JORNADAS FEDERALES DE CIBERSEGURIDAD

ING. ROBERTO GIORDANO

Decano de la Facultad de Ingeniería de la Universidad FASTA de Mar Del Plata

"LA OBTENCIÓN DE EVIDENCIA DIGITAL EN EL PROCESO JUDICIAL"

Santa Cruz Gobierno de la Provincia · UTN Facultad Regional Santa Cruz · UNPA UARG · Jefatura de Gabinete de Ministros Argentina · Dirección Nacional de Ciberseguridad · Datastar · NUTANIX

La obtención de evidencia digital en el proceso judicial

Ing. Roberto Giordano Lerena

AGENDA

- ✓ Mundo Digital
- ✓ Informática Forense
- ✓ El profesional de informática en la investigación criminal
- ✓ Evidencia Digital
- ✓ El Modelo PURI
- ✓ Bibliografía

El pronóstico de mundo digital

"Ser digital es diferente.

No se trata de una invención, sino que está aquí y ahora.

Podríamos decir que es genético por naturaleza, ya que cada generación será más digital que la que la precede".

Nicholas Negroponte. Being Digital. 1995.

El mundo digital

La explosión de las tecnologías de la información y la comunicación ha transformado nuestras vidas, nuestra sociedad, nuestra cultura, "digitalizándonos". Ya nadie duda que somos "digitales", irreversiblemente "digitales".

El mundo, tal como lo percibimos, sigue siendo un lugar estrictamente analógico. Desde un punto de vista macroscópico, no es digital en absoluto, sino continuo. No obstante, está cada vez más soportado por información digital.

En cientos de situaciones que vivimos a diario interactuamos de diversas maneras con la tecnología de la información y la comunicación.

El mundo digital

Por el solo hecho de vivir en sociedad, en el “mundo digital”, consumimos y producimos información digital (o provocamos su producción). Y en ese ser y vivir digital, dejamos permanentemente huellas o “rastros digitales”; información digital que habla de nosotros y de nuestras acciones. Evidencias digitales de nuestro paso por la vida.

La informática forense posibilita la detección y recuperación de la información digital que sirve de evidencia a la hora de reconstruir un hecho o sucesión de ellos. La actuación forense en informática permite recuperar y enhebrar esos rastros digitales de nuestro paso por la vida, garantizando su valor probatorio.

Informática en la Forensia

- ✓ **Informática Aplicada**

Auxilio al Proceso Forense (ADN, Análisis, Simulaciones, etc.) y a la Investigación Criminal (UFED, I2, Investiga).

- ✓ **Informática Forense (Según InFo-Lab)**

Es la aplicación forense de las ciencias informáticas.
Es una rama de las ciencias forenses que trabaja con datos que han sido procesados electrónicamente y guardados en un medio computacional.
Persigue descubrir cómo fueron las cosas, qué pasó y cómo probarlo.

Es el uso de Tecnologías de la Información para recuperar "evidencia digital".

Informática Forense

- ✓ Según **INTERPOL**: Es una rama de las ciencias forenses que se encarga de la identificación, adquisición, procesamiento, análisis y presentación de datos almacenados en una computadora, dispositivos digitales o cualquier otro medio de almacenamiento digital.
- ✓ Según el **National Institute of Standards and Technology** (NIST): Análisis Forense Digital es el campo de la ciencia forense que se ocupa de recuperar, almacenar y analizar datos electrónicos que pueden ser útiles en investigaciones criminales. Incluye información de computadoras, teléfonos móviles y otros dispositivos de almacenamiento de datos.

Informática Forense

- ✓ Forensia en Equipos *(Computer Forensics)*
- ✓ Forensia en Dispositivos Móviles *(Mobile Devices Forensics)*
- ✓ Forensia en Redes *(Networking Forensics)*
- ✓ Forensia en Análisis de Datos *(Forensic Data Analysis)*
- ✓ Forensia en Bases de Datos *(Database Forensics)*

Computer Forensics

Involucra el análisis Forense sobre computadoras y dispositivos de almacenamiento persistente y volátil.

- ✓ Recuperación de archivos existentes (activos y eliminados): Audio, texto, video, imágenes, base de datos, configuración, entre otros.
- ✓ Recuperación de archivos eliminados desde el FileSystem
- ✓ Recuperación de archivos eliminados por Carving de Disco (reconst. desde fragmentos)
- ✓ Recuperación de la actividad de un usuario en Internet (logs, cookies, marcadores)
- ✓ Recuperación de la actividad de un usuario en el equipo (archivos de registro, configuración)
- ✓ Recuperación y análisis de datos de procesos en memoria volátil.
- ✓ Análisis rápido mediante herramientas de Triage

Mobile Device Forensics

Implica la recuperación de la información contenida en un dispositivo móvil. La diferencia con la *computación forense* reside en que estos dispositivos pueden contener información de comunicaciones, sistemas de almacenamiento propietarios y mayor dificultad en el acceso a la información por las características propias de seguridad.

- ✓ Extracción de Información del Equipo, Listado de Contactos, Registro de llamadas entrantes/salientes, Reporte de mensajes enviados/recibidos (SMS), Redes Inalámbricas, Reporte de Navegación: Información de geo-referenciación, cookies, cuentas de usuario.
- ✓ Extracción de archivos (Audio, Imágenes, Video, Texto, Base de Datos, Configuraciones), Aplicaciones (Facebook, WhatsApp, Twitter, etc)

Networking Forensics

Está relacionado con la supervisión y análisis del tráfico de Red de equipos, tanto LAN como WAN/Internet, con el fin de recopilar evidencia digital y/o detectar intrusos.

