Departamento:
Departamento de Ingeniería e Investigaciones Tecnológicas

Programa de acreditación:
CyTMA2

Programa de Investigación[1]:

Código del Proyecto: C2-ING-073

Título del proyecto: *Análisis del Marco Normativo, Técnico y Legal para la Implementación y Gestión de un Laboratorio de Informática Forense en el DIIT*

PIDC: ☐
Elija un elemento.
PII: ☐
Elija un elemento.

Director: *Mg. Ing. Gioia, Cintia Verónica*
Codirector: *Mg. Lic. Gigante, Nora*

Integrantes:
Dr. Allonca, Juan Cruz González

Ing. Krajnik, Mario Juan

Mg. Lic. Ureta, Walter
Investigador Externo, Asesor- Especialista, Graduado UNLaM:
Lic. Zárate, Emiliano Alejandro

Alumnos de grado: (Aclarar si tiene Beca UNLaM/CIN)
Bonavento, Sergio Gabriel

Saldaña, Fernando Ezequiel

Alumnos de posgrado:

Resolución Rectoral de acreditación: N° 370/20

Fecha de inicio: *01/01/2020*

Fecha de finalización: *31/12/2021*

[1] Los Programas de Investigación de la UNLaM están acreditados con resolución rectoral, según lo indica la Resolución HCS Nº 014/15 sobre **Lineamientos generales para el establecimiento, desarrollo y gestión de Programas de Investigación a desarrollarse en la Universidad Nacional de La Matanza**. Consultar en el departamento académico correspondiente la inscripción del proyecto en un Programa acreditado.

A. Desarrollo del proyecto (adjuntar el protocolo)

A.1. Grado de ejecución de los objetivos inicialmente planteados, modificaciones o ampliaciones u obstáculos encontrados para su realización (desarrolle en no más de dos (2) páginas)

Se detalla el resultado final del proyecto a partir de los objetivos y actividades planificados:

Desarrollo del Marco de referencia para la puesta en marcha de Laboratorios Informáticos Forenses (LabIF)

Con el objetivo de definir y redactar una guía general de arquitectura e implementación de Laboratorios de Informática Forense orientado al abordaje de pericias informáticas de distinta naturaleza y una guía general de gestión de Laboratorios de Informática Forense, se desarrolló un marco de referencia para la puesta en marcha de Laboratorios Informáticos Forenses (LabIF) aplicable tanto a la implementación como gestión de los mismos.

Dicho marco de referencia, alineado al marco regulatorio legal nacional, posibilita el desempeño eficiente y de calidad por parte equipos de profesionales en un ámbito de trabajo seguro. Disponer del mismo, favorece la cooperación entre laboratorios de diferentes organismos y entidades al generar una mayor confiabilidad y aceptación del trabajo pericial.

El marco de referencia facilitó el desarrollo de una guía para la puesta en funcionamiento de un LabIF basado en recomendaciones y mejores prácticas, como también del análisis, evaluación y prueba de plataformas y tecnologías necesarias para la implementación y gestión de los mismos.

Diseño de metodología de gestión de servicios de informática forense, llamada ForenseUDE

Se diseñó una propia metodología de gestión de servicios de informática forense, a la que se denominó “ForenseUDE”, aplicable a cualquier tipo de evidencia digital (UDE, Universal Digital Evidence). En la misma se definen y describen las etapas y actividades comunes aplicables a cualquier fuente de evidencia digital garantizando la confiabilidad de las tareas a realizar por parte del investigador y/o perito informático forense y la admisibilidad de la evidencia digital obtenida.

ForenseUDE ha sido diseñado acorde al marco legal y procesal en el que se desarrollan las actividades forenses informáticas en la República Argentina. Se sustenta en ideas y conceptos del modelo PURI (Proceso Unificado de Recuperación de Información) y del modelo EDRM (Electronic Discovery Reference Model), como también en la norma ISO/IEC 27.037.

Informe con propuestas de Tecnologías y Herramientas Informáticas Forenses

La investigación de equipos, herramientas de informática forense y de laboratorios afines nacionales e internacionales, permitió desarrollar diferentes propuestas de implementación de infraestructura tecnológica en base a la disponibilidad de recursos tecnológicos, económicos, físicos y humanos. Las propuestas se efectuaron también en base a información obtenida a través de entrevistas a profesionales referentes en la materia. Se llevó a cabo un análisis y evaluación de las diversas herramientas y equipamientos forenses informáticos existentes y necesarios para la operatoria del laboratorio en su inicio, como en etapas avanzadas, según el tipo de dispositivos involucrados, incluyendo tanto los que poseen licencias pagas, de uso gratuito o de código abierto:

- Equipos y herramientas de informática forense para pericias sobre dispositivos masivos, sobre dispositivos móviles y con fines específicos o tecnologías especiales.

- Duplicadores y bloqueadores. Sistemas operativos forenses. Estaciones Forenses.
- Herramientas de investigación digital. Herramientas para la recuperación de datos. Herramientas complementarias. Herramientas de gestión de laboratorios.

Se han definido alternativas propuestas de tecnologías mínimas a disponer para la implementación de un laboratorio informático forense incluyendo las nuevas herramientas, conforme al avance tecnológico y la incorporación de herramientas de gestión de laboratorios.

Informe de Laboratorios Informático Forenses existentes

Con el objetivo de poder conocer los lineamientos específicos que sirvan de soporte a la ahora de implementar un Laboratorio Pericial Informático Forense se han investigado diversos laboratorios informáticos forenses del país como internacionales, tanto desde sus aspectos estratégicos, organizacionales como de infraestructura para el diseño e implementación de los mismos.

La información obtenida sobre el desarrollo y actividades de dicho Laboratorio han sido de gran aporte para la investigación. Queda pendiente a futuro investigar y analizar procesos de certificación y acreditación de este tipo de laboratorios.

Capacitaciones coordinadas y dictadas por integrantes del equipo de investigación

Se han diseñado, coordinado y dictado diferentes como parte del trabajo del proyecto de investigación. El curso de “Cibercrimen e Informática Forense”, dictado en dos ocasiones en el 2020 (agosto a octubre y de septiembre a noviembre) y una vez en 2021 (octubre y noviembre), con una duración de 10 clases de 3 hs. El curso fue diseñado y coordinado por la Mg. Ing. Cintia Gioia, junto con un plantel de docentes, en el cual es integrante Emiliano Zárate, asesor externo del proyecto de investigación. En el mismo han participado alumnos del país, de diversas provincias y extranjeros de Italia, México, Ecuador, Panamá y Colombia.

El curso de “Análisis de Cibercriminalidad Económica Financiera”, dictado en junio y julio de 2021, con una duración de 8 clases de 3 hs. El curso fue diseñado y coordinado por la Mg. Ing. Cintia Gioia, junto con un plantel de docentes, en el cual es integrante Emiliano Zárate. Han participado alumnos del país, de diversas provincias y alumnos extranjeros de México, Ecuador y Colombia. También han participado profesionales invitados reconocidos en la materia.

Integrantes del proyecto de investigación han sido capacitados a través de estos cursos, con una beca otorgada a través del DIIT a los integrantes del proyecto de investigación

Se han llevado a cabo capacitaciones, entrevistas y diferentes seminarios de capacitación a nivel nacional e internacional por parte de la directora del proyecto.

Propuesta y Diseño de Diplomaturas específicas

Se ha trabajada en 2020 y en 2021 en la propuesta de Diplomaturas y Cursos específicos necesarios para la formación de recursos humanos para la implementación del Laboratorio Informático Forense del DIIT. Por un lado se diseñó y especificó la propuesta y el programa detallado de la Diplomatura de “Informática Forense e Investigación Digital” y luego también de la Diplomatura de “Técnicas Avanzadas de Informática Forense e Investigación Digital”. Se espera poder llevar a cabo las mismas durante el 2022.

B. Principales resultados de la investigación

B.1. Publicaciones en revistas (informar cada producción por separado)

Artículo 1:	
Autores	
Título del artículo	
N° de fascículo	
N° de Volumen	
Revista	
Año	
Institución editora de la revista	
País de procedencia de institución editora	
Arbitraje	Elija un elemento.
ISSN:	
URL de descarga del artículo	
N° DOI	

B.2. Libros

Libro 1	
Autores	
Título del Libro	
Año	
Editorial	
Lugar de impresión	
Arbitraje	Elija un elemento.
ISBN:	
URL de descarga del libro	
N° DOI	

B.3. Capítulos de libros

Autores	
Título del Capitulo	
Título del Libro	
Año	
Editores del libro/Compiladores	
Lugar de impresión	
Arbitraje	Elija un elemento.
ISBN:	
URL de descarga del capítulo	
N° DOI	

B.4. Trabajos presentados a congresos y/o seminarios

B.4.1	
Autores	*Gioia, Cintia; Zárate, Emiliano; Krajnik, Mario; González Allonca, Juan Cruz; Bonavento, Sergio; Gigante, Nora; Blanco, Gabriel; Eterovic Jorge*
Título	*Marco de Referencia para la Implementación y Gestión de Laboratorios de Informática Forense*
Año	*2021*
Evento	*CADI – Encuentro Argentino y Latinoamericano de Ingeniería*
Lugar de realización	*CABA - Argentina*
Fecha de presentación de la ponencia	*7/10/2021*
Entidad que organiza	*Facultad de Ingeniería de la UBA*
URL de descarga del trabajo (especificar solo si es la descarga del trabajo; formatos pdf, e-pub, etc.)	*Descarga de Actas del Congreso:* https://www.researchgate.net/publication/355339220_Actas_Congreso_Argentino_y_Latinoamericano_de_Ingeniería_2021_CADI_CLADI_CAEDI_2021 *Enlace a video de presentación del trabajo en el Congreso:* https://www.youtube.com/watch?v=idtn-JzYCC0

B.4.2	
Autores	*Gioia Cintia; Eterovic Jorge*
Título	*Metodología de Análisis Forense Informático para la Obtención de Evidencia Digital En Base De Datos*
Año	*2021*
Evento	*CADI – Encuentro Argentino y Latinoamericano de Ingeniería*
Lugar de realización	*CABA - Argentina*
Fecha de presentación de la ponencia	*7/10/2021*
Entidad que organiza	*Facultad de Ingeniería de la UBA*
URL de descarga del trabajo (especificar solo si es la descarga del trabajo; formatos pdf, e-pub, etc.)	*Descarga de Actas del Congreso:* https://www.researchgate.net/publication/355339220_Actas_Congreso_Argentino_y_Latinoamericano_de_Ingeniería_2021_CADI_CLADI_CAEDI_2021

B.5. Otras publicaciones

Autores	
Año	
Título	
Medio de Publicación	

C. Otros resultados. Indicar aquellos resultados pasibles de ser protegidos a través de instrumentos de propiedad intelectual, como patentes, derechos de autor, derechos de obtentor, etc. y desarrollos que no pueden ser protegidos por instrumentos de propiedad intelectual, como las tecnologías organizacionales y otros. Complete un cuadro por cada uno de estos dos tipos de productos.

C.1. Títulos de propiedad intelectual. Indicar: Tipo (marcas, patentes, modelos y diseños, la transferencia tecnológica) de desarrollo o producto, Titular, Fecha de solicitud, Fecha de otorgamiento

Tipo	Titular	Fecha de Solicitud	Fecha de Emisión

C.2. Otros desarrollos no pasibles de ser protegidos por títulos de propiedad intelectual. Indicar: Producto y Descripción.

Producto	Descripción
Audiovisual: "Cuidados en Entornos Digitales para niños y niñas" Autores: Cintia Gioia y Emiliano Zárate Organización: DIIT UNLaM Diseño Gráfico, Animación y Desarrollo: Cintia Gioia Idea y Guion: Cintia Gioia y Emiliano Zárate Voz: Cintia Gioia Sonido: Cintia Gioia y Emiliano Zárate YouTube en el siguiente enlace: https://www.youtube.com/watch?v=j3VTjGos3KY  	Desarrollo de un video animado para niñas, niños y adolescentes (NNA) con el objetivo de prevenir, concientizar y orientarlos sobre el uso responsable de las Tecnologías en Internet y cómo actuar ante casos de Grooming. El video incluye subtítulos y audio de manera de poder ser escuchado o leído por personas con discapacidad visual y/o auditiva. El video fue publicado por Departamento de Actividades Socioculturales y Extracurriculares de la Secretaría de Extensión Universitaria en el período de vacaciones de invierno, en representación del DIIT, como parte de las actividades que se hicieron en modalidad virtual por el contexto de la pandemia. Fue difundido por el DIIT y los medios de UNLAM como campaña de prevención. Entrevista Radio Universidad 89.1: http://www.fm891.com.ar/podcast/la-unlam-promueve-la-proteccion-de-ninas-ninos-y-adolescentes-en-internet/

Aplicación Móvil EMMA – Prevención del Grooming Dirección del proyecto de desarrollo a cargo de Mg. Ing. Cintia Gioia. Desarrollada como proyecto final de carrera con estudiantes de la Tecnicatura en Desarrollo Web y Tecnicatura en Desarrollo de Aplicaciones Móviles.	Aplicación Móvil para prevenir el ciber acoso sexual de niñas, niños y adolescentes en medios digitales. Los objetivos principales son capacitar, concientizar y prevenir el Delito de Grooming, detectar y asistir a NNA y a adultos ante la presencia de un caso de Delito de Grooming, alertar situaciones de riesgos, enlazar a números telefónicos para realizar las denuncias y organizaciones de ayuda y recolectar información estadística a partir de la información obtenida desde la aplicación.

D. Formación de recursos humanos. Trabajos finales de graduación, tesis de grado y posgrado. Completar un cuadro por cada uno de los trabajos generados en el marco del proyecto.

D.1. Tesis de grado

Director (apellido y nombre)	Autor (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título de la tesis
Fernández Patricia	Zárate Emiliano	Instituto Universitario de la Policía Federal Argentina (IUPFA)	10 (diez)	10/12/21	Análisis Criminal del Abuso Sexual de Niños, Niñas y Adolescentes en Línea

D.2 Trabajo Final de Especialización

Director (apellido y nombre)	Autor (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título del Trabajo Final

D.2. Tesis de posgrado: Maestría

Director (apellido y nombre)	Tesista (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título de la tesis

D.3. Tesis de posgrado: Doctorado

Director (apellido y nombre)	Tesista (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título de la tesis

D.4. Trabajos de Posdoctorado

Director (apellido y nombre)	Posdoctorando (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título del trabajo	Publicación

E. Otros recursos humanos en formación: estudiantes/ investigadores (grado/posgrado/ posdoctorado)

Apellido y nombre del Recurso Humano	Tipo	Institución	Período (desde/hasta)	Actividad asignada[2]
Bonavento Sergio	*Alumno de Grado*	*UNLAM*	*1/1/2020-31/12/2021*	*Capacitación en Informática Forense. Participación en desarrollo del informe de equipos y herramientas forenses a ser parte de distintas propuestas de implementación del laboratorio informático forense del DIIT.*
Saldaña Fernando	*Alumno de Grado*	*UNLAM*	*1/1/2020-31/12/2021*	*Capacitación en Informática Forense. Participación en el desarrollo de una guía de implementación de laboratorios informático forense.*

F. Vinculación[3]: Indicar conformación de redes, intercambio científico, etc. con otros grupos de investigación; con el ámbito productivo o con entidades públicas. Desarrolle en no más de dos (2) páginas.

REDUNIF

El DIIT de UNLaM **integra** la **REDUNIF desde junio de 2019** con la representación de la Mg. Cintia V. Gioia. Con el proyecto actual y las actividades que se desarrollan desde el mismo se afianza la presencia de UNLaM en la red.

Desde el 1ero de noviembre de 2021 la Mg. Ing. Cintia V. Gioia forma parte de la Comisión Directiva de la REDUNIF cumpliendo el rol de Secretaria General en la misma. El cargo fue obtenido por votación de los integrantes de la red durante la séptima Asamblea de la red llevaba a cabo en modalidad virtual.

La REDUNIF, es la **Red Universitaria de Informática Forense** integrada por las instituciones académicas referentes del país en la temática cuyo objetivo es promover la integración y cooperación interinstitucional en la investigación y el desarrollo de la aplicación forense de la informática a nivel nacional. La Universidad FASTA, con su **laboratorio Info-Lab**, es miembro fundador de la red.

[2] Descripción de la/s actividad/es a cargo (máximo 30 palabras)

[3] Entendemos por acciones de "vinculación" aquellas que tienen por objetivo dar respuesta a problemas, generando la creación de productos o servicios innovadores y confeccionados "a medida" de sus contrapartes.

Ser miembros de la REDUNIF y representados en la misma por un miembro del equipo, posibilitó iniciar un intercambio de conocimientos y acceso a información directa a los equipos que diseñaron y desarrollaron los procesos y documentos mencionados. Se ha participado en diferentes reuniones y actividades de la red sobre temáticas directamente relacionadas con el proyecto de investigación.

InfoLab

Se ha continuó afianzando en la vinculación con **Info-Lab**, **Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense** (iniciativa conjunta desde 2014 de la Universidad FASTA, la Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredón). **Info-Lab** nuclea a un equipo interdisciplinario abocado a la investigación y el desarrollo tecnológico en ciencias de aplicación forense y de apoyo a la investigación criminal. Los avances de investigación y desarrollo de Info-Lab son de gran aporte para el proyecto y gran referencia en especial en aspectos técnicos, legales y estratégicos de la informática forense.

Comisión IRAM

La directora Mg. Ing. Cintia V. Gioia fue convocada por **IRAM** para formar parte de la **Comisión de Informática Forense desde marzo de 2019, en representación de UNLaM**. Dicha convocatoria y participación fue de gran aporte para el proyecto ya que se sigue trabajando directamente con el organismo que analiza las normas internacionales ISO 27.037 (y relacionadas) de Informática Forense para determinar la adopción, modificación o el desarrollo de normas propias adecuadas a la ley nacional vigente, a la estructura del Derecho y a la característica del país federal que es Argentina.

De 2019 a fines de 2021 se trabajó principalmente en la traducción con aclaraciones de la norma IRAM-ISO/IEC 27.037. Hasta fines de abril de 2022 ya se encuentra en discusión pública, en este período de 60 días se esperan recibir observaciones tanto de integrantes del subcomité como otros miembros del IRAM y del público en general, para luego poder publicar la norma definitiva en IRAM.

Hacia mediados de 2021 se empezó a trabajar en la traducción de la **norma IRAM-ISO/IEC 27042:2015** (Tecnología de la información. Técnicas de seguridad. Guías para el análisis y la interpretación de la evidencia digital) y en el desarrollo de la **norma IRAM 36.100** (Procedimiento de instrumentación de la cadena de custodia en Informática Forense) a proponer en Argentina. **Por tal motivo se espera seguir trabajando durante el año 2022.**

El ser parte de la **Comisión de Informática Forense de IRAM** brinda la posibilidad de trabajar directamente con el organismo y con los principales exponentes de la temática a nivel nacional y de los diferentes organizamos de gobierno y judiciales involucrados. Se comparte y analiza con el equipo de investigación los avances del trabajo realizado en la Comisión de Informática Forense de IRAM en relación con la adopción de Estándares Internacionales a nuestro país.

Programa de Ciberseguridad de la OEA

A partir de las becas e invitaciones otorgadas por la **OEA (Organización de Estados Americanos)** a la Mg. Ing. Cintia V. Gioia para participar en sus **Simposios de Ciberseguridad** se espera afianzar el vínculo con el **Programa de Ciberseguridad de la OEA**, en particular con los grupos de experto e investigadores dedicados a debatir y compartir conocimiento y buenas prácticas en prácticas forense informáticas, los desafíos actuales de la informática forense y su aplicación según las regulaciones de cada país de los Estados Americanos.

En el año 2020 y 2021 el Simposio se llevó a cabo en forma virtual y participaron profesionales a quienes se les hizo llegar una invitación personal de participación al **"Simposio de Ciberseguridad de la OEA 2020"** y el **"Simposio de Ciberseguridad de la OEA 2021"** (en ediciones previas del año 2018 y 2019, en Washington DC y Chile, la UNLAM participó a través de becas otorgadas a la Mg. Ing. Cintia V. Gioia).

En el año 2020 se llegó a presentar el proyecto en la solicitud de **Fondo de Innovación para proyectos de Ciberseguridad de la OEA** desarrollados junto a **CISCO y la Fundación Citi** en la Categoría de "Prevención, lucha y clasificación del delito digital". Si bien el proyecto no fue seleccionado, permitió difundir a la Universidad Nacional de la Matanza como la primera universidad nacional con el objetivo de poder implementar un Laboratorio Informático Forense propio de alto nivel que brinde servicios profesionales y académicos, basado en la implementación de plataformas y tecnologías forenses de última generación, al alcance de todos los alumnos y profesionales que quieran desarrollarse en una rama cuya demanda de profesionales peritos informáticos e investigadores digitales crece a un ritmo exponencial.

Laboratorios de Informática Forense de organismos oficiales

Se realizaron relevamientos a **fuerzas de la ley, policiales y cuerpo de investigaciones judiciales** que disponen de laboratorios informáticos forenses, como también a **expertos peritos referentes**, con los cuales se mantuvieron reuniones específicas y se han compartido espacio de capacitación y actualización conjunta. Se inició contacto y se mantuvieron reuniones con Norberto Adrián Gabot, **Director de Investigaciones del Cibercrimen de la Policía de la Provincia de Buenos Aires**, quien se encuentra interesado en firmar un convenio marco, para luego evaluar acciones o actividades específicas en el laboratorio de informática forense a su cargo.

COPITEC y Ministerio Público Fiscal de la Provincia de Buenos Aires

A través de los cursos de "Cibercrimen e Informática Forense" (2020) brindadas a la comunidad por parte del equipo del proyecto se establecieron convenios de capacitación con el **COPITEC** (Consejo Profesional de Ingeniería de Telecomunicaciones, Electrónica y Computación, Persona Jurídica Pública) y con el **Ministerio Público Fiscal de la Provincia de Buenos Aires** a través del Secretario de Política Criminal Dr. Francisco Pont Verges. Ambos en la marco de convenios marcos firmados en años previos entre UNLAM y los organismos mencionados.

Estos convenios continuaron vigentes para los cursos dictados también por parte del equipo del proyecto durante el año 2021: "Curso de Cibercriminalidad Económico-Financiera" y "Cibercrimen e Informática Forense"

Se adjunta detalle y certificados del punto F en el Anexo III de este documento.

