEGRADOR

a. Síntesis explicativa. El Trabajo Final Integrador constituye la instancia de cierre de la diplomatura, orientada a la aplicación práctica e integrada de los conocimientos y competencias desarrollados a lo largo del trayecto formativo.
Consiste en el abordaje de un caso simulado o basado en escenarios reales, en el cual el cursante deberá aplicar metodologías de análisis forense, adquisición y preservación de evidencia digital, interpretación de eventos y respuesta a incidentes, elaborando un informe técnico conforme a estándares profesionales.
El módulo se orienta a que el cursante desarrolle un trabajo estructurado, con sustento metodológico, trazabilidad de procedimientos y claridad en la comunicación de resultados, integrando aspectos técnicos, legales y operativos.

b. Contenidos

N°	Contenidos a desarrollar	Actividad sugerida
1	Presentación del caso integrador (ransomware, acceso indebido, exfiltración, insider, etc.). Definición del problema. Planificación del análisis. Identificación de fuentes de evidencia.	Entrega inicial: planteo del caso + plan de trabajo. Tutoría y ajustes.
2	Desarrollo del análisis: aplicación de metodologías forenses. Integración de evidencia (sistema, red, logs). Elaboración de informe técnico y conclusiones. Preparación de defensa.	Entrega final: informe técnico + informe ejecutivo. Defensa oral simulada (ámbito profesional/judicial).

c. Competencias sugeridas

Objetivos de aprendizaje	Competencias esperadas	Instrumentos de evaluación
Aplicar metodologías de análisis forense en un caso integrador	Ejecuta un proceso completo de análisis DFIR	Trabajo práctico integrador
Integrar evidencia de distintas fuentes	Correlaciona información de sistemas, red y eventos	Informe técnico
Elaborar documentación profesional	Redacta informes técnicos claros, estructurados y fundamentados	Informe escrito
Comunicar resultados de análisis	Expone conclusiones de manera clara y defendible	Defensa oral

d. Bibliografía de referencia

- NIST SP 800-61 – Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- MITRE ATT&CK Framework https://attack.mitre.org
- ISO/IEC 27037 (referencia) https://www.iso.org/standard/44381.html

Complementaria

- Materiales de módulos anteriores
- Informes técnicos modelo (provistos por el docente)
- Casos prácticos simulados

11. PERFIL DE LOS FORMADORES

Módulo	Perfil del formador
1. Fundamentos de Ciberseguridad,	Profesional con formación en informática, sistemas, ciberseguridad, derecho o disciplinas afines, con

Evidencia Digital y Marco Legal	conocimientos sólidos en principios de ciberseguridad, marco legal nacional e internacional, protección de datos personales y ética profesional. Se valorará experiencia en gestión de incidentes, cumplimiento normativo, seguridad de la información y/o actuación técnica en entornos regulados.
2. Arquitectura de Sistemas, Redes y Trazabilidad Digital	Profesional con formación y experiencia en sistemas operativos, redes de computadoras y seguridad informática. Deberá acreditar conocimientos en arquitectura de sistemas, protocolos de red, infraestructura de seguridad y mecanismos de registro y monitoreo. Se valorará experiencia práctica en administración de sistemas, redes o análisis técnico orientado a la trazabilidad y auditoría.
3. Amenazas, Vulnerabilidades y Hacking Ético Orientado a DFIR	Profesional especializado en ciberseguridad ofensiva y defensiva, con conocimientos en análisis de amenazas, gestión de vulnerabilidades y técnicas de hacking ético. Deberá contar con experiencia en el uso de marcos de referencia como OWASP y MITRE ATT&CK, y capacidad para abordar estas técnicas desde una perspectiva analítica orientada a la investigación forense y la respuesta a incidentes.
4. Metodologías de Informática Forense y Cadena de Custodia	Profesional con formación y experiencia comprobable en informática forense, peritaje digital o disciplinas afines. Deberá dominar metodologías forenses, estándares internacionales, procedimientos de cadena de custodia y documentación de evidencia digital. Se valorará experiencia en actuaciones periciales, investigaciones técnicas o asesoramiento en procesos administrativos o judiciales.
5. Adquisición y Preservación de Evidencia Digital	Profesional especializado en técnicas de adquisición y preservación de evidencia digital, con dominio de herramientas y procedimientos forenses. Deberá acreditar experiencia en adquisición de evidencia volátil y no volátil, manejo de dispositivos de almacenamiento y conocimiento de entornos móviles y virtualizados. Se valorará experiencia práctica en laboratorios forenses o equipos de investigación técnica.
6. Análisis Forense de Sistemas (Windows / Linux)	Profesional con sólida experiencia en análisis forense de sistemas operativos Windows y Linux. Deberá acreditar conocimientos en análisis de artefactos, logs, reconstrucción de eventos y construcción de líneas de tiempo forenses. Se valorará experiencia en investigaciones técnicas, análisis de incidentes o peritajes informáticos.