- ✓ Intercepción, Análisis, Filtrado y Almacenamiento de paquetes de red.
- ✓ Análisis Forense de Routers Domiciliarios.
- ✓ Análisis Forense de Routers Empresariales.
- ✓ Análisis Forense en Wireless.
- ✓ Análisis Forense en Voice-IP.
- ✓ Análisis Semántico de los paquetes almacenados.

Computer Forensics Data Analysis

Aborda la detección de patrones de comportamiento en los datos estructurados (bases de datos, datos de aplicaciones), con el fin de determinar los procesos de su producción/manipulación. Interrelación con la Inteligencia Computacional.

- ✓ Búsqueda de información en aplicaciones
- ✓ Búsqueda de información en bases de datos
- ✓ Detección de comportamiento inusual en aplicaciones
- ✓ Uso de técnicas de inteligencia computacional para la detección de actividades mediante patrones de comportamiento.

Data Base Forensics

Aborda el estudio forense de Bases de Datos y sus metadatos relacionados.

- ✓ Análisis Forense de TimeStamp de Registros
- ✓ Análisis Forense de datos guardados en caché
- ✓ Análisis Forense de Auditoría

Informática Forense

Todas las ramas forenses están relacionadas entre sí.

Ante la ocurrencia de un hecho en el que interviene un dispositivo, se requiere la actuación de profesionales informáticos forenses para detectar y recuperar las evidencias respetando buenas prácticas.

Requiere profesionales especialistas…

La necesidad de pericias informáticas

La demanda de pericias informáticas (actuación forense) por parte de la justicia es cada vez mayor, y crece permanentemente, dado que los rastros digitales se multiplican y son cada vez más importantes y determinantes en la investigación.

La necesidad de evidencias digitales válidas que permitan reconstruir los hechos por parte de la justicia es evidente e imperiosa, y la responsabilidad de la justicia respecto de la incorporación de estas evidencias digitales al proceso investigativo y de administrar justicia es ineludible.

El profesional de la informática en la investigación criminal

En la actuación forense o pericia se deben obtener evidencias, a fin de reconstruir la real sucesión de los hechos estudiados.

El perito informático debe trabajar con diferentes tecnologías, diversos métodos de almacenamiento, tecnologías que naturalmente eliminan evidencias, mecanismos de protección de la información, ausencia de herramientas específicas, herramientas que cubren sólo una parte del proceso, diferentes sistemas de criptografía, y otros obstáculos, siempre garantizando un proceso reproducible de adquisición, examinación, análisis, preservación y presentación de la evidencia para que tenga valor probatorio.

El profesional de la informática en la investigación criminal

La Informática Forense demanda de personal entrenado en la materia, que pueda actuar metódicamente, mantener la cadena de custodia y no contaminar la prueba, principios forenses básicos. Con conocimientos de…

- ✓ Sistemas Operativos (nuevos productos y nuevos protocolos implican nuevas formas de registrar y recuperar la información. => Nuevas herramientas).
- ✓ Dispositivos, Redes y Comunicaciones (PCs, teléfonos, routers, etc).
- ✓ Aplicaciones y Bases de datos (rastros de aplicaciones, balística digital, ing. inversa).
- ✓ Viejas y nuevas técnicas de análisis y recuperación (Inteligencia Computacional).
- ✓ Retroalimentación con la seguridad informática y ciberdefensa (saber qué pasó para prevenir y evitar nuevas ocurrencias).

El profesional de la informática en la investigación criminal

Se requiere de profesionales altamente calificados desde lo técnico y respetuosos de los procedimientos que fijan los códigos procesales para la actuación forense. El profesional de la informática puede contribuir a la investigación desde diferentes roles:

Rol de Asesoramiento: El fiscal o el director de la investigación puede necesitar la opinión de un experto para desarrollar las tareas investigativas o probatorias. *Por ejemplo, planificar la ejecución de un registro domiciliario, precisar los datos que han de requerirse a un proveedor de servicios, fijar puntos de pericia o interrogar al perito de la contraparte.*

El profesional de la informática en la investigación criminal

Rol de Asesoramiento (preguntas típicas):

¿Dónde se puede encontrar evidencia digital?

¿Cómo planificar un secuestro?

¿Dónde están los datos?

El profesional de la informática en la investigación criminal

Rol Investigativo: Colaboración en la instrucción de la investigación. Intervención del especialista informático para ejecutar medidas de investigación. Participación en Investigaciones Digitales.
Por ejemplo, secuestro de equipos informáticos, volcados de memoria, obtención de imágenes de disco, etc.).

Rol Pericial: El especialista informático aporta sus conocimientos especiales para conocer o apreciar algún hecho o circunstancia pertinentes a la causa (art. 244 CPP): Adquirir, extraer, analizar y presentar evidencia digital.
Por ejemplo, recuperación de la evidencia digital.

Evidencia Digital

Es cualquier información almacenada o transmitida en formato digital, útil en una investigación judicial. Reside en un soporte físico, pero no es el soporte físico en sí.

- ✓ Evidencia de transición (Medio para… Ej: una dirección IP) => *Función orientadora*
- ✓ Evidencia probatoria (Prueba en juicio. Ej: una archivo alojado en una Tablet o en un Celular) *=> Función probatoria*

Evidencia Digital

Características

- ✓ Es intangible.
- ✓ Es preciso utilizar técnicas de resguardo de su integridad.
- ✓ Puede duplicarse tantas veces como sea necesario, y las copias son idénticas al original.

Evidencia Digital (en el tiempo)

En el proceso de obtención se presentan 2 contextos temporales:

- ✓ Sistema apagado: datos persistentes. Ej.: Forensia en BD, en Equipos, en Dispositivos Móviles.
- ✓ Sistema vivo: datos volátiles. Ej.: Forensia en Memoria, en Redes.