G. Otra información. Incluir toda otra información que se considere pertinente.

1	**Coordinación y Docencia de cursos. Capacitación a integrantes del proyecto.**	**Archivos en Anexo IV**
1.1	**Coordinación y dictado del Curso de Cibercrimen e Informática Forense en DIIT UNLAM (2020)** -Coordinación: Mg. Ing. Cintia Gioia -Docentes del equipo de investigación: Mg. Ing. Cintia Gioia, Lic. Emiliano Zárate -Capacitación a integrantes del equipo de investigación (beca otorgada a través del DIIT): Ing. Mario Krajnik, Fernando Saldaña y Sergio Bonavento El mismo fue dictado en dos ocasiones durante agosto a noviembre del 2020, con una duración de 10 clases de 3 hs, cada uno. En el mismo han participado alumnos del país, de diversas provincias y extranjeros de Italia, México, Ecuador, Panamá y Colombia.	Certificados de Coordinación y Docente del Curso de Cibercrimen e Informática Forense de Cintia Gioia Certificado Docente de Curso de Cibercrimen e Informática Forense de Emiliana Zárate. Certificado de Asistencia al Curso de Cibercrimen e Informática Forense de Mario Krajnik, Sergio Bonavento y Fernando Saldaña. Flyer
1.2	**Coordinación y dictado Curso de Análisis de Cibercriminalidad Económica y Financiera en DIIT y Sec. Ext UNLAM (2021)** -Coordinación: Mg. Ing. Cintia Gioia -Docentes del equipo de investigación: Mg. Ing. Cintia Gioia, Lic. Emiliano Zárate -Capacitación a integrantes del equipo de investigación (beca otorgada a través del DIIT): Ing. Mario Krajnik, Lic. Nora Gigante y Sergio Bonavento El curso se llevó a cabo de junio a julio del 2021, con una duración de 8 clases de 3 hs. Han participado alumnos del país, de diversas provincias y alumnos extranjeros de México, Ecuador y Colombia. También profesionales invitados reconocidos en la materia: Gustavo Presman (Perito reconocido a nivel nacional e internacional), Delbono Patricia (Consejera Titular del COPITEC. Coordinadora de Comisión de Peritos Judiciales del COPITEC), Fernández Noguera Matías (Perito de la Unidad Fiscal Especializada en Delitos Contravencionales Informáticas UFEDyCI del Ministerio Público Fiscal CABA), Bucci Diego (Perito del Laboratorio Informática Forense del CIJ Cuerpo de Investigaciones Judiciales Ministerio Público Fiscal CABA y Jefe del área de Ingeniería Inversa), Borrero Vázquez Nazly (Directora de Colombia Cibersegura. Directora de Fundación Saving Cyber Children Colombia), Quiñonez Urquiza Laura (Perfiladora Criminal), Antin Miguel (Especialista en Ciencia de Datos y en Lavado de Dinero).	Certificados de Coordinación y Docente del Curso de Cibercrimen e Informática Forense de Cintia Gioia Certificado Docente de Curso de Cibercrimen e Informática Forense de Emiliano Zárate. Certificado de Asistencia al Curso de Cibercrimen e Informática Forense de Mario Krajnik y Sergio Bonavento. Flyer

1.3	**Coordinación y dictado Curso de Cibercrimen e Informática Forense en DIIT y Sec. de Extensión UNLAM (2021)** -Coordinación: Mg. Ing. Cintia Gioia -Docentes del equipo de investigación: Mg. Ing. Cintia Gioia, Lic. Emiliano Zárate -Sitio Web: https://cursocibercrimen.unlam.edu.ar El curso se llevó a cabo de junio de octubre a noviembre del 2021, con una duración de 10 clases de 3 hs. En el mismo han participado alumnos del país, de diversas provincias y extranjeros de México, Ecuador, Panamá y Colombia.	Certificados de Coordinación y Docente del Curso de Cibercrimen e Informática Forense de Cintia Gioia Certificado Docente de Curso de Cibercrimen e Informática Forense de Emiliana Zárate. Flyer

2	**Docente de capacitaciones en otras Universidades y organismos en representación de UNLAM**	**Archivos en Anexo IV**
2.1	**Docente en Diplomado de Posgrado en Violencia de Género (2021)** La Mg. Ing. Cintia Gioia se ha desempeñado como docente en Diplomado de Violencia de Género de la Universidad de Hartmann (México), en las clases de informática forense. Plantel Docente Internacional: - Dra. Rita Segato Antropóloga, Universidad de Queens. - Lic. Laura Silisque, Psicóloga Forense del área de Orientación y Denuncia del Ministerio Público de Salta. - Dra. Mary Ellen O'Toole, Psicóloga forense y Perfiladora Criminal Senior del FBI. Conferencista de la Academia de Quántico sobre psicopatía y entrevistas. - Dr. Miguel Ángel Miñones, Médico Legista y Forense, perito. - Mg. Ing. Cintia Gioia, Mg. Ingeniera en sistemas, Departamento de Ingeniería e Investigaciones Tecnológicas de la Univ. Nacional de la Matanza. - Dra. Sheila Queralt, doctora en Ciencias del Lenguaje. Perito judicial en Lingüística Forense. - Dra. Mariana Ruffino, Fiscal especializada en violencia de género, Fiscalía N° 13 de La Plata. - Dr. Pablo Casas, juez de Primera Instancia en el fuero Penal Contravencional y de Faltas Nº 10 CABA - Dra. Nahikari Sánchez, criminóloga. - Dr. Horacio Días, Juez de Cámara en Cámara Nacional de Casación en lo Criminal y Correccional. - Laura Quiñones Urquiza, Diplomada en Criminología, Criminalística y DDHH, Técnica de Perfilación Criminal.	Certificado de Docente de Cintia Gioia Flyers de Difusión
2.2	**Docente en Ciclo de Talleres de Women Of Security Capítulo de Panamá. Webinar: Modalidades Delictivas contra NNA en medios digitales** (Panamá, Agosto 2021) Enlace: https://www.proyecto-aurora.org/genero	Certificados de Docente de Cintia Gioia Carta de Agradecimiento a UNLAM y a Cintia Gioia Archivos en Anexo IV
2.3	Panelista en **1º Foro Internacional de Igualdad de Género. Mujeres que hacen e inspiran** en Ciberseguridad y en Tecnologías, organizado por **Proyecto Aurora ONG** con mas más	Flyer del Foro de Proyecto Aurora Flyer de difusión desde UNLAM

	de 35 Mujeres de LATAM y España, líderes y destacadas profesionales. Panel Grace Murray Hooper. 8 de marzo 2021. CABA, Argentina. Entrevista Radio Universidad 89.1: http://www.fm891.com.ar/podcast/dia-internacional-de-la-mujer-trabajadora-la-mujer-en-el-ambito-de-tecnologias/?fbclid=IwAR1m0ruhX7RpPRXfxjYWyBdyhmcnngvC0hRUbo8eJPuaa5esfLVIugetif4 Publicación en diario digital La Matanza Informa: https://www.lamatanzainforma.com.ar/la-unlam-participara-del-1-foro-internacional-de-igualdad-de-genero/	

3	Exposiciones y entrevistas Nacionales e Internaciones	Archivos en Anexo IV
3.1.	Exposición a cargo de Mg. Ing. Cintia V. Gioia en **"The Global Women in Security Alliance 2020 Virtual Series".** Tema: "Metodología de análisis forense informático para la obtención de evidencia digital en base de datos". **ASIS Internacional, WIS (Woman in Security), World Wide Women in Security (WWWIS).** EEUU. Octubre 2020. Episodio 1863 - The GLOBAL WOMEN IN SECURITY ALLIANCE 2020 VIRTUAL SERIES. Este episodio formó parte de 66 entrevistas con 80 mujeres de 16 países diferentes. Enlace a episodio: https://www.linkedin.com/posts/activity-6745710468737888257-1zi-/?fbclid=IwAR0sWLTyI8wPt-gQta7SdnITwwRYC2RK0aUSTt0VMgum9tzmqEeHOOjVFJ9E	Flyer de Episodio
3.2	Exposición a cargo de Mg. Ing. Cintia V. Gioia en **Webinar "Elaboración de Planes de Prevención de Seguridad de la Información en redes sociales y para el trabajo remoto"** organizado por **ASIS International** para Argentina, Bolivia, Chile, Paraguay, Perú, Uruguay. 19 de Mayo de 2020. Enlace al Webinar: https://youtu.be/SKGwLydgXlE	Flyer de Webinar
3.3	Entrevista en **Radio Universidad FM 89.1 sobre "Seguridad de menores en las redes en tiempos de cuarentena".** Julio 2020. UNLaM. PROGRAMA: Lo Que Mueve - CONDUCCION: María Braga Enlace a la nota: https://www.youtube.com/watch?v=rw3jMV1X0xw	
3.4	Entrevista a Mg. Ing. Cintia Gioia en **Radio Universidad FM 89.1**: **La UNLaM promueve protección de Niñas, Niños y Adolescentes en Internet**.. Presentación de video educativo con el objetivo de prevenir y orientar a niñas, niños y adolescentes sobre el uso responsable de las Tecnologías en Internet y cómo actuar ante un caso de Grooming. 3 de agosto de 2021. UNLaM. PROGRAMA: Lo Que Mueve - CONDUCCION: María Braga Enlace a la nota: http://www.fm891.com.ar/podcast/la-unlam-promueve-la-proteccion-de-ninas-ninos-y-adolescentes-en-internet/	

3.5	Entrevistas en programa **Seguimos Educando, Canal Encuentro sobre Ciberseguridad y Criptografía**. 15 de mayo 2020. 21 de octubre de 2020. Con Darío Sztajnszrajber.	
3.6	Exposición a cargo de Mg. Ing. Cintia V. Gioia "**Modalidades de Violencia de Género Digital**" en seminario organizado por **Proyecto Aurora ONG**. 27 de octubre 2021. CABA, Argentina. Enlace a Seminario: https://www.youtube.com/watch?v=C7sjFlUDL4Q	Flyer de Seminario
3.7	Panelista **"Sin Violencia Digital". Academia Mexicana de Ciberseguridad y Derecho Digital AMCID**. 25 de noviembre 2021. México. Enlace a Webinar: https://www.linkedin.com/video/live/urn:li:ugcPost:6869790991642173440/	Flyer de Webinar
3.8	Entrevistas sobre Ciberseguridad en **el programa multimedial "Somos lo que hacemos"**, programa referente para cambiar la mirada social hacia la discapacidad**.** www.radiowox.com. 88.3 FM. 2020. Desde Mediados de 2020 a la actualidad Mg. Cinta Gioia es columnista de Delitos Informáticos y Discapacidad en el programa. - "Ciberbulliyng y las diferentes modalidades de Hostigamiento y Acoso Digital a personas con Discapacidad". 8 de julio de 2020. https://www.youtube.com/watch?v=spYFqcid26A - "Hablemos de Grooming y Discapacidad- Prevención". 31 de julio de 2020. https://www.youtube.com/watch?v=KAZ_nsejZeg - "El uso Malicioso de Internet para Engañar y Perjudicar". 19 de agosto de 2020. https://www.youtube.com/watch?v=IGNV90W3grI - "Consecuencias de la falta de Accesibilidad para Personas con Discapacidad en la Web". 15 de septiembre de 2020. https://www.youtube.com/watch?v=DzSvV0_wBHc - "Prevención en Niños y Jóvenes con Discapacidad en el uso de Internet". 9 de octubre de 2020. https://www.youtube.com/watch?v=CTbljpcLUgI - "Fake News- Su impacto en las Personas con Discapacidad". 29 de octubre de 2020. https://www.youtube.com/watch?v=k4GDsMvAyqM - "Ley Mica Ortega- Frenemos el Grooming". 23 de noviembre de 2020. https://youtu.be/vfB5p1trXGk - "Sexting- Sextorsión- Consecuencias en menores". 22 de diciembre de 2020. https://www.youtube.com/watch?v=bocS2TE3AH8 - "Violencia Digital a la mujer". 7 de marzo de 2021. https://www.youtube.com/watch?v=74h5CF7fJeg - "Doxing -Práctica de investigar, recopilar y difundir información sobre una persona sin su consentimiento para humillar". 12 de mayo de 2021. https://www.youtube.com/watch?v=MykQwO-ptTs	

	- "Estafas de WhatsApp con el turno de la vacuna contra el COVID19" . 17 de julio de 2021. https://www.youtube.com/watch?v=7a5s-lL5gjM - "Presentación de Campaña de UNLAM de Prevención del Grooming". 14 de agosto de 2021. https://www.youtube.com/watch?v=QNloggsRLGQ - "Violencia de Género Digital. Sextorsion. Pornovenganza. Divulgación de fotos íntimas. Ciberstalking.". 30 de octubre de 2021. https://www.youtube.com/watch?v=xDVUU6BczSI	

4	Concursos	Archivos en Anexo IV
4.1	La Mg. Ing. Cintia Gioia fue nominada y rankeada en **el 2do puesto nacional** de **"Ciberinfluencers", el ranking de líderes en ciberseguridad de Iberoamérica.** Alcanzando el puesto 19 en el top 100 internacional. Los países participantes fueron Argentina, Bolivia, Brasil, Chile, Colombia, Centro América y Caribe, Ecuador, España, México, Paraguay, Perú, Uruguay y Venezuela. Cada país tuvo su top 10 y luego un top 100 entre todos los países participantes. Enlace a resultados del Ranking: https://cyberheroes.app/ciberinfluencers/index.html	Flyer y resultados de Ranking Nacional e Internacional

5	Asistencia a conferencias, congresos, cursos, etc.	Archivos en Anexo IV
5.1	**Capacitación Cibercrimen de la "A" a la "Z"** organizado por Instructor Emiliano Zárate y profesionales reconocidos en la temática. 10 horas. Abril 2020.	Certificado de participación de Cintia Gioia
5.2	**"1er Seminario Internacional de Cibercrimen"**. Hablando del Cibercrimen desde la prevención, capacitación y cooperación internacional" organizado por **Proyecto Aurora con Certificación 360**. Duración 5 hs. Modalidad Online. 11 de junio de 2020.	Certificado de participación de Cintia Gioia
5.3	Participación en **Curso Internacional en Abuso y Explotación Sexual Infantil en Línea (2020). ICMEC (International Centre for Missing & Exploited Children) en conjunto con UNODC (United Nations on Drugs and Crime). 12 sesiones desde el 24 de** Noviembre al 12 de Diciembre.	Certificado de aprobación de Cintia Gioia
5.4	Asistente en Ciclo de **"Búsqueda de Personas Desaparecidas y Extraviadas e Identificación de Personas con identidad Desconocida"** organizada por el **Sistema Federal de Búsqueda de Personas Desaparecidas y Extraviadas (SIFEBU) de la Subsecretaría de Investigación Criminal y Cooperación Judicial del Ministerio de Seguridad de la Nación**. Modalidad Virtual. De noviembre y 3,10 y 17 de diciembre de 2020.	Certificado de asistencia de Cintia Gioia
5.5	Certificado de Asistencia al **12vo. Congreso COLTIC 2021 de "Innovación para la investigación del delito en la nueva realidad".** 6 y 7 de octubre de 2021.	Certificado de asistencia de Cintia Gioia

5.6	**Cursos de actualización** Curso de curso Cibercrimen y Evidencia Digital. Educación IT. 14 hs. Noviembre 2021. Modalidad Virtual. Curso de curso Informática Forense. Educación IT. 15 hs. Noviembre-Diciembre 2021. Modalidad Virtual.	Certificados de Aprobación Cintia Gioia
5.7	**5ta Info-Conf 2021 Conferencia Nacional de Informática Forense**. 23 y 24 de Septiembre de 2021. Facultad de Ingeniería del Ejército. Universidad de la Defensa Nacional.	Certificados de asistencia de Mario Krajnik Certificados de asistencia de Cintia Gioia

Se adjunta certificados y archivos relacionados del punto G en el Anexo IV de este documento.

H. Cuerpo de anexos:

- Anexo I: Copia de cada uno de los trabajos mencionados en los puntos B, C y D, y certificaciones cuando corresponda.[4]
- Anexo II:
  - FPI-013: Evaluación de alumnos integrantes. (si corresponde)
  - FPI-014: Comprobante de liquidación y rendición de viáticos. (si corresponde)
  - FPI-015: Rendición de gastos del proyecto de investigación acompañado de las hojas foliadas con los comprobantes de gastos.
  - FPI-035: Formulario de reasignación de fondos en Presupuesto.
- Nota justificando baja de integrantes del equipo de investigación.

Firma y aclaración
del director del proyecto.

Lugar y fecha: Buenos Aires, 31 de Marzo 2022

- Cargar este formulario junto con los documentos correspondientes **exclusivamente** al Anexo I en SIGEVA UNLaM. Realizar la presentación impresa de los mismos junto con los restantes Anexos en la Secretaría de Investigación de la unidad académica correspondiente**. Límite de entrega: 28 de febrero de 2022.**

[4] En caso de libros, podrá presentarse una fotocopia de la primera hoja significativa o su equivalente y el índice.

ANEXO I

B.4. Trabajos presentados a congresos y/o seminarios

B.4.1

B.4.1 Paper:

CADI 9to. Congreso Argentino de Ingeniería
11vo. Congreso Argentino de Enseñanza de la Ingeniería

"MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN Y GESTIÓN DE LABORATORIOS DE INFORMÁTICA FORENSE"

Gioia, Cintia [a]; Zárate, Emiliano [a]; Krajnik, Mario [a]; González Allonca, Juan Cruz [a]; Bonavento, Sergio [a]; Gigante, Nora [a]; Blanco, Gabriel [a]; Eterovic Jorge Esteban [a]
a Departamento de Ingeniería e Investigaciones Tecnológicas - Universidad Nacional de la Matanza
cgioia@unlam.edu.ar

Resumen

En vista a los acontecimientos delictivos informáticos y el propio devenir tecnológico es crucial disponer de Laboratorios de Informática Forense que brinden servicios profesionales de informática forense y que dispongan de multiplicidad de equipamiento y tecnologías necesarias. La diversidad de tecnologías y el volumen de información a analizar exigen que se dispongan de equipamientos de cómputos de alta prestaciones, diversidad de tecnologías forense y multiplicidad de expertos.

Se necesitan implementar Laboratorios de Informática Forense que, además de la infraestructura, equipamiento y tecnologías forenses, ofrezcan servicios periciales seguros y de calidad basados en un sistema de gestión con metodologías claras de trabajo, procedimientos operativos de actuación, asignación de roles y responsabilidades y la disponibilidad de variedad de herramientas para responder a las necesidades tecnológicas según la naturaleza de la evidencia digital a tratar.

En este trabajo se presenta el desarrollo de un marco de referencia para la puesta en marcha de Laboratorios Informáticos Forenses que esclarece cómo abordar una implementación de un laboratorio de este tipo y su posterior gestión, basado en una estrategia enfocada tanto en la infraestructura y tecnología, como también en los procesos y metodologías de trabajo. La investigación de equipamientos, herramientas y de laboratorios afines, nacionales e internacionales, permitió desarrollar propuestas de implementación según sus capacidades y objetivos, acompañados de una guía integral, que sirve de referencia para la implementación de los mismos, posibilitando el desempeño eficiente y de calidad por parte equipos de profesionales en un ámbito de trabajo seguro.

Abstract

Due to the computer crime events and the technological evolution itself, it is crucial to have Forensic Computer Science Laboratories that provide professional computer forensic services and that have a multiplicity of necessary equipment and technologies. The diversity of technologies and the volume of information to be analyzed require the availability of high-performance computing equipment, diversity of forensic technologies and multiple experts.

It is necessary to implement Forensic Informatics Laboratories that, in addition to the infrastructure, equipment and forensic technologies, offer safe and quality expert services based on a management system with clear work methodologies, operational procedures for action, assignment of roles and responsibilities and the availability of a variety of tools to respond to technological needs according to the nature of the digital evidence to be treated.

This paper presents the development of a reference framework for the implementation of Forensic Computer Laboratories that clarifies how to approach an implementation of a laboratory of this type and its subsequent management, based on a strategy focused on both infrastructure and technology, as well as in work processes and methodologies.

The investigation of equipment, tools and related laboratories, national and international, allowed to develop implementation proposals according to their capacities and objectives, accompanied by a comprehensive guide, which serves as a reference for their implementation, enabling efficient and quality performance. by teams of professionals in a safe work environment.

Palabras clave: Laboratorio informático forense, Informática Forense, Evidencia Digital, Pericia Informática.

CADI 5to. Congreso Argentino de Ingeniería 11vo. Congreso Argentino de Enseñanza de la Ingeniería

INTRODUCCIÓN

Hoy en día la demanda mundial de Laboratorios de Informática Forense es cada vez mayor. Dada la variedad de tecnologías involucradas en delitos informáticos se hace indispensable disponer de laboratorios que brinden soporte pericial a múltiples tecnologías, garantizando la aplicación de herramientas adecuadas por parte de personal calificado. El tratamiento de la evidencia digital en todo su ciclo de vida es uno de los puntos más críticos en un trabajo pericial forense, ya que si el proceso de adquisición y recolección de la misma no es el adecuado desde un principio se tiende a que todo el proceso pierda su validez.

Se espera esclarecer cómo abordar una implementación y gestión de un Laboratorio Informático Forense basado en una estrategia enfocada tanto en la infraestructura y tecnología como en los procesos y metodologías de trabajo que ordenen, guíen y garanticen la confiabilidad de los datos recogidos, la integridad de los medios y el análisis detallado de los datos.

Muchos de los actuales laboratorios pertenecientes a organismos gubernamentales, fuerzas de seguridad o cuerpos judiciales se encuentran colapsados por la cantidad de casos a procesar y la disponibilidad limitada de recursos humanos o tecnológicos.

El presente trabajo es parte de los avances realizados en el marco del proyecto de "Análisis del Marco Normativo, Técnico y Legal para la Implementación y Gestión de un Laboratorio de Informática Forense en el DIIT", denominado LabIF-Unlam, perteneciente al Departamento de Ingeniería e Investigaciones Tecnológicas (DIIT) de la Universidad Nacional de la Matanza.

DESARROLLO

Marco de Estudio

Existen importantes trabajos relacionadas con la implementación y gestión de laboratorios informáticos que proporcionaron significativos antecedentes y elementos para abordar el desarrollo del presente proyecto.

En primer lugar mencionar la "Guía Técnica para el Diseño, Implementación y Gestión de Laboratorios de Informática Forense" [1] desarrollada por Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab). En esta Guía se presentaron algunos desafíos a resolver en torno al diseño, implementación y gestión de este tipo de laboratorios: estándares sobre su diseño, construcción, organización y operatividad, así como necesidades espaciales, organizacionales y de infraestructura específicas. En conjunto con esta guía se resalta el gran aporte del trabajo "Guía Técnica para la Implementación de un Laboratorio Judicial" [2] en especial a lo relacionado a la sistema de gestión de calidad.

El trabajo "Lineamientos para la creación de laboratorios informáticos forenses" [3] del Poder Judicial de la provincia de Rio Negro, brinda elementos generales y una guía tentativa para la creación de un laboratorio pericial informático. Se resalta del mismo la exposición de un modelo de trabajo basado en un cambio de paradigma centrado en niveles de maduración que permite brindar un mejor servicio a largo plazo.

Otro trabajo a mencionar es el "Plan Estratégico para la implementación de un Centro de Servicios de Informática Forense" [4] formulado con el objetivo de estudiar y definir una metodología científica para el desarrollo del proceso de pericias informáticas para el Poder Judicial de la Provincia de Salta. El plan propone cuatro etapas, la definición de la misión y la visión de un Centro de Servicios de Informática Forense, el análisis del contexto externo e interno, la formulación de estrategias y el plan de acción.

Planteo General de la Solución

Se propone un marco de referencia para la puesta en marcha de Laboratorios Informáticos Forenses (LabIF) aplicable tanto a la implementación como gestión de los mismos. Dicho marco de referencia, alineado al marco regulatorio legal nacional, posibilita el desempeño eficiente y de calidad por parte equipos de profesionales en un ámbito de trabajo seguro. Disponer del mismo, favorece la cooperación entre laboratorios de diferentes organismos y entidades al generar una mayor confiabilidad y aceptación del trabajo pericial.

El marco de referencia facilitó el desarrollo de una guía para la puesta en funcionamiento de un LabIF basado en recomendaciones y mejores prácticas, como también del análisis, evaluación y prueba de plataformas y tecnologías necesarias para la implementación y gestión de los mismos.

En primer lugar plantea una estrategia de implementación progresiva y evolutiva según los objetivos y capacidades de recursos humanos y técnicos, basado en un plan estratégico como base de la propuesta, con previa definición de la misión, visión, objetivos, análisis contexto del mismo y la identificación del público objetivo.

