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

Departamento: de Ingeniería e Investigaciones Tecnológicas

Programa de acreditación:
CyTMA2

Programa de Investigación[1]:

Código del Proyecto: C2-ING-054

Título del proyecto
Análisis del Marco Normativo Técnico Legal del Ciclo de Vida de la Evidencia Digital

PIDC: ☐
Elija un elemento.

PII: ☐
Elija un elemento.

Director: *Ing. Igarza, Aldo Santiago*

Director externo:

Codirector: *Mg. Ing. Gioia, Cintia Verónica*

Integrantes:
Mg. Eterovic Jorge Esteban, Mg. Ureta Walter, Ing. Krajnik Mario Juan, Dr. González Allonca Juan Cruz, Dr. Conde Sergio

Investigador Externo, Asesor- Especialista, Graduado UNLaM:

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

Alumnos de posgrado:

Resolución Rectoral de acreditación: N° 102/2019

Fecha de inicio: *01-01-2018*

Fecha de finalización: *31/12/2019*

[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)

En relación con el **Marco Legal Nacional**, se avanzó sobre la investigación y análisis de las diferentes legislaciones nacionales vinculadas a delitos informáticos y todos los aspectos técnicos legales que involucran a la informática forense y la actuación de los peritos informáticos. En este punto se realizó un análisis del estado actual de la legislación nacional, los desafíos del debido proceso penal en un contexto de creciente criminalidad, la responsabilidad penal de las personas jurídicas en la delincuencia informática, la pericia en el juicio oral acusatorio y por jurados, entre otros temas relacionados.

Se realizó una investigación del **Marco Legal Internacional**, sobre el estado actual y avances en relación con el Convenio de Budapest y la Cibercriminalidad, considerando las diferentes consecuencias de la aplicación del Convenio a nivel Nacional.

Se avanzó sobre la investigación de la **aplicación de computación forense en la nube**, su aplicación a nivel nacional, legislación vinculada y los proyectos que involucran alojamiento de datos en el Exterior, considerando las limitaciones de la jurídico legales actuales. A partir de la investigación del Marco Legal Nacional, Internacional y la aplicación de computación forense en la nube se desarrolló un informe base para la publicación del paper "**Análisis del Marco Normativo de la Protección de los Datos Personales a Aplicarse en la Argentina en Proyectos de Cloud Computing Implementados en el Exterior del País**" en la 3er Conferencia Nacional de Informática Forense INFOCONF 2019.

Sobre la investigación a aplicarse sobre **normas estándares internacionales relacionados con el tratamiento de la evidencia digital** se logró un importante avance. Previo a disponer de las normas IRAM relacionadas, se realizó un trabajo de investigación a partir de informes o publicaciones de otros grupos de investigación, de expertos y de entidades y de información recabada en Congresos, Jornadas y Capacitaciones a lo largo del año. En 2019 la Codirectora del proyectos Mg. Ing. Cintia V. Gioia fue convocada por IRAM (en representación de UNLaM) para formar parte de la **Comisión de Informática Forense Nacional de IRAM,** para lo cual se pudo disponer de las normas internacionales completas para su lectura y análisis. Cabe aclarar que de la lista inicial de normas ISO que se plantearon analizar en el proyecto de investigación, se enfocó la investigación en las que IRAM tomó como base de conocimiento para la aplicación de las mismas a nivel nacional, conformadas las normas ISO 27.037:2012, ISO 27.041:2015, ISO 27.042:2015, ISO 27.043:2015, ISO 27.050-1:2016, ISO 27.050-2:2018 e ISO 27.050-3:2017. En relación con la norma ISO/IEC 17025:2017, "Requisitos generales para la competencia de los laboratorios de prueba y calibración", la misma quedó fuera del alcance ya que se redefinió focalizarse en las normas que se estaban trabajando en la Comisión de Informática Forense de IRAM, reemplazando la misma por el estudio y análisis de la norma ISO 27.050-2:2018, ISO 27.050-3:2017. En esta Comisión se seguirá trabajando durante el año 2020 también.

En relación con los **Procesos y Buenas Prácticas** se estudió en detalle el proceso PURI "Proceso Unificado de Recuperación de Información", la "Guía Integral de Empleo de la Informática Forense en el Proceso Penal" y el Proyecto PAIF-PURI "Protocolo de Actuación en Informática Forense" desarrollados por el equipo de investigación de la Universidad FASTA a través de su Laboratorio de Informática Forense Info-Lab. En este punto también se investigó el "Protocolo unificado de los Ministerios Públicos de la República Argentina. Guía para el levantamiento y conservación de la Evidencia" del Programa nacional de Criminalística del Ministerio de Justicia y Derechos Humanos en conjunto con el Consejo Federal de Política Criminal y el Consejo de Procuradores, Fiscales, Defensores y Asesores Generales de Argentina. Al ser desde el 2019 convocada UNLAM a formar parte de la **REDUNIF** (Red de Informática Forense Nacional) se facilitó el acceso a la información mencionada y se pudo realizar una investigación detallada al respecto.

Se llevaron a cabo diversas **investigaciones de temáticas específicas** de manejo de la evidencia digital. Se adelantó sobre la investigación de los distintos **protocolos** de obtención, preservación y tratamiento de evidencia digital que se aplican en nuestro país.

Se desarrolló una investigación detallada y comparativa de las herramientas de informática forenses necesarias para la conformación de un **Laboratorio Informático Forense**. Dicha investigación se basó en **relevamientos realizados a fuerzas de la ley, policiales, fiscalías y cuerpo de investigaciones judiciales como también a expertos peritos referentes**, analizando las herramientas que utilizaban o necesitarían utilizar y como debería conformarse tecnológicamente un laboratorio informático forense que pueda brindar servicios de pericias a dichos organismos o particulares. Los informes realizados al respecto son:

- Informe de **Estrategia para la implementación de un Laboratorio Informático Forense.**
- Informe **detallado y comparativo de Herramientas de Informática Forense**, tanto software como hardware, aplicables para realizar pericias sobre dispositivos de almacenamiento masivo y/o móviles. De las mismas se investigaron las características funcionales, proveedores locales, precios, opciones de licenciamiento, ventajas, desventajas, etc.
- **Propuesta de implementación de Laboratorio Informático Forense**, justificando la elección de herramientas que lo conformarían. Se validó dicha propuesta con expertos referentes en pericias informáticas de fuerzas de la ley y particulares.

Se logró realizar un **Análisis Comparativo Integrador** basado en la comparación de los diferentes modelos, procesos, fases y componentes del ciclo de vida de la evidencia digital investigados. A partir de dicho análisis se lograron definir las **Buenas Prácticas esenciales para el tratamiento de la Evidencia Digital** a aplicar en cada una de las etapas del tratamiento de la evidencia digital (se decidió avanzar más sobre estos puntos que sobre la implementación de Laboratorio Informático Forense en sí).

Como resultado final del proyecto se logró alcanzar un objetivo adicional y realmente muy importante, que fue la definición de una **propia Metodología informática forense aplicable a cualquier tipo de evidencia digital**, la cual se denominó **UDE (Universal Digital Evidence)**, en la cual se logró aplicar y reflejar todos los conocimientos y experiencia logrados con el desarrollo del proyecto de investigación.

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	*Igarza, Santiago; Gioia, Cintia; Eterovic, Jorge*
Título	*Análisis del Marco Normativo Técnico Legal del Ciclo de Vida de la Evidencia Digital*
Año	*2018*
Evento	*XX Workshop de Investigadores en Ciencias de la Computación*
Lugar de realización	*Corrientes, Argentina*
Fecha de presentación de la ponencia	*Poster. 26 y 27 de abril 2018*
Entidad que organiza	*Red de Universidades con Carreras en Informática (RedUNCI)*
URL de descarga del trabajo (especificar solo si es la descarga del trabajo; formatos pdf, e-pub, etc.)	*http://sedici.unlp.edu.ar/handle/10915/68349*

B.4.2.	
Autores	*Juan González Allonca, Cintia Gioia, Jorge Eterovic, Mario Krajnik, Walter Ureta, Sergio Conde, Sergio Bonavento, Santiago Igarza*
Título	*Análisis del Marco Normativo de la Protección de los Datos Personales a Aplicarse en la Argentina en Proyectos de Cloud Computing Implementados en el Exterior del País*
Año	*2018*
Evento	*3era Conferencia Nacional de Informática Forense*
Lugar de realización	*Universidad Nacional de Córdoba (UNC), Córdoba, Argentina*
Fecha de presentación de la ponencia	*6 de junio de 2019*
Entidad que organiza	*Red Universitaria de Informática Forense (RED UNIF).*
URL de descarga del trabajo (especificar solo si es la descarga del trabajo; formatos pdf, e-pub, etc.)	*ISBN: 978-950-33-1553-8.*

B.5. Otras publicaciones

Autores	*Cintia Gioia*
Año	*2019*
Título	*"Comunidad pedófila: el horror tiene más de un sitio en la web".*
Medio de Publicación	*El Observador. Diario Perfil.*

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

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

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
Jorge Eterovic	*Cintia V. Gioia*	*UNLAM*	*10 (diez)*	*9/12/2019*	*Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos*

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*	*1/1/2018-31/12/2019*	*Investigación de Protocolos de obtención, preservación y tratamiento de evidencia digital. Entrevistas a referentes del Poder Judicial sobre procesos, procedimientos, protocolos, buenas prácticas, equipos de trabajo y tecnologías utilizadas.*

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

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.

Gracias a la participación y presencia del equipo de investigación en Congresos, Jornadas, Capacitaciones Nacionales e Internacionales, a los avances en la investigación y la organización de jornadas en UNLaM, la UNLaM fue convocada a integrar la red REDUNIF. De esta forma **UNLAM integra REDUNIF desde junio de 2019** con la representación de la Mg. Cintia V. Gioia.

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.** 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 avanzó sobre 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.

La codirectora Mg. Ing. Cintia V. Gioia fue convocada por **IRAM** para formar parte de la **Comisión de Informática Forense a partir de marzo de 2019, en representación de UNLaM**. Dicha convocatoria y participación fue de gran aporte para el proyecto ya que se estuvo trabajando directamente con el organismo que analizó 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. La objetivo de la misma es tomar como base de conocimiento la información emergente internacional y formar la propia norma nacional, con el fin de no dañar al ciudadano argentino. Las normas sobre las que trabajó la Comisión en 2019 formaban parte del marco normativo a investigar dentro de los ítems de investigación del proyecto de investigación. El ser parte de la Comisión de Informática Forense de IRAM brindó 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 compartió y analizó 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

[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.

A partir de las becas otorgadas por la **OEA (Organización de Estados Americanos)** a la Mg. Ing. Cintia V. Gioia para participar en el **"Simposio de Ciberseguridad de la OEA 2018"** y el **"OEA Cyberwoman Challenge"** en Washington DC, Estados Unidos del 24 al 28 de Septiembre de 2018 y en el "**Simposio de Ciberseguridad de la OEA 2019**" en Santiago de Chile del 24 al 27de Septiembre de 2018, se espera afianzar el vínculo con el **Programa de Ciberseguridad de la OEA**, en particular con los grupos de expertos 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.

Se realizaron relevamientos a **fuerzas de la ley, policiales y cuerpo de investigaciones judiciales** como también a expertos peritos referentes, con los cuales se mantuvieron reuniones específicas y se han compartido espacio de capacitación y actualización conjunta.

Se validó la información analizada y estudiada con **profesionales expertos tanto del área Legal como Informática**, como también especialistas en Criminalística.

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

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

Asistencia continua a Congresos, Jornadas, Capacitaciones organizados por las diferentes Fuerzas de Seguridad, Poder Judicial, Ministerio de Justicia, Ministerio de Seguridad, Fiscalías, Ministerio Público Fiscal de la Provincia de Buenos Aires, Organizaciones específicas, Universidades, Proveedores, Peritos Expertos, ONG, etc. de manera de obtener una visión integral y real desde el punto de vista y enfoque de cada uno de los actores involucrados (Policial – Justicia – Peritos informáticos).
Se organizó como actividad de apoyo y difusión y capacitación de peritos informáticos la **Jornada "Cibercrimen y los Rastros Digitales: Desafíos en la Investigación del Cibercrimen y la Práctica Forense Informática**" el 22 de octubre de 2018 en el Aula Magna de **UNLAM**. En la misma se resaltó la importancia del trabajo multidisciplinario entre abogados e informáticos para enfrentar los delitos informáticos, los desafíos del tratamiento de la evidencia digital y la investigación en medios tecnológicos como medios para recopilar información que permita resolver crímenes. **Se contó con 130 asistentes estudiantes, egresados y docentes de las carreras de Informática y Abogacía.** La Jornada contó con la participación especial de Francisco Pont Verges, Secretario de Política Criminal de la Procuración General de la SCJB, quien junto con la abogada María Laura Giménez de la Fiscalía de Delitos contra trata de personas, pornografía infantil y Grooming de La Matanza, expusieron sobre las experiencias y el rol del Ministerio Público Fiscal de la Provincia de Buenos Aires en la investigación criminal en entornos digitales. También se contó con la participación de expositores y peritos referentes de la Dirección General de Prevención e **Investigación de Delitos Tecnológicos, de la** Policía de la Ciudad, del Cuerpo de Investigaciones de Judiciales (CIJ) de CABA, del Poder Judicial de la Nación y Peritos de Parte, como también de las mamás fundadoras de la ONG Mamá en Línea.

