GRUPO DE INVESTIGACIÓN

ESCENARIOS · INFORMACIÓN · INCIDENCIA · INTELIGENCIA

Modelo Metodológico de Investigación Periodística

MANUAL DE OSINT PERIODÍSTICO

Metodologías de Fuente Abierta para el Periodismo de Investigación y la Verificación de Datos

Gabriel Hidalgo Andrade

Yalilé Loaiza

ESCENARIOS
Hipótesis prospectivas

INFORMACIÓN
Recopilación sistemática

INCIDENCIA
Análisis de actores

INTELIGENCIA
Síntesis verificada

Financiado por:

Proyecto "Comunidad Informada"

Con el apoyo de:

PRÓLOGO

El periodismo que el mundo necesita

> *"Vivimos en el momento más complejo —y más fértil— de la historia para el periodismo de investigación. La saturación digital ha democratizado el acceso a los datos, pero también ha multiplicado los vectores de desinformación a una escala sin precedentes."*

En 2026, el tráfico generado por agentes de inteligencia artificial escala **ocho veces más rápido** que el tráfico humano: la señal y el ruido compiten en condiciones absolutamente asimétricas. El periodista de investigación moderno no puede limitarse a publicar el hallazgo; debe permitir que el lector, el editor y el tribunal lo reproduzcan. **El proceso se convierte en evidencia.**

La metodología E3I —**Escenarios, Información, Incidencia, Inteligencia**— que estructura este manual no es un marco teórico abstracto. Nació en sala de redacción, fue templada en la cobertura de conflictos, estafas digitales y corrupción transnacional en América Latina, y fue refinada por la práctica forense
de equipos como Bellingcat, el Digital Verification Corps de Amnistía Internacional y las investigaciones colaborativas del ICIJ.

Este manual cubre la disciplina completa: desde la epistemología del dato hasta la gestión del trauma vicario; desde los operadores booleanos avanzados hasta el análisis acústico de ejecuciones extrajudiciales; desde la detección de deepfakes hasta los protocolos de seguridad digital y física para el periodista
en campo.

Lo que permanece cuando todo cambia

Las plataformas cambian, los algoritmos se actualizan, las APIs desaparecen. Lo que permanece es el método: la hipótesis, el cruce de fuentes, la cadena de custodia, la falsación sistemática y la rendición de cuentas pública. Con ese método, cualquier periodista —con o sin presupuesto, con o sin credencial internacional— puede construir evidencia que resiste el escrutinio más severo.

ESTRUCTURA DEL MANUAL

- 16 capítulos + casos de estudio
- 4 partes temáticas
- +60 herramientas referenciadas
- ⚖ Código deontológico propio
- Casos de América Latina y global
- Protocolos de seguridad digital y de campo

ÍNDICE

Tabla de Contenidos

PARTE I — FUNDAMENTOS TEÓRICOS Y EPISTEMOLÓGICOS

Cap. 1 El Nuevo Ecosistema Informativo y el Paradigma OSINT 04

Cap. 2 El Modelo E3I — Marco Metodológico Central 06

Cap. 3 Ética y Deontología del Investigador OSINT 10

PARTE II — HERRAMIENTAS Y TÉCNICAS OPERATIVAS

Cap. 4 Búsqueda Avanzada y Conectores de Datos 13

Cap. 5 Análisis y Visualización Avanzada de Datos 17

Cap. 6 Verificación Multimedia y Forense Visual 20

Cap. 7 Detección de Contenido Generado por IA y Deepfakes 23

Cap. 8 Investigación de Redes de Desinformación y Estafas Digitales 26

Cap. 9 Uso de IA y Agentes Digitales en la Investigación 28

PARTE III — SEGURIDAD

Cap. 10 Análisis de Riesgos Digitales 30

Cap. 11 Análisis de Riesgos en Campo 33

Cap. 12 Seguridad Operativa (OPSEC) en Investigaciones Sensibles 36

PARTE IV — PUBLICACIÓN Y COLABORACIÓN

Cap. 13 Del Análisis a la Narrativa Publicable 38

Cap. 14 Investigación Colaborativa y Redes Transnacionales 40

Cap. 15 Casos de Estudio Integrales 43

Cap. 16 Aplicación del Modelo E3I — Ejercicios Prácticos 47

Apéndice Conclusiones y Fuentes Bibliográficas 49

CAPÍTULO 01 PARTE I — FUNDAMENTOS TEÓRICOS

El Nuevo Ecosistema Informativo y el Paradigma OSINT

La práctica de la investigación periodística ha experimentado una transformación sin precedentes. El paradigma ha migrado de la **escasez** a la **saturación**: la información ya no es el cuello de botella; lo es la verificación.

PARADIGMA ANTERIOR

ESCASEZ

Lainformación eraescasa, su acceso era privilegiado. El analista extraía valor de fuentes limitadas.

→

PARADIGMA 2026

SATURACIÓN

Elproblemaestratégicoyano es conseguir el dato. Es identificar la señal relevante en un océano de ruido algorítmico.

Consecuencias directas para el periodismo

⚡ **Velocidad ≠ ventaja**

La velocidad de publicación ya no es ventaja competitiva si no va acompañada de verificación rigurosa.

🔬 **Credibilidad = transparencia**

La credibilidad se construye sobre la transparencia metodológica, no sobre la exclusividad del dato.

🧩 **Triple rol del periodista**

Actuar simultáneamente como investigador, analista forense y comunicador de evidencia.

🌐 **Cobertura colaborativa**

La cobertura colaborativa y transnacional es más efectiva que el modelo del periodista solitario.

📊 **Dato clave — 2026**

El tráfico generado por agentes de inteligencia artificial escala **8× más rápido** que el tráfico humano. Durante un evento crítico, es posible registrar **1.200 publicaciones en redes sociales en apenas cinco minutos**. El investigador E3I no puede trabajar solo en la fase de ingestión.

1.2 OSINT vs. OSI — Una Distinción Crítica

Para el periodista de investigación moderno, la distinción no es semántica. La **OSI** (Investigación de Fuente Abierta periodística) exige transparencia radical: cada hallazgo debe poder ser reproducido y refutado por cualquier tercero con las mismas herramientas.

DIMENSIÓN	OSINT (INTELIGENCIA ESTATAL)	OSI (PERIODISMO DE INVESTIGACIÓN)
Origen	Agencias de inteligencia militar y civil	Periodismo y sociedad civil (Bellingcat, OCCRP)
Finalidad	Informe clasificado, decisión interna	Publicación pública, rendición de cuentas
Metodología	Reservada, no reproducible	**Transparente, auditable y falsable**
Audiencia	Estado, comité restringido	Ciudadanía, tribunales, sociedad civil
Verificación	Interna y confidencial	**Reproducible por terceros independientes**

1.3 Jerarquía Epistemológica — Del Ruido a la Evidencia

Antes de seleccionar una sola herramienta, el investigador OSINT debe interiorizar esta jerarquía. Es el antídoto contra el error más frecuente: publicar datos como si fueran evidencia.

▲ DEL RUIDO A LA INTELIGENCIA ▲

🧠 **INTELIGENCIA ESTRATÉGICA**
Síntesis de múltiples evidencias verificadas → toma de decisiones editoriales o judiciales

↑

✅ **EVIDENCIA**
Informaciónvalidada sistemáticamente bajo una hipótesis verificable. Ej: sincronización de sombras en SunCalc confirma lugar de una ejecución extrajudicial.

↑

📋 **INFORMACIÓN**
El dato interpretado en su contexto temporal, espacial y relacional. Ej: esa coordenada corresponde a un patio en Bengasi, el 17 de julio de 2017.

↑

📍 **DATO AISLADO**
El elemento bruto, sin contexto. Ej: una coordenada geográfica (32.0231, 20.0291). Punto de partida, nunca punto de llegada.

> ⚠ **El Error Más Frecuente en el Periodismo Digital**
> Publicar **datos** como si fueran **evidencia**, o evidencia parcial como si fuera conclusión definitiva. Sin una epistemología clara, la tecnología no acelera la investigación: **acelera la propagación del error**.

