

TU ABOGADO DIGITAL

MÓDULO 4 – GUÍA PROFESIONAL DEL ESTUDIANTE

Lineamientos específicos para la obtención y tratamiento de evidencias digitales desde una perspectiva técnico-forense integral.

I. INTRODUCCIÓN TÉCNICO-FORENSE

La evidencia digital exige una metodología rigurosa debido a su alta vulnerabilidad a alteraciones técnicas y cuestionamientos procesales. Un procedimiento incorrecto puede comprometer la autenticidad, integridad y confiabilidad del indicio. Esta guía desarrolla cada lineamiento explicando su finalidad operativa, su lógica pericial y su impacto probatorio dentro del proceso penal.

PROTECCIÓN DEL SITIO DIGITAL

La protección tiene como finalidad preservar el estado original del sistema y evitar interferencias remotas o manipulación de terceros. Se enfoca en impedir la pérdida de información volátil y la alteración de metadatos críticos.

- Retirar al usuario activo sin intervenir el sistema.
- Mantener el equipo encendido cuando sea necesario preservar memoria volátil.
- Deshabilitar conexiones susceptibles de interferencia externa.
- Evitar inserción de dispositivos que modifiquen metadatos.
- Aplicar aislamiento físico y lógico.

OBSERVACIÓN Y BÚSQUEDA

Esta fase construye el contexto técnico del hallazgo. La observación documenta el estado inicial del sistema, mientras que la búsqueda debe ser metódica y orientada al hecho investigado.

- Documentar hora y estado del dispositivo.
- Registrar conexiones visibles y periféricos.
- Identificar dispositivos IoT relacionados.
- Explorar puertos y soportes externos.

FIJACIÓN Y DOCUMENTACIÓN

La fijación permite reproducibilidad técnica en juicio. Asegura que el estado del sistema pueda demostrarse posteriormente sin depender exclusivamente de la memoria del perito.

- Fotografiar pantalla sin intervenir el sistema.
- Registrar conexiones externas.

- Identificar IMEI y SIM en móviles.
- Ilustrar topología de red cuando aplique.

COLECCIÓN Y ADQUISICIÓN

La adquisición debe realizarse mediante copias verificables. El cálculo de funciones hash garantiza la integridad del contenido. Trabajar directamente sobre el original incrementa el riesgo de contaminación probatoria.

- Realizar imagen forense bit a bit cuando sea posible.
- Calcular hash SHA-256 antes y después de la copia.
- Utilizar bloqueadores de escritura.
- Documentar herramientas y versiones empleadas.

TRASLADO Y RESGUARDO

La continuidad de custodia es esencial para evitar cuestionamientos sobre autenticidad. Toda transferencia debe registrarse de forma detallada y mantenerse bajo control estricto.

- Embalaje antiestático y sellado inviolable.
- Etiquetado con código único y referencia al expediente.
- Registro de entrega y recepción con fecha y hora.
- Almacenamiento en entorno seguro con control de acceso.