En base al avance de las investigaciones realizadas, la bibliografía adquirida y el material e información obtenida en Congresos, Jornadas y capacitaciones, se generó **nuevo material de estudio teórico práctico de informática forense aplicable a la materia de "Auditoria y Seguridad Informática"** de la carrera de Ingeniería en Informática y las materias **"Seguridad y Calidad en Aplicaciones Web" y "Calidad en Aplicaciones Móviles"** de las Tecnicaturas Universitarias en Desarrollo Web y para Dispositivos Móviles respectivamente, el cual se empezó a utilizar en parte a partir del primer cuatrimestre del 2019 y como también la generación de nuevo material para el año 2020.

Se adjunta detalle y certificados del punto G en el Anexo I 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.
- Anexo III: Alta patrimonial de los bienes adquiridos con presupuesto del proyecto (FPI 017)
- Nota justificando baja de integrantes del equipo de investigación.

_____

Firma y aclaración
del director del proyecto.

Lugar y fecha :……..

- Presentar una copia impresa firmada del presente documento junto con los Anexos, y enviar todo en archivo PDF por correo electrónico a la Secretaría de Investigación Departamental. **Límite de entrega: 28 de febrero de 2020**

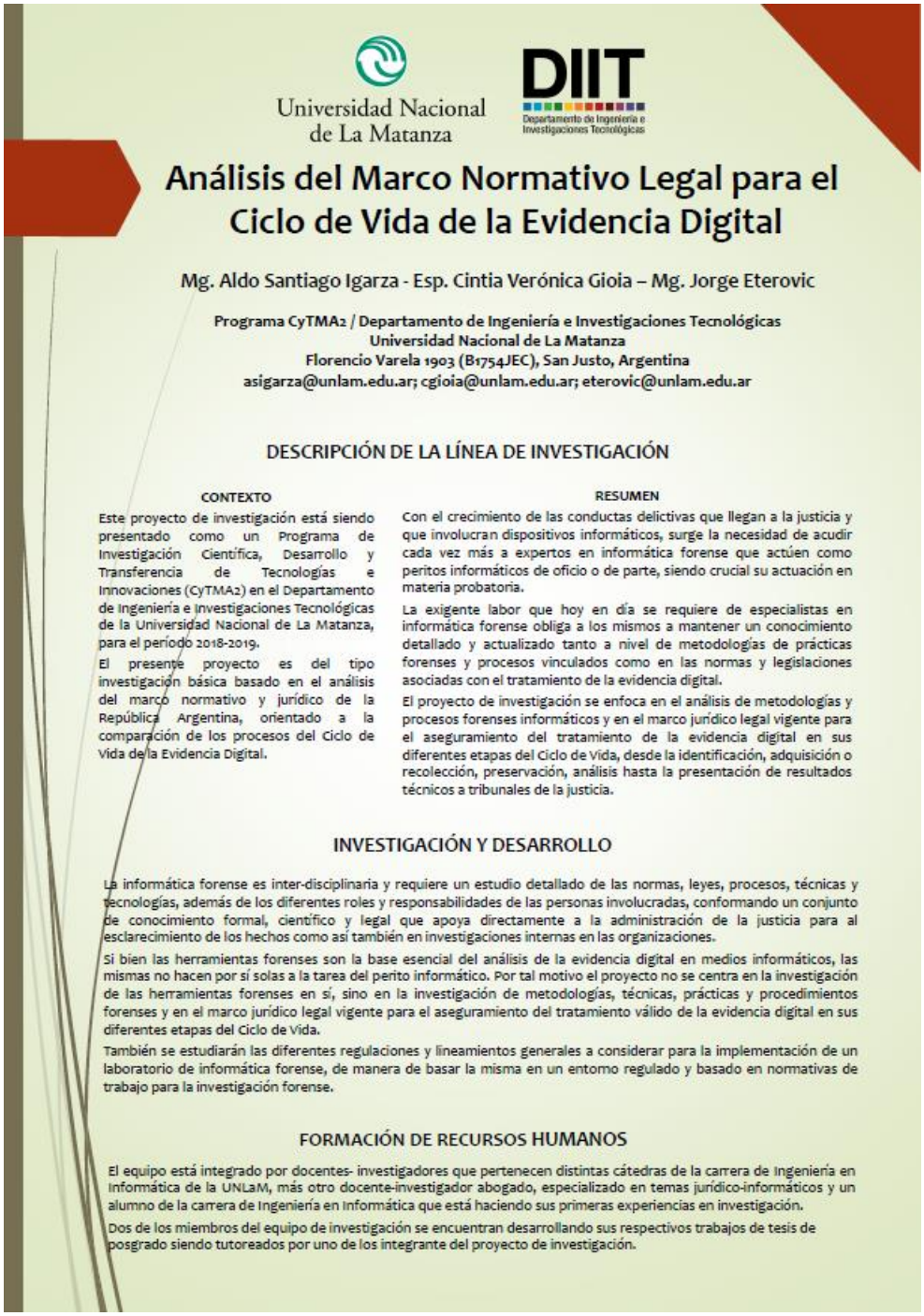
[4] En caso de libros, podrá presentarse una fotocopia de la primera hoja significativa o su equivalente y el índice.

ANEXO I

Trabajos presentados en Congresos y/o Seminarios (B.4.)

B.4.1. Poster presentado: "Análisis del Marco Normativo Legal para el Ciclo de Vida de la Evidencia Digital". XX Workshop de Investigadores en Ciencias de la Computación – Corrientes, Argentina. WICC 2018. 26 y 27 de abril 2018

(Archivo: WICC 2018 - Poster - Análisis del Marco Normativo Legal para el Ciclo de Vida de la Evidencia Digital.pdf)



Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

Análisis del Marco Normativo Legal para el Ciclo de Vida de la Evidencia Digital

Mg. Aldo Santiago Igarza - Esp. Cintia Verónica Gioia – Mg. Jorge Eterovic

Programa CyTMA2 / Departamento de Ingeniería e Investigaciones Tecnológicas
Universidad Nacional de La Matanza
Florencio Varela 1903 (B1754JEC), San Justo, Argentina
asigarza@unlam.edu.ar; cgioia@unlam.edu.ar; eterovic@unlam.edu.ar

DESCRIPCIÓN DE LA LÍNEA DE INVESTIGACIÓN

CONTEXTO

Este proyecto de investigación está siendo presentado como un Programa de Investigación Científica, Desarrollo y Transferencia de Tecnologías e Innovaciones (CyTMA2) en el Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza, para el período 2018-2019.

El presente proyecto es del tipo investigación básica basado en el análisis del marco normativo y jurídico de la República Argentina, orientado a la comparación de los procesos del Ciclo de Vida de la Evidencia Digital.

RESUMEN

Con el crecimiento de las conductas delictivas que llegan a la justicia y que involucran dispositivos informáticos, surge la necesidad de acudir cada vez más a expertos en informática forense que actúen como peritos informáticos de oficio o de parte, siendo crucial su actuación en materia probatoria.

La exigente labor que hoy en día se requiere de especialistas en informática forense obliga a los mismos a mantener un conocimiento detallado y actualizado tanto a nivel de metodologías de prácticas forenses y procesos vinculados como en las normas y legislaciones asociadas con el tratamiento de la evidencia digital.

El proyecto de investigación se enfoca en el análisis de metodologías y procesos forenses informáticos y en el marco jurídico legal vigente para el aseguramiento del tratamiento de la evidencia digital en sus diferentes etapas del Ciclo de Vida, desde la identificación, adquisición o recolección, preservación, análisis hasta la presentación de resultados técnicos a tribunales de la justicia.

INVESTIGACIÓN Y DESARROLLO

La informática forense es inter-disciplinaria y requiere un estudio detallado de las normas, leyes, procesos, técnicas y tecnologías, además de los diferentes roles y responsabilidades de las personas involucradas, conformando un conjunto de conocimiento formal, científico y legal que apoya directamente a la administración de la justicia para al esclarecimiento de los hechos como así también en investigaciones internas en las organizaciones.

Si bien las herramientas forenses son la base esencial del análisis de la evidencia digital en medios informáticos, las mismas no hacen por sí solas a la tarea del perito informático. Por tal motivo el proyecto no se centra en la investigación de las herramientas forenses en sí, sino en la investigación de metodologías, técnicas, prácticas y procedimientos forenses y en el marco jurídico legal vigente para el aseguramiento del tratamiento válido de la evidencia digital en sus diferentes etapas del Ciclo de Vida.

También se estudiarán las diferentes regulaciones y lineamientos generales a considerar para la implementación de un laboratorio de informática forense, de manera de basar la misma en un entorno regulado y basado en normativas de trabajo para la investigación forense.

FORMACIÓN DE RECURSOS HUMANOS

El equipo está integrado por docentes- investigadores que pertenecen distintas cátedras de la carrera de Ingeniería en Informática de la UNLaM, más otro docente-investigador abogado, especializado en temas jurídico-informáticos y un alumno de la carrera de Ingeniería en Informática que está haciendo sus primeras experiencias en investigación.

Dos de los miembros del equipo de investigación se encuentran desarrollando sus respectivos trabajos de tesis de posgrado siendo tutoreados por uno de los integrante del proyecto de investigación.

B.4.1. Certificado de Autores del Artículo "Análisis del Marco Normativo Técnico Legal del Ciclo de Vida de la Evidencia Digital". XX Workshop de Investigadores en Ciencias de la Computación – Corrientes, Argentina. WICC 2018. 26 y 27 de abril 2018.

(Archivo: WICC 2018 - Certificado de Autores.pdf)

WICC 2018

XX Workshop de Investigadores en Ciencias de la Computación

RedUNCI UNNE

Se certifica que:

Igarza Santiago, Gioia Cintia, Eterovic Jorge E.

han participado en calidad de autores del artículo:

Análisis del Marco Normativo Legal para el Ciclo de Vida de la Evidencia Digital

aceptado en el XX Workshop de Investigadores en Ciencias de la Computación, realizado en la ciudad de Corrientes, los días 26 y 27 de abril de 2018.

LIC. PATRICIA PESADO
COORDINADORA RED UNCI

FACULTAD DE CIENCIAS EXACTAS Y NAT. Y AGRIMENSURA
UNIVERSIDAD NACIONAL DEL NORESTE
CORRIENTES

MGTER. GLADYS DAPOZO
COMITÉ ORGANIZADOR UNNE

B.4.2. Paper: "<u>Análisis del Marco Normativo de la Protección de los Datos Personales a Aplicarse en la Argentina en Proyectos de Cloud Computing Implementados en el Exterior del País</u>". 3era Conferencia Nacional de Informática Forense, INFOCONF 2019, Red Universitaria de Informática Forense (RED UNIF) - Córdoba, Argentina, 6 y 7 de junio de 2019.

(Archivo: InfoConf2019 - Paper Protección de los Datos Personales-Cloud Computing vf0.pdf)

Análisis del Marco Normativo de la Protección de los Datos Personales a Aplicarse en la Argentina en Proyectos de Cloud Computing Implementados en el Exterior del País

Juan González Allonca[1], Cintia Gioia[1], Jorge Eterovic[1], Mario Krajnik[1], Walter Ureta[1], Sergio Conde[1], Sergio Bonavento[1] and Santiago Igarza[1]

[1] Universidad Nacional de La Matanza (UNLaM), Departamento de Ingeniería e Investigaciones Tecnológicas, Florencio Varela 1903, B1754JEC San Justo, Buenos Aires, Argentina
{gonzalezallonca, cgioia, eterovic, mkrajnik, wureta, sconde, sbonavento, asigarza}@unlam.edu.ar

Resumen. Al momento de iniciar un proyecto de cómputo en la nube (cloud computing) es determinante adecuarse a la normativa local y a su vez, analizar las cláusulas relativas a la seguridad de la información, especialmente a la protección de los datos personales. Existe legislación aplicable que determina la extensión de responsabilidad de usuario y proveedor. Este estudio se propone presentar un proceso de análisis que permita describir y evaluar las regulaciones aplicables en la Argentina relacionadas con servicios de cómputo en la nube en el exterior del país, como la transferencia internacional de datos personales y la prestación por cuenta de terceros de servicios de tratamiento de datos personales. El proceso de análisis propuesto logra identificar y valorar el grado de cumplimiento con la normativa local, lo que facilitará la toma de decisiones informadas, basadas no sólo en criterios técnicos o económicos, sino también regulatorios. A su vez, identifica los principales ejes donde se deben abordar pericias en contextos de cómputo en la nube.

1 Introducción

En los últimos años, gran cantidad de empresas se han visto atraídas por las ventajas técnicas y los bajos costos de mantenimiento que ofrece el esquema de cómputo en la nube [1]. Flexibilidad, accesibilidad, autoservicio bajo demanda, escalabilidad, gestión de grandes volúmenes de datos, son algunos beneficios que ofrece este esquema. Sin embargo, estas ventajas muchas veces no contemplan cuestiones críticas como la seguridad de la información, cumplimiento normativo y privacidad de los datos [2].