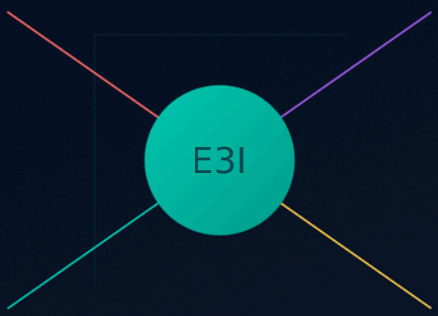
CAPÍTULO 02

El Modelo E3I
Marco Metodológico Central

No es una secuencia lineal de pasos, sino un **sistema dinámico de retroalimentación** en el que cada pilar alimenta y corrige a los demás. Su fortaleza reside en transformar la recopilación caótica de datos en conocimiento estructurado, verificable y accionable.

PILAR 1
ESCENARIOS
¿Qué podría estar pasando?
Hipótesis prospectivas y falsables. Construir al menos 3 escenarios alternativos.

PILAR 2
INFORMACIÓN
¿Qué datos existen?
Recopilación sistemática y preservación. Preservar antes de analizar.



PILAR 3
INCIDENCIA
¿Quién moldea la narrativa?
Redes de amplificación, actores, sesgo. Identificar al Paciente Cero.

PILAR 4
INTELIGENCIA
¿Qué sabemos con certeza?
Síntesis verificada para decisión editorial o judicial.

↺ SISTEMA DINÁMICO DE RETROALIMENTACIÓN — CADA PILAR ALIMENTA Y CORRIGE A LOS DEMÁS ↻

2.2 Los Cuatro Pilares en Detalle

PILAR 1

01

ESCENARIOS

"Pensar en lo que podría estar pasando antes de buscar lo que encontré"

- Construir mínimo 3 escenarios: el más probable, el más peligroso, el más contraintuitivo
- Previene el sesgo de confirmación
- AI Slop, Hybrid Fake, Propaganda Lego, Impersonación de marca

PILAR 2

02

INFORMACIÓN

"Preservar antes de analizar — toda fuente digital es volátil"

- Preservar inmediatamente con Archive.today o Wayback Machine Registrar cadena de custodia (timestamp, URL, investigador)
- Categorizar por nivel de confianza desde el inicio
- IA como primer filtro, nunca árbitro final

PILAR 3

03

INCIDENCIA

"¿Quién amplifica esta narrativa y con qué intereses?"

- Red de amplificación: ¿quiénes repostean y cuándo?
- Narrativa dominante: ¿sirve a algún actor identificable?
- Identificar al Paciente Cero: fuente original del contenido

PILAR 4

04

INTELIGENCIA

"La diferencia entre datos y conocimiento accionable"

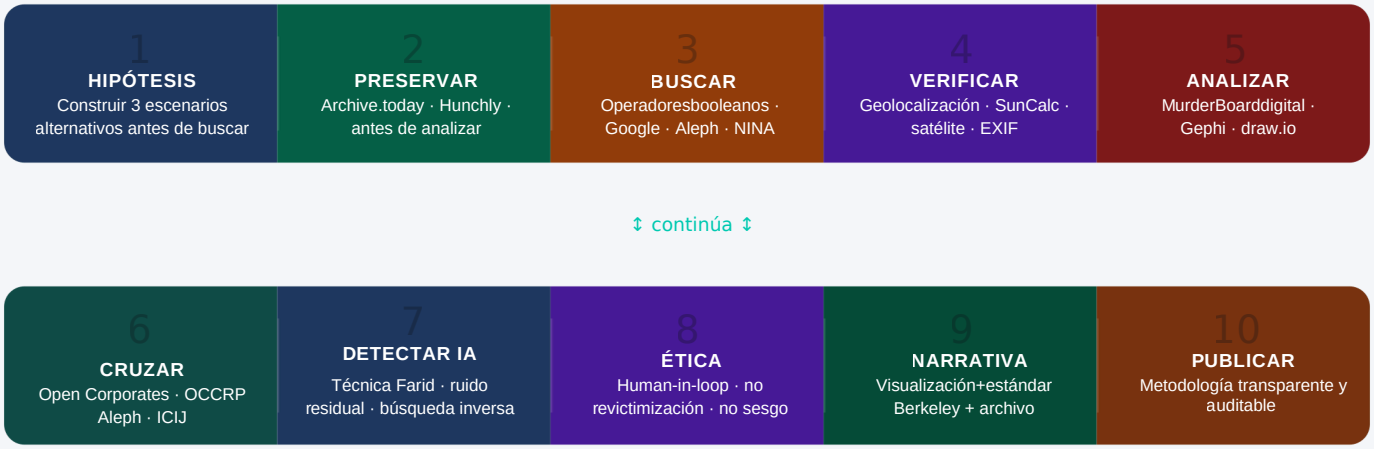
- Síntesis: recopilado + verificado + contrastado + accionable
- Narrativa publicable Y documentación judicial-grade
- Presentaciones para organismos internacionales
- Materiales de advocacy con evidencia forense

2.3 Matriz de Verificación E3I (Plantilla Operativa)

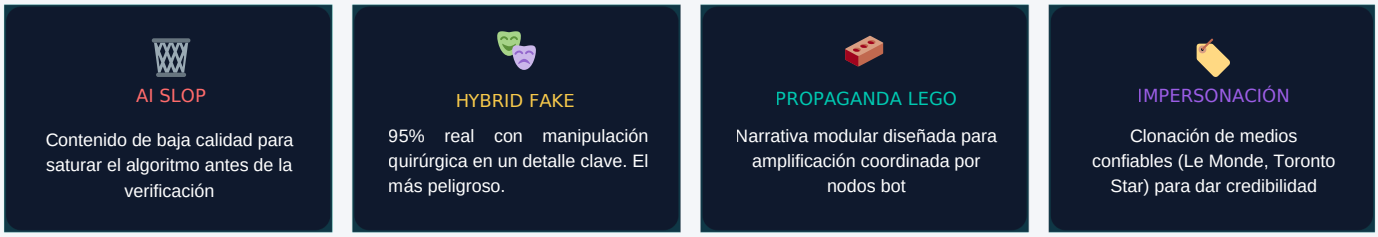
FUENTE	NIVEL DE CERTEZA	INTERESES / NARRATIVA	MÉTODO DE VERIFICACIÓN	ESTADO
Canal de Telegram X	Probable	Afín a grupo armado; busca impacto viral	Cruce con SunCalc, imágenes satelitales	⏳ En proceso
Fact-checker estatal (GFCN/TASS)	No verificado	Propaganda disfrazada de fact- checking	Contraste con satélite de alta resolución.	❌ Descartado
Perfil de red social (testigo)	Confirmado	Testigo presencial (Paciente Cero)	Geolocalización positiva en Nominatim	✅ Verificado
Documento PDF oficial	Probable	Fuente primaria gubernamental	Metadatos, firma digital, cruce documental	⏳ En proceso

Flujo de Trabajo Completo E3I — 10 Pasos

Diagrama del proceso completo de investigación OSINT, desde la hipótesis inicial hasta la publicación con estándar de auditoría.



Tipos de Contenido Sintético — Alerta Temprana



Herramientas Clave por Pilar E3I

PILAR	HERRAMIENTAS PRINCIPALES	FUNCIÓN EN LA INVESTIGACIÓN
ESCENARIOS	Árboles de hipótesis, análisis de narrativa, mapas de actores	Prevenir sesgo de confirmación; construir hipótesis alternativas antes de buscar
INFORMACIÓN	Google (ops), OCCRP Aleph, NINA, Archive.today, Hunchly, Pinpoint	Recolección sistemática con cadena de custodia documentada
INCIDENCIA	Gephi, CrowdTangle, Bot Sentinel, Botometer, análisis de grafo	Mapear redes de amplificación; identificar Paciente Cero y coordinación de bots
INTELIGENCIA	Matrices E3I, NotebookLM, Flourish, QGIS, draw.io	Síntesis y comunicación de evidencia verificada a editores y tribunales

Plataformas Regionales — América Latina

NINA (CLIP)
21 países latinoamericanos. Mapear contratistas y flujos de fondos públicos. Cruzar con registros de propiedad.

