DEVELOPMENT OF A FORENSIC ANALYSIS METHODOLOGY

Grupo 3

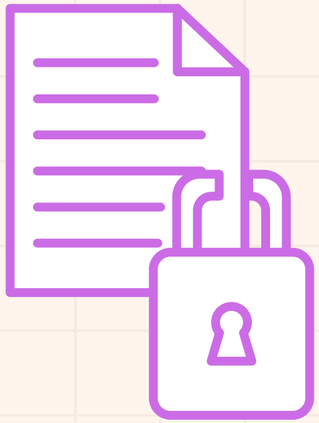
INTRODUCCIÓN Y MISIÓN

Nuestra empresa de ciberseguridad nos ha encomendado, como equipo forense, la creación de una metodología de análisis propia. Este proyecto tiene como objetivo diseñar un proceso metódico y robusto para el manejo de evidencias digitales, desde su descubrimiento hasta su presentación, basándonos en normas y estándares forenses reconocidos a nivel mundial.

ESTÁNDARES FORENSES DE REFERENCIA

ISO/IEC 27037

Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital.



ISO/IEC 27042

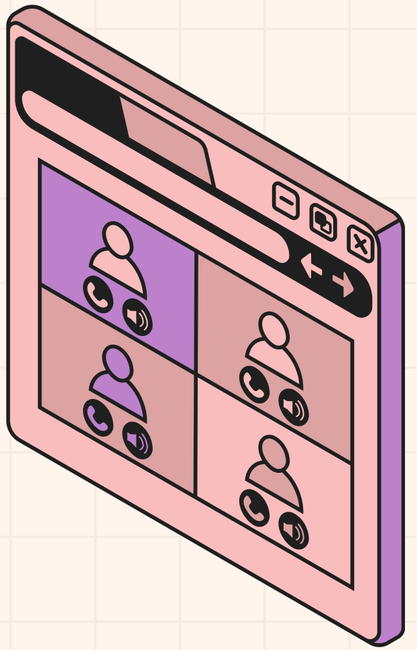
Normas para el análisis e interpretación de la evidencia, asegurando continuidad y reproducibilidad.

NIST SP 800-86

Guía para integrar técnicas forenses en la respuesta a incidentes (Incident Response).

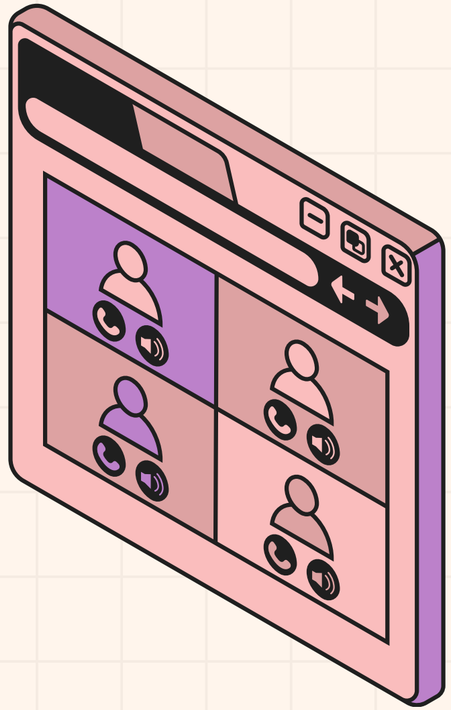
ANÁLISIS DE ESTÁNDARES: ISO/IEC 27037
MANEJO INICIAL DE LA EVIDENCIA

- **Alcance**: Manejo inicial de la evidencia (identificación, colección, adquisición y preservación).
- **Objetivo**: Minimizar alteraciones y asegurar la integridad con documentación exhaustiva.
- **Cobertura**: Soportes de PC, móviles, cámaras, navegación y redes TCP/IP.
- **Enfoque**: Facilitar la transferencia entre jurisdicciones con procedimientos trazables.



ANÁLISIS DE ESTÁNDARES: ISO/IEC 27042
ANÁLISIS E INTERPRETACIÓN DE LA EVIDENCIA

- **Principios Clave:** Continuidad del rastro, validez de métodos y reproducibilidad del análisis.
- **Documentación:** Detalle de procesos y parámetros para permitir revisión externa.
- **Competencia:** Mecanismos para demostrar la aptitud del equipo analista.
- **Selección de Técnicas:** Justificación de métodos adaptados al tipo de evidencia.



ANÁLISIS DE ESTÁNDARES: NIST SP 800-86
INTEGRACIÓN CON LA RESPUESTA A INCIDENTES (IR)

- **Fases Operativas:** Recogida, examen, análisis e informe integrados en el flujo de IR.
- **Buenas Prácticas:** Estandarizar procedimientos para acciones consistentes y admisibles.
- **Capacidades:** Clarifica roles, formación y cooperación entre equipos.
- **Cobertura Técnica:** Orientación por categorías de datos (SO, red, aplicaciones).