Actualmente, la información es el activo más importante de las organizaciones [3], por lo que asegurar la privacidad de la información durante su ciclo de vida es crucial a la hora de utilizar estos servicios.

El desconocimiento o la no aplicación de la normativa vigente pueden transformarse tanto en pérdida de confianza o daño en la imagen de una empresa o perjuicio económico como en responsabilidades jurídicas [4][5]. Las preocupaciones por estos inconvenientes, por lo general, son lo suficientemente importantes para algunas empresas y organizaciones, tanto que las llevan a evitar implementar sus sistemas en arquitecturas de cómputo en la nube.

En el mundo conviven múltiples legislaciones relacionadas con la transferencia internacional [6], lo que dificulta establecer una estrategia global en términos de la utilización de servicios de cómputo en la nube.

Como señala Etro [7], en un informe realizado por el Foro Económico Mundial en 2010, en el que se consultaba al sector industrial, gobiernos y académicos respecto de los principales obstáculos para la adopción de servicios cloud, sus respuestas se concentraban en tres cuestiones de localización de los datos: privacidad, confidencialidad y las relacionadas con la propiedad y los derechos de los datos en la nube.

Por este motivo, a partir del presente estudio se define un proceso de análisis que permite a las empresas u organismos locales describir y evaluar la reglamentación vigente referida a la protección de datos personales en proyectos de cómputo en la nube en el exterior del país. Este proceso de análisis posibilita verificar el grado de cumplimiento con la normativa vigente, sumando el aspecto regulatorio a los análisis de viabilidad de un proyecto de cómputo en la nube.

2 El Modelo de Cloud Computing

Hablar de Cloud Computing es presentar un concepto de servicios de cómputo por demanda [8]. Se trata de un nuevo esquema en el uso de los recursos de tecnológicos y de sus modelos de consumo y distribución [9]. Este modelo

presenta un cambio importante en el paradigma computacional actual, la transformación de la infraestructura y las aplicaciones, de un mundo claramente dominado y administrado por las organizaciones, a otro donde un tercero confiable y conocido le brinda servicios de infraestructura y uso de aplicaciones [9].

La Cloud Security Alliance (CSA) es la Guía para la Seguridad en áreas críticas de atención en cloud computing y describe cinco características esenciales que evidencian similitudes y diferencias con las estrategias de computación tradicionales:

- Autoservicio por demanda. Un consumidor puede abastecerse unilateralmente de tiempo de servidor y almacenamiento en red, según sus necesidades, de forma automática sin requerir la interacción humana con cada proveedor de servicios.
- Amplio acceso a la red. Las capacidades están disponibles en la red y se accede a ellas a través de dispositivos estándar (p.ej., PC, teléfonos móviles y tablets).
- Reservas de recursos en común. Los recursos, como por ejemplo el almacenamiento, el procesamiento o la memoria del proveedor, son compartidos y pueden ser utilizados por múltiples clientes. Estos recursos son asignados dinámicamente y reasignados en función de la demanda de los consumidores. El cliente, por lo general, no tiene control o conocimiento exacto sobre la ubicación de los recursos. Usualmente, el proveedor no revela el lugar, aunque se puede especificar una ubicación genérica, como región o país.
- Rapidez y elasticidad. Las capacidades pueden suministrarse de manera rápida y elástica, en algunos casos, de manera automática, para poder realizar el redimensionado correspondiente rápidamente. Para el consumidor, las capacidades disponibles para abastecerse a menudo aparecen como ilimitadas y pueden adquirirse en cualquier cantidad y en cualquier momento.
- Servicio supervisado. Los sistemas de nube controlan y optimizan el uso de los recursos de manera automática, utilizando una capacidad de evaluación en algún nivel de abstracción adecuado para el tipo de servicio (p.ej., almacenamiento, procesamiento, ancho de banda, y cuentas de usuario activas).

3 Descripción del Problema

Como quedó demostrado, la implementación de servicios de cómputo en la nube ofrece múltiples ventajas, tanto desde un enfoque técnico (flexibilidad, accesibilidad, autoservicio bajo demanda, escalabilidad, gestión de grandes volúmenes de datos, etc.) como económico (bajos costos de implementación y mantenimiento, facturación por demanda, entre otros). Sin embargo, una de las grandes dificultades que se presentan a la hora de implementar estos servicios es de índole legal, más precisamente, cuando se transfieren datos personales de un país a otro para luego aplicarles un proceso informático [10][11][12][13][14][15].

Por lo tanto, al momento de iniciar un proyecto de cómputo en la nube, es necesario adecuarse a la normativa local y analizar las cláusulas relativas a la seguridad de la información, especialmente a la protección de los datos personales. Existe legislación aplicable que determina la extensión de responsabilidad, tanto del cliente, como del proveedor de servicios de cómputo en la nube. Aunque, aún no existe como práctica generalizada realizar un análisis previo en este sentido, donde se le permita al usuario conocer su nivel de riesgo y de cumplimiento normativo. Según Enrique Larrieu-Let (2013), presidente del Instituto de Auditores Internos de Argentina, “actualmente se carece de un marco de trabajo específico estructurado y completo para la identificación y evaluación de riesgos en Cloud Computing, es decir, la panacea aún no existe”.

A su vez, Mather [16] describe los contradictorios puntos de vista y nociones existentes en distintos países sobre los derechos a la privacidad y la protección de los datos personales, lo que genera múltiples batallas legales, disputas políticas y regulaciones conflictivas. Algunos ejemplos de regulaciones en tensión que presentan los autores son las Reglas Federales de Procedimiento Civil de EE. UU. (FRCP) y la Directiva de la Unión Europea sobre protección de datos personales.

Debido a que existen múltiples proveedores en distintos países, sumado a diferentes modelos y formas de despliegue de cómputo en la nube, las metodologías actuales no definen una serie de pasos a seguir para realizar un proceso de análisis que permita describir y evaluar la reglamentación local vigente referida a la protección de datos personales en proyectos de cómputo en la nube. A la falta de un proceso de análisis regulatorio se le suman riesgos propios de ese modelo de negocio, que podrían generar responsabilidades legales tanto en el país de origen como en el de destino.

En este contexto, el proceso de análisis propuesto logra identificar y valorar el grado de cumplimiento con la normativa local, lo que facilitará la toma de decisiones informadas, basadas no sólo en criterios técnicos o económicos, sino también regulatorios. A tales fines, resulta pertinente determinar las garantías y requisitos necesarios para proteger adecuadamente los datos personales que se transfieran a países sin legislación adecuada en los términos del artículo 12 del Anexo I al Decreto N° 1558/01.

El proceso permite efectuar un análisis de la normativa y de los riesgos en la implementación de un servicio de cómputo en la nube, que permite controlar la aplicación del derecho fundamental a la protección de datos de los titulares. Luego del análisis, es posible contar con un registro directo de los incumplimientos normativos identificados y promueve la adopción de las medidas necesarias para eliminarlos o mitigarlos.

Uno de los principales beneficios de esta metodología radica en que, a partir de su realización, en las etapas iniciales de la implementación de un servicio de cloud computing se logran identificar los posibles riesgos y corregirlos anticipadamente, evitando los costos y complicaciones derivados de descubrirlos a posteriori, cuando el servicio está en funcionamiento o, lo que es peor, cuando la lesión de los derechos se ha producido, lo que implica pérdidas económicas y también daños a la imagen para la organización, cuya reputación se ve afectada.

A su vez, la ejecución de este proceso otorga transparencia a la gestión de los datos personales, base de una relación de confianza entre su titular y el usuario de ellos. Esto permite planificar las medidas ante posibles impactos en la privacidad y gestionar los vínculos con terceras partes implicadas en la transferencia de datos, otorgando más garantías para ellas.

4 Marco Legal: Legislación y Jurisdicción Aplicable

¿Cuál es la importancia de la privacidad y por qué la legislación argentina la protege? Es decir, ¿de dónde surge la necesidad de tomar medidas técnicas para su protección? La privacidad es un derecho humano fundamental y se encuentra receptado en tratados internacionales, leyes, disposiciones y jurisprudencia. Es el derecho que protege la libertad individual y de expresión, la intimidad y la dignidad personal, e incluye el derecho a la protección de datos personales y la figura del Habeas Data.

Ahora bien, ¿cuál es la relación que existe entre privacidad, protección de datos y habeas data? “De manera general, se puede decir que la protección a la privacidad es el género y la protección de datos la especie. Y todavía en un sentido más estricto queda la figura de habeas data, la cual se opera como un derecho de acceso a la información personal dentro del régimen de datos personales” [17].

El derecho a la privacidad se sustenta en principios fundamentales como el honor y la dignidad personal. Como lo afirma la Secretaría de Asuntos Jurídicos, OEA (2012), “el derecho a la privacidad va más allá de la protección de datos, abarca el respeto de la vida familiar, preferencias religiosas, políticas y sexuales, la intervención de las comunicaciones, el uso de cámaras ocultas, los análisis genéticos, etc. La protección de la vida privada y la protección de la intimidad son necesarias para el orden jurídico y como garantía de respeto a la dignidad personal”.

La protección de datos es un derecho a la intimidad personal que tienen las personas contra un tratamiento incorrecto, no autorizado o contrario a las normativas vigentes de sus datos personales por tratadores de datos. Al proteger los datos personales frente al riesgo de la recopilación y el mal uso de sus datos personales, se ampara, en consecuencia, la privacidad de las personas.

Dentro del derecho de protección de datos personales, como se muestra en la Figura 1, se encuentra la acción de Habeas Data. Se trata de un recurso legal mediante el cual las personas agraviadas pueden informarse sobre datos referidos a ellos y el propósito de su recolección. A su vez, permite exigir, dependiendo el caso, su rectificación, actualización o supresión de información personal alojada en bancos o registros de datos, públicos o privados.

Fig. 1 Relación entre Privacidad, Protección de Datos y Habeas Data

Nuestro país cuenta con una amplia tradición en materia de protección de datos personales, que se manifiesta en tres niveles distintos. En el primer nivel, se encuentra la Constitución Nacional que, luego de su reforma en el año 1994, incluyó el artículo 43 que, en su párrafo tres, contempla el llamado habeas data, de la siguiente forma: Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

Como se advierte, esta reforma de la Constitución Nacional ha establecido un instituto que carecía de antecedentes en el derecho federal, aunque ya se encontraba en las constituciones provinciales: la acción de habeas data [6]. Se trata de un procedimiento especialmente necesario a partir del aumento del uso de las computadoras, que pueden compilar la información y datos personales afectando el honor y la privacidad de las personas [4]. La acción también está establecida para tomar conocimiento de estos datos y, en su caso, exigir la supresión, rectificación, confidencialidad o actualización.

El segundo nivel está representado por la Ley N° 25.326 de Protección de los Datos Personales, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre. A su vez, el Poder Ejecutivo reglamentó dicha ley por medio del decreto N° 1558/01, en el que se crea la Dirección Nacional de Protección de Datos Personales, que es el órgano de control de la ley, primero en América Latina y el tercero del hemisferio sur.

En tercer nivel, está la interpretación y la aplicación que hacen los jueces de estas normas. A partir de este desarrollo legislativo, Argentina fue declarada país adecuado por la Unión Europea en materia de Protección de Datos Personales, de conformidad con la Directiva 95/46/CE [18].

5 Fases del Proceso de Análisis de Cumplimiento Normativo

El modelo de un procedimiento de análisis que permite describir y evaluar la reglamentación local vigente referida a la protección de datos personales en proyectos de cómputo en la nube, a través de proveedores en el exterior del país, que busca encontrar una solución al problema planteado, con el fin de identificar y valorar el grado de cumplimiento con la normativa local, lo que facilita la toma de decisiones informadas, basadas no sólo en criterios técnicos o económicos, sino también regulatorios.

Esta herramienta metodológica de evaluación de cumplimiento normativo permite evaluar el grado de impacto en la protección de datos personales para servicios de cloud computing, lo que permite tomar las medidas necesarias para evitar o minimizar los impactos negativos.

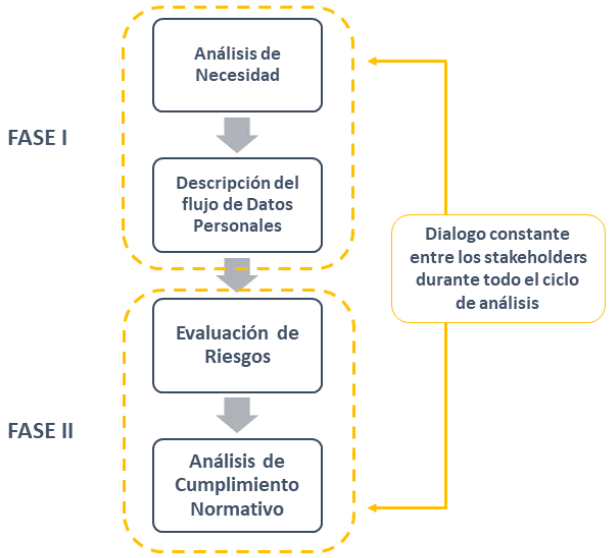


Fig. 2 Etapas del Proceso de Análisis de Cumplimiento Normativo.

El uso de servicios de cómputo en la nube permite una amplia variedad de beneficios para los usuarios en términos de agilidad, movilidad y reducción de costos vinculados a los recursos de procesamiento por lo que el procesamiento de datos sin duda crecerá [19].