Cruzagrafos
Brasil (Abraji). Grafo interactivo: candidatos, empresas, deudores. Ideal para elecciones.

OpenCorporates
130+ países. Registros de empresas y directores. Detectar empresas fantasma con mismo agente.

OCCRP Aleph
Global. Búsqueda en filtraciones masivas: Panama Papers, FinCEN Files, Pandora Papers.

Offshore Leaks
ICIJ. Estructuras offshore y beneficiarios reales. Cruzar con funcionarios públicos.

OpenSanctions
Global. Personas y entidades en listas de sanciones. Verificar antes de publicar nombres.

💡 **Consejo Operativo — Combinación Poderosa**

Combinar site: con filetype: es especialmente poderoso para extraer bases de datos gubernamentales que no están enlazadas en la navegación principal. Muchos portales de contratación pública tienen decenas de documentos indexados por Google que **nunca aparecen en su buscador interno**.

CAPÍTULO 03

Ética y Deontología del Investigador OSINT

En el ecosistema informativo de 2026, la ética no es un freno moralista a la investigación: es su **infraestructura de credibilidad**. La integridad del proceso técnico es tan crítica como el hallazgo mismo.

Código Deontológico — Protocolo 2026

🚫

Prohibición Absoluta de Hacking y Doxxing
El acceso se limita estrictamente a fuentes abiertas y legales. La obtención de datos mediante acceso no autorizado no convierte la información en legítima.

🔍

Verificación del Paciente Cero
Obligación de rastrear la fuente original de todo contenido antes de cualquier publicación. La fuente cero distingue al testigo ocular del nodo de amplificación bot.

🤖

Human-in-the-Loop
Ninguna herramienta de IA sustituye el juicio final del investigador humano. La IA produce *leads*, no veredictos. El criterio editorial siempre es humano.

📦

Preservación de Evidencia Volátil
Uso obligatorio de Archive.today / Hunchly. Los sitios de estafas desaparecen en menos de 24 horas. Preservar es el primer acto de toda investigación.

🎯

Mitigación del Sesgo de Confirmación
El investigador E3I debe buscar activamente evidencia que **falsifique** su propia hipótesis, no solo evidencia que la confirme.

📢

Transparencia Metodológica Total
Mostrar el camino, no solo el resultado. El lector, el editor y el tribunal deben poder reproducir el proceso de verificación con las mismas herramientas.

🛡️

No Revictimización
Manejo sensible de "desecaciones digitales", videos de IA que recrean víctimas de crímenes, y material que pueda causar daño secundario.

🏷️

Detección de Impersonación de Marca
Verificar dominios y metadatos antes de citar una fuente como legítima. Evitar ser vectores de redes que clonan medios confiables.

3.3 La Tensión Berkeley: Periodismo vs. Estándar Judicial

El Protocolo de Berkeley, diseñado para la admisibilidad de pruebas en tribunales internacionales, establece un estándar de preservación digital exhaustivo que a menudo entra en tensión con las necesidades del periodismo de alto impacto.

⚖ Estándar Berkeley

- Cadena de custodia formal y completa
- Hash criptográficos de cada captura
- Metadatos de preservación exhaustivos
- Admisibilidad en cortes internacionales

⟺

Periodismo de Alto Impacto

- Rendición de cuentas pública inmediata
- Velocidad de publicación como factor
- Recursos y tiempo limitados
- Audiencia ciudadana, no jueces

✅ Solución Práctica E3I

Adoptar el **estándar Berkeley como mínimo metodológico**, pero documentar explícitamente las decisiones editoriales que se apartan de él y por qué. Una investigación que puede demostrar su proceso —aunque no cumpla todos los requisitos de admisibilidad judicial— es infinitamente más robusta que una que no documenta nada.

Dilemas Éticos Frecuentes

⚠ DILEMA — EL INFORMANTE INVOLUNTARIO

El ciudadano que documenta sin saberlo

Situación: Un ciudadano publica en redes sociales un video que documenta una violación de derechos humanos sin saber que lo está haciendo.

Tensión: Usar ese video puede exponer al publicador a represalias. No usarlo puede dejar sin documentación un crimen.

- P1 Archivar el contenido inmediatamente con hash criptográfico
- P2 Intentar contactar a la persona para obtener consentimiento informado
- P3 Si el riesgo es alto, usar la evidencia solo en forma desglosada sin atribución directa
- P4 Coordinar con organizaciones de protección de periodistas si hay riesgo real

PARTE II

Herramientas & Técnicas Operativas

Capítulos 4 al 9: búsqueda avanzada, visualización, verificación multimedia, detección de deepfakes, investigación de estafas y uso de inteligencia artificial como herramienta analítica.

CAP. 4 — BÚSQUEDA

CAP. 5 — VISUALIZACIÓN

CAP. 6 — MULTIMEDIA

CAP. 7 — DEEPFAKES

CAP. 8 — DESINFORMACIÓN

CAP. 9 — IA ANALÍTICA

CAPÍTULO 04

Búsqueda Avanzada y Conectores de Datos

Los operadores booleanos y los operadores especiales de Google permiten filtrar millones de resultados con precisión quirúrgica. Esta es la base de cualquier investigación OSINT.

4.1 Operadores de Google para Periodismo de Investigación

site:
Restringe la búsqueda a un dominio específico
`site:contraloría.gob.ec licitación`

filetype:
Busca tipos de archivo específicos (pdf, xls, doc)
`filetype:pdf contrato minero`

"frase"
Busca la cadena de texto exacta
`"acuerdo de no divulgación"`

allintitle:
Solo páginas con las palabras en el título
`allintitle:lavado constructora`

inurl:
Palabras clave en la URL de la página
`inurl:declaracion patrimonial`

AND/OR/-
Combinar o excluir términos de la búsqueda
`corrupción AND -deporte`

before:
Filtrar resultados anteriores a una fecha
`before:2023-01-01`

cache:
Ver versión cacheada de una página eliminada
`cache:sitio-estafa.com`

4.3 Google Pinpoint — Gestión Forense de Archivos Masivos

Pinpoint identifica automáticamente entidades (personas, lugares, organizaciones, fechas) en miles de PDFs, imágenes escaneadas y archivos de audio. Crea un índice de búsqueda inmediato sobre documentos que requerirían semanas de lectura manual.

▶ FLUJO DE TRABAJO CON PINPOINT

1. Paso 1: Subir el corpus documental (contratos, facturas, declaraciones, audios) en bloque.
2. Paso 2: Usar la búsqueda de entidades para identificar personas y organizaciones en múltiples documentos.
3. Paso 3: Exportar los fragmentos relevantes con su referencia de documento y página.
4. Paso 4: Cruzar las entidades identificadas con bases de datos externas (OpenCorporates, OCCRP Aleph).
5. Paso 5: Usar "Clusters" para identificar documentos relacionados temáticamente que no comparten palabras clave obvias.

4.4 Preservación de Evidencia Digital — El Imperativo del Archivo

La evidencia digital es inherentemente volátil. Las páginas de estafas desaparecen en menos de 24 horas. Los posts son eliminados antes de que el primer artículo se publique. La preservación inmediata no es una práctica opcional: **es el primer acto de toda investigación OSINT.**

HERRAMIENTA	FUNCIÓN	VENTAJA CLAVE	CUÁNDO USARLA
Archive.today (archive.ph)	Captura inmutable de páginas web	URL permanente, jurídicamente admisible, incluye metadatos de tiempo	Primer paso ante cualquier fuente web
Wayback Machine	Historial de versiones de páginas web	Detectar cambios retroactivos en páginas institucionales	Verificar si una página fue modificada
Hunchly	Registro automático de páginas visitadas	Timestamps y hash criptográficos automáticos para cada captura	Durante toda la fase de investigación
HTTrack	Descarga de sitios web completos	Incluye imágenes, CSS y JavaScript antes de que sean eliminados	Ante inminente desaparición de un sitio
yt-dlp	Descarga de videos con metadatos	Preserva timestamps, geolocalización y metadatos originales del video	Videos en redes sociales que pueden borrarse

> ⚡ **Regla de Oro de la Preservación**
>
> **Preservar antes de analizar.** Nunca hacer clic en "compartir" o "citar" antes de haber guardado el original con hash criptográfico. Una fuente sin preservación es una fuente perdida.