En segundo lugar presenta un modelo de trabajo basado en una metodología de informática forense de desarrollo propio, llamada ForenseUDE, que establece los lineamientos para garantizar la aplicación adecuada de los procedimientos, herramientas y resultados sobre los medios informáticos analizados, considerando al abordaje de pericias informáticas de distinta naturaleza y definiendo roles y responsabilidades en la administración de los casos. Este modelo es la base del desarrollo de protocolos de trabajo y actuación en base a la política institucional del organismo donde se implementa el laboratorio y del desarrollo de procedimientos operativos estandarizados y especializados según diversos escenarios y tecnologías.

En tercer lugar presenta diferentes propuestas de infraestructura tecnológicas para la implementación evolutiva de un LabIF en base a las capacidades y los servicios a ofrecer.

Misión, Visión, Objetivos y Contexto

Se plantea primordial previo al diseño de la estrategia de implementación, determinar la misión, la visión, los objetivos y el análisis de contexto del LabIF a implementar.

Definir la misión, cuál es la razón de ser, el propósito, a quién está dirigido, qué lo distingue y las aspiraciones que se proponen realizar por parte de la institución que lo promueve y en el contexto en que se llevaría a cabo. Analizar y determinar la proyección futura del mismo, con visión estratégica para delinear el camino a seguir y la definición de los objetivos en concordancia con los de la institución a la que responden.

Es preciso analizar el contexto interno y externo de la organización donde se implementará el LabIF, los contextos tecnológicos, sociales, jurídicos, la evolución de la comisión de delitos y las investigaciones, entre otros, los cuales afectan directa e indirectamente a la estrategia a plantear.

Público Objetivo

Además de brindar servicios profesionales periciales y de investigación digital, el objetivo es que los LabIF ofrezcan un ámbito académico de capacitación y desarrollo profesional. En esta punto es importante definir quiénes podrán demandar los diferentes servicios del laboratorio.

El público objetivo abarca desde cuerpo de profesionales judiciales, fiscalías de departamentos judiciales, organismos gubernamentales, empresas, fuerzas de seguridad, entre otros. También se considera como público aquellos estudiantes universitarios, profesionales y funcionarios públicos interesados en formarse y especializarse en informática forense e investigación digital.

Es crucial establecer alianzas estratégicas que permitirán aumentar y fomentar el servicio en distintos espacios, tanto públicos como privados. También se plantea beneficioso trabajar en cooperación con otros laboratorios afines.

Estrategia de Implementación Evolutiva

Como estrategia se propone una implementación evolutiva basada en diferentes etapas de maduración, en las cuales gradualmente se amplía el espectro de servicios, en base a disponibilidad y previsiones de recursos tecnológicos, humanos y profesionalización de los mismos. La misma garantiza una implementación escalonada para dar respuesta a la demanda creciente y cada vez más especializada de servicios de LabIF.

Las etapas, sus requerimientos mínimos y servicios se plantean ideales, pudiendo variar según los objetivos, naturaleza y metas del laboratorio y de la organización que impulsa su implementación como también de la disponibilidad de recursos económicos y humanos, el avance de la tecnología y la demanda de servicios. En todas las etapas se plantea el cumplimiento de tareas periciales, de investigación digital y de asesoramiento.

A. Implementación Inicial

La primera etapa se basa en la implementación inicial del laboratorio, la cual incluye satisfacer los requerimientos mínimos para la puesta en funcionamiento del mismo a través de la implementación de la infraestructura mínima, la incorporación de los recursos que trabajarán en el mismo y la normalización de procesos. Los requerimientos mínimos incluyen:

- Estructura organizacional y funcionalidades.
- Infraestructura Edilicia Mínima.
- Infraestructura Tecnológica Mínima.
- Normalización de procesos.
- Contratación de recursos humanos calificados y especializado en las distintas disciplinas.
- Capacitación interna del equipo de trabajo.

Los servicios iniciales son:

- Servicios forenses informáticos básicos sobre dispositivos masivos y dispositivos celulares.
- Servicios de investigación en fuentes abiertas.
- Asesoría y capacitaciones.

B. Implementación de Automatización de Procesos y Servicios Periciales Avanzados

La segunda etapa plantea la maduración y automatización de los procesos, teniendo como base el nivel de conocimientos y experiencia adquiridos dentro del laboratorio junto con la profesionalización de los recursos humanos. Para poder ampliar los servicios se debe:

- Automatizar y optimizar los procesos.
- Contratar más recursos humanos calificados.
- Posibilitar que los recursos ya especializados puedan cumplir roles con mayores desafíos.
- Ampliar y especializar la Infraestructura Tecnológica.
- Ampliar la infraestructura edilicia.
- Capacitar a la comunidad educativa y profesional.

En esta segunda etapa se propone adicionar:

- Servicios forenses informáticos avanzados sobre dispositivos masivos y celulares.
- Servicios de investigación digital basados en técnicas avanzadas (variedad de fuentes, naturaleza y volumen de datos).
- Servicios a organismos públicos/privados a través de Unidad Forense especializada.

C. Servicios Periciales Especializados

Esta etapa plantea una maduración tecnológica y de disponibilidad de recursos humanos especializados, posibilitando al laboratorio ofrecer análisis forenses sobre escenarios o tecnologías complejas basados en la multiplicidad y complejidad de tecnologías existentes. Para poder ofrecer estos servicios se debe considerar:

- Incorporar profesionales especializados en determinadas tecnologías (nube, internet de las cosas IoT, redes, dispositivos médicos, cámaras de seguridad analógicas y por IP, drones, consolas de videojuegos, entre otros).
- Incorporar infraestructura tecnológica avanzada y especializada acorde.
- Ampliar la infraestructura edilicia.
- Optimización de procesos existentes y especificación de procesos especializados.

En esta tercera etapa se propone adicionar:

- Servicios periciales sobre tecnologías complejas o especiales.
- Servicios de investigación digital basados en técnicas especializadas.
- Asistencias en Allanamientos.

D. Servicios de Tercerización de Personal y Alquiler de Recursos del Laboratorio

En muchas ocasiones existen profesionales, organismos o incluso otros laboratorios afines que necesitan de equipamiento y herramientas específicas, sea porque no pueden invertir en la compra de los mismos o porque necesitan realizar un trabajo puntual que no justifica que lo adquieran. Se plantea la posibilidad de ofrecer alquiler de equipos y herramientas forenses como también ofrecer la tercerización de recursos calificados. Para ofrecer estos servicios se debe:

- Ampliar Infraestructura Edilicia.
- Ampliar y generar redundancia en Infraestructura Tecnológica.
- Implementar un sistema de gestión y control de alquiler de herramientas y equipos.
- Disponer de profesionales encargados de la preparación y control de equipos a alquilar y de ofrecer servicios profesionales a terceros.
- Realizar capacitaciones especializadas a quienes alquilen recursos del laboratorio.

En esta última etapa se propone adicionar:

- Alquiler de herramientas y equipos forenses (modo housing y servicio).
- Alquilar espacios del laboratorio.
- Ofrecer servicios profesiones de recursos capacitados del laboratorio (tercerización).

Gestión de Servicios Informáticos Forenses: ForenseUDE

Se diseñó una propia metodología de gestión de servicios de informática forense, llamada ForenseUDE [5], aplicable a cualquier tipo de evidencia digital (UDE, Universal Digital Evidence). En la misma se definen y describen las etapas y actividades comunes aplicables a cualquier fuente de evidencia digital garantizando la confiabilidad de las tareas a realizar por parte del investigador y/o perito informático forense y la admisibilidad de la evidencia digital obtenida.

ForenseUDE ha sido diseñado acorde al marco legal y procesal en el que se desarrollan las actividades forenses informáticas en la República Argentina. Se sustenta en ideas y conceptos del modelo PURI (Proceso Unificado de Recuperación de Información) [6-7] y del modelo EDRM (Electronic Discovery Reference Model) [8], como también en la norma ISO/IEC 27.037 [9].

ForenseUDE surge ante la necesidad de disponer de un proceso universal de tratamiento de la evidencia digital integral y detallado. Los

modelos existentes hacían énfasis en determinadas etapas o el nivel de detalle no era suficiente como para tomarlos como referencia única. En consecuencia, a partir de dichos modelos y la experiencia profesional se definieron las fases, actividades y el detalle de las tareas aplicables a cada una.

En base al concepto de proceso y esquema planteado por el modelo PURI, la metodología ForenseUDE se basa en un proceso dividido en un conjunto de fases que permiten focalizar los objetivos de cada fase, facilitan su tratamiento y la interconexión de las mismas como un todo. El proceso se entiende como una serie de fases a seguir, las cuales podrían variar de acuerdo con el objeto origen. En cada una de las fases se describen actividades, las cuales a la vez agrupan tareas específicas.

La definición de las fases y el proceso iterativo de ForenseUDE también tuvo su influencia a partir del modelo internacional EDRM, un modelo de referencia del descubrimiento electrónico (e-discovery), que se refiere a cualquier proceso en el que se busca, localiza, asegura y examina datos electrónicos con la intención de usarlos como evidencia digital. Este modelo también se basa en una serie de fases que brindan mejores prácticas sin puntualizar en ningún dispositivo.

De la norma ISO/IEC 27.037:2012 se consideraron los lineamientos generales para la identificación, recolección, adquisición y preservación de la evidencia digital, las buenas prácticas en el proceso de manejo de la evidencia digital y el mantenimiento de la debida cadena de custodia. Es un estándar establecido para el primer contacto con la evidencia electrónica, orientada al procedimiento de la actuación pericial en el escenario de la recolección, identificación y secuestro de la evidencia digital.

ForenseUDE se plantea justificable, auditable, repetible y reproducible cumpliendo con los requisitos de confiabilidad. A partir de la misma se plantea el desarrollo de protocolos de implementación, preparación de infraestructura tecnológicas y protocolos de actuación.

Roles Actuantes en ForenseUDE

Los roles actuantes establecen un conjunto de expectativas asociadas con la función, independientes de la persona o el puesto que ocupa en la estructura organizacional del LabIF. Se plantean en parte análogos a los del modelo PURI [6-7], adicionando los roles de director en informática forense, el especialista en identificación y diferenciando el especialista en evidencia digital universal del especialista forense en tecnologías especiales.

- **Director Informática Forense (DIF)**: Profesional encargado de planificar la estrategia general, coordinar las actividades y realizar el seguimiento y control en las diferentes fases.
- **Responsable de Identificación (RI):** Profesional idóneo en las tareas de identificación.
- **Especialista en Identificación (EI):** Especialista en las tareas de identificación vinculadas a tecnologías especiales o complejas que requieran de un profesional calificado.
- **Especialista en Recolección (ER):** Persona autorizada, entrenada y calificada para recolectar objetos físicos pasibles de tener evidencia digital.
- **Especialista en Adquisición (EA):** Persona autorizada, entrenada y calificada para adquirir distintos tipo de evidencia digital.
- **Especialista en Evidencia Digital Universal (EUDE):** Experto que realiza las tareas de adquisición. Posee conocimientos y habilidades para manejar un amplio rango de situaciones técnicas y la realización de una pericia informática sobre tecnologías de uso frecuente.
- **Especialista Forense en Tecnologías Especiales (EFTE):** Profesional experto en tecnologías especiales. El mismo puede asesorar o actuar en las diferentes fases de la metodología.

Fases de ForenseUDE

La metodología propone ocho fases principales: Preparación Inicial, Relevamiento e Identificación, Recolección, Adquisición, Preparación y Procesamiento, Extracción y Análisis, Producción y Presentación, Evaluación Final. Además tres actividades transversales: Cadena de Custodia, Preparación de Herramientas, Seguimiento y Control. En la Figura 1 se visualizan las fases.

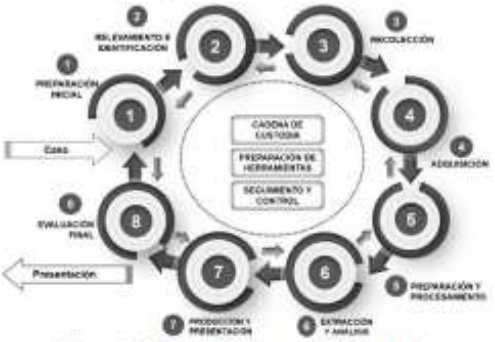


Figura 1: Red para una gramática estándar

CADI 5to. Congreso Argentino de Ingeniería
11vo. Congreso Argentino de Enseñanza de la Ingeniería

Las actividades se encuentran vinculadas de tal forma que sugieren un orden en el que podrían ser llevadas a cabo en las diferentes fases, orientando los procedimientos, estableciendo directrices de preservación y recolección de la evidencia digital, asegurando no contaminar la evidencia digital, priorizando la recolección según orden de volatilidad y manteniendo la debida cadena de custodia, como también el seguimiento de intercambio de evidencias digitales entre intervinientes. Las fases se presentan en un modelo iterativo, donde cada una puede retroalimentar a las fases previas y el final de cada iteración retroalimenta a un nuevo inicio.

Fase 1: Preparación Inicial

Objetivo: Analizar la factibilidad de resolución del requerimiento de análisis forense informático y planificar la estrategia asociada acorde a la disponibilidad y capacidades de los recursos.
Roles Actuantes: DIF, RI
Tareas: En la Tabla 1 se enumeran las tareas.

Tabla 1: Fase 1

Tareas de Fase de Preparación Inicial
Recepción del caso o requerimiento
Analizar criticidad, prioridad y naturaleza del caso
Revisión de Capacidades de tiempo, equipos y RRHH
Revisión de Equipamiento necesario
Análisis de factibilidad
Definición del alcance general
Planificación y Diseño de Estrategia acorde al Requerimiento y las Capacidades
Análisis de Riesgos
Preparación de equipos y herramientas

Fase 2: Relevamiento e Identificación

Objetivo: Conocer en detalle el caso a tratar. Relevar e identificar las potenciales fuentes de evidencia. Relevar las tecnologías de software y hardware involucradas.
Roles Actuantes: RI, EI
Tareas: En la Tabla 2 se enumeran las tareas.

Tabla 2: Fase 2

Tareas de Fase de Relevamiento e Identificación
Relevamiento de documentación legal, administrativa
Relevamiento de documentación técnica
Relevamiento de Infraestructura de IT
Identificación de fuentes de evidencia digital
Identificación de las características de la Evidencia Digital
Clasificación de la Evidencia Digital
Ajuste de Planificación y Diseño de Estrategia
Gestión de pedidos de allanamientos
Preparación de los equipos y herramientas
Detallar Requisitos de Recolección y Adquisición

Fase 3: Recolección

Objetivo: Preservar la evidencia digital original aplicando procedimientos forenses adecuados para evitar contaminar la misma.
Roles Actuantes: ER, EA
Tareas: En la Tabla 3 se enumeran las tareas.

Tabla 3: Fase 3

Tareas de Fase de Recolección
Preparación de elementos para la recolección y/o traslado de la evidencia digital
Inspección de Infraestructura de IT
Adquisición de datos volátiles o en vivo
Aplicar algoritmos de Hash
Desconexión de los equipos o dispositivos a recolectar
Recolección, secuestro, aislamiento, embalaje y transporte de objetos
Fotografiar y/o filmar
Acta de allanamiento
Formulario de cadena de custodia

Fase 4: Adquisición

Objetivo: Adquirir la evidencia digital basada en el orden de volatilidad y relevancia.
Roles Actuantes: EA, EUDE, EFTE
Tareas: En la Tabla 4 se enumeran las tareas.

Tabla 4: Fase 4

Tareas de Fase de Adquisición
Identificar y clasificar los dispositivos a adquirir
Preparación de los equipos y herramientas
Preparar dispositivos de almacenamiento
Definir la estrategia de adquisición
Adquisición de datos volátiles o en vivo
Adquisición y análisis de datos específicos en vivo
Adquisición en medios de almacenamiento persistentes
Adquisiciones especiales
Validación y resguardo
Acta pericial
Formulario de cadena de custodia
Transporte con requisitos de protección adicionales

Fase 5: Preparación y Procesamiento

Objetivo: Ejecutar la restauración de imágenes forenses y el procesamiento inicial de datos.
Roles Actuantes: EUDE, EFTE
Tareas: En la Tabla 5 se enumeran las tareas.

Tabla 5: Fase 5

Tareas de Fase de Preparación y Procesamiento
Acondicionar lugar de almacenamiento
Ensamblado y descompresión de imágenes forenses
Validar integridad de las imágenes forenses y archivos
Identificación de tecnologías de información
Preparación de extracción
Preparación del ambiente
Procesamiento
Planificación de estrategia de Extracción y Análisis

Fase 6: Extracción y Análisis

Objetivo: Extraer y analizar la información relevante en relación con los puntos de pericias.
Roles Actuantes: EUDE, EFTE
Tareas: En la Tabla 6 se enumeran las tareas.

Tabla 6: Fase 6

Tareas de Fase de Extracción y Análisis
Extracción
Adquisiciones en ambientes virtualizados
Análisis de contenidos
Análisis de relaciones

Fase 7: Producción y Presentación

Objetivo: Producir el dictamen y los resultados finales en tiempo y forma. Preparar las presentaciones que sean solicitadas, tanto a particulares como para presentar en un juicio.
Roles Actuantes: DIF, EUDE, EFTE
Tareas: En la Tabla 7 se enumeran las tareas.

Tabla 7: Fase 7

Fase de Producción y Presentación
Armado y presentación de dictamen final y anexos
Armado y presentación de informes técnicos
Exposición del caso en juicio o a los solicitantes.

Fase 8: Evaluación Final

Objetivo: Evaluar los resultados del trabajo y proponer mejoras o buenas prácticas a las actividades, técnicas y procedimientos.
Roles Actuantes: DIF, EUDE, EEDE
Tareas: En la Tabla 8 se enumeran las tareas.

Tabla 8: Fase 8

Fase de Preparación Inicial
Evaluación Final
Informe de calidad, riesgos y mejoras

Actividad Transversal: Cadena de Custodia.

La cadena de custodia es el registro cronológico de la manipulación de todos los elementos incautados e identificados durante el proceso. En la misma se registra en todo momento en qué lugar está la evidencia, bajo responsabilidad de quién, desde su identificación hasta su presentación final. Debe ser actualizada en todas las tareas en las cuales se realicen acciones sobre la evidencia digital, incluso de custodia, desde el momento en que se encuentran en el lugar del hecho hasta en su análisis en el laboratorio. Se debe iniciar un Formulario de Cadena de Custodia por cada elemento involucrado en el caso y debe acompañar a la evidencia correspondiente durante todo el ciclo.

Actividad Transversal: Preparación de Equipos y Herramientas

En esta actividad se desarrollan las buenas prácticas relacionadas a la preparación de los equipos y herramientas en las diferentes fases:

1. Conocer los equipos y herramientas

Conocer el potencial y el alcance de cada equipo y las herramienta a utilizar. Conocer la forma de trabajo, cómo funcionan, sus módulos, cómo utilizarlas/os, cuáles, cuándo y las ventajas y desventajas frente a escenarios posibles.

2. Validar los equipos y herramientas

Validar que los equipos y herramientas realizan funcionalmente lo que el fabricante dice que hacen. Probar los equipos y herramientas previamente a utilizarlos en un caso real.

3. Comprobar la integridad de las herramientas

Obtener y almacenar el hash de los archivos ejecutables de instalación y de ejecución de las herramientas para verificar su integridad.

4. Verificar las licencias

Verificar que se posea licencias válidas y actualizadas de equipos y herramientas forenses, como también del sistema operativo y de cualquier software que se utilice en el proceso.

5. Contar con variedad de equipos y herramientas

Disponer de variedad de equipos y herramientas para enfrentar los diferentes desafíos y escenarios que se pueden presentar.

6. Preparar las estaciones forenses

Configurar y validar las configuraciones de las estaciones forenses (deshabilitar actualizaciones automáticas, chequear las configuraciones de energía y la zona horaria, etc.).

Actividad Transversal: Seguimiento y Control

El responsable principal de esta actividad es el Director en Informática General (DIF), quien está a cargo de verificar la ejecución de la planificación y diseño de la estrategia general planteada, como también de la gestión de los desvíos, riesgos y ejecución de planes de contingencia. Los diferentes roles actuantes mantienen una comunicación constante y fluida con el DIF.

Infraestructura Tecnológica

La investigación de equipos, herramientas de informática forense y de laboratorios afines nacionales e internacionales, permitió desarrollar diferentes propuestas de implementación de infraestructura tecnológica en base a la disponibilidad de recursos tecnológicos, económicos, físicos y humanos. Las propuestas se efectuaron también en base a información

obtenida a través de entrevistas a profesionales referentes en la materia. Se llevó a cabo un análisis y evaluación de las diversas herramientas y equipamientos forenses informáticos existentes y necesarios para la operatoria del laboratorio en su inicio, como en etapas avanzadas, según el tipo de dispositivos involucrados, incluyendo tanto los que poseen licencias pagas, de uso gratuito o de código abierto:

- Equipos y herramientas de informática forense para pericias sobre dispositivos masivos.
- Equipos y herramientas de informática forense para pericias de dispositivos móviles.
- Equipos y herramientas de informática forense con fines específicos o tecnologías especiales.
- Duplicadores y bloqueadores.
- Sistemas operativos forenses.
- Herramientas de investigación digital.
- Estaciones Forenses.
- Herramientas complementarias.
- Herramientas para la recuperación de datos.

En este punto se incluye también la implementación de la infraestructura de red, el equipamiento informático de base y de soporte y todos los aspectos de seguridad lógica y física.

CONCLUSIONES

El marco propuesto promueve un modelo de tratamiento de la evidencia digital y gestión de causas donde se optimiza la adquisición y análisis de datos, mejorando la brecha de tiempos para resolver los casos basado en el paralelismo de operaciones y el escalamiento gradual para dar respuesta a la demanda, garantizando la confidencialidad de la información digitalizada y electrónica, en base a un modelo ágil de gestión Forense para la comunidad judicial y privada.

En el proyecto de investigación se han avanzado en diferentes aspectos que no han sido detallados en el presente documento a fines de respetar la extensión del mismo. Quedaron por fuera del alcance de este documento lo que refiere a la infraestructura edilicia, estructura organizacional, seguridad física de las instalaciones, el detalle de las propuestas de Infraestructura Tecnológica, entre otros.

Como parte de las futuras líneas de investigación, se destaca la necesidad de investigar en detalle los procesos de certificación y acreditación que deben poseer los laboratorios que brindan servicios a la Justicia y a diferentes organismos públicos y privados tanto a nivel nacional como internacional.

AGRADECIMIENTOS

Se agradece al Decano Mg. Jorge Eterovic y al Vicedecano Mg. Gabriel Blanco del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza (Buenos Aires, Argentina) por el apoyo al trabajo realizado.

REFERENCIAS

[1] Di Iorio, A. et.al. (2019). *Guía técnica para el diseño, implementación y gestión de laboratorios de informática forense*. Universidad FASTA Mar del Plata, Buenos Aires, Argentina.

[2] Di Iorio, A et al. (2016). *Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense*. REDI - Repos. Digital. la Univ. FASTA,1-6.

[3] Semprini, G. (2016). *Lineamientos para la creación de laboratorios informáticos forenses*. SID 2016, 16º Simposio Argentino de Informática y Derecho, CABA, Argentina.

[4] Appendino, S. et.al. (2015). *Plan Estratégico para la implementación de un Centro de Servicios de Informática Forense*. XXI Congreso Argentino de Ciencias de la Computación, IV Workshop de Seguridad Informática (WSI), Buenos Aires, Argentina.

[5] Gioia, C. (2019). Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos. Tesis de Maestría en Informática. Universidad Nacional de la Matanza. Escuela de Posgrado, Buenos Aires, Argentina, 85-189.