7. Forense de Redes, Malware y Análisis de Incidentes	Profesional con experiencia en análisis de tráfico de red, detección de intrusiones y análisis básico de malware. Deberá contar con conocimientos en herramientas de análisis de red, generación de indicadores y correlación de evidencias. Se valorará experiencia en equipos SOC, CSIRT o investigaciones de incidentes de seguridad.
8. Respuesta a Incidentes, Gestión de Crisis y CSIRT	Profesional con formación y experiencia en respuesta a incidentes de seguridad informática y gestión de crisis. Deberá acreditar conocimientos en modelos de respuesta a incidentes, coordinación interáreas, comunicación en crisis y organización de equipos CSIRT. Se valorará experiencia en liderazgo técnico, gestión operativa de incidentes y elaboración de procedimientos institucionales.
9. Trabajo Final Integrador	Profesional con experiencia integral en ciberseguridad, informática forense y respuesta a incidentes, con capacidad para tutorizar y evaluar trabajos aplicados. Deberá acreditar experiencia en dirección de proyectos técnicos, elaboración de informes y evaluación académica. Se valorará experiencia del formador y participación en investigaciones o intervenciones complejas.

12. Perfil del Egresado

El/la egresado/a de la *Diplomatura Universitaria en Informática Forense y Ciberseguridad* será un/a profesional con formación teórico-práctica capaz de intervenir en el análisis de incidentes de seguridad y en procesos que involucren evidencia digital, aplicando metodologías y herramientas propias del campo.

Contará con competencias para identificar, preservar, adquirir y analizar evidencia digital en distintos entornos, interpretar eventos a partir de registros de sistemas y redes, y colaborar en la reconstrucción de incidentes mediante el uso de técnicas de análisis forense.

Asimismo, estará capacitado/a para participar en procesos de respuesta a incidentes, aplicar criterios de trazabilidad y resguardo de la información, y elaborar informes técnicos claros y fundamentados, integrando aspectos técnicos, metodológicos y legales.

Su formación le permitirá desempeñarse en equipos interdisciplinarios, actuando con responsabilidad profesional, criterio ético y respeto por el marco normativo vigente.

13. Alcances del Título

El título de *Diplomado/a Universitario/a en Informática Forense y Ciberseguridad* habilita a su poseedor/a a desempeñarse en actividades vinculadas al análisis técnico, prevención e intervención en incidentes de seguridad de la información y eventos que involucren evidencia digital, tanto en el ámbito público como privado.

El/la egresado/a podrá participar en tareas de:

- Identificación, recolección y preservación de evidencia digital en entornos informáticos.
- Análisis técnico de sistemas, redes y registros digitales en el marco de investigaciones.
- Apoyo técnico en procesos administrativos, organizacionales o judiciales que requieran análisis de evidencia digital.
- Participación en equipos de respuesta a incidentes de seguridad (CSIRT).
- Elaboración de informes técnicos y documentación vinculada a incidentes de seguridad y análisis forense.
- Implementación de buenas prácticas de seguridad de la información.