Conectividad Global — Bases de Datos Esenciales

BASE DE DATOS	COBERTURA	TIPO DE INFORMACIÓN	PRO-TIP
OCCRP Aleph	Global	Panama Papers, FinCEN, Pandora Papers, documentos gubernamentales	Buscar el nombre en múltiples idiomas y variaciones
OpenCorporates	130+ países	Registros de empresas, directores, agentes registrados	Buscar empresas con mismo agente en múltiples jurisdicciones
Offshore Leaks (ICIJ)	Global	Estructuras offshore, beneficiarios reales, paraísos fiscales	Cruzar con listas de funcionarios públicos y contratos
OpenSanctions	Global	Personas y entidades en listas de sanciones internacionales	Verificar antes de publicar nombres de sospechosos

CAPÍTULO 05

Análisis y Visualización Avanzada de Datos

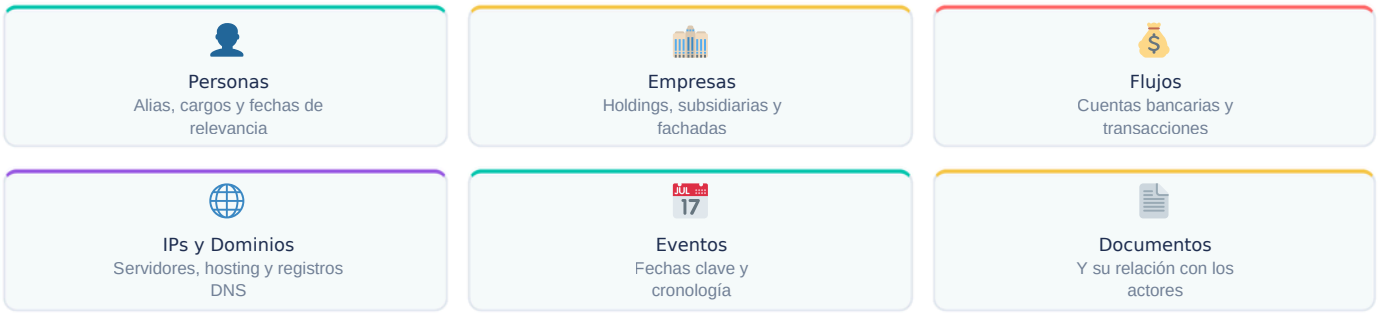
La visualización no es decoración editorial: es una **herramienta cognitiva** que permite ver patrones que el análisis tabular no revela, y al lector comprender relaciones complejas en segundos.

Kit de Herramientas de Visualización E3I

HERRAMIENTA	TIPO DE ANÁLISIS	APLICACIÓN PERIODÍSTICA	NIVEL
Gephi	Análisis de redes (grafo)	Mapear redes de influencia, estructuras de corrupción transnacional	Avanzado
Flourish	Narrativa visual interactiva	Mapas de calor, gráficos animados, timelines de eventos	Básico
Graphext	Análisis masivo sin código	Detectar relaciones inusuales en licitaciones y redes sociales	Intermedio
QGIS / uMap	Cartografía de datos	Incidentes georreferenciados, zonas de conflicto, contratos por región	Intermedio
Datawrapper	Gráficos publicables	Integración directa en artículos digitales, sin código requerido	Básico
Palladio (Stanford)	Análisis histórico de redes	Conexiones entre personas y organizaciones a lo largo del tiempo	Intermedio
draw.io	Murder Board digital	Conectar IPs, URLs y empresas fachada en investigaciones de estafas	Básico

5.2 El Murder Board Digital — Conectando los Puntos

El "Murder Board" —el tablero de evidencia de los thrillers policiales— tiene su equivalente digital en las herramientas de mapeo de relaciones. Para investigaciones de crimen organizado, el investigador E3I construye un grafo visual que conecta:



5.3 NotebookLM y la IA como Interlocutor Analítico

NotebookLM (Google) permite cargar un corpus documental —contratos, informes, filtraciones— y hacerle preguntas en lenguaje natural. **Técnica Adversarial Red Teaming:** cargar el corpus completo y pedirle a la IA que argumente en contra de tu hipótesis principal. Esto revela las debilidades antes de la publicación y fortalece la investigación.

CAPÍTULO 06

Verificación Multimedia y Forense Visual

La verificación de imágenes y videos es una disciplina forense que combina análisis geoespacial, cronológico y técnico. La geolocalización es el arte de leer el espacio; la cronolocalización convierte el tiempo en evidencia.

6.1 Geolocalización — Herramientas y Metodología

HERRAMIENTA	FUNCIÓN	APLICACIÓN FORENSE
SunCalc	Calcular posición solar para una fecha y lugar	Verificar hora y fecha de una foto/video por ángulo de sombras
Google Earth Pro	Visualización satelital histórica	Comparar escenas pasadas y presentes; medir distancias
Sentinel Hub / TerraServer	Imágenes satelitales de alta resolución	Verificar cambios en el terreno; confirmar coordenadas
Nominatim (OpenStreetMap)	Geocodificación y mapas colaborativos	Identificar calles, edificios y referencias geográficas en imágenes
What3Words / Plus Codes	Sistemas de coordenadas por palabras	Precisar ubicaciones en zonas sin dirección convencional
ExifTool	Extracción de metadatos EXIF	Obtener coordenadas GPS, cámara, fecha y hora de captura

📍 CASO DE ESTUDIO — GEOLOCALIZACIÓN FORENSE

Werfalli y la Brigada Al-Saiqa (Libia, 2017)

La metodología de las "migajas forenses": una ejecución extrajudicial documentada y admitida en la Corte Penal Internacional usando exclusivamente fuentes abiertas.

- E1 Identificar las coordenadas de un patio en Bengasi (32.0231, 20.0291) desde imágenes en redes
- E2 sociales Sincronizar ángulo de sombras con SunCalc → confirmar fecha: 17 de julio de 2017
- E3 Cruzar con imágenes satelitales de TerraServer → identificar 15 manchas oscuras en el patio
- E4 Combinar evidencias → pieza OSINT admitida como prueba en la CPI

6.3 Forense de Audio y Balística Acústica

El análisis acústico permite identificar el tipo de arma utilizada en un incidente armado, la posición del tirador relativa a la cámara, y si los disparos ocurrieron antes o después del video. En el caso Abelardo Liz (Colombia), la "balística del silencio" —el tiempo entre el destello y el sonido — permitió reconstruir la escena del asesinato.

💡 **Pro-tip Acústico**

El sonido viaja a ~343 m/s. Cada segundo de diferencia entre el destello y el disparo = ~343 metros de distancia al tirador.

CAPÍTULO 07

Detección de Contenido Generado por IA y Deepfakes

La frontera más peligrosa del periodismo en 2026 es el **Hybrid Fake**: el 95% de la imagen es real, con una manipulación quirúrgica en un detalle clave. La "estética Hollywood" es la primera señal de alerta.

