**ESPECIALIZACIÓN EN INGENIERÍA EN SISTEMAS DE INFORMACIÓN**

**MAESTRÍA EN INGENIERÍA EN SISTEMAS DE INFORMACIÓN**

***1. Nombre de la actividad curricular:*** Forensia Digital

***2. Año Académico:*** 2020

***3. Docente:*** Dra. Ing. H. Beatriz Parra de Gallo

***4. Fundamentación***

Las tecnologías de la información y de las comunicaciones (TIC) han invadido todas las áreas de la sociedad. El quehacer diario de las personas está vinculado de una forma u otra a las tecnologías informáticas, ya sea como usuario final mediante un celular, una PC o una Tablet, o como entidad que cumple un rol social, económico o comunitario, en el cual exige a sus integrantes una interacción virtual.

Esta inclusión de las tecnologías en la sociedad ha posibilitado importantes mejoras en las actividades en general, notándose su mayor impacto en el ámbito de las comunicaciones interpersonales mediante las redes sociales, la mensajería instantánea y el correo electrónico.

Pero de igual forma, así como ha favorecido la vida de las personas, también se utiliza para el desarrollo de actividades delictivas, en las cuales las TIC participan con idéntica fuerza que en el resto de los quehaceres sociales.

Ubicados en el contexto legal, a partir de 1990 surge la necesidad de convocar a peritos informáticos para que actúen como auxiliares de la justicia cuando se presenta una prueba digital. Con el transcurso del tiempo, y la evolución de las tecnologías, esta primera acción del profesional informático que solo hacía un aporte técnico pasó a convertirse en una rama de la disciplina informática con entidad propia.

Proveniente de la Informática aplicada, el desarrollo de la *Informática Jurídica* tuvo una variante distintiva cuando se abordaron las pericias informáticas. Así, surge primeramente la Informática Forense y se transforma en lo que hoy se conoce como Forensia Digital.

A partir del año 2000, comienzan a surgir los ataques a la seguridad informática, lo que produce un crecimiento en las normas y procesos necesarios para atender la problemática de hacking e intrusión sobre los sistemas informáticos. Ya en el 2005, con la incorporación de aplicaciones web, se hace más crítica la cuestión de la seguridad y resguardo de los datos, al punto de tener que generar esquemas de seguimiento y búsqueda de vulnerabilidades. Aparecen nuevas formas de la seguridad informática (hacking ético, por ejemplo) y allí se formaliza la Forensia Digital, para dar una respuesta al análisis de los incidentes de seguridad informática.

Por su parte, la Informática Forense toma para sí las herramientas y métodos de la Forensia Digital y le agrega algunos de los procedimientos propios de la criminalística como la cadena de custodia.

Se toma como definición de *Informática Forense* la propuesta por el Grupo de Investigación en Sistemas Operativos e Informática Forense de la UFASTA (Di Ioro et al., 2017) que dice: "*La Informática Forense es considerada una rama de las ciencias forenses que se encarga de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital. Es el uso de las Tecnologías de la Información para recuperar evidencia digital*".

Asimismo, se adhiere a la definición de *Forensia Digital* propuesta por (Zuccardi et al., 2006) que dice: "*Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática".*

La Forensia Digital se aplica principalmente en dos áreas: en el ámbito de la justicia mediante las pericias informáticas con la inclusión de las evidencias digitales, y en el ámbito empresarial/institucional cuando se analizan fallas de seguridad y acciones de intrusión indebidas.

Esta asignatura está dirigida a los profesionales informáticos interesados en obtener una capacitación formal sobre Forensia Digital, para lo cual se abordará el marco teórico de esta disciplina, así como las metodologías y herramientas forenses necesarias para el tratamiento de la evidencia digital.

## *5. Objetivos*

Al finalizar el cursado de la asignatura se pretende que el asistente sea capaz de:

- Conocer acerca del estado del arte de la Forensia Digital
- Comprender el proceso de tratamiento de la evidencia digital en todas sus etapas (identificación, adquisición, análisis, preservación y presentación)
- Conocer acerca de las cuestiones básicas del Derecho Procesal aplicable a la realización de pericias
- Utilizar y evaluar diferentes herramientas forenses.

## *6. Contenidos*

El contenido a impartir en la asignatura incluye las siguientes unidades temáticas:

- **Unidad I: Forensia Digital**

Definición de Forensia Digital. Conceptos fundamentales, clasificación y tipos. Marco teórico que abarca la Forensia Digital, su relación con otras disciplinas (Criminalística, Informática Forense, Seguridad Informática). Otras instancias de la Forensia Digital: Antiforensia, Hacking Ético. Principios del Derecho y legislación relacionada con la Forensia Digital. Normativa argentina e internacional.