La presente diplomatura **no habilita por sí sola** para el ejercicio como perito judicial ni sustituye los requisitos de matriculación, registro o acreditación que pudieran exigir las normativas vigentes de cada jurisdicción u organismo competente.

14. COMPETENCIAS ADQUIRIDAS

a. Conocimientos

El/la egresado/a adquirirá conocimientos teóricos y conceptuales en:

- Fundamentos de ciberseguridad y seguridad de la información.
- Tipologías de amenazas, vulnerabilidades y técnicas utilizadas en ciberataques.
- Arquitectura básica de sistemas operativos y redes informáticas.
- Principios de evidencia digital, su clasificación y características.
- Metodologías de informática forense y modelos de análisis (NIST, ISO, entre otros).
- Procedimientos de adquisición y preservación de evidencia digital.
- Técnicas de análisis forense en sistemas, redes y entornos digitales.
- Conceptos básicos de análisis de malware desde una perspectiva forense.
- Procesos de respuesta a incidentes de seguridad y funcionamiento de equipos CSIRT.
- Marco normativo vigente en materia de delitos informáticos y protección de datos.

b. Habilidades generales y específicas

El/la egresado/a desarrollará habilidades para:

- Identificar y reconocer fuentes de evidencia digital en distintos entornos.
- Aplicar procedimientos básicos de adquisición y preservación de información digital.
- Analizar registros de sistemas y redes para reconstruir eventos.
- Interpretar indicadores de compromiso (IOCs) y patrones de actividad maliciosa.
- Correlacionar información proveniente de distintas fuentes digitales.
- Elaborar informes técnicos claros, estructurados y fundamentados.
- Participar en procesos de respuesta a incidentes de seguridad.

- Utilizar herramientas básicas de análisis forense y monitoreo.
- Integrar conocimientos técnicos y metodológicos en la resolución de casos.

c. Actitudes y valores

El/la egresado/a desarrollará actitudes y valores orientados a:

- Actuar con responsabilidad profesional en el tratamiento de la información.
- Respetar la confidencialidad, integridad y legalidad en el manejo de datos.
- Aplicar criterios éticos en el uso de herramientas y técnicas de análisis.
- Mantener una actitud crítica y analítica frente a incidentes de seguridad.
- Trabajar de manera colaborativa en equipos interdisciplinarios.
- Actualizarse de manera continua frente a la evolución tecnológica.
- Desempeñarse con rigurosidad metodológica en el análisis de evidencia digital.

15. METODOLOGÍA

La Diplomatura se desarrollará bajo una modalidad e-learning combinada, estructurada sobre un modelo pedagógico orientado a la formación de adultos (andragogía), con enfoque modular, progresivo y aplicado.

El diseño metodológico prioriza el aprendizaje significativo, la integración teoría–práctica y el desarrollo de competencias técnicas, favoreciendo la participación activa del cursante y la aplicación de los contenidos en contextos reales o simulados.

15.1 Modalidad e-learning sincrónica y asincrónica

La propuesta formativa se organiza mediante una modalidad e-learning que combina instancias sincrónicas y asincrónicas de manera alternada y complementaria.

El cursado se desarrollará de forma semanal, con actividades académicas los días:

- **Viernes:** de 16:00 a 20:00 hs
- **Sábado:** de 08:00 a 12:00 hs

El esquema pedagógico contempla:

- **Semanas sincrónicas:**
  Clases en vivo a través de plataforma Zoom, destinadas al desarrollo conceptual de los contenidos, análisis de casos, demostraciones prácticas y orientación docente.
- **Semanas asincrónicas:**
  Trabajo autónomo guiado a través de plataforma Moodle, mediante materiales estructurados, actividades prácticas, foros de discusión, material audiovisual, o clases grabadas complementarias y evaluaciones parciales.