Dado que es difícil imaginar una organización que no tenga una cierta cantidad de datos personales (relacionados con los empleados, por ejemplo), es probable que externalizarlos sea un potencial obstáculo para el procesamiento de datos en la nube. Por lo tanto, para asegurarse de que esta actividad no colisiona con las normas locales, una organización tendrá que determinar si un proveedor de servicios en la nube procesará sus datos personales ajustado a derecho.

Una solución a este problema es la aplicación de una metodología que permita describir y evaluar la reglamentación local vigente referida a la protección de datos personales en proyectos de cómputo en la nube y la evaluación de riesgos en materia de protección de datos personales para servicios de cloud computing. A través de esta metodología, que consiste en un enfoque analítico para mejorar la gestión del tratamiento de datos personales, será posible identificar la norma aplicable, los riesgos y establecer un nivel de criticidad sobre ellos. La aplicación de esta metodología se aplica de forma simultánea y complementaria con la legislación vigente que los responsables del tratamiento de datos deben cumplir.

Con este procedimiento se intenta brindar a los responsables del tratamiento de información de carácter personal y, a su vez, permitirles:

- Tener un punto de vista racional de los riesgos derivados del procesamiento de datos personales en el exterior del país;
- Determinar medidas de seguridad necesarias y suficientes con el fin de "adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. (artículo 9, Ley N° 25.326, 2000).

La propuesta de proceso aquí planteada facilita un marco común a organizaciones tanto del ámbito público como privado, que procesen datos personales en la nube fuera del país, independientemente de si se encuentran en un país con legislación adecuada o no.

Este proceso establece una serie de medidas que deben implementarse en conjunto con la normativa local en materia de protección de datos, por ello, quienes implementen servicios de cloud computing, no sólo deberán analizar si éste

se adecúa a la norma, sino también, si por el carácter o tipo de información que se trata, no son necesarias medidas adicionales de acuerdo con la normativa argentina.

Fase I - Definición de Conveniencia y Lineamientos del Proyecto: En la primera fase del proceso se realizan las acciones necesarias para establecer las bases del proyecto, identificar las partes involucradas, evaluar el impacto de la implementación de un servicio de cómputo en la nube en la organización y analizar el flujo de datos personales.

Fase II - Evaluación de Riesgos y Cumplimiento Normativo: La evaluación de riesgos se utiliza en diversas áreas (seguridad aérea, finanzas, seguridad física, etc.) Esta metodología se centra en la seguridad de la información, más precisamente, en los riesgos vinculados con los datos personales.

En el tratamiento de datos es posible identificar como riesgos aquellos provenientes del tratamiento de datos de carácter personal. Dichos riesgos están compuestos por un incidente determinado y todas aquellas amenazas que lo pueden hacer posible; cómo estos incidentes pueden hacerse realidad.

Es posible estimar los riesgos en el tratamiento de protección de los datos personales en términos de severidad (la magnitud del riesgo) y probabilidad. En el caso de cómputo en la nube, esencialmente depende del nivel de identificación de los datos personales y el nivel de consecuencia de los potenciales impactos.

La probabilidad representa la factibilidad de que un hecho pueda ocurrir. En esencia, depende del nivel de vulnerabilidad de los factores de soporte frente al nivel de capacidad para explotarlo de las fuentes de riesgo.

6 Principales ejes a donde se deben abordar pericias en contextos de cómputo en la nube

La adquisición y el tratamiento de la evidencia digital son actividades estratégicamente decisorias, al momento de generar pruebas informáticas que permitirán dirimir situaciones dudosas y los respectivos autores o culpables. Es importante considerar las nuevas alternativas y problemática que se generan al abordar pericias en contextos de cómputo en la nube, lo cual se centra en el debido conocimiento y control de la gestión en la nube, el cumplimiento contractual entre el prestador y el cliente, la disponibilidad del servicio en la nube y la confiabilidad, seguridad y confidencialidad sobre los servicios [20].

Actualmente existe un vacío normativo en relación con el tratamiento de la evidencia digital en servidores externos que puede ser causa de que la evidencia no sea aceptada en una instancia judicial. La evidencia digital en la nube plantea nuevos ejes técnicos y legales que deben considerarse:

En términos legales:

- Conocer las responsabilidades legales tanto en el país de origen como en el de destino. Considerar la legislación y jurisdicción aplicable que determina la extensión de responsabilidad, tanto del cliente, como del proveedor de servicios de cómputo en la nube.
- Aplicar la metodología de Análisis de Cumplimiento Normativo (descripta en la sección anterior) de forma reactiva, de manera que permita describir y evaluar el grado de cumplimiento de la reglamentación local vigente referida a la protección de datos personales en proyectos de cómputo en la nube y así delimitar la investigación forense a realizar.

En términos técnicos:

- La evidencia digital está ubicada en un servidor externo de un tercero y sólo es accesible a través de este.
- El tercero puede ser conocido o no, estar en la misma jurisdicción o en otra diferente, aunque mayormente es en el extranjero.
- Tipos de nubes: públicas (recursos de la nube propiedad de terceros), privadas (recursos informáticos exclusivos de una organización) o híbridas.

- Existen múltiples proveedores en distintos países, con diferentes modelos y formas de despliegue de cómputo en la nube.
- La mayoría de los proveedores de servicios en la nube sólo entregan información mediante orden judicial, lo cual implica que las solicitudes de acceso a evidencia digital remota deben ser realizadas por el Juzgado.
- Los proveedores de servicios poseen sus propias políticas de entrega de información a las autoridades, junto con diversas condiciones unilaterales impuestas por los mismos, como ser los períodos de retención establecido por sus términos y condiciones y las formas en que deben ser realizados los pedidos de información, sean de conexión, tráfico o de contenido.

En Argentina, la recolección de evidencia en la nube suele realizarse de dos formas. La primera consiste en la solicitud de conservación de datos al proveedor de servicios. Dicha petición suele ser aceptada por los proveedores de servicios en la nube, si la misma es efectuada por un oficial de las fuerzas de la ley, desde una dirección de correo oficial de la fuerza a la que reporta. La segunda forma es la obtención de datos, la cual puede requerir una orden judicial o un exhorto diplomático. Todo este proceso está fuertemente influenciado por los términos y condiciones de cada empresa que presta el servicio, los cuales suelen establecer la forma en que deben ser hechos los pedidos [21].

Existen diferentes escenarios de discusión que con el crecimiento de la computación en la nube se hace esencial que sean tratados, como ser:

- Recolección remota de evidencia ubicada en el servidor externo, previa autorización del Juez.
- Obtención de evidencia digital recopilada desde perfiles públicos de redes sociales o diversas fuentes abiertas, tratadas como información pública.
- Obtención de evidencia digital mediante orden de allanamiento, en donde se verifica si se utiliza la facilidad de acceso a la nube para almacenar datos. En caso afirmativo, se deberá tratar de obtener las características de acceso a tal información, a los efectos que la misma sea "bajada¨ a un dispositivo, para luego ser secuestrado y posteriormente analizado [20], previa orden del Juez.

7 Conclusiones

Como conclusión del presente trabajo, se desprende que, al momento de iniciar un proyecto de Cloud Computing, no sólo deben evaluarse variables relativas a la rentabilidad, capacidad tecnológica y ventaja de negocios, sino también analizar el cumplimiento normativo y las cláusulas sobre seguridad de la información, especialmente las relativas a la protección de los datos personales. Aplicar la legislación local en materia de protección de datos personales le permite al usuario de servicios de cómputo en la nube conocer la extensión de su responsabilidad y la de su proveedor ante un eventual incidente. De este modo, el usuario podrá valorar qué delega en este modelo y qué cuestiones prefiere reservarse, pudiendo tomar una decisión basada en información concreta.

Por otro lado, este trabajo presenta las bases de una metodología de evaluación de riesgos en materia de protección de datos personales en servicios de cómputo en la nube que permitirá cuantificar la magnitud de los riesgos existentes y, en consecuencia, jerarquizar racionalmente su prioridad de corrección.

En términos de pericias en contextos de cómputo en la nube, se plantean nuevos paradigmas, desafíos y escenarios que obliga a los peritos informáticos a capacitarse y prepararse para manejar nuevos aspectos no solo técnicos sino legales en el tratamiento de la evidencia digital almacenada en la nube, de manera de evitar errores en los procedimientos que vuelvan inválida la prueba recolectada.

Referencias

1. Gartner, Mindy Cancila, Douglas., Toombs, Alan D Waite, y Elias Khnaser. «2017 Planning Guide for Data and Analytics.» 2017, Recuperado 3 de marzo 2019.
2. Rao, R, y K Valemadhava & Selvamani. «Data Security Challenges and Its Solutions in Cloud Computing.» Procedia Computer Science, nº 48, 2015: 204-209.
3. World Economic Forum, WEF. «Unlocking the Value of Personal Data: From Col-lection to Usage. Industry Agenda.» Editado por Geneva. Word Economic Forum, 2013: 7-9.

4. Peyrano, G. Régimen legal de los datos personales y el habeas data. Buenos Aires, Argentina. ISBN: 9501418626., Buenos Aires, Argentina: De-palma., 2002.
5. Palazzi, P. La protección de los datos personales en la Argentina. Buenos Aires, Argentina. Errepar, 2004.
6. Palazzi, P. «La transmisión internacional de datos personales y la protección de la privacidad.» Ad-Hoc. ISBN: 950-894-318-1, Buenos Aires, Argentina, 2002.
7. Etro, F. «The Economic Consequences of the Diffusion of Cloud Computing» en Dutta, Soumitra; Mia, Irene. The Global Information Technology Report 2009 – 2010 ICT for Sustainability.Foro Económico Mundial - INSEAD. Londres. 2010.
8. Mell, P, y T Grance. «The Nist Definition of Cloud Computing.» NIST Special Publication 800-145, National Institute of Standards and Technology, Department of Commerce, U. S., 2011, Recuperado 15 de marzo 2019.
9. Catteddu , D, y Hogben , G. «Cloud Computing - Benefits, and risks recommendationes for information security.» Enisa, 2009.
10. Anuar, N, Gani, A, Hashem, I.A, Khan, S.U., Mokhtar, S., y Yaqoob, I. The rise of "big data" on cloud computing: Review and open research issues. Vol. 47. Infrmation System, 2015.
11. Bernardino, J., Cámara, J., Neves, P.C., y Schmerl, B.R. Big Data in Cloud Computing: features and issues. 2016, recuperado 10 de marzo 2019.
12. Azer, M., y El.Zoghby, A. «Cloud computing privacy issues, challenges and solutions.» 12th International Conference on Computer Engineering and Systems (ICCES). 2017. 154 - 160.
13. Brodkin, J. «Gartner: Seven cloud-computing security risks.» Infoworld, 2008, 1 - 3.
14. Pavolotsky, J. Top Five Legal Issues for The Cloud. Forbes. Forbes, 2010, Recuperado 16 Marzo de 2019.
15. Pearson, S, y A Benameur. «Privacy, security and trust issues arising from cloud computing. Cloud Computing Technology and Science (CloudCom).» IEEE Second International Conference on IEEE, 2010.
16. Mather T, Kumaraswamy S, Latif S. «Cloud Security and Privacy» O'Reilly Media, Inc., Sebastopol, CA. 2009
17. Organización de los Estados Americanos (OEA). «Interrelación entre protección a la privacidad, protección de datos y habeas data.» Secretaria de Asuntos Jurídicos, 2012, Recuperado 4 de abril de 2019.
18. European Parliament and of the Council. «Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.» 1995.
19. Orban, S. «The Fast and the Furious: How the Evolution of Cloud Computing Is Accelerating Buil-der Velocity. AWS Cloud Enterprise Strategy Blog.» Recuperado 17 de marzo 2019.
20. Piccirilli, Mg.Lic. Darío A. Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia – forensia y cibercrimen). La Plata, Buenos Aires: Tesis Doctoral en Ciencias Informáticas - UNLP - Facultad de Informática, 2015.
21. Asociación por los derechos civiles. La investigación forense informática en América Latina. Vol. 2. ADC por los Derechos Civiles, 2018, Recuperado 20 de abril de 2019.

B.4.2. Certificado de Asistencia a 3ra Conferencia Nacional de Informática Forense" INFOCONF 2019) de la Red Universitaria de Informática Forense (RED UNIF) - Córdoba, Argentina, 6 y 7 de junio de 2019.

(Archivo: InfoConf2019 - 3ra Conferencia de Inf Forense - Certificado Asistencia JA.pdf)

Otras Publicaciones (B.5.)

B.5.1. Publicación en El Observador. Diario Perfil. 1 de junio de 2019.

(Archivo: NotaDiarioPerfil.docx

Link: https://www.perfil.com/noticias/elobservador/comunidad-pedofila-el-horror-tiene-mas-de-un-sitio-en-la-web.phtml)

el Observador
INVESTIGACION Y ANALISIS

ESCONDIDOS PERO NO TANTO

Comunidad pedófila: el horror tiene más de un sitio en la web

En cuestiones como la pornografía infantil, la demanda es parte fundamental del problema. Una experta explica cómo actúan sus usuarios en la "dark web" y brinda algunas claves para detectar peligros.