[6] Di Iorio, A.; Castellote, M.; Bruno, C. (2017). *El Rastro Digital del Delito. Aspectos técnicos, legales y estratégicos de la Informática Forense*. Universidad FASTA. Ediciones. Mar del Plata, Buenos Aires, Argentina, Cap. 3.

[7] Di Iorio, A. H. (2016). *Guía Integral de Empleo de la Informática Forense en el Proceso Penal (2da edición)*. Universidad Fasta, Mar del Plata, Buenos Aires, Argentina, 47-57. Recuperado de http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1592/PAIF.pdf? sequence=1

[8] EDRM. (2014). *Modelo EDRM*. EDRM (Electronic Discovery Reference Model) Recuperado de https://www.edrm.net/frameworks-and-standards/edrm-model/

[9] ISO/IEC 27037:2012. (2012). Information *Technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence*. ISO. Estados Unidos.

B.4.2 Video de presentación del proyecto en el Congreso CADI 2021:

https://www.youtube.com/watch?v=idtn-JzYCC0

B.4.1 Certificado:


CADI/CLADI CAEDI

.UBAfiuba FACULTAD DE INGENIERÍA confedi CONDEFI

Se certifica que los autores

Cintia Verónica Gioia, Emiliano Alejandro Zárate, Nora Cristina Gigante, Mario Juan Krajnik, Walter Ureta, Juan Cruz González Allonca, Sergio Gabriel Bonavento y Fernando Saldaña

han presentado el trabajo titulado

Marco de Referencia para la Implementación y Gestión de Laboratorios de Informática Forense

en el **Encuentro Argentino y Latinoamericano de Ingeniería CADI / CLADI / CAEDI**, organizado por la Facultad de Ingeniería de la Universidad de Buenos Aires y llevado a cabo los días 5, 6 y 7 de octubre de 2021, de manera virtual.

Dr. Ing. Oscar Pascal	Inga. Alejandra Acuña V.	Ing. Alejandro M. Martínez	Dr. Ing. Luis Fernandez Luco	Dra. Cristina Vázquez
CONFEDI	CONDEFI	Facultad de Ingeniería - UBA	Comité Académico	Comité Organizador
Presidente	Presidenta	Decano	Presidente	Presidenta

**** Ya he reclamado reiteradas veces a la organización del evento que el certificado fue emitido con los nombres de los autores erróneos. Aún no tuve ninguna respuesta al respecto. Di aviso de esta situación a la Secretaría de Investigación del DIIT.*

B.4.2

B.4.2 Paper:

CADI 5to. Congreso Argentino de Ingeniería
11vo. Congreso Argentino de Enseñanza de la Ingeniería

"METODOLOGÍA DE ANÁLISIS FORENSE INFORMÁTICO PARA LA OBTENCIÓN DE EVIDENCIA DIGITAL EN BASE DE DATOS"

Gioia, Cintia Verónica [a]; Eterovic, Jorge Esteban [a]
a Departamento de Ingeniería e Investigaciones Tecnológicas - Universidad Nacional de La Matanza
cgioia@unlam.edu.ar

Resumen

En la actualidad la tecnología brinda la posibilidad de almacenar gran cantidad de información en base de datos y recuperarla en segundos. Ante esta situación, crecen los delitos informáticos asociados y la necesidad de aplicar informática forense en dichas bases. Se plantea el desafío de obtener evidencia digital válida como medio de prueba en un proceso judicial. Prevenir los riesgos de invalidar una prueba se convierte en una responsabilidad y un reto profesional.

Previo a este trabajo no existía ninguna metodología informática forense específica para base de datos relacionales y menos aún que haga frente a la heterogeneidad y complejidad de las tecnologías existentes. Tampoco se halló un marco único con un nivel de detalle que aplicara como base general para el desarrollo de la misma.

Se presenta el desarrollo de una metodología de análisis forense informático para base de datos relacionales que guía la actuación pericial especializada garantizando la confiabilidad de las actividades de identificación, recolección, adquisición y análisis de evidencia digital. La misma está diseñada a partir del desarrollo de tres metodologías: una metodología informática forense aplicable a todo tipo de evidencia digital, una metodología informática forense en base de datos y una metodología de auditoría universal de base de datos. La metodología sobrepasa las limitaciones o retos tecnológicos de cada tipo de base de datos y la dependencia de expertos que ofrecen soluciones según su visión tecnócrata, incluso muchas veces, sin poder garantizar la admisibilidad judicial de la evidencia digital.

Abstract

Today, the technology offers the possibility of storing a large amount of information in a database and retrieving it in seconds. In this situation, associated cybercrime increases and the need to apply forensic computer in databases is greater. It is a professional responsibility and challenge to prevent risks of invalidating a proof.

Prior to this work, there was no specific computer forensic methodology for relational databases and less that applies to the heterogeneity and complexity of existing technologies. Neither was found a base methodology with a level of detail that would be applied as a general basis for its development.

This paper presents the development of a computer forensic analysis methodology for databases that guides specialized action, guaranteeing the reliability of the activities of identification, collection, acquisition and analysis of digital evidence. It´s based on three own methodologies: a forensic computer methodology applicable to all types of digital evidence, a database forensic computer methodology and a database universal audit methodology. The methodology overcomes the limitations or technological challenges of database and the dependence on experts who offer solutions according to their technocratic vision, sometimes, without being able to guarantee the judicial admissibility of digital evidence.

Palabras clave: Metodología Informática Forense, Metodología Informática Forense en Base de Datos, Auditoría Forense Informática, Evidencia Digital.

CADI 9no. Congreso Argentino de Ingeniería
11vo. Congreso Argentino de Enseñanza de la Ingeniería

INTRODUCCIÓN

A partir de la denuncia o detección de un caso potencialmente delictivo vinculado con el uso de la tecnología de base de datos surge la necesidad de aplicar la ciencia de informática forense a las mismas, procurando respetar los principios forenses para lograr obtener evidencia digital válida como medio de prueba para su efectiva sanción en un proceso judicial.

En primer lugar es importante aclarar la diferencia entre informática forense y la informática forense en base de datos. El forense de base de datos enfoca su investigación específicamente en la base de datos en sí y el servidor que la contiene, es decir la capa de datos. No se incluye dentro del universo de su investigación el servidor de aplicaciones, el servidor web o las aplicaciones que interactúan con los usuarios.

Tal como afirma Jeimy Cano [1], las principales limitaciones en computación forense en base de datos se deben a la dependencia de la mismas con herramientas propias de cada sistema gestor de las bases (SGBD), al elevado nivel de experiencia, el conocimiento requerido, a la alta probabilidad de modificación de datos en el proceso de extracción y a la falta de un procedimiento estándar que apoye al análisis forense en las mismas. Esto provoca que surjan dudas sobre la confiabilidad de las herramientas utilizadas y la validez de las pruebas obtenidas.

Para el desarrollo de este trabajo se han estudiado y analizado diversas metodologías, guías, protocolos y normas [2]-[5], incluso varios documentos publicados por organismos públicos [6],[7], que si bien han sido de gran aporte y referencia, se llegó a la conclusión que ninguno de ellos describía de forma detallada las actividades relevantes y obligatorias a tener en cuenta a lo largo de la investigación y análisis informático forense de un caso, y menos aún, para casos relacionados con tecnologías específicas de base de datos relacionales.

Frente a la heterogeneidad de SGBD y la complejidad de su administración y configuración surge la necesidad de contar con una metodología específica de análisis forense informático que garantice la obtención de evidencia en las base de datos y que permita identificar de manera efectiva los hechos acontecidos logrando responder a preguntas claves del análisis forense: qué, cómo, cuándo y quién.

DESARROLLO

Diseño general de la solución

La solución propuesta comprende el desarrollo de una metodología integral de análisis forense informático para el tratamiento de evidencia digital en base de datos relacionales denominada AUDBForense (Auditoria Forense de Base de Datos).

La solución fue diseñada y desarrollada en base a tres metodologías de desarrollo propio que abarcaron desde el tratamiento de la evidencia digital de todo tipo, para luego definir en base a la misma, lo específico a base de datos relacionales (BDR), complementadas con una metodología de generación de evidencia digital a partir de la ejecución de auditorías de datos.

AUDBForense integra las siguientes tres metodologías (ver Figura 1):

- Metodología de auditoría universal de base de datos (AUDB).
- Metodología de informática forense universal (ForenseUDE).
- Metodología de informática forense en base de datos (ForenseDB).

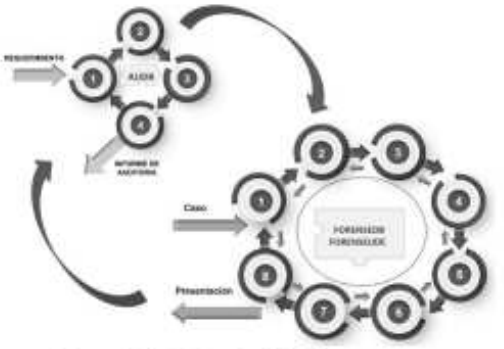


Figura 1: Metodología AUDBForense

ForenseDB se especificó en base a ForenseUDE. AUDB proporciona evidencia digital relevante a través de la ejecución de auditorías.

En primer lugar se desarrolló una metodología informática forense con el detalle necesario de las actividades y tareas a realizar para un análisis forense informático sobre cualquier tipo de evidencia digital a través de un proceso que brinda garantías de confiabilidad y calidad, denominada ForenseUDE (UDE corresponde a las siglas de Universal Digital Evidence).

Por otro lado, se planteó como parte de la solución el desarrollo y la aplicación de una metodología de auditorías de base de datos que posibilita generar y obtener la evidencia digital de operaciones y actividades que los usuarios, procesos o aplicaciones realizan sobre los datos que se consideran más sensibles, denominada AUDB. A partir de la evidencia digital generada por las auditorías se puede conocer, analizar y controlar las actividades de los usuarios tanto para detectar acciones maliciosas que puedan afectar la confidencialidad, integridad o disponibilidad de la información, como también para prevenir las mismas a futuro

Básicamente en la solución propuesta, ForenseDB se centra en el tratamiento de la evidencia digital en base de datos, mientras que los resultados de la implementación de auditorías de datos, basadas en la metodología AUDB, proporcionan evidencia digital relevante y precisa para la investigación forense informática de casos. Del mismo modo el resultado de las investigaciones y análisis forense resultantes de aplicar ForenseDB nutren y retroalimentan a las auditorías de datos, sus configuraciones y la estrategia implementada en AUDB como parte de un proceso iterativo de mejora continua.

Cabe aclarar, que si bien se recomienda aplicar ambas metodologías, ForenseDB puede aplicarse de manera independiente a AUDB.

Se plantean de esta manera metodologías que se retroalimentan, especifican y complementan entre sí, conformando la metodología de análisis forense informática integral AUDBForense que actúa de manera preventiva, probatoria y correctiva en pos del resguardo de la confidencialidad, integridad y disponibilidad de los datos sensibles.

Metodología AUDB

AUDB se basa en la Metodología de Auditoría Universal de Base de Datos No Invasiva [8-9] como marco de referencia para la configuración, ejecución y control de auditorías de bases de datos. AUDB es una versión mejorada y ampliada de la misma, la cual incorporó además principios de auditoría forense en base de datos [10].

AUDB posibilita configurar auditorías que dejan rastros de acciones sensibles, dudosas o maliciosas, de las cuales no se podría recuperar evidencia o el detalle necesario si no se dispusiera de las mismas. De esta manera, actúa como base de generación de evidencia digital para la investigación forense, posibilitando que la metodología ForenseDB pueda realimentarse con la recolección de resultados de auditorías preventivas de AUDB como evidencia digital admisible, posibilitando no solo obtener información más valiosa del contexto de los hechos, sino reconstruir los sucesos en una línea trazable de tiempo (auditoria forense).

AUDB brinda un nivel de abstracción necesario para focalizarse en las auditorias de datos en sí y la prevención de intrusiones sobre los mismos, sin conocer en detalle las características técnicas de cada SGBD, sin impactar en el desempeño de la misma y facilitando la puesta en práctica de los requisitos de las leyes de Protección de Datos Personales nacionales e internacionales. En materia de protección de datos personales en la Rep. Argentina se aplica la Ley 25.326 (Ley de Habeas Data, año 2000). A nivel internacional es relevante el Reglamento General de Protección de Datos (RGPD) 2016/679 de la Unión Europea.

En la Figura 2 se visualizan las fases de AUDB: (1) Relevamiento y Diagnóstico, (2) Evaluación de Riesgos, (3) Configuración de Ejecución de Auditorías, (4) Análisis de Resultados.

Figura 2: Metodología AUDB

Para comprender en detalle la metodología AUDB incorporada como parte de la solución de AUDBForense, se recomienda la lectura de los trabajos publicados sobre la misma para lograr una visión completa y detallada de la misma[8-9].

Metodología ForenseUDE

ForenseUDE tiene como objetivo ofrecer un proceso de tratamiento de la evidencia digital en respuesta a la necesidad de disponer de una guía completa y detallada para la actuación pericial informática que garantice la confiabilidad de las actividades de identificación, recolección, adquisición y análisis de evidencia digital admisible como prueba en un proceso judicial.

CADI 9no. Congreso Argentino de Ingeniería 11vo. Congreso Argentino de Enseñanza de la Ingeniería

ForenseUDE se sustenta en ideas y conceptos del modelo PURI (Proceso Unificado de Recuperación de Información) [2],[3], del modelo EDRM (Electronic Discovery Reference Model) [4] y en la norma ISO/IEC 27.037 [5]. Comprende fases y actividades comunes a los modelos mencionados como también distintivos o propios en base a la experiencia profesional en la actuación forense informática y la especificación de determinados aspectos necesarios. En base al concepto de proceso y esquema del modelo PURI, se basa en un proceso iterativo dividido en fases, que permiten focalizar los objetivos de cada una, facilitando su comprensión, tratamiento y la interconexión de las mismas.

En ForenseUDE se definen y describen las etapas y actividades aplicables a cualquier tipo de evidencia digital, lo que en la metodología se denomina evidencia digital universal (UDE, Universal Digital Evidence). La metodología es versátil y adaptable al máximo de situaciones posibles, incluyendo las actividades y tareas relevantes y obligatorias a tener en cuenta en los escenarios más habituales, tanto en casos judicializados o privados. Por tal motivo, se plantea como base y marco de referencia para el diseño de metodologías en tecnologías específicas, como en el caso del presente trabajo, para Base de Datos Relacionales.

ForenseUDE garantiza las características de relevancia, confiabilidad, suficiencia y validez legal de la evidencia digital tratada durante el proceso. Un proceso que se plantea justificable, auditable, repetible y reproducible, cumpliendo con los requisitos de confiabilidad y el registro de la debida cadena de custodia para asegurar la confiabilidad de la información recolectada y registrar la trazabilidad exacta de la misma, es decir, saber en todo momento, en qué lugar está la evidencia digital, bajo responsabilidad de quién, desde su identificación, hasta su presentación.

Metodología ForenseDB

ForenseDB es una metodología forense informática para Base de Datos Relacionales (BDR) basada en ForenseUDE. ForenseDB asegura una actuación metódica basada en un orden lógico de actividades a ejecutar, evitando contaminar la evidencia digital en las bases de datos y manteniendo la debida cadena de custodia, de manera de preservar la información recolectada como potencial prueba. Tiene como principal foco los datos contenidos en las base de datos en sí y no el servidor que la contiene.

La metodología brinda confiabilidad, trazabilidad, integridad y suficiencia al proceso de análisis forense en BDR especificando las tareas propias a considerar en las mismas. El objetivo de la aplicación de dicha metodología es evitar errores u omisiones en el manejo de la evidencia digital, en la ejecución de procedimientos o en la aplicación de técnicas, que pueden poner en riesgo toda una investigación o actuación pericial.

La metodología ForenseDB aplica a las BDR en general, no puntualiza en un tipo de motor de base de datos. Se centra en la obtención de evidencia digital basada en cualquier dato o registro de información procesado electrónicamente y almacenado en BDR o artefactos vinculados, como ser registros de log u archivos, pudiendo ser de valor para casos judicializados o en investigaciones solicitadas por parte de personas u organizaciones.

La metodología presta especial atención al tratamiento de los datos personales y la propiedad industrial, de manera de garantizar que tanto el acceso a información de carácter privado o información de una organización sea bajo el consentimiento previo del responsable de dichos datos o mediante autorización judicial.

ForenseDB clasifica la evidencia digital en los siguientes datos:

- Registros almacenados en tablas
- Archivos físicos de datos, configuraciones, parámetros, logs, control, backup, transacciones, temporales, entre otros.
- Datos volátiles en memoria y caché.
- Resultados de ejecución de vistas de datos, consultas SQL, exportación de datos.
- Resultados de procesos de auditorías, control, logs, entre otros.

Fases de Metodología ForenseDB

Las fases generales de ForenseDB y ForenseUDE son similares (Ver Figura 3). Las fases describen actividades y tareas generales (ForenseUDE) y específicas sobre base de datos relacionales (ForenseDB).

La metodología propone 8 fases principales: (1) Preparación Inicial, (2) Relevamiento e Identificación, (3) Recolección, (4) Adquisición, (5) Preparación y Procesamiento, (6) Extracción y Análisis, (7) Producción y Presentación, (8) Evaluación Final. Además, se adicionan tres actividades transversales: (1) Cadena de Custodia, (2) Preparación de Herramientas y (3) Seguimiento y Control.

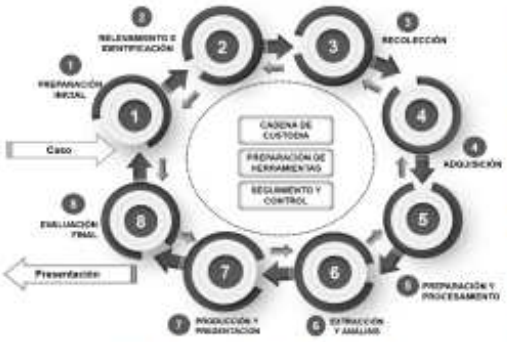


Figura 3: Fases de ForenseDB

1. Fase de Preparación Inicial

Descripción General

Recepción del caso o requerimiento de análisis forense informático. Análisis de criticidad y prioridad del casos. Validación y revisión de las capacidades de tiempo, equipos y recursos humanos. Definición del alcance general. Diseñar un plan de acción y un análisis de riesgos.

Recomendaciones

Analizar el nivel de especificación del requerimiento. Observar la naturaleza de la organización para deducir criticidad de los datos, y alguna legislación particular asociada. Gran parte de los casos pertenecen a organizaciones donde la disponibilidad de las base de datos es crucial. Se deben analizar alternativas factibles para evitar desconectar el servidor donde se aloja, el motor de base de datos o los servicios vinculados, de manera de no afectar la operatoria.

Para la revisión de capacidades y equipamiento, considerar las tecnologías asociadas a los SGBD como también los servidores donde se migren o repliquen las mismas (sean ambientes de producción, contingencia, preproducción, prueba, etc.). En caso de que existan, incluir las base de datos de configuración y resultados de auditorías AUDB.

2. Fase de Relevamiento e Identificación

Descripción General

Relevamiento de la documentación legal, administrativa, técnica y de infraestructura IT. Identificación de fuentes de evidencia digital. Clasificación de la evidencia digital. Identificación de escenarios de recolección y adquisición.

Recomendaciones

Relevar la infraestructura tecnológica relacionada a las BDR involucradas: identificar los servidores, bases de datos y la arquitectura implantada. Obtener información de configuración y acceso en los servidores y bases de datos: tipo de servidores, virtualización de servidores, servidores en la nube, tipo y versiones de SGBD, formas de acceso o conexión, estrategias de seguridad implantadas, sistemas o aplicaciones que las utilizan, transferencia de datos, auditorías de datos, entre otros aspectos relevantes al caso. No se debe obviar analizar las políticas de resguardo, el acceso y disponibilidad a los archivos de backups y los planes de contingencia.

Relevar tablas que contengan los datos relacionados al caso. Determinar qué usuarios y sistemas manipulan la información, de qué forman gestionan el acceso, información que se visualiza o modifica a través de los diferentes sistemas y equipos, horarios habituales de acceso, entre otras variables de entorno relevantes para el diagnóstico de criticidad.

Relevar si existe algún tipo de replicación total o parcial de las tablas. Investigar el contenido y acceso a las bases de datos involucradas en ambientes de desarrollo, prueba y preproducción.

Identificar servicios de integración, servicios de análisis, servicios de reportes, y toda servicio que interactúe con las bases de datos involucradas.

Identificar si existe información cifrada en la base de datos y su estrategia de implementación.

En el caso que exista la aplicación de AUDB relevar la estrategia implantada.

Categorizar la evidencia digital en base de datos con las que se deberá trabajar en las siguientes fases según la volatilidad y relevancia.

Determinar el alcance de los datos personales involucrados, si corresponden al ámbito nacional o internacional y determinar las leyes de datos personales que aplican. Según el caso gestionar las autorizaciones judiciales necesarios para el tratamiento de datos personales.

Preparar los equipos y herramientas necesarias para las tareas en BDR.

3. Fase de Recolección

Descripción General

Recolección de la evidencia digital. Preservación de los equipos físicos y/o posibles fuentes de evidencia digital. Aplicación de acciones de aislamiento de la evidencia digital para evitar contaminarla. Adquisición de datos volátiles o de sistemas encendidos en el lugar del hecho. Transporte de la evidencia digital.

Recomendaciones

Aplicar procedimientos adecuados de preservación asegurando no contaminar la

evidencia digital en BDR. Se debe recolectar la misma según el orden de volatibilidad.

La evidencia digital en BDR podrá ser recolectada o analizada "in situ". En general, no será factible secuestrar o desconectar servidores de SGBD o detener los servicios de base de datos dada la criticidad de los mismos, por lo cual será necesario realizar la adquisición de datos volátiles o de sistemas encendidos.

Considerar que se pueden requerir discos de almacenamiento de gran capacidad para resguardar las imágenes forenses adquiridas en vivo, adquisición de datos volátiles o en vivo o incluso el resultado de análisis en el lugar del hecho. En el caso de recolectar archivos de backups, analizar si se dispone de los mismos o se necesita hacer un nuevo backup en línea y en tal caso dimensionar su volumen.

Aplicar tareas de inspección de la actividad en el lugar del hecho. Estas inspecciones pueden ser oculares como también a partir del uso de técnicas y herramientas específicas. En el caso de allanamientos, es importante que previamente, se indiquen las medidas a llevar a cabo para que estén autorizadas judicialmente y se conste en el acta de allanamiento las operaciones realizadas.

Realizar el trabajo en presencia de testigos. Es recomendable fotografiar y filmar las acciones.

Efectuar el correcto registro en el formulario de Cadena de Custodia con el inventariado de los elementos recolectados. Es muy importante identificar el nombre del servidor, la base de datos, tablas, campos sobre las que se recolecta información, datos sobre la arquitectura general. En el caso de recolecciones a partir de resultados de análisis, adjuntar como anexo los scripts de SQL ejecutados y/o el detalle de las aplicaciones utilizadas. Indicar el nombre, tamaño y extensión de los archivos resultantes, como también el tipo de contenido de los mismos y el valor de hash.

4. Fase de Adquisición

Descripción General

Adquisición de la evidencia digital basada en el orden de volatilidad y relevancia para su posterior análisis. Adquirir datos volátiles y persistentes.

Recomendaciones

Aplicar herramientas para la adquisición de datos volátiles relacionados a las base de datos, como ser datos del caché, páginas de los índices, sentencias de SQL, estado del servidor, procesos en memoria, sesiones de base de datos, etc.