El manejo de la Evidencia Digital (Principios Generales)

Relevancia: La evidencia debe ser útil para las necesidades investigativas y/o los puntos probatorios de cada caso concreto. No ser sobre-abundante o superflua (ej. art. 338 del CPP provincia BA). Este principio opera fundamentalmente como criterio de selección de evidencia.

Suficiencia: Las evidencias obtenidas y eventualmente analizadas deberían ser suficientes para lograr los fines investigativos.

Validez legal: Para que la evidencia sea admisible, debe haber sido obtenida respetando las garantías y formas legales.

Confiabilidad: Para asegurar la confiabilidad debemos garantizar que el proceso sea auditable, repetible, reproducible y justificable.

El manejo de la Evidencia Digital (Principios Forenses)

Principios Forenses

- ✓ Evitar la contaminación
- ✓ Controlar la Cadena de Custodia (Destino de los efectos)
- ✓ Actuar metódicamente

El análisis forense trata de extraer información significativa, evidencia digital, manteniendo las huellas evidenciales.

El manejo de la Evidencia Digital

Para evitar la contaminación

- ✓ Minimizar el manejo de los dispositivos originales.
- ✓ Minimizar el manejo de la evidencia digital potencial. Siempre que sea posible, trabajar sobre la imagen forense, y no sobre el original.
- ✓ Responsabilizarse de los cambios realizados y documentar todas las acciones realizadas.
- ✓ No actuar más allá de sus competencias.

El manejo de la Evidencia Digital (Características del proceso)

Auditable: Documentar todas las acciones que realizan y justificar sus decisiones en las etapas del proceso.

Repetible: Se deben obtener los mismos resultados si se aplica el mismo procedimiento, con las mismas herramientas, en las mismas condiciones, en cualquier momento.

Reproducible: Se deben obtener los mismos resultados si se aplica el mismo procedimiento, con herramientas distintas, en condiciones distintas, en cualquier momento.

Justificable: Se debe poder demostrar que las acciones y métodos utilizados son el mejor curso de acción posible => **Método (Garantías)**

PURI: Proceso Unificado de Recuperación de la Información

- ✓ Demanda de informáticos forenses al Grupo de I+D en Sistemas Operativos UFASTA (2010)
- ✓ Proyecto PURI y diseño técnico (2011)
- ✓ Formalización InFo-Lab y Proyecto PAIF-PURI (2014)
- ✓ Aplicación piloto para su validación (2015)
- ✓ Guía Integral de Empleo de la Informática Forense en el Proceso Penal (basada en PURI, 2016). El Rastro Digital del Delito (2016).
- ✓ Resolución 483/16 Procuración General de la Suprema Corte de Justicia PBA

PURI: Proceso Unificado de Recuperación de la Información

- ✓ Familia PURI (Clusters, Móviles, IoT)
- ✓ Modelo utilizado como referencia por otras provincias y países
- ✓ Guía Integral de Informática Forense en el Proceso Penal de Ecuador (2017)
- ✓ Guía para el Diseño, Implementación y Gestión de la Laboratorios de Informática Forense Judiciales (2019)
- ✓ Guía para la Implementación de Sistemas de Calidad en Laboratorios de Informática Forense Judiciales (2022)
- ✓ Ampliación a Procesos Civiles, Comerciales, Laborales y de Familia (JuFeJus).

Guía Integral de Empleo de la Informática Forense en el Proceso Penal (PBA)

PROVINCIA DE BUENOS AIRES
PROCURACIÓN GENERAL DE LA SUPREMA CORTE DE JUSTICIA

La Plata, junio 27 de 2016.

VISTO:

El convenio 5/14 suscripto entre esta Procuración General, la Universidad FASTA y la Municipalidad del Partido de General Pueyrredón, por el cual se integra un Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense ("InFo-Lab"), y

CONSIDERANDO:

endaciones de los usuarios que la aplicaron, la guía
eso Unificado de Recuperación de la Información
de Cadena de Custodia aprobado por Resolución
r sus disposiciones en todo cuanto sea compatible
bibliográficas
uradora General de la Suprema Corte de Justicia,
en uso de sus atribuciones (art. 189 de la Constitución de la Provincia de Buenos Aires y arts. 1°, 2° y 21 de la ley 14.442)

RESUELVE

Artículo 1: Aprobar la "Guía Integral de empleo de la Informática Forense en el Proceso Penal" que obra como Anexo a la presente.

Artículo 2: Recomendar la aplicación y observación de los lineamientos que establece la "Guía Integral de empleo de la Informática Forense en el Proceso Penal" en las

PROVINCIA DE BUENOS AIRES
PROCURACIÓN GENERAL DE LA SUPREMA CORTE DE JUSTICIA

investigaciones que así lo requieran y en la medida que los recursos humanos y materiales existentes lo permitan.

Artículo 3: Regístrese y comuníquese.

REGISTRADO BAJO EL Nº 483/16

PROCURACIÓN GENERAL

MARIA del CARMEN FALBO
Procuradora General
de la Suprema Corte de Justicia

Guía Integral de Empleo de la Informática Forense en el Proceso Penal (PBA)

- **Introducción**
- **Consideraciones generales**
  - La evidencia digital
  - Roles y niveles de actuación procesal
  - Principios generales en el manejo de evidencia digital
  - Fases de intervención del informático forense

Guía Integral de Empleo de la Informática Forense en el Proceso Penal (PBA)

- **Identificación**
  - Concepto y requisitos generales
  - Medios de identificación
  - Cuestiones de jurisdicción y competencia. Mecanismos de cooperación
  - Perfil del Responsable de Identificación
  - Pedidos de medidas de injerencia. Control del contenido de la orden.