CINTIA GIOIA*

Es importante reflexionar sobre el término "pornografía infantil" y el mal uso de la palabra "pornografía". Es un término que se naturalizó, pero que al referirse a la infancia se refiere a un delito que penaliza no solo la distribución sino la tenencia de pornografía infantil, según lo sancionado en la Ley 27.436, modificatoria del Art. 128 del Código Penal de la Nación. Antes de esta ley la simple tenencia era considerada una acción privada. Y ¿por qué penar la tenencia? Indudablemente el que colecciona pornografía infantil, colecciona imágenes y videos de menores de edad en conductas sexuales explícitas, y cada vez quiere más, más y más. La demanda genera la oferta, la oferta genera la necesidad de producción y la producción lleva al abuso sexual. La tenencia de una imagen de un niño que está siendo abusado sexualmente es claramente una violación a la integridad sexual del menor. Cuanta más demanda, más se genera indirecta y directamente el abuso sexual infantil.

Para investigar primero hay que conocer de qué se trata, es muy difícil investigar si desconocemos a qué nos enfrentamos.

Los pedófilos poseen su propia simbología para identificarse ante su comunidad, para dar a conocer sus preferencias sexuales, indicar el menor "disponible" o el material al que puede dar acceso. Cada símbolo tiene un significado diferente, aunque todos transmiten el mensaje subliminal de algo grande que contiene algo pequeño. A partir de una investigación del FBI (Agencia Federal de Investigación e Inteligencia de Estados Unidos) se elaboró una guía de estos símbolos. Un triángulo azul que contiene otro triángulo azul representa el "amor por los niños", si las líneas son finas preferentemente niños pequeños y si no, más grandes. Un corazón rosado conteniendo un corazón más pequeño representa el "amor por las niñas" pequeñas. Una mariposa de cuatro corazones bicolor representa el "amor por las niñas y niños" en cualquier rango de edad sin importar su género sexual. Sin dejar de lado el símbolo universal del pedófilo representado por una figura de un oso de color café que representa cariño, llamado "pedobear".

Orgullo. Como si fuera poco tienen un día de festejo, desde 1998 se convoca al Día Internacional del Amor por los Niños, también conocido como Día del Orgullo Pedófilo. Festejo cuya información podrán encontrar sin necesidad de acceder a lo más profundo de la web, simplemente haciendo una búsqueda en Google. La fecha fijada es el primer sábado después del solsticio de verano, teniendo en cuenta los dos hemisferios, la celebración se realiza dos veces al año, donde se organizan como minoría sexual y no autores de un delito. En Argentina esto pasa entre el 23 y 24 de diciembre, mientras todos se preparan para celebrar la próxima Navidad en familia y amigos, en internet se están distribuyendo grandes volúmenes de pornografía infantil.

Los pedófilos tienen sus técnicas, tácticas, estrategias, pertenecen a comunidades en la red donde se aconsejan sobre cómo acceder, distribuir o pro-

Viene de pág. 66

pornografía, entre otras modalidades delictivas.

Una modalidad que están utilizando los pedófilos, es volver a utilizar las redes de intercambio de archivos P2P, redes "peer to peer", entre pares, en lugar de los sitios de descarga directa. Programas como eMule, eDonkey o Torrent, que funcionan contactando a los usuarios de una red con los contenidos que los demás tienen en sus propias computadoras, las cuales forman una red de nodos de contenidos sin roles fijos, pudiendo ser tanto receptores como proveedores de material.

Whatsapp. Aun así, en la actualidad existe material de pornografía infantil que se intercambia a través de redes sociales conocidas, a través de las cuales los pedófilos comparten enlaces (links) de acceso a material de pornografía infantil, utilizando combinaciones de palabras claves o accesos encubiertos en videos. A medida que esos links dejan de estar disponibles, colaboran entre sí para ir pasándose nuevos links, incluso a enlaces de grupos de Whatsapp, a los cuales con un solo "click" se accede, migrando así también a los servicios de mensajería instantánea.

La gran mayoría de los casos de pornografía infantil que llegan a la Justicia argentina lo hacen a través de la ONG estadounidense Ncmec (The National Center for Missing & Exploited Children), con el objetivo de ayudar a prevenir y disminuir la explotación sexual infantil a través del uso de la tecnología. En EE.UU. existe una Ley Federal que obliga a todas a las empresas proveedoras de servicio de internet a reportar y denunciar los casos donde sus clientes suben material de pornografía infantil, fotos o videos de un niño siendo abusado y deben reportarlos a esta ONG. Se reciben reportes de Google, Microsoft, Whatsapp, Facebook, Twitter, Instagram, etc.

> Los productores de pornografía cuentan con enlaces a grupos de Whatsapp en los que con un click se llega al material

El Ncmec tiene convenio con muchísimos países del mundo para poder poner inmediatamente en conocimiento cuando ocurren estos incidentes de tráfico y distribución de pornografía infantil. Argentina tiene un convenio con dicha ONG desde el año 2013, por lo cual se reciben reportes del Ncmec con los casos de circulación de pornografía infantil que involucran a nuestro país, es decir originados por el accionar de usuarios localizados dentro del territorio argentino.

DETENCION. Los fiscales deben analizar todo el material secuestrado. Se detuvo a Russo en el Hospital Garrahan.

Los reportes de Ncmec tienen categorías que permiten advertir la urgencia de los casos, según se pueda presumir que el menor está en situación de peligro, por ejemplo, si está siendo abusado en un video en vivo, si el menor está o no al alcance o en contacto con el pedófilo o son denuncias de las prestadoras de contenidos de internet.

Fiscalías. El Ministerio Público Fiscal de la Ciudad de Buenos Aires institucionalmente ha firmado este convenio para la recepción de estos reportes por parte de los Cuerpos de Investigaciones Judiciales, quienes los reciben, comienzan los primeros pasos de la investigación y lo derivan para su investigación de acuerdo con la competencia jurisdiccional que corresponda. Desde octubre de 2014 se creó la Red 24/7, es una red de puntos de contactos distribuidos en todo el país, que funciona las 24 horas los 365 días del año, que se encarga de la derivación de casos a otras jurisdicciones fuera de la Ciudad de Buenos Aires, en especial aquellos en que las medidas de protección de las víctimas menores resultan urgentes.

Por otro lado, también se reciben denuncias directas de pornografía infantil en las fiscalías, las cuales son realizadas por personas vinculadas directa o indirectamente a menores afectados o que han recibido algún tipo de material de pornografía infantil, entre otros casos.

Se debe considerar la cifra negra existente, que son esas denuncias que nunca llegan a la fiscalía, no se judicializan, quedan en el núcleo de la familia o personas de confianza, por desconocimiento, porque no creen en la Justicia o simplemente porque quieren "guardar el secreto".

Cada uno de los reportes del Ncmec informan el número de IP (Protocolo de Internet) desde donde se transmitió el contenido, junto con la fecha, la hora exacta y la ubicación aproximada. Los investigadores verifican a qué proveedor de internet pertenece esa IP y se comunican con el proveedor para que le aporte datos del usuario de la IP registrada y conseguir la dirección física asociada. Si bien la dirección IP es un número que identifica de forma única el acceso que un proveedor da a un dispositivo para acceder a internet, esta asignación en la mayoría de los casos es dinámica y por eso para identificar el dispositivo de acceso es fundamental contar con la fecha y hora exacta de conexión.

Bajo el acuerdo de autoridades de diferentes países se generó el Proyecto VIC a través del cual se mantiene una base de datos única de información y material de pornografía infantil actualizada. El proyecto utiliza tecnologías innovadoras de empresas como Netclean y Microsoft PhotoDNA y otros para permitir a los investigadores clasificar material conocido. Las imágenes son identificadas unívocamente a través de un Hash, una cadena alfanumérica de longitud fija que solo puede volver a crearse con esa misma imagen, posibilitando la búsqueda de una copia exacta de una imagen. Cualquier mínima modificación de la imagen, variará su hash. En ese caso, Microsoft PhotoDNA brinda una tecnología que posibilita la búsqueda de imágenes por similitud, permitiendo detectar imágenes que hayan sufrido variaciones a partir de la imagen original.

Evidencias. Posteriormente a los allanamientos, comienza el análisis del contenido de los equipos secuestrados, sean computadoras de escritorio, notebooks, celulares, etc. En la actualidad abundan los discos, tarjetas MicroSD, pendrives y celulares de gran capacidad conteniendo Giga o Tera Bytes de información los que deben ser analizados y categorizados. Un solo terabyte podría tener miles de fotos y videos, según la calidad, tamaño y formato de los archivos. En ese sentido existen programas especializados para el tratamiento de la evidencia digital de delitos sexuales a menores, que permiten procesar eficientemente grandes volúmenes de imágenes, identificar material relevante, categorizar y relacionar imágenes y videos de pornografía infantil, imágenes de víctimas, de lugares, objetos o personas vinculadas. Las categorías se basan tanto en el rango de edad de la víctima como el nivel de desnudez de la imagen. Estos programas permiten integrar sus búsquedas con bases de datos de pornografía infantil.

La disponibilidad, integración y uso de estas tecnologías colaborativas son indispensables para la asistencia en la clasificación a través de un software, aunque de todos modos para determinar si una imagen contiene o no pornografía infantil siempre implica un trabajo y una verificación manual de manera de evitar resultados equivocados. No existe la automatización completa y ese es el motivo por el cual las investigaciones involucran un gran tiempo de análisis.

Para enfrentar este tipo de delitos se necesita un trabajo en equipo y multidisciplinario donde abogados, peritos, investigadores y diversos profesionales trabajan para dar con la ubicación e identidad de los delincuentes aplicando los procedimientos de tratamiento de la evidencia digital que cumplan con los requisitos legales para que no sean cuestionables en un juicio, como también para la identificación de las víctimas. Se debe tener tener muy presente que, si se cometen errores en la investigación o las pericias informáticas realizadas, un menor puede no tener justicia. ■

**Especialista en Criptografía y Seguridad Informática y en Informática Forense.*

PARA TENER EN CUENTA

- ◆ En la dark web existen mercados negros para todo tipo de delitos. No debe confundirse con deep web.
- ◆ La gran mayoría de las denuncias se hacen a través de la ONG Ncmec (The National Center of Missing & Emploited Children.
- ◆ La pornografía infantil no solo se ejerce a través de filmaciones que están en los diferentes sitios de la dark web. Muchos grupos de Whatsapp actúan brindando el material con un solo click.
- ◆ Desde octubre de 2014 existe una red que trabaja en la contención y la recepción de denuncias sobre pornografía infantil. Se recibieron más de 40 mil denuncias.
- ◆ En este caso, la denuncia se originó en los Estados Unidos y también en Brasil. El Ministerio Público, la Fiscalía trabaja en la detección de una red que tiene IPs detectadas en todo el territorio nacional. Hubo otra detención en Córdoba.

UN DELITO DE LARGA DATA

Delincuentes que aprovechan la proximidad y la sumisión para engañar a padres e hijos

LAURA QUIÑONES URQUIZA*

El caso del pediatra del hospital Garrahan, Ricardo Russo, acusado de producción y distribución de pornografía infantil, no es el único. En 2010 Guillermo Gallón Castrillón, un reconocido cirujano pediátrico colombiano y líder de un grupo scout, era uno de los principales proveedores de pornografía infantil en los círculos de pedofilia. El material que aportaba estaba no solo relacionado a las víctimas del turismo sexual infantil que solía hacer en países como Indonesia, India o Tailandia. Muchas de las filmaciones estaban hechas en hoteles con menores, y como es habitual en el material pornográfico infantil, los agresores suelen blurearse u ocultar su rostro con algún sistema. Cobran relevancia en estos casos los sistemas de identificación como nevos, lunares, cicatrices, tatuajes, máculas, biometría de la voz y sistemas informáticos de avanzada que a veces logran eliminar esos métodos de ocultación del rostro salvo que sean materializados y no informáticos. Con esta tecnología y trabajo investigativo junto a España, Brasil, Australia, Alemania, Reino Unido y Colombia, fue que interpol logró dar con Gallón Castrillón y detenerlo cuando volvía de uno de esos viajes. Dentro del material recolectado, por supuesto, había fotografías tomadas con la excusa de ser usadas con fines científicos en congresos o actos académicos. Aprovechando la proximidad y total sumisión de sus pequeños pacientes con anuencia de sus padres, engañándolos y abusando de la confianza que le depositaron, con el mejor camuflaje: el de custodio de la salud de sus hijos, así como sería el modus operandi del pediatra del Garrahan. Tanta confianza habría que ni siquiera fue denunciado por algún adulto basándose en los dichos de su hija o hijo durante la consulta.

CHOCO PERFIL

Espionaje. La distribución de pornografía infantil no es nueva, sino que cambió de método y hoy es informático y globalizado. En 1974 en Reino Unido surgió el Paedophile Information Exchange (intercambio de información de pedofilia), pudo funcionar 10 años abiertamente con la excusa o engaño, era que se trataba de un movimiento de amantes de los niños, este grupo llegó a estar afiliado al Consejo Nacional de Libertades Civiles. Pero buscaban la baja de edad de consentimiento para tener relaciones sexuales a 5 años, a través de correo postal distribuían escritos, intercambiaban fotografías de abusos, de desnudez o de poses lascivas de menores, e información respecto a cómo seducirlos y dónde encontrarlos. Dentro de sus activistas había hasta ex miembros de la KGB. Con este falso y engañoso objetivo se unieron a minorías que tenían objetivos reales de búsqueda de igualdad de derechos como los grupos feministas y homosexuales, pero con el tiempo, las verdaderas intenciones del P.I.E. fueron descubiertas y repudiadas públicamente por sus ex aliados.