Aplicar herramientas para la recolección de imágenes forenses en vivo de servidores o medios de almacenamiento en casos donde sea factible según volumen y naturaleza de los datos.

Aplicar herramientas para adquirir datos persistentes en vivo (archivos, información del registro en el sistema operativo, archivos preexistentes de consultas o de resultados sobre los datos investigados, capturas de pantalla de resultados, configuraciones de base de datos, configuraciones de seguridad, etc).

Emplear estrategias para la recolección de estructuras y datos que no alteren su integridad.

En el caso de recolectar tablas específicas, evaluar si se debe recolectar la tabla completa o determinados campos según el alcance del caso.

En el caso de adquisición o análisis de datos personales (además de gestionar previa autorización judicial), se deben considerar mecanismos de cifrado o de protección adicionales sobre los archivos resultantes.

Según los casos se deberá realizar no solo recolección, sino análisis en vivo, por ejemplo, obtener resultados ejecutando scripts de SQL o exportando datos con herramientas o comandos.

Esta fase involucra aplicar también procedimientos para la adquisición tradicional sobre equipos apagados o medios de almacenamiento extraídos o extraíbles y efectuar una imagen física de los medios relacionados con los SGBD, servidores donde se migren o repliquen BDR y medios de almacenamientos de resguardos.

En el caso de aplicación de AUDB considerar las BDR que almacenan las configuraciones y resultados, tanto para adquisiciones de sistemas vivos como persistentes.

5. Fase de Preparación y Procesamiento

Descripción General

Procesamiento y validación las imágenes forenses y del conjunto de técnicas y herramientas para efectuar la extracción y el análisis. Procesamiento inicial de la evidencia para normalizar los datos y reducir la cantidad de archivos duplicados o irrelevantes. Planificación y diseño de estrategia de extracción y análisis.

Recomendaciones

Identificar las tecnologías de información en los objetos de evidencia digital: tecnologías de BDR, arquitecturas de despliegue, imágenes forenses medios de almacenamientos, exportación de BDR, scripts de SQL de estructuras o datos, archivos de datos, de logs, de auditoria, de backup, de trazas, etc.

Preparar y asegurar el espacio de almacenamiento en disco necesario y el entorno de trabajo para descomprimir, recomponer y validar las imágenes forenses.

Preparar extracción en BDR recreando un entorno similar al inicial de la base de datos a analizar. Preparar en el entorno de trabajo el conjunto de técnicas y herramientas necesarias para efectuar la extracción y el análisis en BDR.

Procesamiento inicial analizando y procesando los datos de las tablas y campos relevantes, descartando los irrelevantes o redundantes.

6. Fase de Extracción y Análisis

Descripción General

Extracción de la información de las imágenes forenses. Selección de la potencial evidencia digital. Análisis de contenidos y relaciones en relación con el caso y a los puntos periciales.

Recomendaciones

En esta fase se lleva a cabo la extracción de la evidencia en BDR, lo que implica extraer datos y estructuras a nivel de base de datos, su motor e información de contexto (propietario, fecha de creación, fecha de modificación, etc.).

Analizar el contenido de la información en los datos extraídos a partir de palabras claves, nombres de objetos, nombres de usuarios, rango de fechas y horarios, patrones claves, etc.

Analizar comandos SQL ejecutados. Revisar los planes de ejecución de sentencias SQL. Analizar información de auditorías y logs.

Buscar información ofuscada u oculta en el contenido de las base de datos (por ejemplo, imágenes embebidas en campos).

Evidenciar y analizar eventos anormales. Ejecución de comandos o transacciones sospechosas, incompletas o pendientes. Recuperación o manipulación de estructuras o datos no autorizadas indebidas o dudosas.

Analizar las relaciones entre los elementos de base de datos extraídos, el contenido recuperado y los elementos previos aportados.

7. Fase de Producción y Presentación

Descripción General

Presentar los resultados obtenidos en un dictamen final, informes técnicos, anexos y la presentación para el juicio o para los solicitantes.

Recomendaciones

Esta fase se basa en el armado de un informe pericial claro, preciso y concreto incluyendo la documentación de todas las actividades y tareas realizadas sobre los objetos de BDR tratados. El armado y presentación de dictamen final y anexos necesarios en BDR deben además incluir los conceptos técnicos de base de datos.

8. Fase de Evaluación Final

Descripción General

Evaluación final del trabajo realizado como parte del proceso de calidad y mejora continua.

Recomendaciones

A partir del análisis proponer mejoras en la metodología AUDBForense.

Con la detección de acciones indebidas, maliciosas o dudosas proponer mejoras en la estrategia de seguridad, en las configuraciones y en las auditorías de datos ejecutadas en las BDR. De no existir previamente una metodología de auditoria implementada (AUDB o cualquier configuración de auditoría de datos), este informe podría sentar las bases para planear una estrategia de auditoría de datos.

CONCLUSIONES

No existía, previo a este trabajo, ninguna metodología forense específica sobre la cual basar las investigaciones o actuaciones periciales en base de datos relacionales.

A nivel tecnológico, AUDBForense es aplicable a la actuación pericial en cualquier tipo de SGBD.

En relación con los aspectos legales vinculados a la actuación forense, la metodología se basa en la legislación de la República Argentina, aunque en general podría ser aplicado a nivel internacional adicionando los aspectos específicos que podrían diferir. No enfoca su aplicación en un fuero judicial en especial, por lo cual puede utilizarse en casos del fuero civil, comercial, penal, laboral, etc.

La metodología puede ser aplicable tanto en casos judicializados como privados, ya que independientemente del caso, la metodología considera la ejecución de actividades y procedimientos necesarios para la admisibilidad de la evidencia digital en un proceso judicial.

La metodología no especifica reglas o directrices específicas para casos donde las bases de datos están contenidas en la nube, correspondan a bases de datos no relacionales o estén contenidas o sincronizadas en dispositivos móviles, lo cual plantea futuras líneas de investigación sobre las cuales avanzar.

Es de gran importancia poder extender y adecuar la metodología de análisis forense informático para poder ser aplicada a bases de datos de datos de gran escala Big Data y poder

realizar pericias sobre datos que vayan más allá de los datos estructurados que pueden ser consultados por SGBD relacionales, como ser, archivos sin estructuras, video digital, imágenes, datos de sensor y cualquier dato que no esté contenido en registros divididos por campos (en un modelo relacional).

La implementación de servicios de cómputo en la nube ofrece múltiples ventajas, sin embargo, una de las grandes dificultades que se presentan a la hora de realizar un análisis forense de estos servicios es de índole legal, más precisamente, cuando se transfieren datos personales de un país a otro para luego aplicarles un proceso informático. Por lo tanto, al momento de iniciar un análisis forense de base de datos en la nube, es necesario considerar la normativa local, teniendo en cuenta también la legislación internacional y analizar las cláusulas relativas a la seguridad de la información, especialmente a la protección de los datos personales.

En términos de pericias en contextos de cómputo en la nube y Big Data, se plantean nuevos paradigmas, desafíos y escenarios que implican la necesidad del diseño de una metodología específica para manejar nuevos aspectos no solo técnicos sino legales en el tratamiento de grandes volúmenes de datos estructurados o no, almacenados en la nube, de manera de asegurar la admisibilidad de las pruebas.

AGRADECIMIENTOS

Se agradece a las autoridades del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza (Buenos Aires, Argentina) por el apoyo al trabajo realizado.

REFERENCIAS

[1] Cano, J. (2011) *Computación Forense en Base de Datos: Conceptos y reflexiones*. ISACA. Colombia, 5-17. Recuperado de http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/l242.pdf

[2] Di Iorio, A.; Castellote, M.; Bruno, C. (2017). *El Rastro Digital del Delito. Aspectos técnicos, legales y estratégicos de la Informática Forense*. Universidad FASTA Ediciones. Mar del Plata, Buenos Aires, Argentina, Cap. 3.

[3] Di Iorio, A. H. (2016). *Guía Integral de Empleo de la Informática Forense en el Proceso Penal (2da edición)*. Universidad Fasta, Mar del Plata, Buenos Aires, Argentina, 47-57. Recuperado de http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1592/PAIF.pdf? sequence=1

[4] EDRM. (2014). *Modelo EDRM*. EDRM (Electronic Discovery Reference Model) Recuperado de https://www.edrm.net/frameworks-and-standards/edrm-model/

[5] ISO/IEC 27037:2012. (2012). Information *Technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence*. ISO. Estados Unidos.

[6] Ministerio de Justicia y Derechos Humanos. (2018). *Protocolo unificado de los Ministerios Públicos de la República Argentina*. Ediciones SAIJ, CABA, Argentina,15-18. Recuperado de: http://www.jus.gob.ar/media/3262247/Protocolo%20unificado.pdf

[7]UFECI. (2016). *Guía de obtención, preservación y tratamiento de evidencia digital*. Ministerio Público Fiscal, CABA, Argentina. Recuperado de: https://www.mpf.gob.ar/resoluciones/PGN/2016/PGN-0756-2016-001.pdf

[8] Gioia, C. (2012). *Desarrollo de una Metodología de Auditoria Universal de Datos a Nivel de Registro*. Tesis de Especialización en Criptografía y Seguridad Teleinformática. Escuela Superior Técnica del Ejército Argentino, Buenos Aires, Argentina, p.15-49.

[9] Gioia, C.; Eterovic, J. (2017). CIBSI 2017. Proposal of a non-invasive universal data audit methodology. Buenos Aires, Argentina: *IX Congreso Iberoamericano de Seguridad Informática, UBA*. Recuperado de: http://cibsi2017.org/programa/Actas_cibsi2017_UBA.pdf, p.83-90.

[10] Gioia, C. (2019). *Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos*. Tesis de Maestría en Informática. Universidad Nacional de la Matanza. Escuela de Posgrado, Buenos Aires, Argentina, 85-189.

B.4.2. Póster:

CADI/CLADI CAEDI

METODOLOGÍA DE ANÁLISIS FORENSE INFORMÁTICO PARA LA OBTENCIÓN DE EVIDENCIA DIGITAL EN BASE DE DATOS

Gioia, Cintia Verónica - Eterovic, Jorge Esteban

Se presenta el desarrollo de una metodología de análisis forense informático para base de datos relacionales que guía la actuación pericial especializada garantizando la confiabilidad de las actividades de identificación, recolección, adquisición y análisis de evidencia digital. La misma está diseñada a partir del desarrollo de tres metodologías: una metodología informática forense aplicable a todo tipo de evidencia digital, una metodología informática forense en base de datos y una metodología de auditoría universal de base de datos. La metodología propuesta sobrepasa las limitaciones o retos tecnológicos de cada tipo de base de datos garantizando la admisibilidad judicial de la evidencia digital.

INTRODUCCIÓN

Frente a la heterogeneidad de las Base de Datos Relacionales (BDR) y su complejidad, surge la necesidad de aplicar la ciencia de informática forense a las mismas procurando respetar los principios forenses para obtener evidencia digital válida como medio de prueba para su efectiva sanción en un proceso judicial.

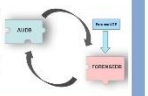
DISEÑO DE LA SOLUCIÓN

La solución propuesta comprende el desarrollo de una metodología integral de análisis forense informático para el tratamiento de evidencia digital en base de datos relacionales denominada: **AUDBForense** (Auditoria Forense de Base de Datos) la cual está integrada por tres metodologías:

- Metodología de auditoría universal de base de datos (**AUDB**).
- Metodología de informática forense universal (**ForenseUDE**).
- Metodología de informática forense en base de datos (**ForenseDB**).

ForenseDB se centra en el tratamiento de la evidencia digital en BDR. Los resultados de la implementación de auditorías de datos de **AUDB** proporcionan evidencia digital relevante y precisa para la investigación forense informática de casos. **ForenseDB** está basada en la metodología **ForenseUDE**.

Se plantean metodologías independientes que se retroalimentan y complementan entre sí, conformando **AUDBForense,** la cual actúa de manera preventiva, probatoria y correctiva en pos del resguardo de la confidencialidad, integridad y disponibilidad de los datos sensibles.



METODOLOGÍA ForenseUDE

ForenseUDE es una metodología informática forense basada en un modelo iterativo dividido en fases con la especificación de actividades y tareas a realizar en un análisis forense informático sobre cualquier tipo de evidencia digital, lo que en la metodología se denomina evidencia digital universal (**UDE, Universal Digital Evidence**).

ForenseUDE plantea un proceso que garantiza las características de relevancia, confiabilidad, suficiencia y validez legal de la evidencia digital tratada durante sus diferentes fases.

ForenseUDE se sustenta en ideas y conceptos de modelos conocidos: PURI (Proceso Unificado de Recuperación de Información) del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab), el modelo internacional EDRM (Electronic Discovery Reference Model) y en la norma ISO/IEC 27.037.

METODOLOGÍA ForenseDB

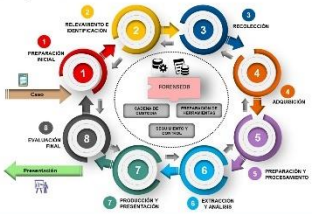
ForenseDB es una metodología forense informática para Base de Datos Relacionales que asegura una actuación metódica basada en un orden lógico de actividades a ejecutar, evitando contaminar la evidencia digital en las bases de datos, de manera de preservar la información recolectada como potencial prueba. Es aplicable a las BDR en general, no puntualiza en un SGBD (Sistema de Gestión de Base de Datos) o plataforma en particular.

ForenseDB se centra en la obtención de evidencia digital basada en cualquier dato o registro de información procesado electrónicamente en BDR o en artefactos vinculados.

Se basa en un proceso que se plantea justificable, auditable, repetible y reproducible, cumpliendo con los requisitos de confiabilidad y el registro de la debida cadena de custodia para casos de BDR.

FASES DE METODOLOGÍA ForenseDB

La metodología utiliza como marco de referencia el proceso desarrollado en ForenseUDE, a partir del cual describe las actividades y tareas específicas aplicables en casos de BDR. Posee ocho fases principales y tres actividades transversales.



METODOLOGÍA AUDB

AUDB es una metodología de auditorías de BDR que posibilita generar la evidencia digital de operaciones y actividades que se realizan sobre los datos sensibles. A partir de esta evidencia digital se puede analizar y detectar acciones maliciosas, sensibles o dudosas que puedan afectar la información.

AUDB posibilita obtener información valiosa del contexto de los hechos y reconstruir los sucesos en una línea trazable de tiempo.

CONCLUSIONES

AUDBForense se basa en la legislación de la República Argentina, aunque podría ser aplicado a nivel internacional especificando los aspectos regulatorios que podrían diferir. Puede utilizarse tanto en casos judicializados como privados, ya que se basa en la ejecución de actividades y procedimientos que garantizan la admisibilidad de la evidencia digital en un proceso judicial.

DIIT
Departamento de Ingeniería e Investigaciones Tecnológicas
Universidad Nacional de La Matanza

B.4.2. Certificado:

CADI/CLADI CAEDI

.UBAfiuba FACULTAD DE INGENIERÍA · confedi · CONDEFI

Se certifica que los autores

Cintia Verónica Gioia y Jorge Estéban Eterovic

han presentado el trabajo titulado

Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos

en el **Encuentro Argentino y Latinoamericano de Ingeniería CADI / CLADI / CAEDI**, organizado por la Facultad de Ingeniería de la Universidad de Buenos Aires y llevado a cabo los días 5, 6 y 7 de octubre de 2021, de manera virtual.

Dr. Ing. Oscar Pascal	Inga. Alejandra Acuña V.	Ing. Alejandro M. Martínez	Dr. Ing. Luis Fernandez Luco	Dra. Cristina Vázquez
CONFEDI	CONDEFI	Facultad de Ingeniería - UBA	Comité Académico	Comité Organizador
Presidente	Presidenta	Decano	Presidente	Presidenta

D.1. Tesis de grado

INSTITUTO UNIVERSITARIO DE LA POLICÍA FEDERAL ARGENTINA
Ciclo de Lic. en Investigación Criminal

Tesina para optar por el título de:
Licenciado en Investigación Criminal

Denominación del título de la tesina:

Análisis Criminal del Abuso Sexual de Niños, Niñas y Adolescentes en Línea

Autor: Emiliano Alejandro Zárate
Directora de Tesina: Abogada Patricia Fernández

23 de septiembre de 2021

Índice de contenido

Lista de anexos

1 Resumen

Análisis Criminal del Abuso Sexual de Niños, Niñas y Adolescentes en Línea (2019 - 2020)

El abuso sexual de niños, niñas y adolescentes en línea ha tomado gran relevancia debido al aumento de casos en todo el mundo, por lo que las organizaciones no gubernamentales (ONG), y organizaciones de la sociedad civil (OSC) se han pronunciado para solicitar la intervención de los Estados. La presente investigación tiene como objetivo realizar un análisis de casos de Grooming y material de abuso sexual de niños, niñas y adolescentes (NNyA) en línea con el fin de aportar un documento actualizado sobre la problemática y las técnicas de investigación criminal. Para lograr el objetivo de la investigación se utiliza el método descriptivo basado en una técnica de revisión documental. En primer lugar, se indican las definiciones y terminologías, el marco jurídico y estadísticas; luego se expone sobre el caso Mica Ortega y el accionar de los Groomers en línea; posteriormente a ello se realiza un análisis sobre el caso Daisy's Destruction y la metodología utilizada para intercambiar el material de abuso sexual de NNyA en línea; seguidamente, se formula la importancia de la preservación de la prueba, las estrategias en informática forense y las técnicas de investigación forense digital; y finalmente se mencionan las herramienta de investigación ICACCOPS y la necesidad de generar acciones para el cuidado y prevención de delitos sexuales contra los NNyA en línea. Al realizar el análisis se observó, el crecimiento acelerado de nuevos canales digitales de comunicación que permite a los delincuentes depredar, organizarse y formar comunidades colaborativas, utilizando herramientas cada día más avanzadas, lo cual dificulta que los cuerpos de investigación judiciales, fuerzas de seguridad y policiales logren mantenerse a la vanguardia.

Palabras clave: Grooming, material de abuso sexual de niños, niñas y adolescentes en línea, pornografía infantil, informática forense, evidencia digital, investigación forense digital, cibercrimen, investigación criminal.

ANEXO II

FC-013

UNLaM - SECyT Programa CyTMA2 FC-013

FORMULARIO DE EVALUACIÓN DE ALUMNOS INTEGRANTES DE EQUIPOS DE INVESTIGACIÓN

Unidad Académica: Departamento de Ingeniería e Investigaciones Tecnológicas
Código: C2 ING 073
Título del Proyecto: Análisis del Marco Normativo, Técnico y Legal para la Implementación y Gestión de un Laboratorio de Informática Forense en el DIIT
Director del Proyecto: Mg. Ing. Cintia Gioia
Fecha de inicio:01/01/2020
Fecha de finalización:31/12/2021

1. Datos del alumno
Apellido y Nombre: Saldaña, Fernando
DNI: 38.346.178
Unidad Académica: Departamento de Ingeniería e Investigaciones Tecnológicas
Carrera que cursa: Ingeniería en Informática
Período evaluado: 01/01/2021 al 31/12/2021

2. Dictamen de evaluación de desempeño del alumno:
Colocar una cruz donde corresponda

2.1 Satisfactorio: X
2.1 No satisfactorio:

Fundamentos del dictamen:
Los conocimientos y experiencia adquirida fueron de gran aporte para el desarrollo de los informes integradores. Ha participado en el desarrollo de la guía de implementación de laboratorios informático forense.

3. Propuesta de continuidad en el proyecto (si corresponde según duración estimada)
Colocar una cruz donde corresponda

3.1 Continuar en el presente proyecto:
3.2 No continuar en el presente proyecto:

28/02/2022 Mg. Ing. Cintia V. Gioia

Lugar y fecha	Firma del Director	Aclaración de firma

UNLaM - SECyT Programa CyTMA2 FC-013

FORMULARIO DE EVALUACIÓN DE ALUMNOS INTEGRANTES DE EQUIPOS DE INVESTIGACIÓN

Unidad Académica: Departamento de Ingeniería e Investigaciones Tecnológicas
Código: C2 ING 073
Título del Proyecto: Análisis del Marco Normativo, Técnico y Legal para la Implementación y Gestión de un Laboratorio de Informática Forense en el DIIT
Director del Proyecto: Mg. Ing. Cintia Gioia
Fecha de inicio:1/1/2020
Fecha de finalización:31/12/2021

1. Datos del alumno
Apellido y Nombre: Bonavento, Sergio
DNI:33.293.881
Unidad Académica: Departamento de Ingeniería e Investigaciones Tecnológicas
Carrera que cursa: Ingeniería en Informática
Período evaluado: 1/1/2021 al 31/12/2021

2. Dictamen de evaluación de desempeño del alumno:
Colocar una cruz donde corresponda

2.1 Satisfactorio: X
2.1 No satisfactorio:

Fundamentos del dictamen:
Los conocimientos y experiencia adquirida fueron de gran aporte para el desarrollo de los informes integradores. Ha participado en el desarrollo del informe de equipos y herramientas forenses a ser parte de distintas propuestas de implementación del laboratorio informático forense del DIIT.

3. Propuesta de continuidad en el proyecto (si corresponde según duración estimada)
Colocar una cruz donde corresponda

3.1 Continuar en el presente proyecto:
3.2 No continuar en el presente proyecto:

28/02/2022		Mg. Ing. Cintia V. Gioia
.....	.....	.....
Lugar y fecha	Firma del Director	Aclaración de firma

ANEXO III

**** Los certificados o imágenes de los archivos relacionados se visualizan al final del Anexo III.*

#	OEA
1	**"Simposio de Ciberseguridad de la OEA 2020" organizado por la OEA (Organización de Estados Americanos).** 28 de septiembre al 2 de octubre de 2020. Invitación especial otorgada por la OEA. **"Simposio de Ciberseguridad de la OEA 2021" organizado por la OEA (Organización de Estados Americanos).** 20 de septiembre al 30 de septiembre de 2021. Invitación especial otorgada por la OEA.
2	**Comprobante de** Solicitud de **Fondo de Innovación para proyectos de Ciberseguridad de la OEA** desarrollados junto a **CISCO y la Fundación Citi** en la Categoría de "Prevención, lucha y clasificación del delito digital".
3	Solicitud de **Fondo de Innovación para proyectos de Ciberseguridad de la OEA** desarrollados junto a **CISCO y la Fundación Citi** en la Categoría de "Prevención, lucha y clasificación del delito digital".
#	**REDUNIF**
4	**Acta de la Asamblea de REDUNIF donde se aprueba la incorporación de UNLAM a la REDUNIF, junio 2019.**
5	**Invitación Asamblea Red UNIF 2020 - Viernes 6/11/2020 18 hs**
6	**Acta de Séptima Asamblea de Red UNIF donde queda registrada la designación por votación de la Mg. Ing. Cintia Gioia como Secretaria General de la Red. 1 de noviembre de 2021.**
#	**IRAM**
7	**Nota de designación de representantes de UNLAM en Comisión de Informática Forense de IRAM firmada por el Rector de UNLAM, 14 de marzo 2019.**
8	**Mails con Avances de Comisión Informática Forense y participación y agradecimiento a integrante de UNLAM por la colaboración de traducción de las normas.** **Mail donde se evidencia que el trabajo continúa en 2022.**
#	**Convenios de Capacitación**
9	**Información de convenios con COPITEC y Ministerio Público Fiscal Bs As aplicados a los curso de "Cibercrimen e Informática Forense" del año 2020 y 2021 y al curso de "Cibercriminalidad Económico-Financiera" del año 2021, dictados por parte del equipo de investigación y coordinados por la Mg. Ing. Cintia Gioia**

Código	FPI-009
Objeto	Guía de elaboración de Informe de avance de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

1. Invitación a “Simposio de Ciberseguridad de la OEA 2020” y “Simposio de Ciberseguridad de la OEA 2021” organizado por la OEA

2. Comprobante de Solicitud de Fondo de Innovación para proyectos de Ciberseguridad de la OEA desarrollados junto a CISCO y la Fundación Citi en la Categoría de "Prevención, lucha y clasificación del delito digital"

Application: 0000000123

Cintia Gioia - cgioia@unlam.edu.ar
Fondo de Innovación en Ciberseguridad

Summary

ID: 0000000123
Last submitted: Dec 4 2020 04:18 AM (UTC)

Application Form

Completed - Nov 24 2020

Application Form

Applicant Information

First Name	Cintia
Last Name	Gioia
Email	cgioia@unlam.edu.ar
Gender	Female

Organization Information

Organization Name	Universidad Nacional de la Matanza
Applicant Job Title	Implementación y Gestión de un Laboratorio de Informática Forense
Type of Organization	Academia
Country	Argentina
LinkedIn URL	https://www.linkedin.com/school/universidad-nacional-de-la-matanza/mycompany/

Consent Disclaimer

Completed - Nov 24 2020

Consent Disclaimer

Disclaimer

By registering and submitting an application, you grant authorization to GS/OAS and Cisco to collect and share your name, title, affiliation and email address and any information included in the application, with other partners, co-organizers and evaluators of the Cybersecurity Innovation Fund for the evaluation of the project and other purposes. This consent can be revoked at any time by contacting cybersecurity@oas.org

I confirm that I have read the above and agree to the terms and conditions.