Guía Integral de Empleo de la Informática Forense en el Proceso Penal (PBA)

- **Adquisición de medios de almacenamiento persistente**
  - Nociones y principios generales
  - Preparación y desarrollo de tareas
- **Labores periciales**
  - Marco procesal e institucional. Principios de actuación.
  - Nociones generales
  - Posición procesal del perito
  - Deber de reserva
  - Límites legales
  - Etapas

Guía Integral de Empleo de la Informática Forense en el Proceso Penal (PBA)

- **Labores periciales**
  - Actos y formalidades iniciales
    - Controles y consultas previas
    - Formalidades de inicio
  - Preparación del análisis
  - Análisis
  - Interpretación
  - Elaboración del dictamen pericial
    - Contenido
    - Forma y redacción

Guía Integral de Empleo de la Informática Forense en el Proceso Penal (PBA)

- **Labores periciales**
  - Presentación del perito en el Juicio Oral
    - Preparación
    - Forma de declaración
  - Destino de las evidencias y copias forenses
    - Dispositivos y evidencia material
    - Evidencia digital
    - Informes y consultas
    - Ejecución y documentación de medidas

Guía Integral de Empleo de la Informática Forense en el Proceso Penal (PBA)

- **Recolección**
  - Concepto general. Escenarios posibles.
  - Principios básicos de actuación.
  - Variables a considerar
  - Recaudos adicionales para teléfonos móviles.
- **Adquisición de datos volátiles**
  - Nociones generales
  - Criterios especiales de actuación

Guía Integral de Empleo de la Informática Forense en el Proceso Penal (PBA)

- **Cadena de custodia**
  - Conceptos generales
  - Principios básicos de actuación
  - Recaudos especiales

Guía Integral de Empleo de la Informática Forense en el Proceso Penal (PBA)

Anexos

- Anexo I: Evidencias en Medios Tecnológicos
- Anexo II: Actas y Formularios
  - Acta de Levantamiento de Soporte de Evidencia Digital
  - Acta de Levantamiento de Evidencia Digital
  - Formulario de Cadena de Custodia
- Anexo III: Técnicas y Herramientas de Informática Forense
- Anexo IV: Consideraciones sobre los aspectos legales y estratégicos del empleo de la informática forense en el proceso penal por parte del Ministerio Público Fiscal.
- Anexo V: Glosario
- Anexo VI: Fuentes bibliográficas y normativas consultadas

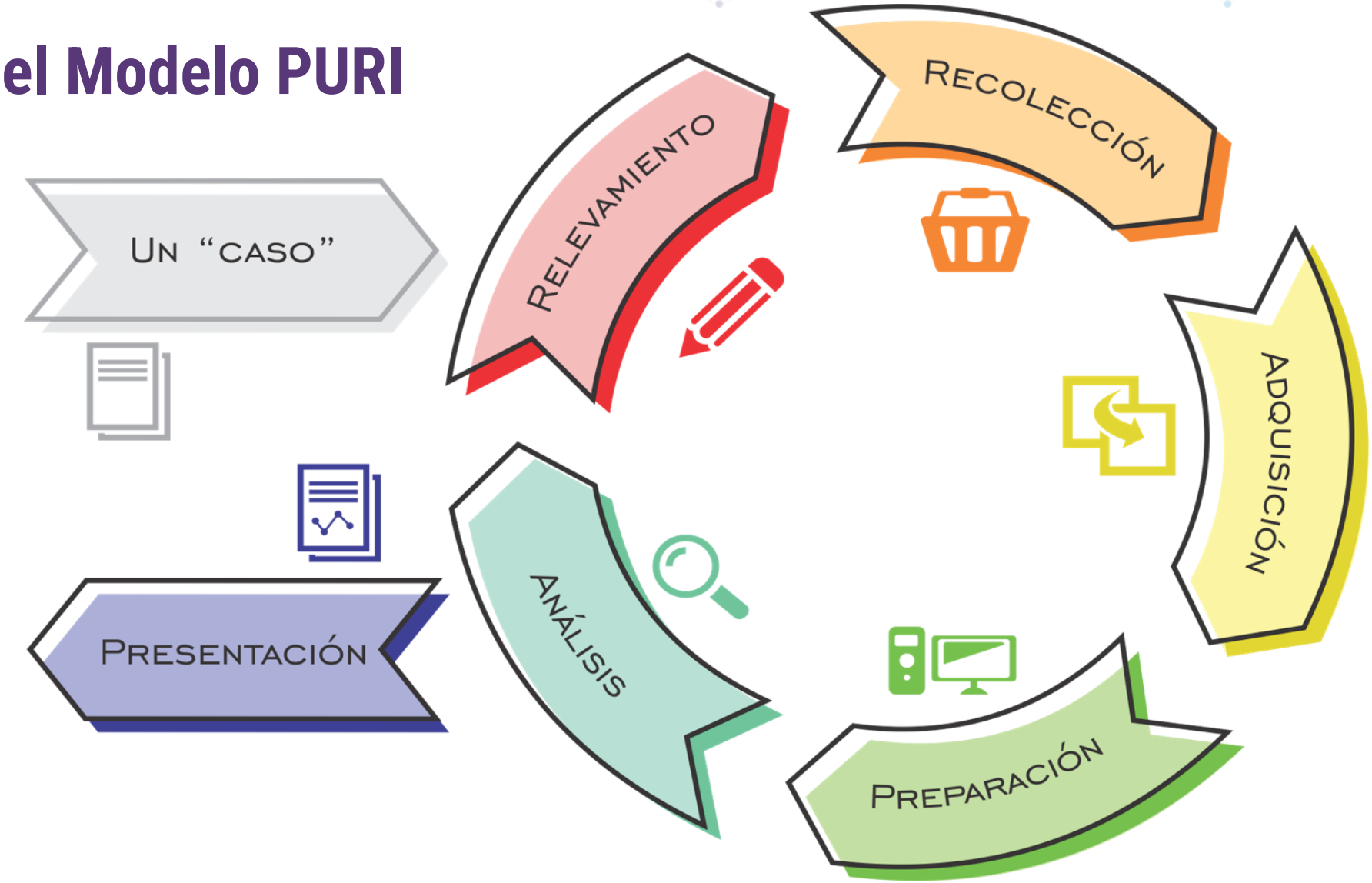
El Modelo PURI

PURI es un modelo que define objetivos, describe métodos y propone una correlación de acciones.