Los pedófilos a diferencia de los pederastas no han pasado aún al acto, algunos no desean hacerlo y poseen una inmensa colección de material orientado a distintas temáticas, a veces son millones de fotos, miles de videos encriptados en discos rígidos para que no sean detectados y que utilizan con fines masturbatorios, y cuyo consumo colabora con la explotación sexual infantil. Esto es algo que a los que hemos colaborado durante investigaciones criminales de estos casos, nos llama la atención luego con el resultado de los allanamientos, en la mayoría de ellos es apabullante la cantidad de material que descargan y guardan, es decir, el coleccionismo aparecería como una compulsión que aparece como absurda. Incluso en esta colección los menores no están en posiciones lascivas o en actos sexuales, a veces se trata de fotos de desnudez totalmente inocentes como por ejemplo durante un baño, y donde el sentido lascivo se lo pone el receptor. Hoy en día existen emblemas de reconocimiento que fueron difundidos por el F.B.I., así como palabras clave que identifican y especifican, incluso en la internet superficial en sitios como e-mule, Youtube, etc., el tipo de material que se posee para vender o intercambiar, la mayoría utiliza las iniciales de C.P. (Child Porn) entre otras distorsiones en castellano que no es conveniente difundir públicamente porque serían contraproducentes para investigaciones en curso. Existen foros de discusión, varios fueron derribados o craqueados en distintas operaciones contra la pornografía infantil del grupo Annonymous, algunos de estos foros o asociaciones como Nambla o Martin lo que buscan es normalizar las relaciones sexuales con menores porque, según ellos, las niñas y niños son seres sexuales y por lo tanto, hay que respetarles ese derecho. Ese es el razonamiento grupal, aberrante y peligroso que les permite abusar de la inocencia o el temor de sus víctimas. ■

> Existen emblemas de reconocimiento, que fueron difundidos por el FBI y palabras clave que identifican a los pedófilos

ducir dicho material e incluso cómo tratar o generar proximidad con sus víctimas para lograr el material deseado. Los pedófilos no solo consumen, no basta con mirar online o descargar el material. Existen organizaciones de delincuentes dedicados a la producción y comercialización de material de pornografía infantil. Nos enfrentamos a delincuentes que se capacitan y especializan día a día, migrando de tecnologías continuamente.

Forman comunidades especiales cuya membresía involucra el envío de material innovador no existente en la red, comercializan el material a través de la venta con criptomonedas, aplican técnicas para ocultar las imágenes o manipularlas para no ser detectadas a simple vista o técnicas de falsificaciones dentro de videos y utilizando palabras claves o tecnologías para lograr su anonimato.

Dark web. Existe un gran mercado de material en sitios de pornografía infantil que no se encuentran fácilmente en internet. Sino que utilizan la dark web la que comprende contenido anónimo y cifrado al que se accede mediante redes, como Tor, I2P o FreeNet, que posibilitan la navegación anónima ocultando la ubicación, identidad y evitando que gobiernos o empresas puedan rastrear e identificar a la persona desde dentro de esta red. En este punto es importante diferenciar con la deep web, que se refiere a todo el contenido que no está indexado en los buscadores habituales Google, Yahoo, Bin. La dark web es un término que suelen confundir con la deep web, pero que básicamente es una parte de ella. En la dark web existen mercados negros de todo tipo, donde se venden de forma ilegal variedad de productos y servicios, drogas, armas, datos personales, tarjetas de créditos, servicios de hackers, trata de personas y

Sigue en pág. 68 ►

SHUTTERSTOCK

*Diplomada en Criminología y Criminalística. Especializada en Técnica de Perfilación Criminal.

Tesis de Posgrado: Maestría (D.2.)

D.2.1 Tesis "Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos". Director: Jorge Eterovic. Tesista: Cintia V. Gioia

(Tesis: Tesis Maestria Informatica_Cintia Gioia - vFINAL.pdf)

UNIVERSIDAD NACIONAL DE LA MATANZA

Escuela de Posgrado

Maestría en Informática

Tesis de Maestría

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

Autora: ***Esp. Ing. Cintia Verónica Gioia***

Director de Tesis: ***Mg. Ing. Jorge Esteban Eterovic***

Buenos Aires - Argentina

Junio 2019

Agradecimientos

A mi hija por comprender mis tiempos dedicados a escribir.

A mi marido compañero incondicional en todo momento.

A mis padres por alentarme siempre.

A mi Director de tesis por guiarme, orientarme y ayudarme con sus sabios consejos y gran experiencia.

Al Departamento de Ingeniería e Investigaciones Tecnológicas y a la Secretaría de Ciencia y Tecnología de la Universidad Nacional de la Matanza que me han brindado un gran apoyo y motivación.

A los profesionales amigos que contribuyeron con el aporte de sus puntos de vista, conocimiento, experiencia y consejos.

A todas las personas e instituciones que han contribuido directa o indirectamente a mi formación y desarrollo profesional en el campo de la informática forense.

RESUMEN

En la actualidad la tecnología brinda la posibilidad de recopilar y 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 computación forense en dichas bases, donde se plantea el desafío de obtener evidencia digital válida como medio de prueba para su efectiva sanción dentro de un proceso judicial. Prevenir los riesgos de invalidar una prueba se convierte en una responsabilidad y un reto profesional.

En este trabajo se propone una metodología forense específica para base de datos relacionales basada en una metodología forense informática general que guía, unifica y garantiza la confiabilidad de las actividades que realiza el perito informático centradas en la obtención y el análisis de evidencia digital. Asimismo, se plantea la obtención de evidencia digital a partir de la configuración y ejecución de auditorías de datos universales aplicables a cualquier motor de base de datos. La metodología planteada sobrepasa las limitaciones o retos tecnológicos individuales de cada tipo de base de datos y la dependencia de expertos en dichas tecnologías que ofrecen soluciones según su visión tecnócrata, en ocasiones incluso, sin garantizar la admisibilidad judicial de la evidencia digital.

PALABRAS CLAVE: Evidencia Digital en Base de Datos - Metodología Informática Forense - Metodología Forense en Base de Datos - Auditoría de Información de Base de Datos - Informática Forense

ABSTRACT

The technology currently makes it possible to collect and store a large amount of information in the database and retrieve it in seconds. For this reason, associated computer crimes are growing as well as the need to apply forensic computing on these bases, so the challenge of obtaining valid digital evidence as a means of proof for its effective sanction in a judicial process is raised. It becomes a responsibility and a professional challenge to prevent the risks of invalidating a proof.

This thesis work proposes a specific forensic methodology for a relational database based on a general computer forensic methodology, which guides, unifies and guarantees the reliability of the activities of the computer expert to obtain and analyze the digital evidence. In addition, it is proposed to obtain digital evidence from the result of the configuration and execution of universal data audits applicable to any database engine. The proposed methodology exceeds the individual technological limitations or challenges of each type of database and the dependence of experts on these technologies that offer solutions according to their technocratic vision, sometimes even without guaranteeing the judicial admissibility of digital evidence.

PALABRAS CLAVE: Database Digital Evidence - Forensic Computing Methodology - Database Forensic Methodology - Database Information Audit - Forensic Computing

ÍNDICE DE CONTENIDOS

Detalle y certificados del punto F

#	OEA	Archivo
1	**"Simposio de Ciberseguridad de la OEA 2019" organizado por la OEA (Organización de Estados Americanos))** en coordinación con el **Gobierno de Chile** en **Santiago de Chile.** 24-27 de septiembre de 2019. (Beca otorgada a través de evaluación del Comité Interamericano Contra el Terrorismo y la Secretaría de Seguridad Multidimensional de la OEA, en base a conocimientos y experiencia sobre ciberseguridad, logros académicos y el impacto potencial para el desarrollo de la ciberseguridad en América Latina y el Caribe). **Curso de "Herramientas de inteligencia abierta y aplicación real de las mismas en el Centro Nacional de Respuesta e Incidentes de Seguridad Informática (CERTuy) del Gobierno de Uruguay"** - 16 hs –**. Dictado en el marco del "Simposio de Ciberseguridad de la OEA 2019"** https://oeacybersimposio19.gob.cl/agenda/	OEA Simposio de Ciberseguridad Chile - Certificado Participacion GC.pdf
2	Concursante del **"OEA Cyberwoman Challenge" organizado por la OEA (Organización de Estados Americanos) en Washington DC, Estados Unidos. 24 de septiembre de 2018.**	OEA Cyberwoman Challenge - Certificacion Participante GC.jpg
3	**"Simposio de Ciberseguridad de la OEA 2018" organizado por la OEA (Organización de Estados Americanos) en Washington DC, Estados Unidos.** 24-28 de septiembre de 2018 (Beca otorgada a través de evaluación del Comité Interamericano Contra el Terrorismo y la Secretaría de Seguridad Multidimensional de la OEA, en base a conocimientos y experiencia sobre ciberseguridad, logros académicos y el impacto potencial para el desarrollo de la ciberseguridad en América Latina y el Caribe). **Taller de Informática Forense Avanzado "Law Enforcement - Digital Forensics" -** 16 hs – Instructor: Ing. Gustavo Presman**. Dictado en el marco del "Simposio de Ciberseguridad de la OEA 2018"**	OEA Simposio de Ciberseguridad Washington- Certificado Participacion GC.pdf
4	**"II Foro Internacional de Género y Ciberseguridad"** organizado por la **OEA (Organización de Estados Americanos), INCIBE (Instituto Nacional de Ciberseguridad de España), el Ministerio de Relaciones Exteriores y Cultos y el Ministerio de Modernización**. 29 y 30 de mayo 2018, CABA, Argentina.	OEA Foro Internacional de Género y Ciberseguridad - Certificado Asistencia GC.pdf
#	**REDUNIF**	**Archivo**
5	**Acta de la Asamblea de REDUNIF donde se aprueba la incorporación de UNLAM a la REDUNIF, junio 2019.**	REDUNIF - Acta Tercer Asamblea - Incorporacion de UNLAM.pdf
#	**IRAM**	**Archivo**
6	**Nota de designación de representantes de UNLAM en Comisión de Informática Forense de IRAM firmada por el Rector de UNLAM, 14 de marzo 2019.**	IRAM - DN-FN 017. Rev.02 Comision Inf Forense UNLaM.pdf

1. **Certificado de participación en "Simposio de Ciberseguridad de la OEA 2019" organizado por la OEA (Organización de Estados Americanos) y el Gobierno de Chile en Santiago de Chile. 24-27 de septiembre de 2019.**

OEA Más derechos para más gente

La Organización de los Estados Americanos y el Gobierno de Chile

Otorgan el presente Certificado a:

Gioia Cintia

Por su participación en la actividad

"Simposio de Ciberseguridad de la OEA"

Santiago, Chile, del 24 al 27 de septiembre de 2019

Alison August Treppel
Secretaria Ejecutiva
Comité Interamericano contra el Terrorismo
Organización de los Estados Americanos

Carlos Landeros
Director CSIRT Gobierno,
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

2. **Certificado Concursante en "OEA Cyberwoman Challenge" organizado por la OEA (Organización de Estados Americanos) en Washington DC, 24 de septiembre de 2018.**

3. Certificado de participación en "Simposio de Ciberseguridad de la OEA" organizado por la OEA (Organización de Estados Americanos) en Washington DC, Estados Unidos. 24-28 de septiembre de 2018. Edificio Principal de la OEA.

4. Certificado de Asistencia a "II Foro Internacional de Género y Ciberseguridad" organizado por la OEA (Organización de Estados Americanos), INCIBE (Instituto Nacional de Ciberseguridad de España), el Ministerio de Relaciones Exteriores y Cultos y el Ministerio de Modernización. 29 y 30 de mayo 2018, CABA

Ministerio de Modernización

Buenos Aires, 01 de junio de 2018.

Por medio del presente se deja constancia que la Srita. Cintia V. Gioia, asistió al II Foro Internacional de Género y Ciberseguridad, realizado los días 29 y 30 de mayo de 2018, en el Palacio San Martín, Ciudad Autónoma de Buenos Aires. El evento estuvo organizado por los Ministerios de Modernización y de Relaciones Exteriores y Culto, la Organización de Estados Americanos (OEA) y el Instituto Nacional de Ciberseguridad de España (INCIBE).

Oscar Morotti
Director de Infraestructuras Críticas
de Información y Ciberseguridad

5. Acta de la Asamblea de REDUNIF donde se aprueba la incorporación de UNLAM a la REDUNIF, 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.

6. 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
N° 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
N° 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 el N° 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.