Ambas instancias poseen igual valor académico, integrándose en un proceso continuo de aprendizaje que permite consolidar conocimientos, desarrollar habilidades prácticas y compatibilizar la formación con la actividad laboral.

15.2 Modelo andragógico modular

La diplomatura adopta un modelo andragógico centrado en el aprendizaje del adulto, reconociendo la experiencia previa de los cursantes y promoviendo su participación activa en el proceso formativo.

La estructura modular permite organizar los contenidos en unidades progresivas y secuenciales, evitando la superposición de temáticas y favoreciendo la construcción gradual del conocimiento.

Cada módulo integra:

- Contenidos teóricos esenciales,
- Actividades prácticas orientadas a la resolución de problemas,
- Análisis de casos reales o simulados,
- Y evaluación continua del aprendizaje.

Este enfoque facilita la comprensión, aplicación y transferencia de los conocimientos al ámbito profesional.

15.3 Certificación por competencias

El proceso formativo se orienta al desarrollo de competencias, entendidas como la integración de conocimientos, habilidades y actitudes aplicadas a situaciones concretas.

La certificación de la diplomatura se basa en la evaluación progresiva de dichas competencias a lo largo del trayecto formativo, considerando:

- la participación en actividades teóricas y prácticas,
- la resolución de ejercicios aplicados,
- la integración de contenidos en cada módulo,
- y la aprobación del Trabajo Final Integrador.

Este enfoque permite garantizar que el egresado no solo adquiera conocimientos, sino que sea capaz de aplicarlos de manera efectiva en contextos reales vinculados a la ciberseguridad y la informática forense.

16. ACTIVIDAD ARANCELADA

La Diplomatura Universitaria en Ciberseguridad e Informática Forense constituye una actividad arancelada**.**

Los aranceles, modalidades de pago, descuentos y condiciones administrativas serán establecidos por la institución organizadora y comunicados oportunamente a los/as interesados/as, conforme a la normativa vigente.

17. EVALUACIÓN Y ACREDITACIÓN

El proceso de evaluación de la diplomatura será continuo, formativo e integrador, orientado a valorar el desarrollo progresivo de competencias a lo largo del trayecto formativo.

Se contemplarán instancias de evaluación teóricas y prácticas en cada módulo, mediante actividades que permitan evidenciar la comprensión de los contenidos, la aplicación de conocimientos y la resolución de situaciones problemáticas.

Las evaluaciones podrán incluir:

- cuestionarios teóricos,

- actividades prácticas guiadas,
- análisis de casos,
- participación en foros,
- ejercicios de aplicación,
- y producciones individuales o grupales.

El proceso de acreditación final requerirá:

- la participación activa en las actividades propuestas,
- la aprobación de las instancias evaluativas de cada módulo,
- y la presentación y aprobación del Trabajo Final Integrador (TFI).

La evaluación del TFI contemplará tanto la calidad del informe técnico presentado como la defensa oral del mismo, considerando la aplicación de metodologías, el análisis de evidencia, la coherencia de las conclusiones y la claridad en la comunicación.

17.1 Condiciones de aprobación y certificación

Al finalizar el cursado, los estudiantes serán evaluados conforme al sistema de acreditación institucional, estableciéndose las siguientes condiciones:

Instancias y resultados final evaluación de cada módulo

En cada módulo, el cursante podrá alcanzar las siguientes condiciones:

- **Certificado:**
  Cuando el cursante apruebe satisfactoriamente las instancias evaluativas de proceso en cada módulo, evidenciando el desarrollo de las competencias previstas.
- **No certificado:**
  Cuando el cursante no logre evidenciar las competencias mínimas requeridas para la aprobación del módulo en la instancia de evaluación de proceso.

Condición para la certificación final de la diplomatura

Accederán a la certificación de egreso aquellos cursantes que:

- hayan obtenido la condición de **"Certificado" en la totalidad de los módulos**,
- y hayan aprobado el **Trabajo Final Integrador (TFI)** conforme a los criterios establecidos.