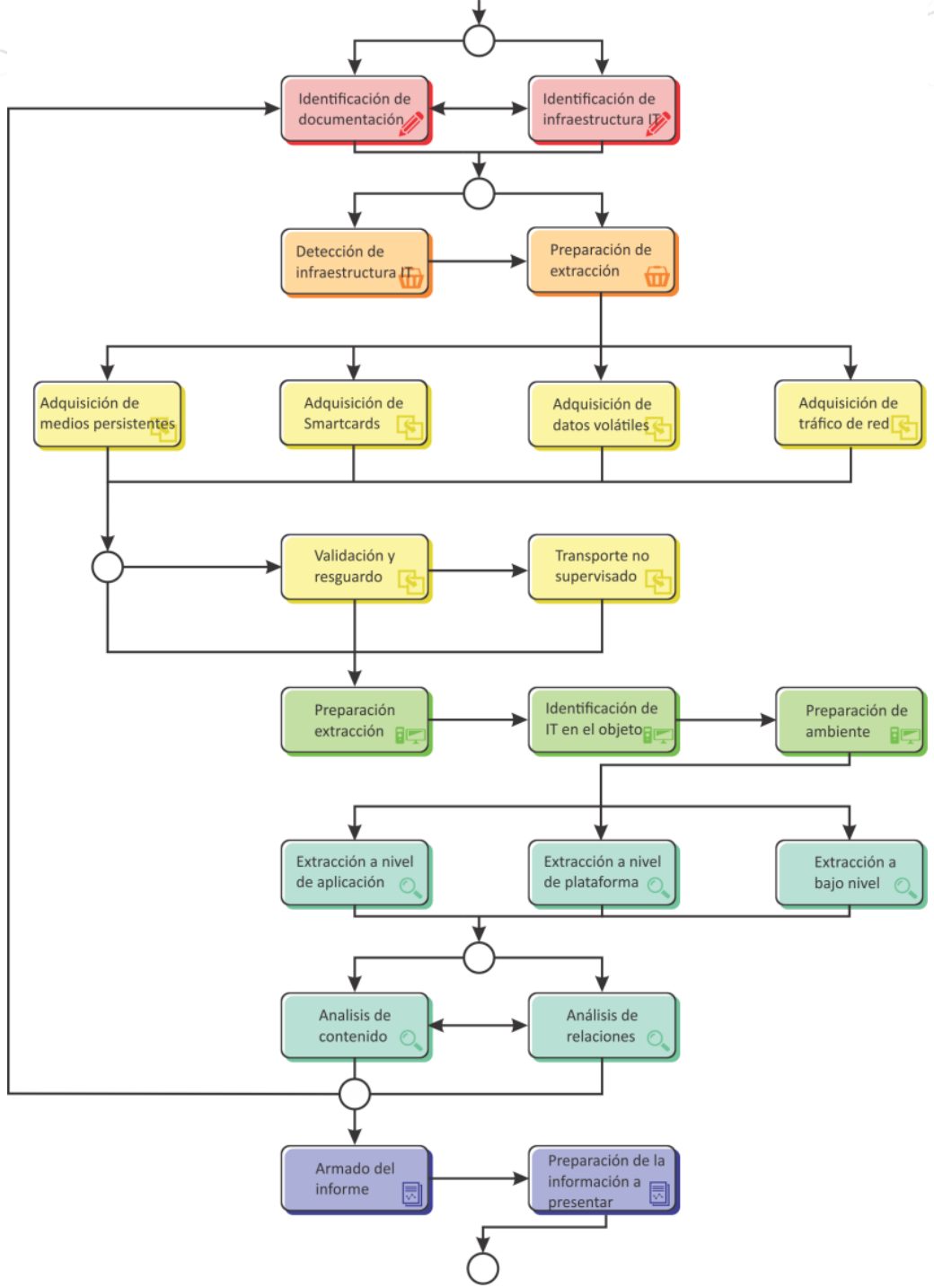
Estructura de PURI:

- ✓ Fases
- ✓ Actividades
- ✓ Tareas
- ✓ Técnicas y Herramientas

Fases del Modelo PURI



Actividades del Modelo PURI



Fase de Relevamiento

La Fase de Relevamiento abarca la investigación que se realiza para conocer el caso a trabajar. En un entorno judicial se corresponde con las medidas de "exploración" del caso. En esta fase se identifican los posibles objetos contenedores de datos de interés susceptibles de transformarse en evidencia digital.

Considerar: Volatilidad de los datos, Objetos de Interés, Objetos que pueden ocultar información (o cuya función no sea evidente), suficiencia de la evidencia.