UNIVERSIDAD NACIONAL DE LA MATANZA

DR. DANIEL EDUARDO MARTÍNEZ
RECTOR
UNIVERSIDAD NACIONAL DE LA MATANZA

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*

DN-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: secretarianorm@iram.org.ar

DN-FN 017 REV: 02

Detalle y certificados del punto G

#	Certificados de participación como exponente 2018	Archivo
1	Exposición en "**Jornada Hablemos de Grooming en Argentina"** organizada por la Diputada Nacional María Gabriela Burgos, el Senador Dalmacio Mera, el Programa de Modernización de la HCDN Honorable Cámara de Diputados de la Nación y la ONG Mamá en Línea en el marco del Día Nacional de la lucha contra el Grooming. Integrante del panel de expertos junto con la Fiscal Daniela Dupuy, a cargo de la Fiscalía Especializada en Delitos Informáticos de CABA, Ricardo Holovat (Arsat) y Brian Arroyo (Policía Ciudad). **13 de noviembre de 2018 en Auditorio de la HCDN del Senado de la Nación.** Link: https://www.youtube.com/watch?v=QbvjkYpMk7w&feature=share&fbclid=IwAR2mv0jnIIdgVIZgRm4a5VUA0vkx4U_CZplH_--OBYK0wY-ANXy7jcVAfmFc&app=desktop	Senado de la Nacion-Hablemos de Grooming en Argentina - Invitacion a Exponer GC.pdf
#	**Certificados de organización de eventos 2018**	**Archivo**
2	**Jornada de "Cibercrimen y los Rastros Digitales: Desafíos en la Investigación del Cibercrimen y la Práctica Forense Informática".** 14 de noviembre de 2018. Aula Magna. **UNLAM**.	Jornada Cibercirmen y los Rastros Digitales - UNLAM - Certificado Organizador GC.pdf
#	**Certificados de asistencia a conferencias, jornadas y cursos 2018**	**Archivo**
3	**"Conferencia OSINT Latam 2018".** Organizado por **Osint Latam Group**. 5 y 6 de diciembre de 2018, CABA, Argentina.	Osint Latam Conference - Certificado Asistencia GC.pdf
4	**Jornada de "Cibercrimen y los Rastros Digitales: Desafíos en la Investigación del Cibercrimen y la Práctica Forense Informática".** 14 de noviembre de 2018. Aula Magna. **UNLAM**.	Jornada Cibercrimen y los Rastros Digitales - UNLAM - Certificado Asistencia MK.pdf Jornada Cibercrimen y los Rastros Digitales - UNLAM - Certificado Asistencia SC.pdf
5	**"Jornada sobre Cibercrimen y Evidencia Digital".** Organizado por la Unidad Ameripol de la Gendarmería Nacional. 22 de octubre de 2018, CABA, Argentina.	Jornada sobre Cibercrimen y Evidencia Digital - Gendarmeria - Certificado Asistencia GC.pdf
6	**"Coltic 2018: 9° Congreso Latinoamericano de Técnicas de Investigación Criminal".** Inteligencia artificial y nuevas tecnologías en la prevención e investigación del delito. Organizado por la **Escuela de Derecho Penal y Ciencias Forenses Aplicadas**. 3-5 de octubre de 2018, CABA, Argentina.	COLTIC 2018 - Certificado Asistencia GC.pdf
7	**"1er Entrenamiento Anual De Cibercrimen Para Funcionarios Públicos"** organizado por la Dirección General de Prevención e Investigación de los Delitos Tecnológicos de la **Policía de la Ciudad de Buenos Aires y la Unidad de Enlace del Consejo de Seguridad y Prevención del Delito**. 25 de junio 2018, CABA, Argentina.	Entrenamiento Cibercrimen para Funcionarios Publicos - Certificado Asistencia GC.pdf
8	Jornada sobre "**Delitos contra la Infancia en la Web**" organizado por el Senador Nacional y presidente de la Comisión de Asuntos Constitucionales, Dr. Dalmacio Mera, conjuntamente con la ONG Mamá en Línea, **Senado Argentina**. 17 de mayo 2018, CABA, Argentina.	Senado de la Nacion-Delitos contra la Infancia en la Web - Invitacion GC.jpg
9	"**LXXXV Congreso y Feria Iberoamericana de Seguridad de la Información**". **SEGURINFO 2018**. 24 de abril 2018, CABA, Argentina.	SegurInfo 2018 - Certificado Asistencia GC.pdf
10	Asistencia **"2ª Conferencia Nacional de Informática Forense" (InFo-Conf 2018).** Organizada por **Info-Lab** Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense de la Universidad Fasta con auspicio de la Procuración General (Suprema Corte de Justicia de la Provincia de Buenos Aires), 12 y 13 de abril de 2018, Mar del Plata, Argentina.	InfoConf - 2da Conferencia de Inf Forense - Certificado Asistencia GC.pdf
11	**"I Jornada de Investigación sobre Informática Forense"**, organizada por la Universidad Católica de Salta (**UCASAL**), 26 de marzo de 2018, CABA, Argentina.	Jornada de Investigacion sobre Informatica Forense - UCASAL - Certificado Asistencia GC.pdf Jornada de Investigacion sobre Informatica Forense - UCASAL - Certificado Asistencia SI.pdf
12	**Curso de "Informática Forense Nivel I"** correspondiente a la Especialización en Informática Forense e Investigación Digital del 4 de abril al 20 de junio de 2018. Universidad del CEMA, CABA, Argentina.	Curso Informatica Forense 1 UCEMA - Certificado Aprobacion GC.pdf

#	Exposiciones y entrevistas 2019	Archivo
13	**Exposición en Tercer Encuentro del Ciclo de Videoconferencias de Ciberseguridad organizado por País Digital, Secretaría de Modernización** para todos los Puntos Digitales del país. Charla sobre **"Prevención del Grooming y la Pornografía Infantil".** 27 de noviembre de 2019. CABA, Argentina. Link: https://youtu.be/ogJzfnISO60	-
14	**Expositora en XIX Congreso Argentino de Psiquiatría Infanto-Juvenil y Profesiones Afines organizado por AAPI** sobre **"Delitos Sexuales contra la Infancia en Medios Digitales".** 15 de agosto de 2019	XIX Congreso Argentino de Psiquiatría API – CG.pdf
15	**Entrevista en programa Resumen parlamentario, Senado TV sobre "Privacidad de Datos, Redes Sociales y Fraudes Financieros".** 14 de agosto de 2019. **Senado de la Nación**. CABA, Argentina. Link: https://youtu.be/YF8Y6TnjXoU.	-
16	**Entrevista en Radio Universidad FM 89.1 sobre "Grooming y Pornografía Infantil".** 26 de julio de 2019. **UNLaM.**	-
17	**Entrevista en programa Resumen parlamentario, Senado TV sobre "Delitos sexuales contra menores en medios digitales".** 5 de Junio de 2019. **Senado de la Nación**. CABA, Argentina. Link: https://youtu.be/fAF3UoQwkMQ.	-
18	Expositora en evento "**La Mujer en el campo de la Seguridad**" organizado por el **Capítulo 215 Buenos Aires** y el **Comité de Mujeres en Seguridad** (**Women In Security - WIS**) de **ASIS International**, dedicado a la memoria de Eliana Krawczyk, Primera Submarinista argentina y tripulante del ARA SAN JUAN, sobre "**Grooming y Delitos contra la infancia en Medios Digitales**". 8 de marzo de 2019 en Edificio Pampa Energía, Maipú 1, CABA.	Jornada Mujer en Campo de Ciberseguridad WIS - CG.pdf
#	**Certificados de Chair y Session Chair**	**Archivo**
19	**Chair** en la categoría **"Aspectos Legales y Profesionales**", Artículos de Inv. en el VII Congreso Nacional de Ingeniería Informática – Sist. de Información. **CONAIISI 2019**. 14-15 de noviembre de 2019. **UNLAM**.	CONAISSI - Chair - Aspectos Legales y Profesionales.pdf
20	**Session Chair** en la categoría **"Aspectos Legales y Profesionales**", Artículos de Inv. en el VII Congreso Nacional de Ingeniería Informática – Sist. de Información. **CONAIISI 2019**. 14-15 de noviembre de 2019. **UNLAM**.	CONAISSI - Session Chair - Aspectos Legales y Profesionales.pdf
#	**Certificados de asistencia a conferencias, jornadas y cursos 2019**	**Archivo**
21	"**ARGENSIG 2019. Tercera Escuela Argentina de Gobernanza de Internet"** organizada por la **Cancillería Argentina** en conjunto con Centro de Capacitación en Alta Tecnología (**CCAT LAT**) y la Escuela del Sur de Gobernanza de Internet (**SSIG**).15 al 17 de octubre de 2019, CABA, Argentina.	ARGENSIG Certificado - CG.pdf
22	**"e-GISART - 6ta Edición"** organizado por **ADACSI** (Asociación de Auditoría y Control de Sistemas de Información)- **ISACA Chapter Bs. As.** 19 de septiembre de 2019, Hotel 725 Continental, CABA, Argentina.	-
23	**"2do Taller Internacional de Lucha contra el Ciberdelito"** organizado por la **Dirección de Investigaciones del Ciberdelito del Ministerio de Seguridad de la Nación**. 10 y 11 de septiembre de 2019, CABA, Argentina.	2do Taller Internacional Lucha Ciberdelito - CG.pdf
24	**"3ra Conferencia Nacional de Informática Forense" (InFo-Conf 2019)** de la **REDUNIF**. Organizada por la Universidad Nacional de Córdoba (UNC) y el FCEFyN el 6 y 7 de junio de 2019, Córdoba, Argentina.	InfoConf2019 - Certificado Asistencia GC.pdf / InfoConf2019 - Certificado Asistencia JA.pdf
25	Curso de "**Litigación en casos de cibercrimen**" – 8 hs. Dictado en el marco de la 3ra Conferencia Nacional de Informática Forense **Info-Conf 2019**. 6 y 7 de junio de 2019. Córdoba, Argentina. Universidad Nacional de Córdoba	InfoConf2019 - Certificado Curso Litigacion GC.pdf
26	**"2do Entrenamiento Anual De Cibercrimen Para Funcionarios Públicos"** organizado por la Dirección General de Prevención e Investigación de los Delitos Tecnológicos de la **Policía de la Ciudad de Buenos Aires y la Unidad de Enlace del Consejo de Seguridad y Prevención del Delito**. 9 y 10 de mayo de 2019, CABA, Argentina.	2do Entrenamiento Anual Cibercrimen - CG.pdf
27	**Entrenamiento DFIR - Digital Forensics** – 20 hs – Marzo 2019 – Instructores: Ing. Emiliano Moraña y Marcelo Romero. Curso Online	-
28	Evento "**La Mujer en el campo de la Seguridad**" organizado por el **Capítulo 215 Buenos Aires** y el **Comité de Mujeres en Seguridad** (**Women In Security - WIS**) de **ASIS International**, 8 de marzo de 2019 en Edificio Pampa Energía, Maipú 1, CABA.	Jornada Mujer en Campo de Ciberseguridad WIS - MK.pdf

1.Invitación a Exposición en "Jornada Hablemos de Grooming en Argentina", 13 de noviembre de 2018 en Auditorio de la HCDN del Senado de la Nación.

Invitación a exponer en la Jornada "Hablemos de Grooming en Argentina" #13Ngrooming Recibidos ×

María Gabriela Burgos mburgos@hcdn.gob.ar a través de ingunlamedu.onmicrosoft.com mié., 7 nov. 2018 15:20

para cgioia

Estimada Cintia Gioia,

Nos dirigimos a usted a fin de invitarla a participar como disertante en la jornada **"Hablemos de Grooming en Argentina" #13Ngrooming"** que realizaremos conjuntamente con el Senador Dalmacio Mera, el Programa de Modernización de la HCDN y la ONGs Mama en Linea, el próximo martes 13 de noviembre de 9:30 a 12:00 hs en el Auditorio de la HCDN, en el marco del Dia Nacional de la lucha contra el Grooming.

A la espera de una respuesta favorable, la saludamos atentamente.

Despacho
Diputada Nacional Dra. Maria Gabriela Burgos

DIPUTADOS
ARGENTINA

2.Certificado de Organización de Jornada de "Cibercrimen y los Rastros Digitales: Desafíos en la Investigación del Cibercrimen y la Práctica Forense Informática". 14 de noviembre de 2018. Aula Magna. UNLAM.

3.Certificado de Asistencia "Conferencia OSINT Latam 2018". Organizado por Osint Latam Group. 5 y 6 de diciembre de 2018, CABA, Argentina.

4.Certificados de Asistencia a Jornada de "Cibercrimen y los Rastros Digitales: Desafíos en la Investigación del Cibercrimen y la Práctica Forense Informática". 14 de noviembre de 2018. Aula Magna. UNLAM.

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

Cibercrimen y los Rastros Digitales

San Justo, 14 de Noviembre de 2018

Se certifica que

Mario Krajnik

DNI: 17.036.268

asistió a la Jornada *"Cibercrimen y los Rastros Digitales: Desafíos en la Investigación del Cibercrimen y la Práctica Forense Informática"*, realizada en esta Casa de Altos Estudios el 14 de Noviembre de 2018.

Mg Gabriel Blanco
Vice Decano

Mg Osvaldo Sposito
Decano

Universidad Nacional de La Matanza

DIIT Departamento de Ingeniería e Investigaciones Tecnológicas

Cibercrimen y los Rastros Digitales

San Justo, 14 de Noviembre de 2018

Se certifica que

Sergio Daniel Conde

DNI: 16513412

asistió a la Jornada *"Cibercrimen y los Rastros Digitales: Desafíos en la Investigación del Cibercrimen y la Práctica Forense Informática"*, realizada en esta Casa de Altos Estudios el 14 de Noviembre de 2018.