- **Unidad II: Evidencia Digital**

Definición. Tipos de evidencia, características legales distintivas. Características de la evidencia digital: no repudio, autenticidad, veracidad. Cadena de custodia: guías de trabajo según área de competencia (Derecho Civil, Comercial, Penal, Internacional, etc.), resguardo digital y material de la evidencia digital. Derecho procesal propio del análisis forense: normas nacionales e internacionales, importancia de la cadena de custodia.

- **Unidad III: Dispositivos y artefactos forenses**

Definición. Clasificación según distintas características (hardware, autonomía, universalidad de acceso, multiplicidad de componentes, etc.). Herramientas para el análisis forense de dispositivos (discos, memorias, VM y celulares). Herramientas para el análisis forense de artefactos (redes sociales, web services, IoT, etc.). Reservorio de herramientas de acceso libre.

- **Unidad IV: Pericias Informáticas**

Metodologías para la realización de pericias: metodología PURI, normas internacionales (ISO, IRAM). Guías de procedimiento para el análisis forense de dispositivos y artefactos. Procedimientos técnicos básicos para la protección de la evidencia digital.

- **Unidad V: Actuación Pericial**

La actuación pericial: funciones y deberes del perito. Tipos de actuación (perito oficial, perito de parte). Etapas de la actuación pericial: posesión del cargo, obtención de la evidencia digital, análisis forense, informe de pericia, audiencias explicativas, impugnación. Procedimiento de posesión del cargo, requisitos y condiciones de validación previa. Cuestiones legales y formales del procedimiento pericial, según cada área del Derecho (Comercial, Penal, Laboral, Familia, etc.). Pertinencia y competencia del perito informático. El Informe Pericial: contenido, estructura, resultados, documentación técnica anexa, Evidencia digital que acompaña el informe: en versión impresa y digital, conveniencia de presentación de cada tipo.

- **Unidad VI: Herramientas para el análisis forense. Aplicaciones de la Informática a la Forensia Digital**

Características a considerar de una herramienta forense: confiabilidad, integridad, visualización, correlación de datos, importación/exportación de datos, etc. Herramientas forenses propias de cada dispositivo y/o artefacto. Estudio comparativo de las principales herramientas para los dispositivos más habituales. Herramientas Integradas

- **Unidad VII: Forensia Digital. Casos de Estudio**

Casos de estudio, problemáticas y como se resolvieron. Impacto de la prueba pericial en la decisión de la causa. Casos de estudio sobre impugnación de la pericia.

### *7. Metodología de Enseñanza y Formación práctica*

El curso se llevará a cabo en 9 (nueve) encuentros presenciales de 5 hs cada uno, más el desarrollo de actividades virtuales sincrónicas y asincrónicas que se desarrollarán en 15 hs.

Las actividades presenciales comprenden el desarrollo de un módulo teórico y la realización de actividades prácticas correspondientes. Éstas se realizarán mediante dinámicas grupales para trabajo en aula, y algunas requerirán del acceso a un laboratorio informático.

Las actividades virtuales consistirán en la realización de un trabajo integrador que será tutorizado mediante una plataforma de e-learning, y será presentado para su exposición mediante alguna herramienta virtual.

### *8. Carga horaria total*

| Unidad Temática | Contenidos Teóricos | Formación Práctica | Total |
|---|---|---|---|
| Unidad I | 2 | | 2 |
| Unidad II | 4 | 4 | 8 |
| Unidad III | 8 | 6 | 14 |
| Unidad IV | 8 | 8 | 16 |
| Unidad V | 4 | 4 | 8 |
| Unidad VI | 2 | 8 | 10 |
| Unidad VII | 2 | | 2 |

| | | | |
|---|---|---|---|
| **Total (horas)** | 30 | 30 | 60 |

| Carga horaria teórica | Carga horaria práctica | Carga horaria total |
|---|---|---|
| 30 | 30 | 60 |

### *9. Modalidad de Evaluación*

El proceso de evaluación del estudiante se realiza a través de instrumentos que permiten procesar los resultados de las actividades propuestas por el docente, entre otros: pruebas de autoevaluación, controles de lectura, trabajos prácticos individuales y grupales. Estas estrategias conforman el proceso de evaluación sumativo, que culmina con la instancia de examen final de la asignatura.

### *10. Requisitos de aprobación y promoción*

Los alumnos deberán registrar un 80% de asistencia, presentar y defender un trabajo práctico final con una calificación superior o igual a 6/10, y aprobar un examen final escrito individual que se tomará después de finalizado el dictado de la asignatura, con una calificación superior o igual a 6/10.