Fase de Relevamiento

Actividades:

- Identificación de Documentación:
  - Relevamiento de documentos legales, técnicos, administrativos
- Identificación de Infraestructura:
  - Relevamiento de documentos de seguridad lógica y física
  - Identificación de servicios internos y externos

Técnicas:

- Pedidos de oficio
- Exploración en Internet (OSINT)

Fase de Recolección

La Fase de Recolección comprende las tareas para hacerse de las evidencias potenciales (por medio de sus soportes). Abarca las acciones y medidas necesarias para obtener los objetos (equipos, medios de almacenamiento, entre otros) sobre los cuales se trabajará posteriormente

Considerar:

Presentación Espontánea (Un tercero o víctima entrega voluntariamente los soportes de evidencia digital).

Allanamiento (Proceder con especial cuidado, ya que se presentan numerosos riesgos durante el secuestro de los soportes de evidencias digitales)

Fase de Recolección

Actividades (Secuestro, Embalaje y Transporte)

- Asegurar la escena. Registrar la escena y los elementos.
- Registrar, fotografiar, filmar…..
- Identificar los elementos.
- Evitar la contaminación.
  - Utilizar guantes. Desconectar la red.
  - Especial atención a la tecla que presionamos en un equipo encendido. (No presionar ninguna). No abrir la tapa de una notebook o netbook si está cerrada.
- Clasificar, embalar, rotular. Cadena de custodia.

Fase de Recolección - Riesgos

- No visualizar todos los equipos de evidencia.
- Roturas no intencionales.
- Secuestro no autorizado.
- Apagado de dispositivo.
- Eliminación de evidencia digital de forma remota.
- Acceso indebido a información.
- Bloqueo de disp. móviles.

Fase de Recolección - Consideraciones

- Suficiencia de la evidencia.
- Podemos hacer adquisición.
- Notas.
- Actas de secuestro.
- Cadena de custodia.
- Preservación adecuada del soporte de evidencia digital.

Fase de Adquisición

La Fase de Adquisición comprende las tareas para recuperar las evidencias potenciales de los soportes.

Es una fase técnica en la que se realizan las copias forenses, se adquieren las imágenes de los medios de almacenamiento originales.

Inicia las tareas propias de los técnicos y se realiza en el Laboratorio de Informática Forense (LIF).

Fase de Adquisición – Documentación y respaldo

Considerar:

Medios persistentes (PCs, pendrives, Móviles): Bloqueo de escritura por Hw o Sw. Resguardo (Hash y BackUp).

Medios volátiles (Memoria): Captura. Resguardo (Hash y BackUp).

Tráfico de Red: Captura de paquetes. Resguardo (Hash y BackUp).

¿Se altera el soporte original ?

Fase de Adquisición – Documentación y respaldo

Acta de pericia

- Descripción pormenorizada
- Fotos
- Imágenes resultantes
- Hashes

Laboratorio de Informática Forense

- Conforme recomendaciones y guías.
- Roles de actuación.
- Duplicadoras (clonadoras?), servidores y firewalls, todos sobre sistemas operativos OpenSource.
  - OpenSource: trazabilidad
  - Costo de Licencias: $0.
- Estructura del LIF:
  - Firewall de control de E/S hacia Internet y redes internas.
  - Redes del laboratorio separadas físicamente.
  - Implementación posible de VPN para acceso remoto.

Fase de Preparación

La Fase de Preparación es una instancia técnica interna del Laboratorio de Informática Forense que involucra las tareas en las que se prepara el entorno de trabajo de acuerdo al caso a analizar.

Esta fase es estructural, ya que implica la reflexión del forense y la selección de las herramientas apropiadas de acuerdo a las tareas que deberá realizar.

Fase de Análisis

La Fase de Análisis comprende las actividades de extracción de la evidencia digital y su posterior análisis.

Es una fase de exploración, búsqueda y descubrimiento de la evidencia digital. Comprende las tareas de extracción de la información de las copias forenses, selección de la potencial evidencia digital, y su análisis en relación al caso y a los puntos periciales o requerimientos de un particular.

En esta fase dse recurre a herramientas ad hoc: Autopsy (OpenSource), UFED Physical Analyzer, Investiga/I2 (grafos)

Fase de Análisis

Considerar:

- ¿Es pertinente? ¿Responde a los puntos de pericia?
- Evidencia Digital !!!

Tareas a nivel aplicación/plataforma: Búsqueda de archivos recientes, Metadatos de archivos, Aplicaciones utilizadas, Logs de aplicaciones, Historiales, Sistemas Operativos, Cloud

Tareas a bajo nivel : archivos, file carving

Fase de Presentación

Fase final. Comprende las actividades vinculadas a la presentación de las tareas realizadas, de los resultados obtenidos, y de la evidencia digital recuperada.

Incluye tanto la presentación escrita como la exposición oral.