7.2 Señales de Alerta — La "Estética Hollywood"

✨ PIEL PERFECTA
Sin poros, arrugas ni imperfecciones naturales

👁 OJOS ANÓMALOS
Reflejo de luz inconsistente o pupilas irregulares

💡 ILUMINACIÓN IRREAL
Sombras que no corresponden a una fuente de luz coherente

📐 GEOMETRÍA RÍGIDA
Simetría perfecta y proporciones físicamente improbables

Protocolo de Verificación de Contenido Sintético — 5 Pasos

PASO	TÉCNICA	PROCEDIMIENTO
PASO 1	**Señales visuales**	Detectar "estética Hollywood": simetría perfecta, piel sin poros, iluminación homogénea e irreal
PASO 2	**Técnica Hany Farid**	Analizar física inconsistente: reflejo de luz en ojos, geometría de la escena, proporciones espaciales
PASO 3	**Ruido residual**	La IA genera firmas estadísticas detectables en el patrón de ruido. Analizar con herramientas especializadas.
PASO 4	**Contexto y metadatos**	Verificar metadatos EXIF, rastrear Paciente Cero, ejecutar búsqueda inversa en Google/TinEye/Yandex
PASO 5	**Human-in-the-Loop**	Ningún detector automático es definitivo. El juicio humano es el árbitro final. La IA produce leads, no veredictos.

Sensity AI
Detección de deepfakes en videos e imágenes. Alta precisión para rostros manipulados.

TrueMedia.org
Plataforma abierta de verificación de contenido sintético para periodistas.

FotoForensics
Análisis de Error Level Analysis (ELA) para detectar manipulaciones en imágenes JPEG.

CAPÍTULO 08

Investigación de Redes de Desinformación y Estafas

El ecosistema criminal digital integra tecnologías de IA generativa, redes publicitarias opacas y estructuras de empresa fantasma para operar estafas a escala global. Investigarlas requiere metodología OSINT de alta precisión.

8.2 Primer Paso Contraintuitivo — Apagar el Bloqueador de Anuncios

> 💡 **Técnica Clave**
>
> Los anuncios de sitios de estafa revelan la red publicitaria que los financia y permiten rastrear al operador. El bloqueador oculta evidencia crucial. **Usar siempre una máquina virtual aislada para esta fase**: nunca el dispositivo de trabajo habitual. Registrar metadatos de los anuncios: URL del tracker, red publicitaria, parámetros de targeting.

8.3 Detección de Fact-Checkers Estatales

La desinformación institucional —propagada por organismos estatales bajo la apariencia de verificación— es una de las formas más peligrosas de manipulación informativa. Algunos actores forman parte de redes como GFCN mientras operan como órganos de propaganda.

SEÑAL DE ALERTA	MÉTODO DE DETECCIÓN	ACCIÓN
Verificaciones que solo desmienten información crítica al gobierno	Analizar historial completo de fact-checks publicados	Catalogar como fuente sesgada, no citar sin atribución clara
Sin metodología pública disponible	Revisar sitio web en busca de sección de metodología	Rechazar como fuente OSINT primaria
Financiamiento estatal directo sin independencia editorial	Verificar declaraciones de conflicto de interés	Tratar como fuente primaria oficial, con reservas

8.4 Flujo de Investigación de Estafas Digitales

▶ PROTOCOLO ANTI-ESTAFA E3I

1. Captura inmediata: Archive.today del sitio. Las páginas de estafa desaparecen en menos de 24 horas.
2. WHOIS y registrosDNS: Identificar registrador, hosting y variaciones del dominio. Buscar dominios hermanos.
3. Análisis de anuncios: Desactivar bloqueador en VM. Capturar URLs de trackers y redes publicitarias.
4. Grafo de dominios: Construir en draw.io el mapa de dominios, IPs y certificados SSL compartidos.
5. Identidades falsas: Verificar con búsqueda inversa de imagen las fotos de "testimonios" y "expertos".
6. Perfil de víctimas: Identificar comunidades afectadas sin exponer a víctimas secundariamente.
7. Ética de publicación: Contactar a las marcas impersonadas antes de publicar. Notificar a autoridades si hay víctimas activas.

CAPÍTULO 09

Uso de IA y Agentes Digitales en la Investigación

La IA no reemplaza al periodista: lo convierte en un analista de inteligencia con capacidades ampliadas. El rol del investigador es la pregunta; el rol de la IA es ampliar el rango de respuestas posibles.

9.2 Chatbots como Detectives — El Arte de la Pregunta Neutral

La manera en que se formula la pregunta a un chatbot determina en gran medida la calidad de la respuesta. El investigador E3I usa preguntas neutras y abiertas para evitar que el modelo confirme sesgos previos.

TIPO DE PREGUNTA	EJEMPLO INEFICAZ ❌	EJEMPLO EFICAZ ✅
Verificación de hipótesis	"¿Es verdad que X funcionario robó fondos?"	"¿Qué factores podrían explicar las discrepancias entre los contratos públicos de X institución?"
Análisis de fuente	"¿Este medio es confiable?"	"¿Qué criterios usarías para evaluar la credibilidad metodológica de este medio?"
Red-teaming	"Confirma mi teoría sobre esta red de estafa"	"¿Qué argumentos refutarían la hipótesis de que estas empresas están coordinadas?"

Herramientas de IA para Investigación Periodística

NotebookLM
Cargar corpus documental y hacer preguntas. Adversarial red-teaming de hipótesis.

Claude / ChatGPT
Análisis, síntesis y generación de hipótesis alternativas. Nunca árbitro final.

Perplexity
Búsqueda con citación directa. Útil para verificación rápida de hechos con fuentes.

Agentes de monitoreo
Tracking automatizado de keywords, dominios y actores en tiempo real.

Whisper (OpenAI)
Transcripción automática de audios y videos para análisis de contenido.

GPT-4 Vision
Análisis de imágenes para descripción de escenas, texto en imágenes y objetos.

⚠ **Límite Irrenunciable**

Ningún modelo de IA puede verificar hechos de manera definitiva. La IA **puede acelerar la investigación** pero nunca puede ser la fuente primaria de una publicación. Toda afirmación generada por IA requiere verificación independiente con fuentes primarias.

PARTE III

Seguridad Digital y de Campo

En varios países de la región, investigar es una actividad de riesgo real. La sección de seguridad, deliberadamente extensa, refleja una realidad incómoda: el oficio que no enseña a sus practicantes a protegerse es un oficio que los abandona.

CAP. 10
Análisis de Riesgos Digitales

CAP. 11
Análisis de Riesgos en Campo

CAP. 12
Seguridad Operativa (OPSEC)

CAPÍTULO 10

Análisis de Riesgos Digitales

La seguridad digital no es un accesorio opcional: es una condición necesaria para el ejercicio del periodismo de investigación. El modelo de amenazas exige **pensar como el adversario** antes de comenzar.

10.1 El Modelo de Amenazas — Pensar como el Adversario

ADVERSARIO TÍPICO	VECTOR DE ATAQUE	CONTRAMEDIDA PRINCIPAL
Actor estatal	Spyware (Pegasus, Predator), interceptación legal	Tails OS + Signal + dispositivos separados
Crimen organizado	Phishing dirigido (spear-phishing), doxing	2FA fuerte + gestores de contraseñas + opsec de identidad
Empresas demandantes	SLAPPs (demandas estratégicas), vigilancia contractual	Comunicación cifrada + documentación de fuentes
Hackers oportunistas	Phishing masivo, malware, ransomware	Actualizaciones automáticas + anti-phishing + backups

Mensajería Segura

- → Signal (protocolo de referencia — protocolo abierto y auditado)
- → Element / Matrix (federado, sin servidor central)
- → Briar (peer-to-peer, funciona sin internet)
- → Evitar WhatsApp para comunicación sensible de fuentes

Anonimización y Red

- → Tor Browser para navegación anónima en investigaciones
- → VPN de confianza (no gratuita; preferir ProtonVPN o Mullvad)
- → Tails OS: sistema operativo amnésico que no deja rastros
- → Máquinas virtuales aisladas por cada investigación activa

Contraseñas y 2FA

- → Bitwarden o KeePassXC (gestores de contraseñas de código abierto)
- → 2FA con app autenticadora (no SMS — vulnerable a SIM swapping)
- → Passkeys cuando disponibles como alternativa superior
- → Contraseñas únicas y aleatorias por cada servicio

Detección de Spyware

- → Mobile Verification Toolkit (MVT) — Amnesty International
- → iVerify para dispositivos iOS
- → Monitorear conexiones de red salientes inusuales
- → Revisar permisos de apps periódicamente y tras actualizaciones

CAPÍTULO 11

Análisis de Riesgos en Campo

El periodista como objetivo físico: en zonas de conflicto o con presencia de crimen organizado, el riesgo no es abstracto. Los protocolos de seguridad en campo son tan importantes como los digitales.