18. RÚBRICAS Y PONDERACIONES SUGERIDAS

El sistema de evaluación se estructurará mediante rúbricas que permitan valorar de manera objetiva y transparente el desempeño de los cursantes, considerando tanto aspectos teóricos como prácticos.

18.1 Criterios generales de evaluación

Se considerarán los siguientes aspectos:

- Comprensión de los contenidos teóricos
- Aplicación práctica de los conocimientos

- Capacidad de análisis e interpretación
- Integración de información de distintas fuentes
- Uso adecuado de herramientas
- Claridad en la comunicación escrita y oral

18.2 Escala de valoración

Se sugiere la siguiente escala:

- **Excelente (9–10):** dominio sólido, aplicación precisa y fundamentada
- **Muy bueno (7–8):** buen manejo de contenidos con adecuada aplicación
- **Bueno (6):** comprensión general con algunas imprecisiones
- **Regular (4–5):** dificultades en la comprensión y aplicación
- **Insuficiente (1–3):** no alcanza los criterios mínimos

18.3 Ponderación de instancias evaluativas

Las siguientes ponderaciones orientan el proceso de evaluación formativa y continua, se propone la siguiente distribución:

- **Actividades prácticas y trabajos por módulo:** 40%
- **Evaluaciones teóricas y cuestionarios:** 20%
- **Participación en foros y actividades asincrónicas:** 10%
- **Trabajo Final Integrador (TFI):** 30%

18.4 Rúbrica del Trabajo Final Integrador (TFI)

Para la evaluación del TFI se considerarán los siguientes criterios:

- Aplicación correcta de metodologías forenses
- Coherencia en la recolección y análisis de evidencia
- Integración de información (sistemas, redes, eventos)
- Fundamentación de conclusiones
- Calidad y estructura del informe técnico
- Claridad y solvencia en la defensa oral

19. REQUISITOS TÉCNICOS Y PRIVACIDAD

19.1. Requisitos técnicos mínimos para el cursado

Para el correcto desarrollo de la Diplomatura, los/as cursantes deberán contar con:

- Computadora personal con sistema operativo actualizado (Windows, Linux o macOS).
- Conexión a internet estable.
- Navegador web actualizado.
- Acceso a plataforma virtual institucional (Moodle u otra).
- Capacidad para instalar y utilizar software específico de uso académico (máquinas virtuales, herramientas de análisis y utilidades forenses básicas).

19.2. Política de grabaciones (Zoom / Moodle)

Las clases sincrónicas podrán ser grabadas con fines **exclusivamente académicos**, para su posterior consulta por parte de los/as cursantes inscriptos.
Las grabaciones estarán disponibles por un período determinado en la plataforma virtual y no podrán ser descargadas, reproducidas, difundidas ni compartidas fuera del entorno institucional, salvo autorización expresa.

19.3. Privacidad y tratamiento de datos (Ley 25.326)

El tratamiento de los datos personales de los/as cursantes se realizará conforme a lo establecido en la **Ley Nº 25.326 de Protección de los Datos Personales** y normativa complementaria vigente.

La información recolectada será utilizada únicamente con fines académicos y administrativos, garantizando la confidencialidad, integridad y seguridad de los datos, y respetando los derechos de acceso, rectificación y supresión previstos por la normativa.

20. RECURSOS

Para el desarrollo de la Diplomatura se dispondrá de los siguientes recursos:

- Plataforma virtual de gestión del aprendizaje.
- Material bibliográfico digital y recursos multimedia.
- Guías de estudio y actividades prácticas.
- Herramientas de análisis y simulación utilizadas con fines educativos.
- Acompañamiento del formador y tutorías académicas.

21. EVALUACIÓN DE IMPLEMENTACIÓN Y RESULTADOS

La implementación de la Diplomatura será objeto de un proceso de **evaluación continua**, considerando:

- El desarrollo efectivo de los módulos y actividades programadas.
- El nivel de participación y desempeño de los/as cursantes.
- Los resultados obtenidos en evaluaciones y trabajos integradores.
- La satisfacción de los/as cursantes y del equipo de formador.