Fase de Presentación

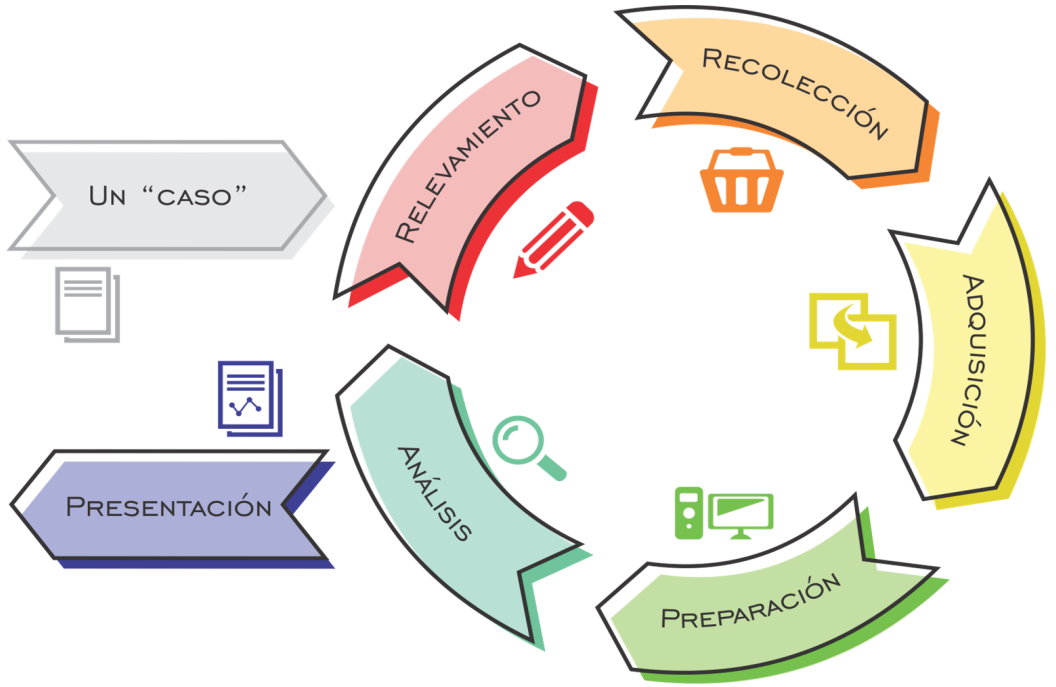
Considerar:

- Armado de Informe
  - Lugar, Fecha, hora, Personas
  - Anexos Documentales
- Preparación de Informe
  - ¿Impresión?
  - Remito
  - Copia de Informe

Niveles de actuación del profesional informático en la labor pericial

Responsable de Identificación (RI): responsable de buscar, reconocer y documentar potencial evidencia digital.

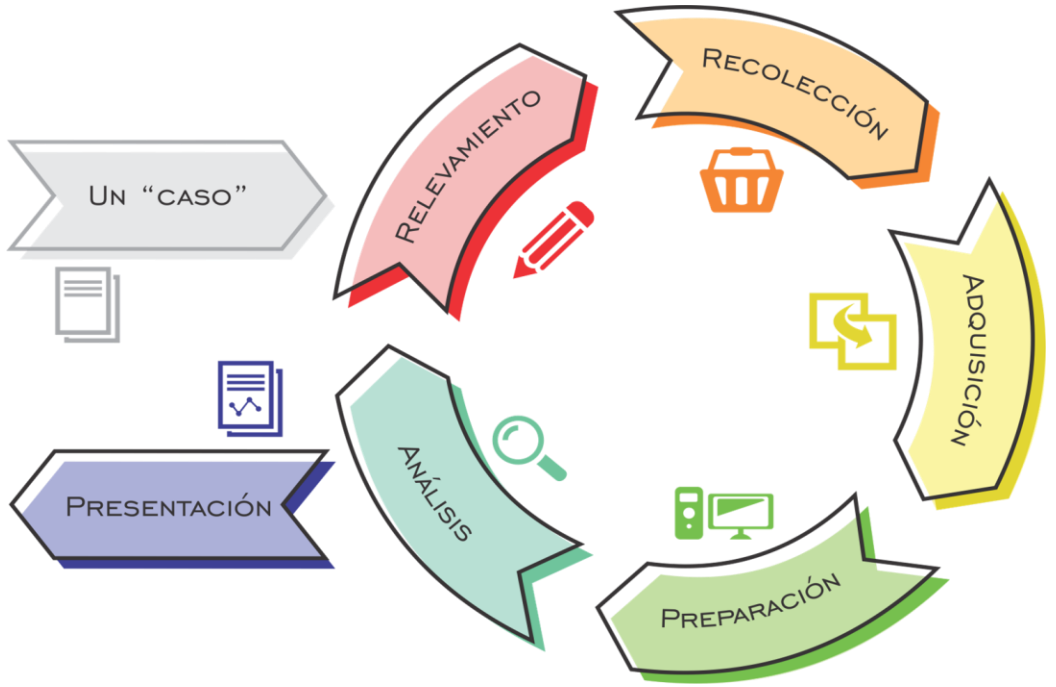
Especialista en Recolección (ER): autorizado, entrenado y calificado para recolectar objetos físicos pasibles de tener evidencia digital. Puede necesitar el auxilio de un Especialista en Adquisición.



Niveles de actuación del profesional informático en la labor pericial

Especialista en Adquisición (EA): autorizado, entrenado y calificado para actuar primero en la escena de un incidente, realizando recolección y adquisición.

Especialista en Evidencia Digital (EED): puede actuar como EA y, además, tiene conocimientos específicos y habilidades que le permiten desarrollar actividades técnicas de extracción, análisis y presentación de ED.



En síntesis

La obtención de evidencia digital en el proceso judicial…

- ✓ Tiene una demanda que crece más que linealmente, en este mundo digital.
- ✓ Supone Principios y Códigos que respetar, más allá de las cuestiones técnicas.
- ✓ Requiere de Métodos (modelos) y de Herramientas ad hoc para cada tarea.
- ✓ Demanda la intervención de profesionales especialistas en permanente actualización

Bibliografía

“El Rastro Digital del Delito”

Puede descargarse desde el sitio:

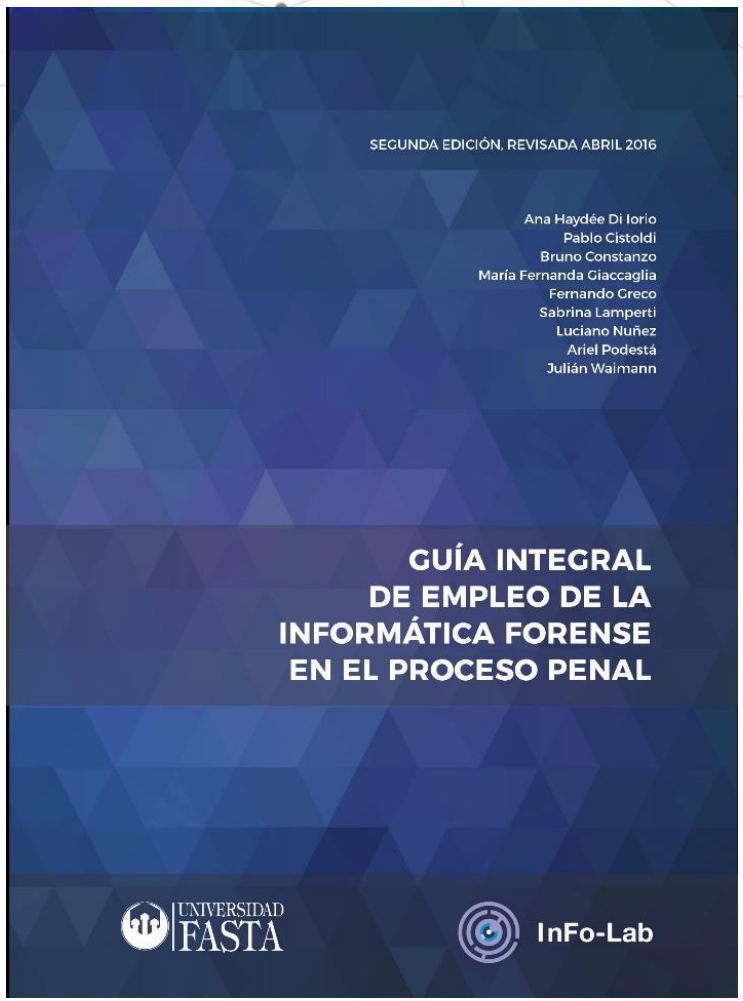
www.info-lab.org.ar

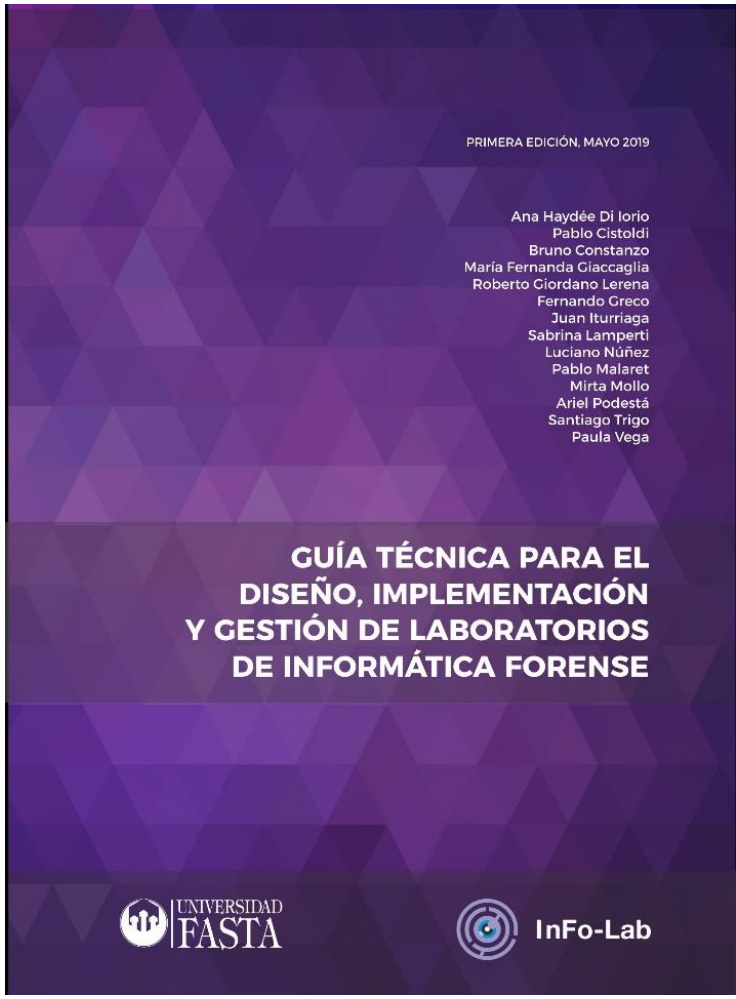
Bibliografía

Guía Integral de Empleo de la Informática Forense en el Proceso Penal.

Guía Técnica para el Diseño, Implementación y Gestión de Laboratorios de Informática Forense.

Pueden descargarse desde el sitio: ***www.info-lab.org.ar***





InFo-Lab

Hacemos Ingeniería !

Creamos, con pasión, compromiso e ingenio,
para mejorar la calidad de vida de las personas !

Hacemos Argentina !

Investigamos y desarrollamos tecnología nacional
para un país justo y soberano !

info-lab.org.ar **Info-lab@ufasta.edu.ar**

¡Muchas Gracias!

Roberto Giordano Lerena

rogiord@ufasta.edu.ar

@rogiord


VI INFO-CONF 2022
MAR DEL PLATA
SEXTA CONFERENCIA NACIONAL DE INFORMÁTICA FORENSE
VIRTUAL Y PRESENCIAL
29 Y 30 DE SEPTIEMBRE
InFo-Lab
UNIVERSIDAD FASTA
FACULTAD DE INGENIERÍA
RED UNIF
RED UNIVERSITARIA DE INFORMÁTICA FORENSE

EXTRAIDO DE

JEFATURA.SANTACRUZ.GOB.AR/CIBERSEGURIDAD2022/