11.2 Evaluación de Riesgo — Antes de Desplazarse

FACTOR DE RIESGO	CÓMO EVALUARLO	FUENTE DE INFORMACIÓN
Presencia de actores armados	Mapeo de incidentes recientes en la zona objetivo	ACLED, Armed Conflict Location, reportes locales
Historial de ataques a periodistas	Búsqueda en bases de datos de agresiones	CPJ, RSF, Fundamedios (Ecuador), FLIP (Colombia)
Sensibilidad del tema a cubrir	Evaluación editorial con editor y equipo legal	Protocolo interno de la redacción
Condiciones de salida y evacuación	Mapear rutas alternativas de evacuación	INSI Risk Assessment, Riskline

11.3 Protocolos de Seguridad en Campo

Antes del desplazamiento

- → Compartir itinerario con editor de confianza
- → Memorizar números de emergencia (sin tenerlos guardados)
- → Acordar protocolo de chequeo periódico

Durante el desplazamiento

- → Chequeos periódicos preestablecidos con el editor
- → Minimizar huella digital (GPS, publicaciones)
- → Rutas alternativas siempre identificadas

Ante detención o amenaza

- → Derecho a asistencia consular y legal
- → No revelar identidad de fuentes bajo ningún motivo
- → Contactar CPJ, RSF o Fundamedios inmediatamente

11.5 Salud Mental y Trauma Vicario

El trauma vicario —el impacto psicológico de estar expuesto de manera continua a contenido violento o traumático a través de la investigación— es uno de los riesgos profesionales menos reconocidos del periodismo de investigación.

Protocolo de Gestión del Trauma Vicario

Establecer límites claros de tiempo de exposición a contenido traumático. Comunicar el impacto emocional al editor. Acceder a apoyo psicológico especializado (Dart Center, Fundación Rory Peck). Crear rutinas de "desconexión" entre sesiones de investigación intensa. El autocuidado no es opcional: es una condición de sostenibilidad profesional.

CAPÍTULO 12

Seguridad Operativa (OPSEC) en Investigaciones Sensibles

La seguridad operativa es el conjunto de prácticas que protegen la investigación, las fuentes y al investigador de forma sistémica. El principio central es la **compartimentación**: nadie conoce más de lo que necesita para su tarea.

12.1 El Principio de Compartimentación

CAPA DE COMPARTIMENTACIÓN	QUÉ SEPARAR	HERRAMIENTA RECOMENDADA
Identidades	Identidad real vs. cuentas de investigación (sock puppets)	Navegadores separados + Tails OS + emails temporales
Dispositivos	Equipo de trabajo habitual vs. equipo de investigación sensible	Dispositivo dedicado + Tails OS en USB cifrado
Investigaciones	Cada investigación activa en un entorno separado	Máquinas virtuales separadas por caso
Comunicaciones	Canales de trabajo vs. canales seguros con fuentes	Signal + email cifrado (Proton Mail)

12.3 Detección de Spyware — Señales de Alerta

🔋 Batería se agota rápidamente

El spyware corre en segundo plano constantemente. Consumo elevado sin justificación puede ser señal de monitoreo activo.

📡 Datos móviles elevados

Transmisión silenciosa de datos al servidor del atacante. Revisar estadísticas de uso por aplicación regularmente.

🌡️ Dispositivo se calienta en reposo

Procesamiento en segundo plano intensivo. Puede indicar actividad de malware o spyware activo.

📱 Comportamientos extraños

Micrófonos o cámaras que se activan solos, pantalla que se ilumina sin interacción, apps no instaladas.

12.4 Organizaciones de Apoyo

Access Now
Línea de asistencia digital 24/7 para periodistas en riesgo. helpline@accessnow.org

CPJ (Protección)
Committee to Protect Journalists. Asistencia en casos de detención y amenaza.

Amnesty Tech
Laboratorio de seguridad digital. Desarrolladores del MVT (Mobile Verification Toolkit).

CAPÍTULO 13

Del Análisis a la Narrativa Publicable

La arquitectura de una pieza OSINT no sigue la pirámide invertida del periodismo tradicional. Debe demostrar el proceso, no solo el resultado. El lector, el editor y el tribunal deben poder reproducirla.

13.1 Arquitectura de una Pieza OSINT

1. **Hallazgo Central (Lead)**
   La conclusión más importante, con la evidencia más sólida que la respalda directamente.
2. **Contexto y Antecedentes**
   Por qué importa. Quién es afectado. Historia previa del fenómeno investigado.
3. **Metodología Explícita**
   Cómo se obtuvo y verificó la evidencia. Qué herramientas se usaron y por qué son confiables.
4. **Evidencia Organizada**
   Piezas de evidencia presentadas en orden lógico, con visualizaciones que facilitan la comprensión.
5. **Derecho a Réplica y Limitaciones**
   Respuesta de los actores señalados. Qué preguntas quedan abiertas. Alcance y limitaciones del trabajo.

13.3 Lista de Verificación Editorial Final — Los 10 Puntos

- [ ] ¿Toda afirmación está respaldada por al menos dos fuentes independientes?
- [ ] ¿Toda fuente digital ha sido preservada con Archive.today o equivalente?
- [ ] ¿Se ha ofrecido derecho a réplica a todos los señalados?
- [ ] ¿La metodología está explicada de manera que un tercero pueda reproducirla?
- [ ] ¿Se han identificado y declarado los conflictos de interés del equipo?
- [ ] ¿La identidad de fuentes en riesgo está protegida en todos los archivos?
- [ ] ¿El equipo legal ha revisado implicaciones de responsabilidad?
- [ ] ¿Las visualizaciones son precisas y no distorsionan los datos?
- [ ] ¿Se han buscado activamente argumentos que refuten las conclusiones?
- [ ] ¿El archivo de evidencia cumple estándar Berkeley para potencial uso judicial?

CAPÍTULO 14

Investigación Colaborativa y Redes Transnacionales

El periodismo de consorcio —en el que múltiples redacciones de distintos países colaboran en una investigación conjunta— ha producido los mayores impactos del periodismo de investigación moderno: Panama Papers, FinCEN Files, Pandora Papers.

14.1 El Modelo de Periodismo de Consorcio

🌐 ICIJ (International Consortium of Investigative Journalists)

Coordinador de las filtraciones más grandes de la historia: Panama Papers (2016), Paradise Papers (2017), FinCEN Files (2020), Pandora Papers (2021). Modelo de referencia de colaboración distribuida.

🔗 OCCRP (Organized Crime and Corruption Reporting Project)

Red de medios de investigación de Europa del Este, Asia Central y América Latina. Especialistas en crimen organizado transnacional.

🔍 Forbidden Stories

Especialistas en continuar el trabajo de periodistas asesinados o amenazados. Coordinaron el Proyecto Pegasus (2021).

🌎 Redes Regionales — América Latina

CONNECTAS, CLIP (Colombia), Abraji (Brasil), El Faro (Centroamérica). Redes regionales con acceso a fuentes y contexto local irreemplazable.

14.2 Plataformas de Colaboración Segura

PLATAFORMA	USO PRINCIPAL	NIVEL DE SEGURIDAD
Signal (grupos)	Comunicación en tiempo real entre el equipo	Alto
ProtonDrive	Almacenamiento compartido de documentos cifrados	Alto
SecureDrop	Recepción anónima de documentos de filtradores	Máximo
Element (Matrix)	Chat seguro con salas dedicadas por investigación	Alto
Keybase	Mensajería cifrada con verificación de identidad	Medio
Google Drive / Notion	Solo para información NO sensible del proyecto	Bajo

⚠ Regla de Oro de la Colaboración

Nunca compartir información sobre fuentes en plataformas no cifradas. El nivel de seguridad de la colaboración se determina por el eslabón más débil de la cadena. Un periodista con seguridad deficiente compromete a todo el consorcio.