Responses Selected:

Checked

Innovation Idea and Proposal

Completed - Dec 4 2020

Innovation Idea and Proposal

Project Category

Please select which category best describes your project

Prevention, counter and classification of digital crime

Proposal

Please download the following template to ensure your attached proposal contains all necessary information.

English Template: Found here

Spanish Template: Found here

Implementacion Laboratorio Informatico Forense UNLAM v1.0.pptx

Filename: Implementacion Laboratorio Informatico Forense UNLAM v1.0.pptx **Size:** 1.8 MB

3. Solicitud de Fondo de Innovación para proyectos de Ciberseguridad de la OEA desarrollados junto a CISCO y la Fundación Citi en la Categoría de "Prevención, lucha y clasificación del delito digital".

En la actualidad la diversidad de tecnologías y el volumen de información a analizar exigen que se dispongan de equipamientos de cómputos de alta prestaciones, diversidad de tecnología forense y multiplicidad de expertos, para el abordaje de los distintos delitos informáticos y la variedad de tecnologías involucradas.

Se hace indispensable disponer de Laboratorios Informáticos Forenses que brinden soporte pericial a múltiples tecnologías, garantizando la aplicación de herramientas adecuadas por parte de personal calificado en la materia, que actúe de forma metódica, mantenga la cadena de custodia y evite la contaminación de la prueba, garantizando la admisibilidad de la evidencia digital en la judicialización de los casos.

Hoy en día la demanda mundial de Laboratorios de Informática Forense es cada vez mayor, resultando fundamental mantener un conocimiento detallado de las normas y regulaciones legales, así como de las técnicas, procesos y procedimientos que permitan mantener la confiabilidad, integridad, confidencialidad, cumplimiento y validez del trabajo realizado por expertos en el Laboratorio Informático Forense.

Nuestra hipótesis se basa en que en disponer de un marco normativo, técnico y legal para la implementación y gestión de un Laboratorio Informático Forense, basado en el análisis detallado de las diferentes normas, estándares, metodologías y tecnologías requeridas, dentro del marco jurídico y legal, es la base esencial para la puesta en funcionamiento de dicho laboratorio y el aseguramiento de la confiabilidad e integridad de la evidencia digital como también del desempeño de profesionales peritos informáticos en un marco de trabajo seguro.

OEA cisco Canadá citi

Solución – Descripción general del proyecto

Se implementará un laboratorio informático forense, con el objetivo de brindar servicios profesionales periciales y de investigación digital y además ofrecer un ámbito académico de capacitación y desarrollo profesional en la materia a alumnos, egresados y profesionales

Se desea establecer un marco de referencia para la puesta en funcionamiento del Laboratorio Informático Forense basado en recomendaciones y mejores prácticas, a partir del análisis comparativo de normas, estándares, guías de buenas prácticas, y procedimientos, como también del análisis, evaluación y prueba de plataformas y tecnologías necesarias para la implementación y gestión de laboratorios periciales informáticos.

Dicho marco de referencia, alineado al marco regulatorio legal nacional, debe asegurar la confiabilidad e integridad de la evidencia digital y posibilitar el desempeño eficiente y de calidad por parte equipos de profesionales peritos informáticos en un ámbito de trabajo seguro.

Definir y redactar una guía general de arquitectura y gestión del Laboratorio de Informática Forense, que garantice la aplicación adecuada de los procedimientos, herramientas y resultados sobre los medios informáticos analizados, orientado al abordaje de pericias informáticas de distinta naturaleza, definiendo roles y responsabilidades en la administración de los casos y garantizando procesos de auditorías de los procedimientos realizados

OEA cisco Canadá citi

Público Objetivo

- Estudiantes universitarios, egresados, profesionales y funcionarios públicos interesados en formarse, especializarse y desempeñarse laboralmente en informática forense e investigación digital.
- Fiscalías de Departamentos Judiciales municipales, provinciales y nacionales.
- Organismos Gubernamentales municipales, provinciales y nacionales.
- Fuerzas de Seguridad bajo a acuerdos.
- Organismos No Gubernamentales involucrados a la temática
- Empresas o personas que necesiten de servicios periciales informáticos.

Descripción detallada de la solución propuesta

Inicialmente se abordará la investigación de equipamientos, herramientas y de la implementación de laboratorios afines, tanto nacionales como internacionales, para desarrollar diferentes propuestas de implementación de Laboratorios Informático Forenses según sus capacidades y objetivos, acompañados de una guía integral de implementación, la cual servirá de base para la implementación de un laboratorio afín en la Universidad

Se fijarán protocolos de implementación, gestión y actuación en base a normas estándares y guías de buenas prácticas forenses que aseguren la calidad y el tratamiento adecuado de la evidencia digital garantizando que la misma pueda ser admisible como prueba ante juicios

Se implementará de forma gradual, según presupuesto y disponibilidad de recursos, la infraestructura, equipos y las herramientas forenses fundamentales para el desarrollo del trabajo pericial e investigativo de los peritos informáticos.

Se llevará a cabo capacitaciones por parte de los integrantes del proyecto a la comunidad educativa y profesional, con la finalidad de capacitar a potenciales profesionales y alumnos que podrían incorporarse a futuro al laboratorio

Metodología General:

- Se analizarán las diferentes normativas, estándares, guías de buenas prácticas y metodologías relacionadas a la implementación y gestión de un Laboratorio Informático Forense, tanto a nivel nacional como internacional
- Se investigarán implementaciones y servicios de Laboratorios Informático Forense implementados a nivel privado, en cuerpos de investigaciones judiciales y diferentes fuerzas o entidades que brinden información al respecto.
- Se investigarán, analizarán, probarán y compararán diferentes herramientas y tecnologías forenses (gratuitas y bajo licencia), su aplicación, ventajas y desventajas.
- Se estudiarán, analizarán y compararán diferentes técnicas, procedimientos, plataformas, tecnologías y herramientas a aplicar en cada una de las fases del Ciclo de Vida de la Evidencia Digital dentro un Marco Normativo y según el tipo de evidencia digital a periciar
- Se validará la información analizada y estudiada con profesionales expertos tanto del área Legal, Seguridad Informática, Seguridad de la Información e Informática Forense.
- Se redactará un informe integral final con el estudio y el análisis comparativo realizado, acompañado de recomendaciones y buenas prácticas como conclusión investigativa.
- Se desarrollará una guía integral de arquitectura e implementación de un laboratorio informático forense orientado al abordaje de pericias informáticas de distinta naturaleza.
- Se implementará un laboratorio informático forense de forma gradual en base a recursos humanos y técnicos disponibles

OEA cisco Canadá citi CIC

Impacto esperado

- Con el financiamiento inicial del proyecto se busca poder implementar un laboratorio informático preliminar que posibilite investigar, capacitar y certificar a miembros del equipo del proyecto en tecnologías y herramientas forenses a aplicar en cada etapa del tratamiento de la evidencia digital y según la naturaleza de la misma.
- Capacitar a alumnos y profesionales interesados en la temática a través de cursos que incluyan prácticas de laboratorios, como también la organización de diversas actividades de apoyo a la formación de peritos informáticos, a través de la organización de charlas, seminarios o talleres que se desarrollarán orientadas a alumnos de las carreras de Ingeniería en Informática, e incluso de Abogacía y profesiones afines o interesadas en la temática.
- Con lo servicios profesionales que se ofrecerían desde el laboratorio se podrá cubrir determinada demanda actual de pericias informáticas e investigaciones digitales, disponibilizando a la Sociedad de un laboratorio informático forense integrado con profesionales capacitados y con la disponibilidad de tecnologías y herramientas informáticas forenses de alto nivel.
- Desarrollar una guía general de arquitectura e implementación de Laboratorios de Informática Forense orientado al abordaje de pericias informáticas de distinta naturaleza en base a la evaluación, investigación, análisis y prueba de diversas tecnologías y plataformas gratuitas y bajo licencia paga.

OEA cisco Canadá citi CIC

Presupuesto

Para comenzar el trabajo de investigación, análisis, evaluación e implementación de herramientas y tecnologías de licencia paga el**presupuesto básico inicial** es:

	Precio US$	Cantidad	Precio Total US$
Magnet Axiom Computer+Mobile con SMS (1 año de licencia)	11.800	1	11.800
Subtotal Forense PC/Móvil			**11.800**
Paliscope Discovery	1.300	1	1.300
Griffeye Analyze Di Pro - Flotante	1.900	1	1.900
Subtotal Herramientas Varias			**3.200**
Ultrablock IDE/SATA (TK35U)	1.050	1	1.050
Ultrablock USB (TK8U)	1.800	1	1.800
Duplicador Forense TD2u	5.000	1	5.000
Subtotal Bloqueadores y Duplicadores			**7.850**
Total US$			**22.850**

Presupuesto

A continuación se detalla el presupuesto necesario para l**adquisición de variedad de las principales plataformas, herramientas y equipos para la implementación de un laboratorio informático forense (en su cantidad mínima)**

	Precio US$	Cantidad	Precio Total US$
UFED 4PC Ultimate (dos años licencia)	33.000	1	33.000
Analytics Desktop Full (dos años de licencia)	24.000	1	24.000
Magnet Axiom Computer+Mobile con SMS (dos años de licencia)	15.000	1	15.000
Subtotal Forense PC/Móvil			**72.000**
Paliscope Discovery	1.300	1	1.300
Griffeye Analyze Di Pro - Flotante	1.900	1	1.900
Subtotal Herramientas Varias			**3.200**
Ultrablock IDE/SATA (TK35U)	1.050	1	1.050
Ultrablock USB (TK8U)	1.800	1	1.800
Duplicador Forense TD2u	5.000	1	5.000
Subtotal Bloqueadores y Duplicadores			**7.850**
Estaciones Forenses	4.500	2	9.000
Monitores	260	4	1.040
Subtotal Estaciones Forenses			**10.040**
Total US$			**93.090**

Presupuesto

A continuación se detalle el presupuesto necesario para l**adquisición de las principales plataformas, herramientas y equipos necesarios para la implementación de un laboratorio informático forense completo, con capacidad de procesamiento en paralelo**:

	Precio US$	Cantidad	Precio Total US$
UFED 4PC Ultimate (dos años licencia)	33.000	2	66.000
Analytics Desktop Full (dos años de licencia)	24.000	2	48.000
Magnet Axiom Computer+Mobile con SMS (dos años de licencia)	15.000	2	30.000
Subtotal Forense PC/Móvil			**144.000**
Paliscope Discovery	1.300	2	2.600
Griffeye Analyze DI Pro - Flotante	1.900	2	3.800
Subtotal Herramientas Varias			**6.400**
Ultrablock IDE/SATA (TK35U)	1.050	1	1.050
Ultrablock USB (TKBU)	1.800	2	3.600
Duplicador Forense TD2u	5.000	2	10.000
Subtotal Bloqueadores y Duplicadores			**14.650**
Estaciones Forenses	4.500	6	27.000
Monitores	260	6	1.560
Subtotal Estaciones Forenses			**28.560**
Total US$			**193.610**

OEA cisco Canadá citi

Equipo

Directora del Proyecto: Mg. Ing. Cintia Gioia

Subdirectora del Proyecto: Mg. Nora Gigante

Docentes Investigadores del Proyecto:

- Dr. Allonca, Juan Cruz González
- Mg. Lic. Walter Ureta
- Ing. Mario Krajnik

Asesores Externos

- Emiliano Zárate

Alumnos Colaboradores:

- Sergio Bonavento
- Fernando Saldaña

OEA cisco Canadá citi

Directora del Proyecto

Mg. Ing. Cintia Gioia

Magister en Informática UNLaM. Ingeniera en Informática UNLaM. Especialista en Criptografía y Seguridad Informática de la Escuela Superior Técnica del Ejército Argentino. Docente Investigadora Universitaria UNLaM. Jefa de Cátedra de Auditoría y Seguridad Informática de Ingeniería en Informática UNLaM.
Coordinadora de Cursos de Cibercrimen, Informática Forense e Inv. Digitales UNLaM. Coordinadora de Tecnicatura en Desarrollo Web/Móviles UNLaM.
Perito Informática Forense. Investigadora Digital.
Miembro de Comisión de Informática Forense de IRAM.
Representante Titular de UNLaM en Red Universitaria de Informática Forense de Argentina, REDUNIF.
Integrante del Instituto de Políticas Públicas de Prevención del Grooming de la Honorable Cámara de Diputados de la Provincia de Buenos Aires.
Profesional con amplia experiencia y trayectoria en gestión de proyectos de Ciberseguridad, Auditoría de Sistemas, Informática Forense e Investigación Digital en diferentes empresas y organismos nacionales e internacionales.

Subdirectora del Proyecto

Mg. Nora Gigante

Máster en Ingeniería de Software por la Universidad Politécnica de Madrid. Licenciada en Administración de la Educación Superior. Analista de Sistemas de información. Egresada de la UNLaM. Certificada en ITIL. Jefe de Cátedra de Gestión de RRHH en proyectos de Tecnología de la Carrera de Ingeniería en Informática UNLaM. Docente investigadora en áreas de Ingeniería de Requisitos y Seguridad.
Responsable del Área de Comunicaciones Institucionales del Departamento de Ingeniería e Investigaciones Tecnológicas de la UNLaM.

Integrante del Proyecto – Docente Investigador

Dr. Juan Cruz González Allonca

Abogado especializado en derecho informático (UBA). Magíster en Ingeniería de Sistemas de Información por la Universidad Tecnológica Nacional (UTN). Forma parte del Consejo de Coordinación deNETmundial Initiative y de la Asociación Latino Americana de Derecho Aeronáutico y Espacial (ALADA). Docente e investigador de la Universidad Nacional de La Matanza (UNLaM) y de la Diplomatura de Derecho 4.0 en la Universidad Austral. Se desempeño como Director Nacional de Protección de Datos Personales de la RepúblicaArgentina.

Integrante del Proyecto –Docente Investigador

Mg. Lic. Walter Ureta

Magíster y Licenciado en Informática.
Gerente y Especialista en Tecnologías de Información en IBM Argentina.
Investigador Universitario, UNLAM. Docente a a cargo de la materia "Seguridad y Calidad en Aplicaciones Web" en Tecnicatura en Desarrollo Web/Móviles
Docente de Posgrado, UBA, Maestría en Ciberdefensa y Ciberseguridad, materia "M9604 Tecnología de la Información".

Integrante del Proyecto– Docente Investigador

Ing. Mario Krajnik

Ingeniero Electromecánico orientación eléctrica, Universidad de Morón
Maestría en Teleinformática y Redes de Computadoras, Universidad de Morón. Certificación CISCO CCNA (administración y mantenimiento de redes). Coordinador del área de simuladores, gestión y mantenimiento de software y Hardware del CIATA / INAC FAA (Centro de Instrucción de Aero navegantes y Técnicos) Base Aérea de Morón.
Docente e Investigador UNLaM.
Consultor en Telecomunicaciones y Redes de Datos.

OEA cisco Canadá citi CIC

Integrante del Proyecto –Asesor Externo

Emiliano Alejandro Zárate

Investigador e Instructor en Informática Forense.
Técnico Superior en Seguridad Pública.
Diplomado en Investigación de Delitos Informáticos y Evidencia Digital.
Integrante del Instituto de Políticas Públicas de Prevención del Grooming de la Cámara de Diputados de la Provincia de Buenos Aires.
Docente en Cursos de Cibercrimen e Informática Forense UNLaM.

OEA cisco Canadá citi CIC

Socios estratégicos

Se brindarán servicio y capacitación a organismos externos que han evidenciado interés y apoyo en el proyecto:

- Fiscalías de Departamento Judicial de La Matanza.
- Fiscalías de Departamentos Judiciales de la Provincia de Buenos Aires.
- Organismos Gubernamentales de la Provincia de Buenos Aires.
- Diversas Fuerzas de Seguridad.
- Organismos No Gubernamentales involucrados a la temática.

Se plantea vincular el proyecto con otros grupos de investigación pertenecientes a Universidades Nacionales de la Red Universitaria de Informática Forense, de la cual UNLaM es miembro activo.

OEA cisco Canadá citi

Sostenibilidad y tracción

El proyecto es la base primordial para el **desarrollo, implementación y puesta en funcionamiento de un Laboratorio Informático Forense dependiente del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de la Matanza**, cuya implementación tiene fines tanto **académicos, investigativos** como **profesionales**, para lograr ofrecer **servicios investigativos y periciales de calidad** desde la Universidad a la Comunidad y Organismos interesados

El laboratorio se proyecta implementar en el actual **Polo Tecnológico de la Universidad de la Matanza,** Centro de Desarrollo en Tecnologías de la Información y las Comunicaciones ubicado en el predio de la Casa de Altos Estudios de la UNLaM. En dicho Polo Tecnológico actualmente se generan continuamente alianzas entre la Universidad y empresas de software y diversos organismos para garantizar la contratación de estudiantes y profesionales desarrollando sus actividades en un predio propio de 2100 metros cuadrados, en el que se instalan diversas empresas y en el que ya se encuentran en funcionamiento dos laboratorios de informática con diversos fines.

Desde la UNLaM se promueve e instala en su Polo Tecnológico el desarrollo de proyectos, empresas de software y organismos interesados que brinden la posibilidad de acceso al **primer empleo de calidad para los jóvenes estudiantes de la zona, que puedan trabajar y estudiar en la misma Universidad**

La finalidad de instalar el laboratorio informático forense en UNLaM es promover el interés y brindar un ámbito académico profesional donde alumnos y profesionales interesados en la temática, puedan capacitarse y desarrollar sus conocimientos y experiencia en el mismo laboratorio.

OEA cisco Canadá citi

Sostenibilidad y tracción

El avance del proyecto y la implementación y crecimiento gradual del laboratorio servirá **como base de conocimiento y capacitación para los actuales y futuros integrantes del Laboratorio Informático Forense**, como también para el **dictado de Cursos y Diplomaturas de Informática Forense e Investigaciones Digitales** que puedan ofrecer no solo capacitación teórica, sino la realización de **talleres prácticos directamente en un laboratorio**.

Dichas capacitaciones se plantean orientadas a alumnos y egresados de la UNLAM y de otras Universidades, como también profesionales interesados, personal de fuerzas de seguridad y de diversos organismos públicos que se desempeñen en un rol u área afín.

El disponer del laboratorio en la Universidad y de los profesionales especialistas permitirá llevar a cabo servicios profesionales y también brindar capacitaciones al alcance de toda la comunidad educativa y profesional **Así se logrará capacitar y disponer de recursos humanos calificados y de los fondos para que el laboratorio pueda crecer y autosustentarse en el tiempo**.

Se espera firmar **convenios con organismos gubernamentales y privados interesados tanto en las capacitaciones como en los servicios profesionales del laboratorio**. Como también **convenios con empresas representantes que comercializan en el país las principales plataformas y herramientas de informática forense e investigación digital**, con el objetivo de obtener alianzas focalizados en la **adquisición** de los mismos como de **certificaciones** de los integrantes del laboratorio en sus productos.

OEA cisco Canadá citi

¿Por qué es innovadora tu propuesta?

La Universidad Nacional de la Matanza se propone ser la primera universidad nacional con un Laboratorio Informático Forense Propio de alto nivel que brinde servicios profesionales y académicos basado en la implementación de plataformas y tecnologías forenses de última generación, al alcance de todos los alumnos y profesionales que quieran desarrollarse en una rama cuya demanda de profesionales peritos informáticos e investigadores digitales crece a un ritmo exponencial a causa de la gran cantidad y variedad de modalidades de delitos vinculados a la informática como medio o fin que cada día aparecen y que necesitan investigarse y se judicializan.

Con esta propuesta se estaría promoviendo el desarrollo de profesionales idóneos en la materia y disponibilizando sus servicios y potencialidad a los organismos gubernamentales, empresas y a la comunidad educativa y en general de un laboratorio informático forense **de primer nivel, independiente y neutral** con el aval de una universidad nacional con gran prestigio académico.

Disponer del laboratorio favorecerá la cooperación entre laboratorios afines de diferentes organismos y entidades.

OEA cisco Canadá citi

4. **Acta de la Asamblea de REDUNIF donde se aprueba la incorporación de UNLAM a la RE-DUNIF en junio 2019.**

Red UNIF
RED UNIVERSITARIA DE INFORMÁTICA FORENSE
ACTA TERCER ASAMBLEA

En la ciudad de Córdoba, Argentina, a los siete días del mes de junio de 2019, en el marco de la Tercera InFo-Conf, se reúnen en la sede de la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de Córdoba los siguientes integrantes de la RED UNIVERSITARIA DE INFORMÁTICA FORENSE - Red UNIF para celebrar la tercer asamblea de la Red

Participan de esta asamblea como miembros formales de la RED UNIF:

- Facultad de Ingeniería de la Universidad FASTA (FI-UFASTA), representada por la Esp. Ing. Ana Haydée Di Iorio
- Centro Regional Universitario Córdoba del Instituto Universitario Aeronáutico de la Universidad de Nacional de la Defensa (CRUC-IUA), representado por el Mg. Ing Eduardo Casanovas.
- Facultad de Ciencias Exactas, Físicas y Naturales de la Universidad Nacional de Córdoba (FCEFN-UNC), representada por el Mg. Ing. Miguel Solinas y el Ing. Alejandro Ambrosini
- Facultad Regional Delta de la Universidad Tecnológica Nacional (UTN-FRD), representada por el Lic. Pedro Asís y la Ing. Carla Daniela Carrillo
- Facultad de Ingeniería del Ejército Argentino de la Universidad Nacional de la Defensa(FI- UNDEF), representada por el el Ing. Pablo Croci.