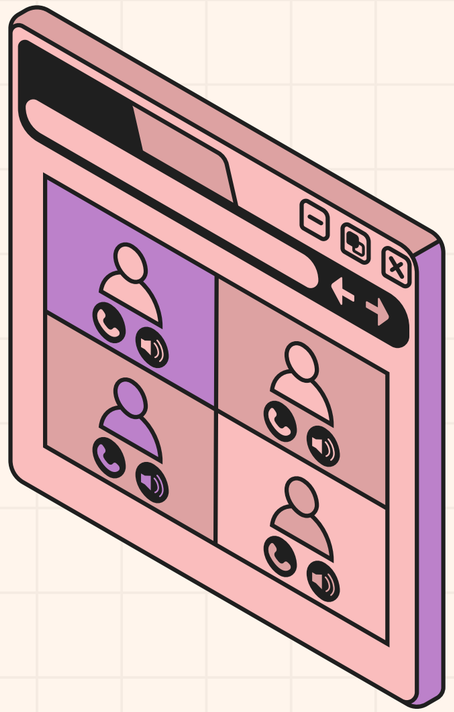


TABLA COMPARATIVA DE ESTÁNDARES

Criterio	ISO/IEC 27037	ISO/IEC 27042	NIST SP 800-86
¿En qué se centra?	encontrar, recoger y preservar evidencia	Analizar e interpretar la evidencia	Integrar análisis forense en la respuesta a incidentes
Tecnología cubierta	Discos, móviles, cámaras y redes; pautas para manejarlos sin alterar datos.	Agnóstico: elegir el método más adecuado para cada caso y tipo de evidencia.	Fuentes típicas: sistema operativo, red y aplicaciones como base de trabajo.
Fortalezas	Fuerte en preservación inicial y cadena de custodia; reduce riesgos de contaminación.	Asegura calidad del análisis y que otros puedan repetirlo; mejor defensa técnica.	Aterriza la forense en el día a día del SOC; facilita coordinación y tiempos de respuesta.
Debilidades	Análisis profundo débil; requiere formación y puede ser costoso de implantar.	Puede ser complejo y exigir alta especialización y validaciones continuas.	Menos formalista que ISO; puede variar su aplicación entre equipos si no se estandariza bien.

NUESTRA METODOLOGÍA FORENSE

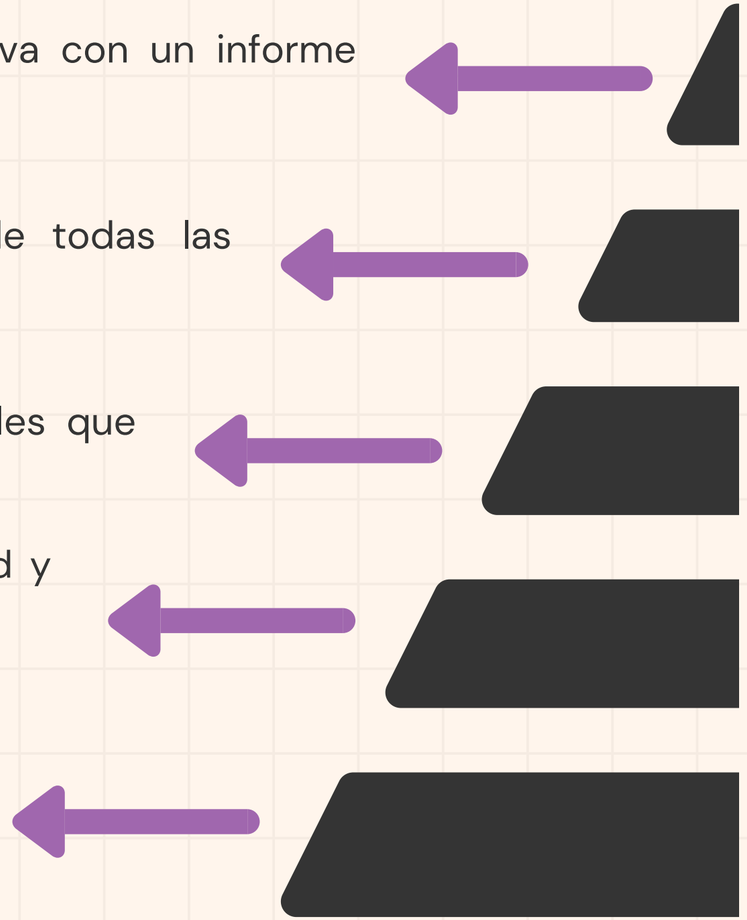
Fase 5. Presentación de resultados: Comunicar los resultados de forma efectiva con un informe técnico detallado y material visual (líneas del tiempo, esquemas)

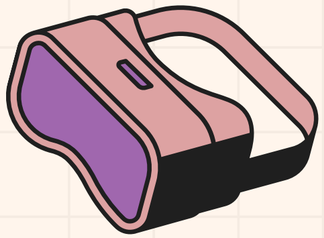
Fase 4. Documentación de hallazgos: Crear un registro claro, completo y de todas las actividades y observaciones para asegurar que podemos defenderlo.

Fase 3. Análisis de las evidencias: Producir hallazgos reproducibles y defendibles que expliquen el qué, cómo, cuándo y quién e impacto.

Fase 2. Preservación y almacenamiento: Para mantener la integridad, autenticidad y trazabilidad de la evidencia.
Embalaje antiestático, sellos de seguridad, etiquetado claro.

Fase 1. Adquisición de evidencia digital: Identificar, recolectar y adquirir la evidencia evitando alteraciones.
Registro obligatorio: quién/cuándo/dónde





GRACIAS

POR SU ATENCIÓN