La calificación se expresará en escala numérica de cero (0) a diez (10) sin decimales. Para la promoción se requerirá la norma mínima de siete (7). (Extraído de la Ordenanza N° 1313)

### *11. Infraestructura y equipamiento*

La infraestructura y ámbitos a utilizar son los siguientes:

- Campus virtual: el material bibliográfico del curso, las presentaciones y los enunciados de las ejercitaciones y trabajos prácticos se encuentran disponibles en el campus virtual de la Facultad Regional Santa Fe.
- Aulas: las clases teóricas de desarrollan en un aula con capacidad para 30 estudiantes, equipo de proyección y acceso a internet mediante conexión WiFi. Todo el equipamiento mencionado es empleado en el dictado de las clases teóricas.
- Laboratorio: las clases prácticas se desarrollan en un laboratorio móvil compuesto por notebooks de la Facultad Regional Santa Fe, o por las notebooks personales de los alumnos.

### *12. Bibliografía*

- Amato, F., Cozzolino, G., & Mazzocca, N. (2017). Correlation of Digital evidences in forensic investigation through semantic technologies. In 31st International Conference on Advanced Information Networking and Applications Workshops (pp. 415–424). https://doi.org/10.1007/978-3-319-49109-7
- B. Yankson and A. Davis, "Analysis of the Current State of Cloud Forensics: The Evolving Nature of Digital Forensics," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 2019, pp. 1-8.
- Bender, A. (2017). La prueba digital. Jurisprudencia y normas del Código Civil y Comercial de la Nación. ElDial.Com Biblioteca Jurídica OnLine.

- C. S. D. Brown, “Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice,” Int. J. Cyber Criminol., vol. 9, no. 1, pp. 55–119, 2015.
- Di Iorio, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. B., ... & Greco, F. (2017). El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense
- Di Ioro, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. B., Nuñez, L. (2017). El rastro digital del delito Aspectos técnicos, legales y estratégicos de la Informática Forense. Mar del Plata: Editorial UFASTA.
- F. Amato, L. Barolli, G. C. B, A. Mazzeo, and F. Moscato, ECT: A Novel Architecture for Evidence Collection in Forensic Investigation, vol. 13. 2018.
- Ferguson, R. I., Renaud, K., Wilford, S., & Irons, A. (2020). PRECEPT: a framework for ethical digital forensics investigations. *Journal of Intellectual Capital*.
- Gerard Johansen (2017) Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents 1st Edición, Packt Publishing
- Gilardi, M., & Unzaga Domínguez, G. (2007). La Prueba Pericial en el Proceso Penal de la Provincia de Buenos Aires. Revista Buenos Aires La Ley, Año 14 Núm., 709.
- Harichandran, V. S., Walnycky, D., Baggili, I., & Breitinger, F. (2016). CuFA: A more formal definition for digital forensic artifacts. Digital Investigation, 18, S125–S137. https://doi.org/10.1016/j.diin.2016.04.005
- Leung, W. S., & Blauw, F. F. (2020). An Augmented Reality Approach to Delivering a Connected Digital Forensics Training Experience. In *Information Science and Applications* (pp. 353-361). Springer, Singapore.
- M. Chopade, S. Khan, U. Shaikh and R. Pawar, "Digital Forensics: Maintaining Chain of Custody Using Blockchain," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 744-747.
- Menéndez Mato, J.C. (2014) Derecho e Informática
- Notario, E., Gallo, B. P. D., Vegetti, M., & Leone, H. (2019). OntoFoCE: Herramienta para el Análisis Forense de Correos Electrónicos. *RISTI-Revista Ibérica de Sistemas e Tecnologías de Informação*, (32), 17-32.
- Palomo, L., Sánchez Piccardi, L., & Guillet, S. M. (2019, June). El big data de la perspectiva de sus implicaciones jurídicas en la evidencia digital. In *XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, Universidad Nacional de San Juan).*
- Parra, B., Vegetti, M., & Leone, H. (2019). Advances in the application of Ontologies in the area of Digital Forensic Electronic Mail. *IEEE Latin America Transactions*, *17*(10), 1694-1705.
- Pico I Junoy, J (2017) Peritaje y Prueba Pericial
- R. Montasari and R. Hill, "Next-Generation Digital Forensics: Challenges and Future Paradigms," 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, United Kingdom, 2019, pp. 205-212.
- Sabillón, R., Cano, M., & Jeimy, J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*, (32), 33-48.
- Tugnarelli, M., & Díaz, F. J. (2019). Forensic readiness: guía de buenas prácticas. In *XXV Congreso Argentino de Ciencias de la Computación (CACIC) (Universidad Nacional de Río Cuarto, Córdoba,*

*14 al 18 de octubre de 2019)*.

- Y. U. Sonmez and A. Varol, "Legal and Technical Aspects of Web Forensics," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-7.