Participan como miembros invitados por los integrantes de la RED UNIF:

- Ing. Roberto Giordano Lerena, decano de la Facultad de Ingeniería de la Universidad FASTA.
- Ing. Karen Beatriz Villalba y el Ing. Sergio Viera docentes e integrantes del Laboratorio de Informática Forense de UTN-FR Delta.
- Lic. Verónica Mangini, Universidad Nacional del Noroeste de la Provincia de Buenos Aires (ET y ECEyJ - UNNOBA)
- Ing. Cintia Gioia, docente investigador del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza
- Ing. Liliana Figueroa, docente investigador de la Facultad de Ciencias Exactas y Tecnológicas de la Universidad Nacional de Santiago del Estero

Temas tratados:

Siendo las 15 hs, se da inicio a la reunión, tratando los temas acordados en agenda previa.
En primer lugar la Ing. Di Iorio informa sobre las invitaciones enviadas durante el periodo 2018: UNRN, UNSE, UAI, UNLAM.
A continuación se trata la incorporación de la UNLAM. Se le cede la palabra a la Ing. Gioia a fin de que presente su grupo de investigación al resto de los integrantes. Se aprueba su incorporación por unanimidad.
El Ing. Miguel Solinas expone los resultados de trabajos presentados, cantidad de asistentes, etc. de la III InFo-Conf.
Se acordó publicar los trabajos presentados en la InFo-Conf en formato de revista temática, la que abordará conceptos de ciencias forenses e informática forense. La revista contendrá secciones permanentes y un espacio

para la publicación de artículos con referato. En primera instancia el formato será digital. La UNC se ocupará del proceso de registro - ISBN - de la revista.
Se acordó que la UNC dispondrá de un espacio para el hosting y la creación del sitio web de la red.
Se decide iniciar un proceso de estandarización de las propuestas de capacitaciones en la temática que ofrecen las distintas universidades de la red. Éstas propuestas estarán a disposición desde el sitio web.
Se da por aprobado el Manual de Identidad, desarrollado y enviado a los representantes por la UFASTA.
Se acordó dejar para otro momento la tramitación de la personería jurídica.
El Ing. Giordano y el Ing. Ambrosini se comprometen a elaborar una propuesta de estatuto de la red referido a la incorporación de universidades extranjeras, y a las posibles categorías miembros.
Se reciben las siguientes postulaciones para la organización de la IV InFo-Conf:

1) La FIE-UNDEF
2) La FCEFyN-UNC en conjunto con la Facultad de Ingeniería del CRUC-IUA de la UNDEF

En oportunidad de la votación se convoca online a la Facultad de Ingeniería de la Universidad Católica de Salta (FI-UCASAL), representada por el Ing. Sergio Appendino.
Se realizan las votaciones, resultando elegido por 4 a 3 la opción 2).
Se aprueba por unanimidad la postulación de la FIE-UNDEF como sede de la V InFo-Conf en 2021 y la FI-UFASTA como sede de la VI InFo-Conf en 2022.
Se procede a la renovación de autoridades, quedando seleccionados por unanimidad para el período 2019-2021:

- Presidente, el Mg. Ing. Eduardo Casanovas (UNDEF-CRUC-IUA)
- Vicepresidente, el Mg. Ing. Miguel Solinas (FCEFyN-UNC)
- Secretario General Permanente: Esp. Ing. Ana Di Iorio (UFASTA)

Siendo las 17.30 se da por cerrada la asamblea.

5. Invitación Asamblea Red UNIF 2020 - Viernes 6/11/2020

Invitación Asamblea Red UNIF – Vie 6/11 18 hs

Respondió el Jue 19/11/2020 13:41.

redunif@googlegroups.com en nombre de
Ana Haydeé DI IORIO <diana@ufasta.edu.ar>
Vie 16/10/2020 14:37
Para: redunif@googlegroups.com; Roberto GIORDANO LERENA <rogiord@ufasta.edu.ar>; Kaml

Estimados integrantes de la Red UNIF

Espero se encuentren muy bien.

Habiendo culminado la IV edición tan exitosa de la InFo-Conf, los invitamos a reunirnos en asamblea el día **Viernes 6/11 de 18 a 20 hs.** desde el link https://meet.google.com/avr-xewt-afw

Se les compartió un borrador de reglamento tentativo elaborado por Eduardo, Miguel, Alejandro y Roberto.
Les solicitamos por favor que lo lean, comenten, y nos hagan llegar a secretaría vuestros comentarios antes del viernes 29/10.
Es intención poder tratar el reglamento en la próxima asamblea.

La agenda tentativa es:

1) Informe Info-Conf 2020. Toman la palabra Eduardo Casanovas y Miguel Solinas.
2) Tratamiento de Incorporación UAI - Universidad Abierta Interamericana.
Desde Secretaría se da lectura a la nota recibida.
El Lic. Kamlofsky presenta su trabajo y equipo de investigación.
3) Informar: Incorporación a redes de CONFEDI
4) Definiciones próximo InFo-Conf 2021.
Toman la palabra representantes de la FIE para informar avances.
5) Tratamiento del Reglamento Borrador.
Toman la palabra Eduardo Casanovas y Miguel Solinas para presentar el trabajo realizado en conjunto con Alejandro Ambrosino y Roberto Giordano.
Se invita a Alejandro y Roberto a tomar la palabra.

Será un gran gusto volver a encontramos virtualmente!
Cariños

Esp. Ing. Ana Haydée Di Iorio
Secretario General Red UNIF
diana@ufasta.edu.ar
+54 9 2236826955
Logo Red Unif-color-transparente-01.png

--
Has recibido este mensaje porque estás suscrito al grupo "redunif" de Grupos de Google.
Para cancelar la suscripción a este grupo y dejar de recibir sus mensajes, envía un correo

6. Acta de Séptima Asamblea de Red UNIF donde queda registrada la designación como Secretaria General de la Mg. Ing. Cintia Gioia

Red UNIF
RED UNIVERSITARIA DE INFORMÁTICA FORENSE
ACTA SÉPTIMA ASAMBLEA

En la ciudad de Buenos Aires, Argentina, al primer día del mes de noviembre de 2021, se reúnen virtualmente los siguientes integrantes de la RED UNIVERSITARIA DE INFORMÁTICA FORENSE - Red UNIF para celebrar la sexta asamblea plenaria.

Participan de esta asamblea como miembros formales de la RED UNIF:

- Facultad de Ingeniería de la Universidad FASTA (FI-UFASTA), representada por la Esp. Ing. Ana Haydée Di Iorio y el Ing. Bruno Constanzo
- Centro Regional Universitario Córdoba del Instituto Universitario Aeronáutico de la Universidad de Nacional de la Defensa (CRUC-IUA), representado por el Mg. Ing Eduardo Casanovas.
- Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de Córdoba (FCEyN-UNC) representada por el Mg. Miguel Solinas y el Dr. Alejandro Ambrosino.
- Facultad Regional Delta de la Universidad Tecnológica Nacional (UTN-FRD), representada por la Ing. Carla Daniela Carrillo
- Facultad de Ingeniería del Ejército Argentino de la Universidad Nacional de la Defensa(FI- UNDEF), representada por el Ing. Pablo Croci.
- Facultad de Ingeniería de la Universidad Nacional de La Matanza (UNLaM) representada por la Ing. Cintia Gioia
- Facultad de Ingeniería de la Universidad Católica de Salta (UCASAL), representada por la Ing. Beatriz Parra de Gallo y el Ing. Sergio Appendino.
- Facultad de Ingeniería de la Universidad Abierta Interamericana (UAI), representada por el Ing. Raúl Oscar Romero.

Temas tratados:

Siendo las 18.00 hs se da inicio a la séptima asamblea extraordinaria de la Red Universitaria de Informática Forense, tratándose los siguientes temas:

- Se da inicio el proceso de votación del reglamento, aprobándose por unanimidad.
- Se da inicio al proceso de elecciones, con dos propuestas: Lista 1: Miguel Solinas (presidente), Bruno Constanzo (vicepresidente), Beatriz Parra (Secretaria); Lista 2: Ing. Sergio Appendino (Presidente) el Ing. Bruno Constanzo (vicepresidente) y como Secretaria General, Ing. Cintia Gioia. Quedando electo por unanimidad la lista 2
- Se presenta la postulación de UCASAL como sede de InFo-Conf 2023, quedando aprobada por unanimidad.

Siendo las 19.39 se da por finalizada la sesión.

**** Por contexto de COVID la Asamblea se llevó a cabo de manera virtual. Se procederá a la firma física del acta en la próxima Asamblea que se estima será presencial.*

7. Nota de designación de representantes de UNLAM en Comisión de Informática Forense de IRAM firmada por el Rector de UNLAM, 14 de marzo 2019.

Buenos Aires, 14 de marzo de 2019

Sr. Director de Normalización
Ing. Osvaldo D. Petroni
IRAM, Instituto Argentino de
Normalización y Certificación

Asunto: ***Representación de nuestra organización en los Organismos de Estudio de Normas del IRAM***

De mi mayor consideración:

Tengo el agrado de dirigirme a usted con el objeto de informarle que han sido designados por nuestra organización los siguientes representantes en los respectivos organismos de estudio de Normas del IRAM según se indica.

Apellido y nombre: Gioia, Cintia Verónica
Organismo(s) de estudio del IRAM para el(los) que ha sido designado: Comité de Informática Forense
Tratamiento (Sra, Sr, Ing, Tco, Lic, Arq, etc): Ing
Nº de CUIL/CUIT (del representante): 27-25385204-1
Correo electrónico: cgioia@unlam.edu.ar
Teléfono/fax: 1144808900 int. 8630/ 1136673809
Dirección postal: Florencio Varela 1903 (B1754JEC)

Apellido y nombre: Igarza, Aldo Santiago
Organismo(s) de estudio del IRAM para el(los) que ha sido designado: Comité de Informática Forense
Tratamiento (Sra, Sr, Ing, Tco, Lic, Arq, etc): Ing
Nº de CUIL/CUIT (del representante): 20-17645102-6
Correo electrónico: asigarza@unlam.edu.ar
Teléfono/fax: 1144808900 int 8837/ 1150257684
Dirección postal: Florencio Varela 1903 (B1754JEC)

(Por favor, repetir estos datos para cada representante designado. Nº de CUIL/CUIT del representante es un dato obligatorio sin el que no se podrá procesar ninguna Alta, Baja o Modificación)

La representación arriba indicada y los datos suministrados deben considerarse válidos a partir de la fecha de la presente. Todo cambio al respecto, será comunicado a usted por esta misma vía.

Sin otro particular, saludo a usted muy atentamente.

FIRMA y SELLO DE LA ORGANIZACIÓN
(del representante titular ante IRAM o personal superior autorizado para tal fin)

(aclaración de firma y cargo que desempeña en la organización)

Razón social de la organización: *Universidad Nacional de la Matanza*

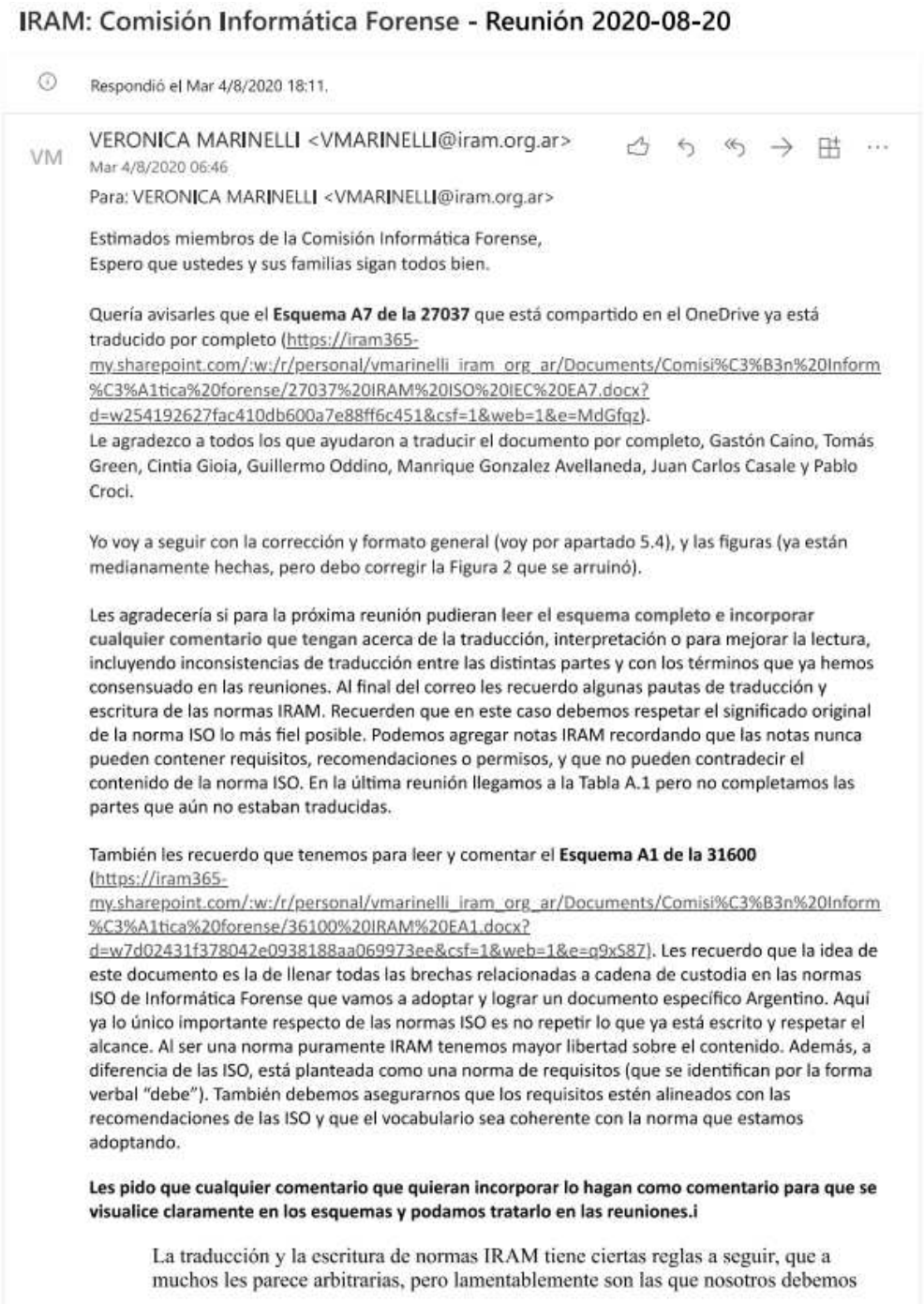
GN FN 017 REV: 02

Nº CUIT de la organización: *30646228685*

Enviar a:	INSTITUTO ARGENTINO DE NORMALIZACIÓN Y CERTIFICACIÓN Por correo : Perú 552 / 556 - (C1068AAB) Buenos Aires Por fax : 011 - 4346 - 0601 Por correo electrónico: secretariaonm@iram.org.ar

DN-FN 017 REV: 02

8. Mail con Avances de Comisión Informática Forense en 2020 y participación de UNLAM en traducción de las normas



IRAM: Comisión Informática Forense - Reunión 2020-08-20

Respondió el Mar 4/8/2020 18:11.

VM

VERONICA MARINELLI <VMARINELLI@iram.org.ar>
Mar 4/8/2020 06:46
Para: VERONICA MARINELLI <VMARINELLI@iram.org.ar>

Estimados miembros de la Comisión Informática Forense,
Espero que ustedes y sus familias sigan todos bien.

Quería avisarles que el **Esquema A7 de la 27037** que está compartido en el OneDrive ya está traducido por completo (https://iram365-my.sharepoint.com/:w:/r/personal/vmarinelli_iram_org_ar/Documents/Comisi%C3%B3n%20Inform%C3%A1tica%20forense/27037%20IRAM%20ISO%20IEC%20EA7.docx?d=w254192627fac410db600a7e88ff6c451&csf=1&web=1&e=MdGfqz).
Le agradezco a todos los que ayudaron a traducir el documento por completo, Gastón Caino, Tomás Green, Cintia Gioia, Guillermo Oddino, Manrique Gonzalez Avellaneda, Juan Carlos Casale y Pablo Croci.

Yo voy a seguir con la corrección y formato general (voy por apartado 5.4), y las figuras (ya están medianamente hechas, pero debo corregir la Figura 2 que se arruinó).

Les agradecería si para la próxima reunión pudieran leer el esquema completo e incorporar cualquier comentario que tengan acerca de la traducción, interpretación o para mejorar la lectura, incluyendo inconsistencias de traducción entre las distintas partes y con los términos que ya hemos consensuado en las reuniones. Al final del correo les recuerdo algunas pautas de traducción y escritura de las normas IRAM. Recuerden que en este caso debemos respetar el significado original de la norma ISO lo más fiel posible. Podemos agregar notas IRAM recordando que las notas nunca pueden contener requisitos, recomendaciones o permisos, y que no pueden contradecir el contenido de la norma ISO. En la última reunión llegamos a la Tabla A.1 pero no completamos las partes que aún no estaban traducidas.

También les recuerdo que tenemos para leer y comentar el **Esquema A1 de la 31600** (https://iram365-my.sharepoint.com/:w:/r/personal/vmarinelli_iram_org_ar/Documents/Comisi%C3%B3n%20Inform%C3%A1tica%20forense/36100%20IRAM%20EA1.docx?d=w7d02431f378042e0938188aa069973ee&csf=1&web=1&e=g9xS87). Les recuerdo que la idea de este documento es la de llenar todas las brechas relacionadas a cadena de custodia en las normas ISO de Informática Forense que vamos a adoptar y lograr un documento específico Argentino. Aquí ya lo único importante respecto de las normas ISO es no repetir lo que ya está escrito y respetar el alcance. Al ser una norma puramente IRAM tenemos mayor libertad sobre el contenido. Además, a diferencia de las ISO, está planteada como una norma de requisitos (que se identifican por la forma verbal "debe"). También debemos asegurarnos que los requisitos estén alineados con las recomendaciones de las ISO y que el vocabulario sea coherente con la norma que estamos adoptando.

Les pido que cualquier comentario que quieran incorporar lo hagan como comentario para que se visualice claramente en los esquemas y podamos tratarlo en las reuniones.i

La traducción y la escritura de normas IRAM tiene ciertas reglas a seguir, que a muchos les parece arbitrarias, pero lamentablemente son las que nosotros debemos

9. Información de participación y convenios en curso de Cibercrimen e Informática Forense del COPITEC y MPF Bs As.

Convenio Marco COPITEC

Asunto Nº 23880
Entrada 28 JUN 2013

Buenos Aires, 28 de junio de 2013

Señor
Coordinador Comisiones Internas
Técnico. Juan C. Gamez
S / D

REF: Convenio Universidad de La Matanza-Copitec

La Comisión de Comunicaciones y la de Ejercicio Profesional en la reunión del miércoles 26 de junio recibieron al Ing. Alejandro Pérez, coordinador de la carrera de Ingeniería en la Universidad de la Matanza. Concurrió en representación del rector y por la gestión que realizó el Tco. Claudio Scarveglione para proponer la firma de un convenio marco de Cooperación entre la Universidad y el Consejo.

Presentó el modelo de Convenio Marco que utiliza la Facultad para que lo analicen las autoridades del Consejo, se adjunta el modelo.

Se hablo de la posibilidad de utilizar equipamiento de la Universidad para realizar proyectos con los matriculados (ej. Tema del laboratorio de informática) y la elaboración de un proyecto de ley de Telecomunicaciones.

Quedando a disposición por cualquier consulta, saludamos atentamente,

Ing. Roberto Barneda
Coord. Comisión Ejercicic Profesional

Ing. Roberto González
Coordinador Comisión Comunicaciones

MPF BsAs:

Re: UNLaM - Curso "Cibercrimen e Informática Forense" - MPF Prov Bs As

Hola Cintia. Tomo nota y te cuento que en el primer día de difusión ya tenemos dos interesados.

Ni bien tenga la lista completa la estaré remitiendo.

Francisco Pont Vergés
Secretario de Política Criminal
Coordinación Fiscal e Instrucción Penal
Procuración General ante la SCJBA

El 12/08/2020 18:24, CINTIA GIOIA escribió:

> Estimado Dr. Francisco Pont Verges,
>
> Tal como conversamos telefónicamente quedamos a la espera del listado de personas del Ministerio Público Fiscal de la Provincia de Bs. As. que estén interesadas en realizar el curso. De esta manera podremos corroborar la aplicación del descuento del 10%.
> Agrego en copia en este mail al Decano Jorge Eterovic y el Vicedecano Gabriel Blanco.
> Desde ya muchísimas gracias.
> Nos mantenemos en contacto.
>
> Saludos Cordiales,
>
> Ing. Cintia Gioia
>
> ---
>
> **De:** fpontverges <fpontverges@mpba.gov.ar>
> **Enviado:** sábado, 8 de agosto de 2020 16:00
>
> **Para:** CINTIA GIOIA <cgioia@unlam.edu.ar>
> **Asunto:** Re: UNLaM - Curso "Cibercrimen e Informática Forense" - Fecha Inicio: 25/08/2020
>
> Hola Cintia.
>
> Que alegría saber que finalmente van a concretar este curso!
>
> Me parece muy interesante y atractivo en función del programa, que es muy adecuado para lo que se busca hoy de un investigador informático.
>
> Desde ya me comprometo a difundirlo.
>
> Podemos hablar el lunes sobre acciones para articular entre ustedes y nosotros.

ANEXO IV

1.1. Certificado de Coordinación, dictado y asistencia del Curso de Cibercrimen e Informática Forense 2020 en DIIT UNLAM

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

CIBERCRIMEN E INFORMÁTICA FORENSE

San Justo, Diciembre de 2020

Se certifica que

Cintia Gioia

ha participado como docente del curso *"Cibercrimen e Informática Forense"* Módulos: Investigación del Cibercrimen, Delitos Informáticos, Informática Forense, Investigación Digital, Aspectos Procesales, con una duración total de 30hs., dictado en forma virtual por el Departamento de Ingeniería e Investigaciones Tecnológicas de Esta Casa de Altos Estudios.

Mg. Gabriel Blanco
Vicedecano DIIT

Mg. Jorge Eterovic
Decano DIIT

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

CIBERCRIMEN E INFORMÁTICA FORENSE

San Justo, Diciembre de 2020

Se certifica que

Emiliano Zárate

ha participado como docente del curso *"Cibercrimen e Informática Forense"* Módulos: Investigación del Cibercrimen, Delitos Informáticos, Informática Forense, Investigación Digital, Aspectos Procesales, con una duración total de 30hs., dictado en forma virtual por el Departamento de Ingeniería e Investigaciones Tecnológicas de Esta Casa de Altos Estudios.

Mg. Cintia Gioia
Coordinadora Académica

Mg. Jorge Eterovic
Decano DIIT

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

CIBERCRIMEN E INFORMÁTICA FORENSE

San Justo, Diciembre de 2020

Se certifica que

Sergio Bonavento

DNI: 33.293.881

ha aprobado el curso "*Cibercrimen e Informática Forense*" Módulos: Investigación del Cibercrimen, Delitos Informáticos, Informática Forense, Investigación Digital, Aspectos Procesales, con una duración total de 30hs., dictado en forma virtual por el Departamento de Ingeniería e Investigaciones Tecnológicas de Esta Casa de Altos Estudios.

Mg. Cintia Gioia
Coordinadora Académica

Mg. Jorge Eterovic
Decano DIIT

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

CIBERCRIMEN E INFORMÁTICA FORENSE

San Justo, Diciembre de 2020

Se certifica que

Fernando Saldaña

DNI: 38.346.178

ha aprobado el curso "*Cibercrimen e Informática Forense*" Módulos: Investigación del Cibercrimen, Delitos Informáticos, Informática Forense, Investigación Digital, Aspectos Procesales, con una duración total de 30hs., dictado en forma virtual por el Departamento de Ingeniería e Investigaciones Tecnológicas de Esta Casa de Altos Estudios.