CAPÍTULO 15

Casos de Estudio Integrales

Tres investigaciones reales que aplicaron la metodología OSINT y alcanzaron impacto judicial, mediático o de política pública. Cada uno ilustra un conjunto diferente de técnicas del modelo E3I.

CASO 1 — LIBIA, 2017-2020

Werfalli y la Brigada Al-Saiqa — La Metodología de las Migajas Forenses

El comandante libio Mahmoud Mustafa Busayf al-Werfalli fue identificado como responsable de ejecuciones extrajudiciales usando exclusivamente fuentes abiertas. La evidencia fue admitida en la Corte Penal Internacional.

- T1 Videos publicados en redes sociales con ejecuciones → preservación inmediata con Archive.today
- T2 Geolocalización con Google Earth → patio en Bengasi (coordenadas 32.0231, 20.0291)
- T3 SunCalc → sincronización de sombras confirma fecha: 17 de julio de 2017
- T4 Imágenes TerraServer → 15 manchas oscuras en el patio corroboran la escena
- R **Resultado:** Pieza OSINT admitida como evidencia en la CPI. Primer caso de este tipo en la historia.

CASO 2 — COLOMBIA

Asesinato de Abelardo Liz — La Balística del Silencio

El análisis acústico del video del asesinato permitió reconstruir la escena completa: posición del tirador, tipo de arma y distancia al objetivo. Una técnica de forense de audio aplicada al periodismo.

- T1 Video capturado por testigo → preservar metadatos originales del audio antes de cualquier procesamiento
- T2 Análisis de la diferencia temporal entre el destello del disparo y el sonido de detonación
- T3 Cálculo: tiempo × 343 m/s = distancia al tirador. Identificación del tipo de arma por firma acústica.
- R **Resultado:** Reconstrucción forense completa de la escena del crimen aportada a investigación judicial.

CASO 3 — REGIONAL, 2024

Red de Estafas de Inversión con Impersonación de Marca

Una red de 47+ dominios usaba logos de medios internacionales para dar credibilidad a estafas de inversión con IA. Investigación llevó al desmantelamiento de la red y notificación a las marcas afectadas.

- T1 Anuncio en redes sociales → desactivar bloqueador en VM → capturar URL del tracker publicitario
- T2 WHOIS y registros SSL → identificar hosting compartido con 46 dominios adicionales
- T3 Grafo en draw.io: 47 dominios, 3 IPs, 2 registradores, 1 red publicitaria central
- T4 Búsqueda inversa de imágenes de "testimonios" → todos eran fotos de stock o deepfakes
- R **Resultado:** 47 dominios desmantelados. Notificación a medios impersonados. Denuncia a autoridades.

CAPÍTULO 16

Aplicación del Modelo E3I — Ejercicios Prácticos

Dos ejercicios guiados que aplican la metodología E3I completa. Están diseñados para realizarse en equipos de 2-3 personas con tiempo límite para simular condiciones reales de redacción.

Ejercicio 1 — Verificación de Video Viral

Objetivo: Determinar la autenticidad, origen y contexto de un video viral en redes sociales en menos de 2 horas.

▶ PROCEDIMIENTO PASO A PASO

1. Preservación inmediata (5 min): Archive.today del post original. Capturar metadata del video con ExifTool si es accesible.
2. Búsqueda inversa (15 min): Subir captura del video a Google Lens, TinEye y Yandex Images. Buscar apariciones anteriores del mismo contenido.
3. Análisis de metadatos (10 min): Verificar si el video tiene coordenadas GPS, fecha de creación o información de dispositivo en los metadatos EXIF.
4. Geolocalización (30 min): Identificar elementos visuales (edificios, señales, vegetación, terreno). Comparar con Google Earth, Mapillary, Street View.
5. Cronolocalización (20 min): Si hay sombras, usar SunCalc para el lugar identificado. Confirmar si la hora y fecha coinciden con el contexto declarado.
6. Rastreo del Paciente Cero (20 min): Identificar cuál fue la primera publicación del video antes de su viralización. ¿La fecha del contexto original coincide con el contexto del Paciente Cero?
7. Síntesis y conclusión (20 min): Completar la Matriz de Verificación E3I. Clasificar: Verificado / No verificado / Falso / Contexto erróneo.

Ejercicio 2 — Investigación de Contratista Público

Objetivo: Mapear las redes de contratación pública de un funcionario o empresa en una semana de trabajo.

▶ PROCEDIMIENTO PASO A PASO

1. Búsqueda inicial (Día 1): Nombre en OCCRP Aleph, Offshore Leaks y registro civil de empresas local.
2. Contratos públicos (Día 2): `site:contraloría.gob.ec + filetype:pdf` con nombre del contratista. Guardar todos los resultados en Pinpoint.
3. Redes corporativas (Día 3): OpenCorporates para buscar empresas con el mismo agente registrado o directores cruzados. ¿Hay un cluster de empresas relacionadas?
4. Mapeo visual (Día 4): Construir grafo en Gephi o draw.io con: personas, empresas, contratos, montos y fechas. Identificar los nodos más conectados.
5. Verificación cruzada (Día 5): Cruzar con World-Check y OpenSanctions. Verificar declaraciones patrimoniales públicas si están disponibles.
6. Derecho a réplica (Día 6): Contactar a los señalados con preguntas específicas. Dar tiempo razonable para respuesta.
7. Publicación (Día 7): Completar lista de verificación editorial de 10 puntos del Cap. 13. Publicar con metodología explicada.

CONCLUSIONES

El Periodismo como Práctica de Inteligencia Verificable

> *"El periodismo de investigación moderno no es una profesión de héroes solitarios. Es una disciplina colectiva, metodológica y transparente que construye evidencia que resiste el escrutinio más severo. El proceso se convierte en la historia."*
>
> *— Modelo E3I, 2026*

🔭 Lo que cambia

Las plataformas, los algoritmos, las APIs. Las herramientas de IA generativa se actualizan cada semana. Los operadores que hoy funcionan pueden no funcionar mañana.

🧭 Lo que permanece

La hipótesis, el cruce de fuentes, la cadena de custodia, la falsación sistemática, la rendición de cuentas pública. El método no cambia; las herramientas sí.

Fuentes y Referencias Bibliográficas

OSINT Y PERIODISMO

Bellingcat — Online Investigation Toolkit (2023)
OCCRP — Investigation Handbook
Silverman, C. — Verification Handbook (EJC)
First Draft — Essential Guide to Understanding Information Disorder
Deibert, R. — Black Code: Surveillance, Privacy, and the Dark Side

SEGURIDAD DIGITAL

Amnesty International — Security Lab Resources
Access Now — Digital Security Helpline Guidelines
CPJ — Digital Safety Kit for Journalists
EFF — Surveillance Self-Defense
Committee to Protect Journalists — Journalist Safety Guide

DESINFORMACIÓN Y IA

Wardle, C. & Derakhshan, H. — Information Disorder (2017)
Farid, H. — Photo Tampering Throughout History
Stanford Internet Observatory — Research on Coordinated Inauthentic Behavior
Ovadya, A. — Generative Media and the Future of Fact-Checking

INTELIGENCIA ANALÍTICA

Heuer, R. — Psychology of Intelligence Analysis (1999)
Moore, D. — Critical Thinking and Intelligence Analysis (2007)
Marrin, S. — Improving Intelligence Analysis (2011)
Protocolo de Berkeley — Digital Open Source Investigations

REFERENCIA RÁPIDA

Manual OSINT E3I — Tarjeta de Campo

JERARQUÍA EPISTEMOLÓGICA

- DATO → sin contexto, punto de partida, nunca de llegada
- INFORMACIÓN → dato interpretado en contexto temporal, espacial y relacional
- EVIDENCIA → información validada bajo hipótesis falsable
- INTELIGENCIA → síntesis verificada para decisión editorial o judicial