Los resultados de esta evaluación permitirán introducir mejoras en futuras ediciones, fortaleciendo la calidad académica y la pertinencia del trayecto formativo.

22. ANTECEDENTES CONSULTADOS

- Instituto Nacional de Estándares y Tecnología (NIST). (2006). SP 800-86: Guía para la Integración de Técnicas Forenses en la Respuesta a Incidentes. Centro de Recursos de Seguridad Informática del NIST (CSRC). https://csrc.nist.gov/publications/detail/sp/800-86/final
- Instituto Nacional de Estándares y Tecnología (NIST). (2012). SP 800-61 Rev. 2: Guía para el manejo de incidentes de seguridad informática. NIST CSRC. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- Instituto Nacional de Estándares y Tecnología (NIST). (2006). SP 800-92: Guía para la gestión de registros de seguridad informática. NIST CSRC. https://csrc.nist.gov/publications/detail/sp/800-92/final
- Instituto Nacional de Estándares y Tecnología (NIST). (2008). SP 800-115: Guía técnica para pruebas y evaluación de seguridad de la información. NIST (Publicaciones NVL). https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf

- Organización Internacional de Normalización (ISO). (2013). ISO/IEC 27037: Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital. ISO. https://www.iso.org/standard/44381.html
- Organización Internacional de Normalización (ISO). (2022). ISO/IEC 27001: Sistemas de gestión de la seguridad de la información — Requisitos. ISO. https://www.iso.org/isoiec-27001-information-security.html
- Organización Internacional de Normalización (ISO). (2022). ISO/IEC 27002: Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información. ISO. https://www.iso.org/standard/75652.html
- Organización Internacional de Normalización (ISO). (2016). ISO/IEC 27035: Gestión de incidentes de seguridad de la información. ISO. https://www.iso.org/standard/60803.html
- Grupo de Trabajo de Ingeniería de Internet (IETF). (2002). RFC 3227: Directrices para la recopilación y el archivo de evidencias. IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc3227
- The MITRE Corporation. (s. f.). *MITRE ATT&CK® Framework*. MITRE. es una base de conocimiento globalmente accesible sobre tácticas y técnicas de adversario basada en observaciones del mundo real https://attack.mitre.org/
- Fundación OWASP. (2021). OWASP Top 10: Los diez riesgos más críticos para la seguridad de las aplicaciones web. OWASP. https://owasp.org/www-project-top-ten/
- Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia (Convenio de Budapest). Consejo de Europa (Oficina del Tratado / PDF). https://rm.coe.int/1680081561
- Instituto Nacional de Justicia (NIJ). (2008). Investigación electrónica de la escena del crimen: Guía para personal de primera respuesta (2.ª ed.). Departamento de Justicia de los Estados Unidos. https://nij.ojp.gov/library/publications/electronic-crime-scene-investigation-guide-first-responders
- Agencia de la Unión Europea para la Ciberseguridad (ENISA). (s. f.). Guía de buenas prácticas- gestión de incidentes. ENISA- https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
- Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST). (s. f.). Marco de Servicios CSIRT. FIRST. https://www.first.org/standards/frameworks/csirt-services-framework
- República Argentina. (s. f.). *Ley 25.326 – Protección de los Datos Personales (texto actualizado)*. InfoLEG – Ministerio de Justicia y Derechos Humanos. https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

- República Argentina. (s. f.). *Ley 26.388 – Delitos Informáticos*. InfoLEG – Ministerio de Justicia y DDHH. https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=141790
- República Argentina. (s. f.). *Ley 27.078 – Argentina Digital (texto actualizado)*. InfoLEG – Ministerio de Justicia y DDHH. https://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm
- Agencia de Acceso a la Información Pública (AAIP). (s. f.). *Protección de datos personales – Recursos y normativa*. Gobierno de la República Argentina. https://www.argentina.gob.ar/aaip/datospersonales