Mg. Cintia Gioia
Coordinadora Académica

Mg. Jorge Eterovic
Decano DIIT

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

CIBERCRIMEN E INFORMÁTICA FORENSE

San Justo, Diciembre de 2020

Se certifica que

Mario Juan Krajnik

DNI: 17.037.268

ha aprobado el curso *"Cibercrimen e Informática Forense"* Módulos: Investigación del Cibercrimen, Delitos Informáticos, Informática Forense, Investigación Digital, Aspectos Procesales, con una duración total de 30hs., dictado en forma virtual por el Departamento de Ingeniería e Investigaciones Tecnológicas de Esta Casa de Altos Estudios.

Mg. Cintia Gioia
Coordinadora Académica

Mg. Jorge Eterovic
Decano DIIT

1.2. Certificado de Coordinación, dictado y asistencia del Curso de Análisis de Cibercriminalidad Económica Financiera 2021 en DIIT UNLAM

Código	FPI-009
Objeto	Guía de elaboración de Informe de avance de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

SEU Secretaría de Extensión Universitaria

ANÁLISIS DE CIBERCRIMINALIDAD ECONÓMICA FINANCIERA

San Justo, Septiembre de 2021

Se certifica que

Cintia Gioia

25.385.204

ha participado como Coordinadora del curso *"Análisis de Cibercriminalidad Económica Financiera. Módulos: Introducción al Cibercrimen Económico-Financiero, Prácticas del Analista Digital, Análisis de Ciberdelitos Financieros, Análisis de Ciberdelitos Económicos"*, con una duración total de 24 hs., dictado en forma virtual por el Departamento de Ingeniería e Investigaciones Tecnológicas de esta Casa de Altos Estudios.

Mg. Gabriel Blanco
Vicedecano del DIIT

Mg. Jorge Eterovic
Decano del DIIT

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

SEU Secretaría de Extensión Universitaria

ANÁLISIS DE CIBERCRIMINALIDAD ECONÓMICA FINANCIERA

San Justo, Septiembre de 2021

Se certifica que

Emiliano Alejandro Zárate

32.814.318

ha participado como Docente del curso *"Análisis de Cibercriminalidad Económica Financiera. Módulos: Introducción al Cibercrimen Económico-Financiero, Prácticas del Analista Digital, Análisis de Ciberdelitos Financieros, Análisis de Ciberdelitos Económicos"*, con una duración total de 24 hs., dictado en forma virtual por el Departamento de Ingeniería e Investigaciones Tecnológicas de esta Casa de Altos Estudios.

Mg. Cintia Gioia
Coordinadora Académica

Mg. Jorge Eterovic
Decano del DIIT

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

SEU Secretaría de Extensión Universitaria

ANÁLISIS DE CIBERCRIMINALIDAD ECONÓMICA FINANCIERA

San Justo, Septiembre de 2021

Se certifica que

Mario Juan Krajnik

17.036.268

ha aprobado el curso *"Análisis de Cibercriminalidad Económica Financiera. Módulos: Introducción al Cibercrimen Económico-Financiero, Prácticas del Analista Digital, Análisis de Ciberdelitos Financieros, Análisis de Ciberdelitos Económicos"*, con una duración total de 24 hs., dictado en forma virtual por el Departamento de Ingeniería e Investigaciones Tecnológicas de esta Casa de Altos Estudios.

Mg. Cintia Gioia
Coordinadora Académica

Mg. Jorge Eterovic
Decano del DIIT

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

SEU Secretaría de Extensión Universitaria

ANÁLISIS DE CIBERCRIMINALIDAD ECONÓMICA FINANCIERA

San Justo, Septiembre de 2021

Se certifica que

Sergio Bonavento

33.293.881

ha aprobado el curso *"Análisis de Cibercriminalidad Económica Financiera. Módulos: Introducción al Cibercrimen Económico-Financiero, Prácticas del Analista Digital, Análisis de Ciberdelitos Financieros, Análisis de Ciberdelitos Económicos"*, con una duración total de 24 hs., dictado en forma virtual por el Departamento de Ingeniería e Investigaciones Tecnológicas de esta Casa de Altos Estudios.

Mg. Cintia Gioia
Coordinadora Académica

Mg. Jorge Eterovic
Decano del DIIT

1.3. Certificado de Coordinación, dictado y asistencia del Curso de Cibercrimen e Informática Forense 2020 en DIIT UNLAM

Esta **certificado** ha sido registrado en la Secretaría de Extensión Universitaria de la UNLM, bajo **N°138.273 hoja 116 del libro de registros N° 16.**
San Justo, 28 de marzo de 2022..

La Universidad Nacional de La Matanza certifica que,

CINTIA VERÓNICA GIOIA, DNI 27.25.385.204

ha participado como docente para el Curso de **Cibercrimen e Informática Forense -**

Módulos: **Investigación del Cibercrimen | Fundamentos del Delito Informático | Informática Forense |**

Aspectos Procesales | Investigación Digital,

cuyo dictado estuvo a cargo del Departamento de Ingeniería e Investigaciones Tecnológicas

en conjunto con la Secretaría de Extensión Universitaria.

Dicho curso - que se realizó en forma Virtual - tuvo lugar del 19 de octubre al 30 de noviembre del corriente año,

con una carga horaria de 30 horas.

Se extiende el presente certificado en San Justo, al 07 de marzo de 2022.

LIC. ROBERTO AYUB
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

MG. JORGE ETEROVIC
DECANO DEPARTAMENTO DE INGENIERÍA E INVESTIGACIONES TECNOLÓGICAS

socio culturales · SEU Secretaría de Extensión Universitaria · DIIT · UNLaM

Esta **certificado** ha sido registrado en la Secretaría de Extensión Universitaria de la UNLM, bajo **N°138.268 hoja 116 del libro de registros N° 16**.
San Justo, 28 de marzo de 2022..

La Universidad Nacional de La Matanza certifica que,

EMILIANO ALEJANDRO ZÁRATE, DNI 32.814.318

ha participado como docente para el Curso de **Cibercrimen e Informática Forense -**

Módulos: **Investigación del Cibercrimen | Fundamentos del Delito Informático | Informática Forense |**

Aspectos Procesales | Investigación Digital,

cuyo dictado estuvo a cargo del Departamento de Ingeniería e Investigaciones Tecnológicas

en conjunto con la Secretaría de Extensión Universitaria.

Dicho curso - que se realizó en forma Virtual - tuvo lugar del 19 de octubre al 30 de noviembre del corriente año,

con una carga horaria de 30 horas.

Se extiende el presente certificado en San Justo, al 07 de marzo de 2022.

MG. CINTIA GIOIA
COORDINADORA ACADÉMICA

LIC. ROBERTO AYUB
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

MG. JORGE ETEROVIC
DECANO DEPARTAMENTO DE INGENIERÍA E INVESTIGACIONES TECNOLÓGICAS

socio culturales · SEU Secretaría de Extensión Universitaria · DIIT · UNLaM

2.1. Docente en Diplomado de Posgrado en Violencia de Género - Universidad de Hartmann (México)

UNIVERSIDAD HARTMANN – RECONSTRUCCIÓN FORENSE ESPECIALIZADA

Buenos Aires, 20 de diciembre de 2021

DIPLOMADO DE POSGRADO EN VIOLENCIA DE GÉNERO

Por la presente y ante quien corresponda, hago extensiva esta constancia de **DOCENTE** para la **ING. CINTIA VERÓNICA GIOIA**, que se desempeñó como docente a cargo de ***2 clases - Clase 7: Evidencia y acoso en línea. Puntos periciales en casos de violencia de género.*** Y ***Clase 8: Análisis forense sobre dispositivos de almacenamiento masivo. Búsqueda de información específica. – en el DIPLOMADO DE POSGRADO EN VIOLENCIA DE GÉNERO*** dictado de forma online a cargo de la Universidad Hartmann de México (RVOE/SEG/025/2013) y Reconstrucción Forense Especializada de Argentina (Personería Jurídica Nro. 185 "A"/18) quienes acreditan ***3 horas cátedras***.

Se extiende dicha constancia a los 20 días del mes de diciembre del año 2021.

Federico Baudino
Director Académico
Reconstrucción Forense Especializada

2.2. Docente en Ciclo de Talleres de Women Of Security capítulo de Panamá. Webinar: Modalidades Delictivas contra NNA en medios digitales (2021)

CERTIFICADO DE PARTICIPACIÓN

Concierne a:

Mg. Ing. Cintia Verónica Gioia

Por su participación como expositora en el webinar de agosto
"Modalidades Delictivas contra niñas, niños y adolescentes en medios digitales"

Celebrado en la ciudad de Panamá a los 31 días del mes de agosto del 2021.

Otorgado por:
Women Of Secuirty (WoSEC) Capítulo de Panamá

WOMEN OF SECURITY

CAPÍTULO DE PANAMÁ

Panamá, 01 de septiembre del 2021

Carta de agradecimiento

A nombre de Women Of Security capítulo de Panamá, por medio de la presente carta, queremos agradecer por todo el apoyo a la Mg. Ing. Cintia Verónica Gioia y la Universidad Nacional de la Matanza (Argentina), por haber creído en nuestra misión de fomentar el crecimiento profesional a mujeres en el área de ciberseguridad, mediante el tema "Modalidades Delictivas contra niñas, niños y adolescentes en medios digitales", impartido el 31 de agosto del 2021 .

Estamos convencidas de que el tiempo, soporte y conocimiento brindado será de gran aprovechamiento por cada una de las miembros y participantes que estuvieron presentes en la exposición.

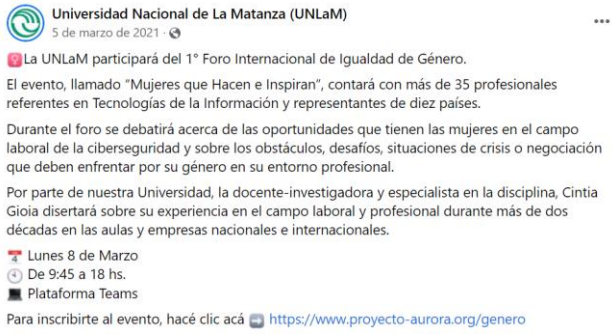
Esperamos de igual forma seguir contando con su presencia para futuros talleres, charlas o proyectos.

Atentamente,

Staycy Guevara
Communicator Officer - WoSEC Panamá
info@wosecpanama.com

www.womenofsecurity.com

2.3 Flyer 1º Foro Internacional de Igualdad de Género. Mujeres que hacen e inspiran en Ciberseguridad y en Tecnologías, organizado por Proyecto Aurora ONG.



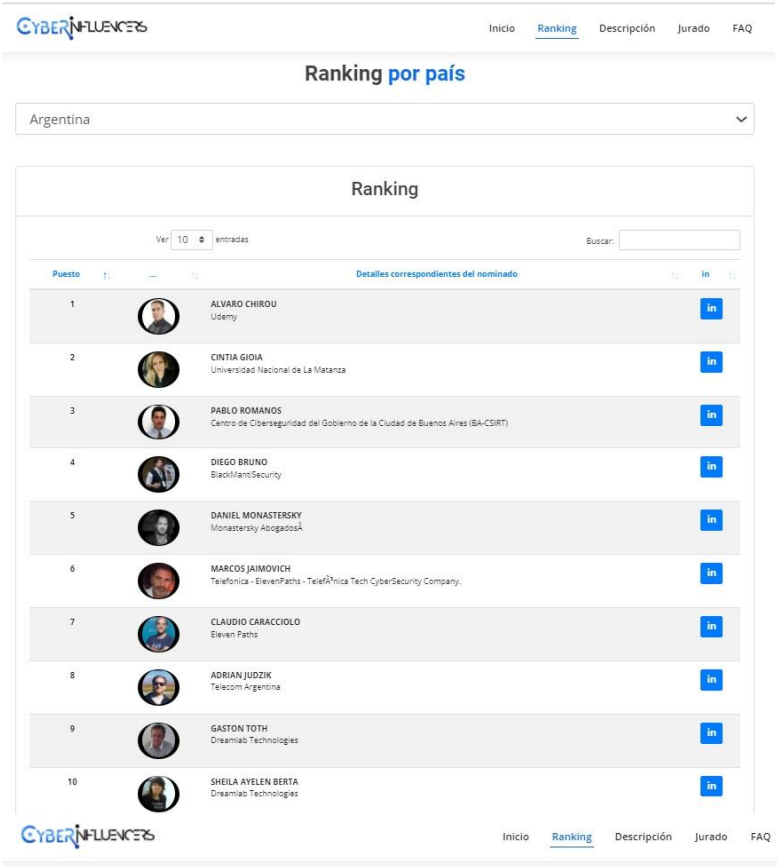
3.1. Exposición a cargo de Mg. Ing. Cintia V. Gioia en "The Global Women in Security Alliance 2020 Virtual Series". ASIS International.

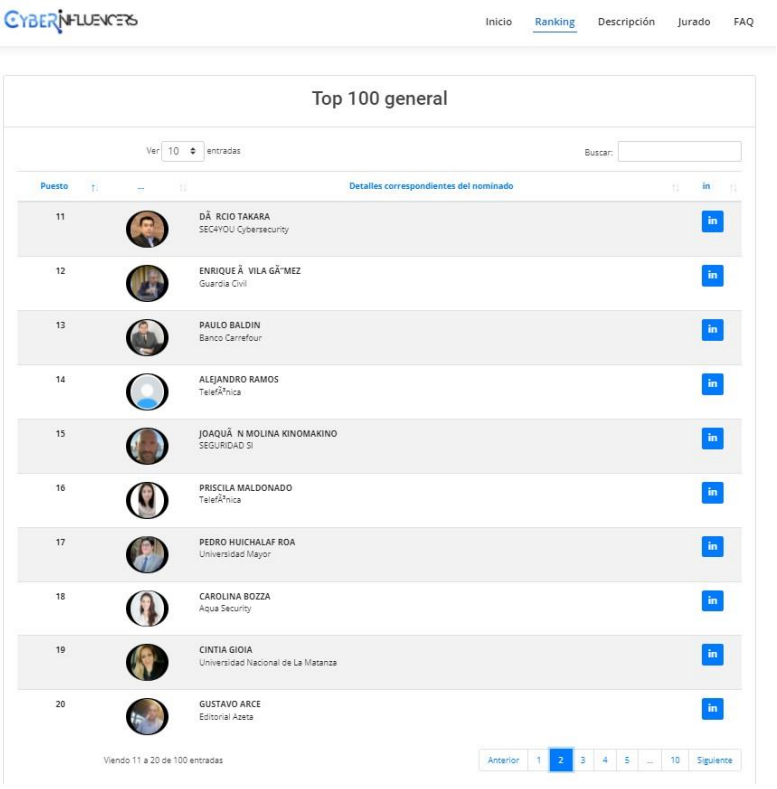
3.2. Flyer Webinar "Elaboración de Planes de Prevención de Seguridad de la Información en redes sociales y para el trabajo remoto". ASIS International.

3.6. Flyer Seminario "Modalidades de Violencia de Género Digital" en seminario organizado por Proyecto Aurora ONG.

3.7. Flyer Seminario "Sin Violencia Digital" organizado por Academia Mexicana de Ciberseguridad y Derecho Digital AMCID.

4.1 2º puesto Nacional y puesto 19º Internacional en el ranking de líderes en ciberseguridad de Iberoamérica “Ciberinfluencers”.





DIIT UNLaM
La votación cierra el 9/12, todavía estás a tiempo de dar tu voto!

Mg. Cintia Gioia, Coordinadora de las Tecnicaturas Web y Móviles, ha sido nominada, en representación de Argentina y de la UNLaM, en el Ranking de CiberInfluencers de Líderes en Ciberseguridad en Iberoamérica.

El ganador recibirá premios para la institución a la que pertenece.

Ayudanos votando en:
https://cyberheroes.app/ciberinfluencers/#nominar

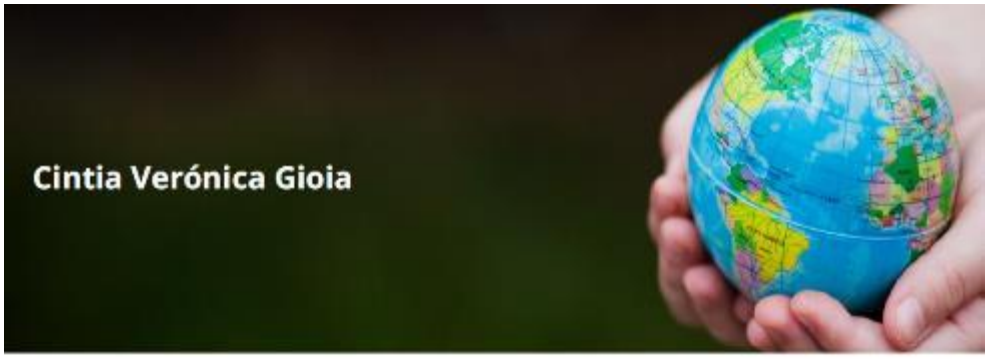
#ciberseguridad #diitunlam

Fotos de la biografía · 4 dic. 2020 ·

5.1 Certificado de Asistencia a Capacitación de “Cibercrimen de la A a la Z”

5.2. Certificado de Asistencia a 1er Seminario Internacional de Cibercrimen

5.3. Certificado de Participación en Curso Internacional en Abuso y Explotación Sexual Infantil en Línea (2020). ICMEC en conjunto con UNODC.



Se hace acreedor del presente certificado de participación por haber completado con éxito el curso de formación básica de 12 sesiones
"Abuso y explotación sexual infantil en línea: una perspectiva integral"
celebrado del 24 de septiembre al 10 de diciembre de 2020

BOB CUNNINGHAM
Chief Executive Officer
International Centre

NAYELLY LOYA MARIN
Head of the Global Programme on Cybercrime
UNODC

5.4 Certificado de Asistencia a Ciclo de "Búsqueda de Personas Desaparecidas y Extraviadas e Identificación de Personas con identidad Desconocida"

Ministerio de Seguridad Argentina

Subsecretaría de Investigación Criminal y Cooperación Judicial

SIFEBU

Mg. Ing. Cintia Verónica Gioia

ha participado como Asistente en el Ciclo **"Búsqueda de personas desaparecidas y extraviadas e identificación de personas con identidad desconocida"**, organizado por el **Sistema Federal de Búsqueda de Personas Desaparecidas y Extraviadas (SIFEBU)**, de la **Subsecretaría de Investigación Criminal y Cooperación Judicial del Ministerio de Seguridad de la Nación**, y realizado en modalidad virtual durante los días 26 de noviembre y 3, 10 y 17 de diciembre del año 2020.

Lic. Valentina María NOVICK
Subsecretaria de Investigación Criminal y Cooperación Judicial

5.5 Certificado de Asistencia al 12vo. Congreso COLTIC 2021 de "Innovación para la investigación del delito en la nueva realidad".

COLTIC 2021

CERTIFICADO DE ASISTENCIA

Por cuanto

CINTIA GIOIA

Ha participado de COLTIC 2021, *Innovación para la investigación del delito en la nueva realidad*, los días 6 y 7 de Octubre.

MANUEL DE CAMPOS
PRESIDENTE

FERNANDO CARDINI
VICEPRESIDENTE

JIMENA JATIP
COORDINADORA EJECUTIVA

5.6. Capacitación de actualización para integrantes del proyecto

EDUCACIÓN IT

Certificado de Aprobación

Cintia, Gioia

Ha completado y aprobado el curso:
Cibercrimen y Evidencia Digital

Duración:
14hs

Lorena Sommer
Coordinadora Académica

08/12/21
Fecha

EDUCACIÓN IT

Certificado de Aprobación

Cintia, Gioia

Ha completado y aprobado el curso:
Informática Forense

Duración:
15hs

Lorena Sommer
Coordinadora Académica

21/12/21
Fecha

5.7 5ta Info-Conf 2021 Conferencia Nacional de Informática Forense

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Puntos de vistas de Jueces y Fiscales de CABA, en referencia a Cibercrimenes y Ciberdelitos"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Consideraciones para el Análisis Forense en ambientes Industriales"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Preconstitución de pruebas en el entorno digital"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Los desafíos de la evidencia digital en las investigaciones de fraude corporativo"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Normalización en informática forense y la IRAM-ISO/IEC 27037"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"La seguridad tecnológica de las empresas proveedoras de servicios en Internet como prevención situacional del ciberdelito"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Forensia Digital, Imágenes Digitales e Inteligencia Artificial"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Evolución de las Investigaciones Forenses Digitales en América LATINA"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Ciberseguridad en la industria"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Baseline metodológico para la difícil recolección de datos en dispositivos móviles. Visión desde la comunidad de expertos de la ASIIF"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Evidencia digital: nuevos desafíos para la cooperación internacional"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Aplicación del Convenio de Budapest : adecuación a la regulación"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Cibercrimen y Pandemia"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Ciberinteligencia como elemento proactivo en Ciberseguridad"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Desarrollo Guía para abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Investigaciones digitales dentro del proceso de respuesta a incidentes en el sector privado: Casos reales"

Se extiende el presente CERTIFICADO a ***Mario Juan KRAJNIK*** *por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Los imperativos legales estratégicos en Ciberseguridad, Ciberdefensa y Soberanía de Datos"

*Se extiende el presente CERTIFICADO a **Mario Juan KRAJNIK** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Gestión del Estado ante los incidentes de seguridad informática. ¿Es posible mejorar desde las políticas?"

*Se extiende el presente CERTIFICADO a **Mario Juan KRAJNIK** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Propuesta de una Metodología para la Forensia de IoT"

*Se extiende el presente CERTIFICADO a **Mario Juan KRAJNIK** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Puntos de vistas de Jueces y Fiscales de CABA, en referencia a Cibercrimenes y Ciberdelitos"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Consideraciones para el Análisis Forense en ambientes Industriales"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Preconstitución de pruebas en el entorno digital"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Los desafíos de la evidencia digital en las investigaciones de fraude corporativo"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Normalización en informática forense y la IRAM-ISO/IEC 27037"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"La seguridad tecnológica de las empresas proveedoras de servicios en Internet como prevención situacional del ciberdelito"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Forensia Digital, Imágenes Digitales e Inteligencia Artificial"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Evolución de las Investigaciones Forenses Digitales en América LATINA"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Ciberseguridad en la industria"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Esteganografía y CTF"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Baseline metodológico para la difícil recolección de datos en dispositivos móviles. Visión desde la comunidad de expertos de la ASIIF"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 23 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Evidencia digital: nuevos desafíos para la cooperación internacional"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Aplicación del Convenio de Budapest : adecuación a la regulación"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Cibercrimen y Pandemia"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Ciberinteligencia como elemento proactivo en Ciberseguridad"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Desarrollo Guía para abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Investigaciones digitales dentro del proceso de respuesta a incidentes en el sector privado: Casos reales"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Blockchain Forensic"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Primeros pasos forenses para analizar infección de Ransomware"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Los imperativos legales estratégicos en Ciberseguridad, Ciberdefensa y Soberanía de Datos"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO

FIE

Facultad de Ingeniería del Ejército "Grl Div Manuel Nicolás Savio"
Universidad de la Defensa Nacional

5ta Info-Conf Conferencia Nacional de Informática Forense
"Gestión del Estado ante los incidentes de seguridad informática. ¿Es posible mejorar desde las políticas?"

*Se extiende el presente CERTIFICADO a **Cintia GIOIA** por participar vía streaming de la mencionada jornada, realizada el día 24 de septiembre de 2021.*

Ciudad Autónoma de Buenos Aires, Octubre de 2021

Licenciado RICARDO FERNANDO PEÑA
SECRETARIO DE EXTENSIÓN UNIVERSITARIA

Coronel ALBERTO RICARDO NADALE
DIRECTOR FACULTAD DE INGENIERÍA DEL EJÉRCITO