📘 UNIDAD (6-3) — PERITO INFORMÁTICO

2° Año TUP – UTN | Legislación | Profesora: Dra. Marcela Paola Lonati

🧠 IDONEIDAD Y REGLAMENTACIÓN DEL PERITO INFORMÁTICO

Tanto el Código Procesal Civil y Comercial como el Código Procesal Penal reglamentan la idoneidad para actuar como perito en causas judiciales.
Ambos cuerpos legales establecen que:

- **Si la profesión está reglamentada, los peritos deben poseer título habilitante en la ciencia, arte, industria o actividad técnica especializada relacionada con la cuestión que se analiza.**

- **Solo en el caso de que la profesión no esté reglamentada o no haya peritos diplomados o inscriptos, podrá designarse a una persona de conocimiento o práctica reconocida en el área.**

Esto busca garantizar que el profesional que intervenga tenga conocimientos técnicos suficientes para emitir dictámenes confiables ante la justicia.
La figura del perito informático es especialmente importante en una era donde gran parte de las pruebas y evidencias tienen soporte digital.

📜 Regulación provincial y ejemplo Tucumán
La mayoría de las provincias argentinas regulan el ejercicio profesional informático mediante leyes o normativas propias, que definen quién puede ejercer, bajo qué condiciones y con qué responsabilidades éticas.

En la provincia de Tucumán, por ejemplo, el Colegio de Graduados en Ciencia y Tecnología Informática (C.G.C.T.I.T) reglamenta el ejercicio profesional del informático a través de la Ley 7490, la cual establece los requisitos de matriculación, el cumplimiento ético, y la obligación de actuar conforme a los principios de la profesión.

🏛️ Función de los Colegios o Consejos Profesionales
Los colegios profesionales son asociaciones conformadas por quienes ejercen una profesión liberal. Estas instituciones suelen estar amparadas por el Estado, y sus miembros —llamados colegiados— deben cumplir las normas y códigos éticos establecidos en sus estatutos.

Las principales finalidades de los colegios son:

- **Velar por el cumplimiento ético y la buena práctica profesional.**

- **Supervisar el ejercicio responsable de la profesión.**

- **Mantener un estatuto interno que defina los principios, derechos y obligaciones de los profesionales matriculados.**

- **Proteger tanto al profesional como al cliente o institución que requiere sus servicios, garantizando que la labor se realice con transparencia, competencia y rigor técnico.**

==========

💾 PERICIA Y ANÁLISIS FORENSE DE MEMORIA

El Análisis Forense de Memoria consiste en la adquisición y estudio de los datos almacenados en la memoria principal (RAM) de un sistema informático, con el fin de obtener información relevante sobre su funcionamiento o sobre posibles actividades ilícitas.

Este tipo de pericia es fundamental en informática forense, ya que la memoria RAM contiene información temporal y volátil, como procesos activos, conexiones de red, sesiones abiertas, contraseñas en uso o datos no guardados en disco.

📍 Características del análisis forense de memoria

- **Se utilizan volcados de memoria (memory dumps) para obtener una copia del contenido de la RAM, lo que permite realizar un análisis sin alterar el sistema original.**
- **Este método garantiza una intrusión mínima, reproducibilidad del proceso y consistencia de los resultados.**
- **La correcta selección de herramientas es esencial:**
    - **Si se trata de un hardware, hay que verificar compatibilidad y puertos disponibles.**
    - **Si se trata de un software, debe considerarse que el programa se cargará en memoria y puede alterar parte de los datos que intenta capturar.**

🧩 Estructuras de interés
Una vez obtenido el volcado, se analizan las estructuras internas del sistema operativo donde se almacena información crítica:

- **Procesos: programas activos y su estado.**
- **Threads (hilos): subprocesos ejecutándose dentro de cada aplicación.**
- **Módulos: bibliotecas o componentes cargados.**
- **Conexiones y sockets: comunicaciones de red establecidas.**
- **Drivers: controladores de dispositivos conectados.**
- **Entradas de registro: configuraciones y rastros de programas ejecutados.**

Estas estructuras varían según el sistema operativo, su versión y la arquitectura del procesador. Conocerlas permite extraer información que solo existe en la memoria, incluso si fue borrada o nunca guardada en disco.

🧠 **Definición de Volcado de Memoria**

Un volcado de memoria es una copia no estructurada del contenido de la memoria RAM en un momento determinado.