Mg Gabriel Blanco
Vice Decano

Mg Osvaldo Sposito
Decano

5.Certificado de Asistencia a "Jornada sobre Cibercrimen y Evidencia Digital". Organizado por la Unidad Ameripol de la Gendarmería Nacional. 22 de octubre de 2018, CABA, Argentina.

REPÚBLICA ARGENTINA
GENDARMERÍA NACIONAL

CERTIFICADO

La Unidad Ameripol de Gendarmería Nacional
otorga el presente certificado de asistencia a:

Cintia GIOIA

por haber participado de la "Jornada sobre Cibercrimen y Evidencia Digital"
dictada por esta Institución en el marco de las acciones de
capacitación y lucha contra el cibercrimen .-

Buenos Aires, 22 de octubre de 2018.-

PEDRO HERNÁNDEZ
COMANDANTE PRINCIPAL
JEFE UNA AMERIPOL GNA

JAVIER ALBERTO LAPALMA
COMANDANTE GENERAL
DIRECTOR DE INVESTIGACIÓN GNA

6.Certificado de Asistencia a "Coltic 2018: 9° Congreso Latinoamericano de Técnicas de Investigación Criminal". Inteligencia artificial y nuevas tecnologías en la prevención e investigación del delito. Organizado por la Escuela de Derecho Penal y Ciencias Forenses Aplicadas. 3-5 de octubre de 2018, CABA, Argentina.

Coltic 2018

9º Congreso Latinoamericano de Técnicas de Investigación Criminal

"Inteligencia artificial y nuevas tecnologías en la prevención e investigación del delito"

3 al 5 de Octubre - Asoc. Médica Argentina • Av. Santa Fé 1171 • CABA

Se certifica que

Cintia Gioia

ha participado en carácter de ASISTENTE

Dr. Manuel de Campos
Comité Organizador

Dr. Fernando Cardini
Comité Organizador

Organizan:

www.coltic.com.ar • info@coltic.com.ar

Realiza:

7.Certificado de Asistencia a "1er Entrenamiento Anual De Cibercrimen Para Funcionarios Públicos". Dir. Gral. de Prevención e Inv. de Delitos Tecnológicos de la Policía CABA y la Unidad de Enlace del Consejo de Seguridad y Prevención del Delito. 25 de junio 2018. CABA.

POLICÍA DE LA CIUDAD

SUPERINTENDENCIA DE INVESTIGACIONES

DIRECCION GENERAL DE PREVENCION EN INVESTIGACION DE LOS DELITOS TECNOLOGICOS

CINTIA VERONICA GIOIA

Asistió al **" I ENTRENAMIENTO ANUAL DE CIBERCRIMEN PARA FUNCIONARIOS PUBLICOS"**, organizado por la *Dirección General de Prevención e Investigación de los Delitos Tecnológicos de la Policía de la Ciudad de Buenos Aires* y la *Unidad de Enlace del Consejo de Seguridad y Prevención del Delito.*

CIUDAD AUTÒNOMA DE BUENOS AIRES, 25 DE JUNIO DEL 2018

Comisionado Mayor Simón Rodrigo
Jefe Departamento de Investigación Informática.
POLICIA DE LA CIUDAD

Comisionado General Carlos Gabriel Rojas
Director de Prevención e Investigación de los Delitos Tecnológicos.
POLICIA DE LA CIUDAD

Ezequiel Sallis
Auxiliar A
POLICIA DE LA CIUDAD

8.Jornada sobre "Delitos contra la Infancia en la Web" organizado por el Senador Nacional y presidente de la Comisión de Asuntos Constitucionales, Dr. Dalmacio Mera, conjuntamente con la ONG Mamá en Línea, Senado Argentina. 17 de mayo 2018, CABA, Argentina.

SENADO
ARGENTINA

El Senador Nacional y Presidente de la Comisión de Asuntos Constitucionales,
Dr. Dalmacio Mera, conjuntamente con la ONG Mamá en Línea
tienen el agrado de invitar a usted a la
Jornada sobre "Delitos contra la Infancia en la Web".

Este encuentro se llevará a cabo el jueves 17 de mayo a las 08:45 horas
en el Salón Arturo Illia del Palacio Legislativo.

S.R.C.
Tel.: (011) 2822-5812
despacho.mera@gmail.com

Rogamos presentar esta tarjeta
H. Yrigoyen 1849, 1º Piso
Ciudad Autónoma de Buenos Aires

9.Certificado de Asistencia a "LXXXV Congreso y Feria Iberoamericana de Seguridad de la Información". SEGURINFO 2018. 24 de abril 2018, CABA, Argentina.

SEGURINFO ARGENTINA 2018

LXXXV Congreso y Feria Iberoamericana de Seguridad de la Información

24 de abril, Centro de Convenciones, Sheraton Buenos Aires Hotel

Cintia Verónica Gioia

ha asistido a la Octogésima Quinta Edición del *Congreso y Feria Iberoamericana de Seguridad de la Información*, en carácter de **Participante**.

Cosme Belmonte
Presidente Comité Académico
SEGURINFO

Juan José Dell´Acqua
Presidente
SEGURINFO

10.Certificado de Asistencia "2ª Conferencia Nacional de Informática Forense" (InFo-Conf 2018). Organizada por Info-Lab con auspicio de la Procuración General (Suprema Corte de Justicia de la Prov. de Bs. As), 12 y 13 de abril de 2018, Mar del Plata, Argentina.

11.Certificados de Asistencia a "I Jornada de Investigación sobre Informática Forense", organizada por la Universidad Católica de Salta (UCASAL), 26 de marzo de 2018, CABA, Argentina.

12 Certificado de.Curso de "Informática Forense Nivel I" correspondiente a la Especialización en Informática Forense e Investigación Digital del 4 de abril al 20 de junio de 2018. Universidad del CEMA, CABA, Argentina.

14. Certificado de exposición en XIX Congreso Argentino de Psiquiatría Infanto-Juvenil y Profesiones Afines organizado por AAPI (Asociación de Psiquiatría Infanto-Juvenil) sobre "Delitos Sexuales contra la Infancia en Medios Digitales". 15 de agosto de 2019.

XIX Congreso Argentino de Psiquiatría Infanto-Juvenil y Profesiones Afines

Desafíos actuales en la Clínica Infanto-Juvenil. Abordajes integrativos en la práctica profesional.

Por cuanto

CINTIA GIOIA

ha participado en el

XIX Congreso Argentino de Psiquiatría Infanto-Juvenil y Profesiones Afines

en calidad de

DISERTANTE

'Delitos Sexuales contra la Infancia en Medios Digitales'

se le extiende el presente Certificado.

Buenos Aires, 16 de agosto de 2019

Dr. Pedro Kestelman
Comité Científico

Dra. Celina R. Fabrykant
Presidente AAPI

15 y 16 Agosto 2019

18. Certificado de exposición en evento "La Mujer en el campo de la Seguridad" organizado por el Capítulo 215 Buenos Aires y el Comité de Mujeres en Seguridad (Women In Security - WIS) de ASIS International.

ASIS INTERNATIONAL® | Buenos Aires, Argentina Chapter

Por el presente Diploma certificamos la participación de

Esp. Ing. Cintia Verónica Gioia

en la actividad *"La Mujer en el Campo de la Seguridad"*, en calidad de ***Instructora***, organizada por el Comité Mujeres en Seguridad - WIS del Capítulo 215 – Buenos Aires, Argentina, de **ASIS International**.

Fecha: 8 de marzo de 2019
Lugar: Edificio Pampa Energía, Ciudad de Buenos Aires
Tema: Certificación y Desarrollo Profesional
Duración: 180 min.

José G. Barone, PSP	Alejandro Liberman, CPP	Ali Ferrer, CPP, PSP	Lucas de la Rosa
Presidente	Vicepresidente	Secretario	Tesorero
ASIS Capítulo 215	ASIS Capítulo 215	ASIS Capítulo 215	ASIS Capítulo 215

19.Certificado de Chair en la categoría "Aspectos Legales y Profesionales", Artículos de Inv. en el VII Congreso Nacional de Ingeniería Informática – Sist. de Información. CONAIISI 2019. 14-15 de noviembre de 2019. UNLAM.

20.Certificado de Session Chair en la categoría "Aspectos Legales y Profesionales", Artículos de Inv. en el VII Congreso Nacional de Ingeniería Informática – Sist. de Información. CONAIISI 2019. 14-15 de noviembre de 2019. UNLAM.

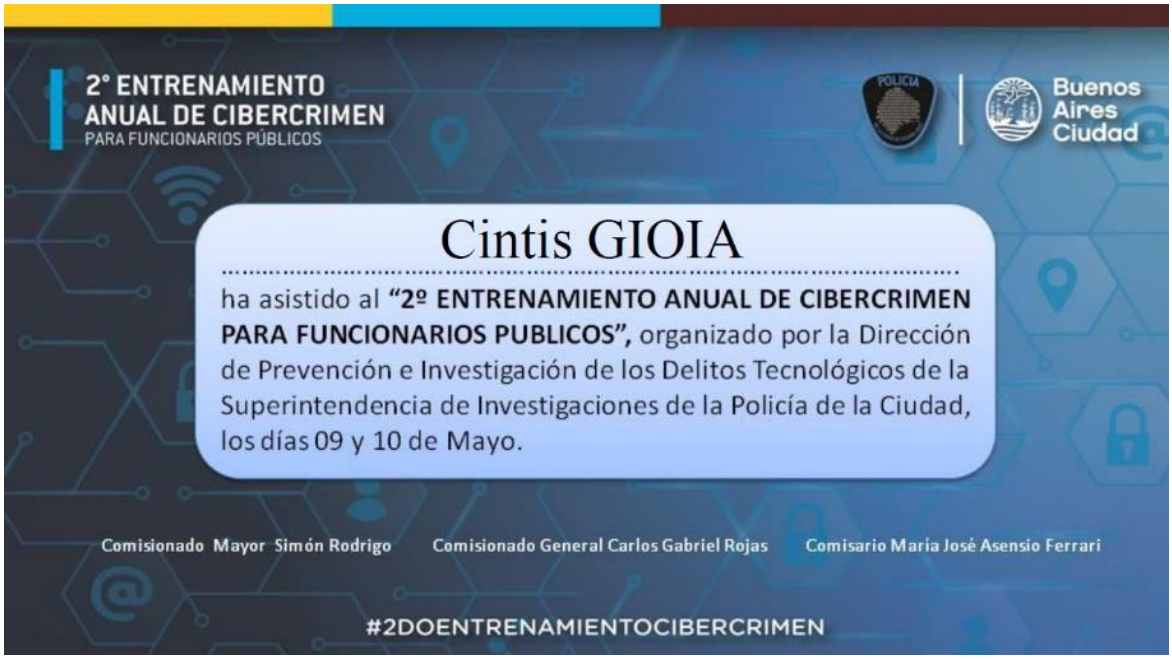
21.Certificado de Asistencia a "ARGENSIG 2019.

23.Certificado de Asistencia a "2do Taller Internacional de Lucha contra el Ciberdelito" organizado por la Dirección de Investigaciones del Ciberdelito del Ministerio de Seguridad de la Nación.

24.Certificado de Asistencia a "3ra Conferencia Nacional de Informática Forense" (InFo-Conf 2019) de la REDUNIF.

25.Certificado de Asistencia a Curso de "Litigación en casos de cibercrimen" – 8 hs. Dictado en el marco de la 3ra Conferencia Nacional de Informática Forense InfoConf 2019.

26.Certificado de Asistencia a "2do Entrenamiento Anual De Cibercrimen Para Funcionarios Públicos" organizado por la Dirección General de Prevención e Investigación de los Delitos Tecnológicos de la Policía de la Ciudad de Buenos Aires y la Unidad de Enlace del Consejo de Seguridad y Prevención del Delito.



28.Certificado de Asistencia a Evento "La Mujer en el campo de la Seguridad" organizado por el Capítulo 215 Buenos Aires y el Comité de Mujeres en Seguridad (Women In Security - WIS) de ASIS International.

ASIS INTERNATIONAL® | Buenos Aires, Argentina Chapter

Por el presente Diploma certificamos la participación de

Mario Krajnik

en la actividad *"La Mujer en el Campo de la Seguridad"*,
organizada por el Comité Mujeres en Seguridad - WIS
del Capítulo 215 – Buenos Aires, Argentina, de **ASIS International**.

Fecha: 8 de marzo de 2019
Tema: Certificación y Desarrollo Profesional
Expositoras: Lic. Silvina Urreaga, Esp. Ing. Cintia V. Gioia, Lic. Graciela Pataro, May. Gladys Martínez y Lic. Laura Quiñones Urquiza
Duración: 180 min.

José G. Barone, PSP	Alejandro Liberman, CPP	Ali Ferrer, CPP, PSP	Lucas de la Rosa
Presidente	Vicepresidente	Secretario	Tesorero
ASIS Capítulo 215	ASIS Capítulo 215	ASIS Capítulo 215	ASIS Capítulo 215