Suele utilizarse para:

- **Depurar programas que fallaron o se cerraron de forma anormal.**
- **Analizar el comportamiento del sistema.**
- **Realizar pericias informáticas sin alterar el equipo original.**

==========

⚙️ PROCEDIMIENTO FORENSE DE ANÁLISIS DE MEMORIA

El análisis forense de memoria se desarrolla en varias etapas técnicas bien definidas.

🔸 **Etapas del procedimiento**

1. **Captura del dump (volcado de memoria).**
2. **Reconocimiento de estructuras en memoria.**
3. **Reconocimiento de relaciones entre estructuras.**
4. **Análisis automático de los datos recolectados.**
5. **Análisis forense manual o interpretativo.**
6. **Elaboración de conclusiones.**

🧰 **Distribución de tareas**

- **El forense informático interpreta la información, la contextualiza y elabora las conclusiones finales.**
- **Las herramientas de análisis automatizan la detección y clasificación de datos, pero no sustituyen el criterio profesional.**

📊 **Detalle técnico de las etapas**

- **Reconocimiento de estructuras: identificación de los artefactos detectables en el volcado (procesos, módulos, conexiones, etc.).**
- **Reconocimiento de relaciones: asociación lógica entre los artefactos, determinando cómo interactúan entre sí.**
- **Análisis automático: aplicación de reglas predefinidas por el software para generar reportes o alertas.**

- **Análisis manual o interpretativo: revisión profunda por parte del especialista, quien evalúa la relevancia de los hallazgos en el contexto de la investigación.**

💡 Utilidad del análisis de memoria
Permite:

- **Inferir el uso que se le dio al equipo.**
- **Detectar malware activo que haya controlado el sistema.**
- **Evitar errores judiciales, como acusar a un usuario inocente cuando un atacante remoto manipuló su equipo.**
- **Extraer contraseñas, claves de cifrado y sesiones almacenadas temporalmente en RAM.**

🧮 Aplicaciones investigativas

1. **Contexto de seguridad de procesos: identificación de privilegios, procesos padres, y relaciones entre ellos (por ejemplo, estructuras _TOKEN en Windows).**
2. **Búsqueda de información oculta o volátil: contenido cifrado, fragmentos de texto de archivos o correos abiertos.**
3. **Conexiones y sockets: vinculación entre direcciones IP remotas y procesos internos mediante PID.**
4. **Dispositivos periféricos: detección de drivers cargados en memoria que indiquen el uso de USB u otros.**
5. **Software específico: detección de procesos sospechosos, módulos o entradas de registro vinculadas a una aplicación concreta.**

📄 Análisis complementario
También se busca información que no esté asociada directamente a estructuras conocidas, como el contenido parcial de páginas web, chats o fragmentos de documentos abiertos al momento del volcado.

==========

💽 INTERPRETACIÓN Y ADQUISICIÓN DE VOLCADOS DE MEMORIA

Los datos presentes en un volcado pueden almacenarse de diferentes maneras y no siempre forman parte de estructuras reconocibles. Por eso, es esencial comprender su formato y la herramienta utilizada para capturarlo.

🔧 Factores a considerar durante la adquisición
Si se utiliza software de volcado, el analista debe conocer:

- **Qué procesos ejecuta la herramienta durante su funcionamiento.**

- **Cuánto espacio ocupa en memoria.**
- **Qué tipo de volcado genera (completo o parcial).**
- **Qué formato utiliza y qué información vuelca al archivo resultante.**

📚 Tipos de volcados de memoria

Tipo de volcado	Descripción
Crash dump	Volcado generado automáticamente por Windows cuando ocurre un fallo crítico del sistema.
Raw dump	Copia completa del contenido de la memoria al momento de su generación.
Otros formatos	Varían según la herramienta empleada y el nivel de detalle requerido.

⏱️ Importancia de la adquisición temprana
La adquisición del volcado de memoria debe realizarse in situ y de forma prioritaria, debido a la alta volatilidad de los datos.
Cada segundo que pasa puede modificar la información activa en RAM, y cualquier acción externa (como abrir programas o copiar archivos) puede alterar o sobrescribir evidencias digitales.

🎯 Factores de éxito del análisis

- **Elegir correctamente la herramienta de adquisición.**
- **Evaluar el nivel de volatilidad de los datos antes de proceder.**
- **Garantizar que el volcado se realice con procedimientos estandarizados y documentados.**
- **Un volcado bien ejecutado permite reconstruir eventos, detectar intrusiones, recuperar contraseñas y establecer responsabilidades dentro de un caso judicial o corporativo.**