MODELO E3I — NÚCLEO

- **ESCENARIOS:**construir 3 hipótesis antes de buscar (probable, peligroso, contraintuitivo)
- **INFORMACIÓN:**preservar antes de analizar — Archive.today es el primer paso
- **INCIDENCIA:**identificar Paciente Cero y red de amplificación; ¿coordinarán los bots?
- **INTELIGENCIA:**síntesis verificada, publicable y con estándar Berkeley

ÉTICA — IRRENUNCIABLE

- No hacking · No doxxing · No revictimización
- Human-in-loop: la IA produce leads, no veredictos
- Transparencia metodológica total siempre
- Buscar activamente evidencia que falsifique tu hipótesis
- Verificar Paciente Cero antes de cualquier publicación

SEGURIDAD — BÁSICA

- Signal para comunicación con fuentes sensibles
- Tor + VPN para investigación de alto riesgo
- Tails OS para investigaciones más sensibles
- 2FA con app autenticadora, nunca por SMS
- Dispositivos separados por nivel de riesgo

HERRAMIENTAS ESENCIALES

PRESERVAR	BUSCAR	VERIFICAR
Archive.today · Hunchly	OCCRP Aleph · NINA · Pinpoint	SunCalc · Google Earth · ExifTool
Wayback Machine	OpenCorporates · Offshore Leaks	TinEye · Yandex · Gephi

CAP. 1 — AMPLIACIÓN

Taxonomía Completa de Fuentes OSINT

No toda fuente abierta tiene el mismo peso epistemológico. Esta taxonomía ordena las fuentes por su naturaleza, confiabilidad inherente y utilidad en distintas fases del modelo E3I.

1.4 Clasificación de Fuentes por Nivel de Confiabilidad

NIVEL	TIPO DE FUENTE	EJEMPLOS	CÓMO VERIFICAR
A — Alta	Registros oficiales primarios	Registro mercantil, Contraloría, sentencias judiciales, BOE, Gazeta Oficial	Firma digital, sello oficial, cruce con segunda fuente oficial
A — Alta	Filtraciones verificadas y auditadas	Panama Papers (ICIJ), FinCEN Files, Pandora Papers	El ICIJ y OCCRP tienen protocolos de verificación propios
B — Media	Medios de referencia con metodología clara	Reuters, AP, BBC, NYT (con sección de metodología visible)	Verificar que citen fuentes primarias; cruzar con otras dos fuentes
B — Media	Bases de datos académicas y gubernamentales	ACLED, SIPRI, UNHCR, World Bank Open Data	Revisar metodología de recopilación; verificar fecha de actualización
C — Baja	Redes sociales y foros	Twitter/X, Telegram, Reddit, Facebook grupos	Nunca citar sin verificación cruzada; buscar Paciente Cero primero
C — Baja	Medios sin metodología pública	Sitios de agregación, blogs sin autoría, medios estatales	Tratar como pista, no como fuente. Requiere confirmación independiente
D — Rechazar	Fact-checkers estatales de regímenes	TASS "verificaciones", medios de propaganda disfrazados	Analizar historial completo; identificar patrón de selectividad ideológica

1.5 Fuentes OSINT por Tipo de Investigación

💰 Corrupción y Fondos Públicos

OpenSpending, Contraloría nacional, SEACE (Perú), CompraNet (México), Portal de Contrataciones Ecuador, OCCRP Aleph. Cruzar montos con declaraciones patrimoniales.

🏢 Estructuras Corporativas

OpenCorporates, Offshore Leaks ICIJ, registro local de empresas, agentes registrados compartidos (señal de cluster de empresas relacionadas).

🌍 Conflictos y Violaciones de DD.HH.

ACLED, Armed Conflict Location & Event Data, Airwaves (rastreo de aviones), Flightradar24, MarineTraffic, imágenes satelitales Sentinel Hub.

🤖 Desinformación y Redes de Bots

Bot Sentinel, Botometer, Stanford Internet Observatory, DFRLab (Digital Forensic Research Lab), Graphika reportes, CrowdTangle (solo para investigadores).

🌐 Infraestructura Digital

Shodan (dispositivos conectados), Censys, VirusTotal (análisis de dominios), URLScan.io, SecurityTrails (historial DNS), BuiltWith (tecnología de sitios).

✈ Tráfico y Logística

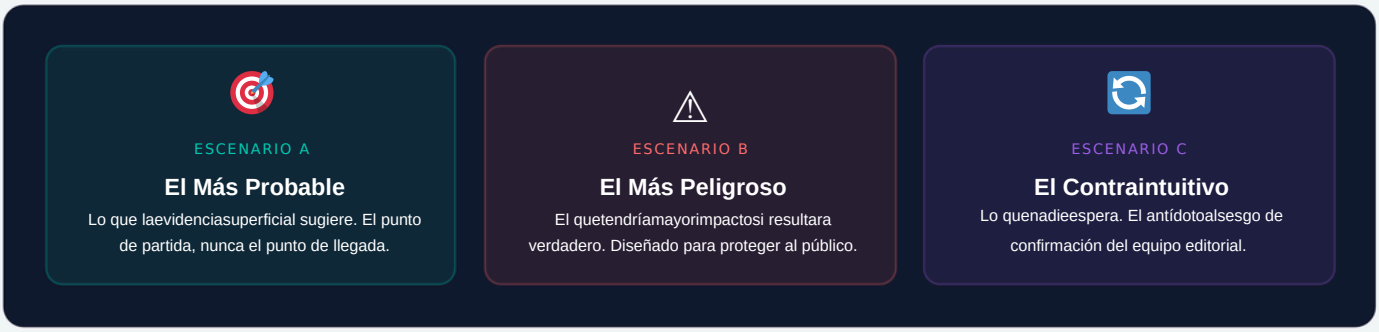
Flightradar24, ADS-B Exchange (sin filtros militares), MarineTraffic, VesselFinder, Global Fishing Watch para actividad pesquera irregular.

CAP. 2 — ESCENARIOS EN PROFUNDIDAD

El Arte del Pensamiento Hipotético Estructurado

El pilar Escenarios es el más contraintuitivo del modelo E3I: exige detener la búsqueda antes de comenzarla y construir hipótesis alternativas, incluyendo aquellas que contradicen la intuición inicial del investigador.

2.4 Metodología de Construcción de Hipótesis — El Triángulo E3I



2.5 Los Cinco Sesgos Cognitivos que Destruyen una Investigación

SESGO	DESCRIPCIÓN	SEÑAL DE ALERTA	ANTÍDOTO
Confirmación	Buscar solo evidencia que confirma la hipótesis inicial	"Todo apunta a que..." antes de completar la búsqueda	Dedicar 30% del tiempo a buscar evidencia contraria
Anclaje	Sobrevalorar el primer dato encontrado	Cambiar raramente la hipótesis inicial a pesar de nueva evidencia	Reconstruir la hipótesis desde cero cada 48 horas
Disponibilidad	Sobrevalorar lo fácil de encontrar sobre lo difícil	Citar solo fuentes de fácil acceso online	Buscar activamente fuentes de difícil acceso
Agrupamiento	Ver patrones en datos aleatorios	"Es demasiada coincidencia para ser casual"	Verificar la base estadística antes de concluir coordinación
Retrospectivo	"Siempre lo supe" — reescribir la memoria del proceso	No documentar los momentos de duda durante la investigación	Llevar un diario de hipótesis con fechas y estados

💡 Técnica del Abogado del Diablo

En cada reunión editorial, designar a un miembro del equipo para argumentar activamente en contra de la hipótesis principal. No como ejercicio retórico, sino como búsqueda genuina de evidencia que la falsifique. Esta práctica —tomada de la inteligencia analítica militar— ha detenido errores graves en redacciones de investigación como el ICIJ y Bellingcat.

CAP. 3 — ÉTICA AVANZADA

Derecho a la Privacidad vs. Interés Público

La tensión entre el derecho a la privacidad y el interés público no tiene resolución universal. El investigador OSINT debe navegarla caso a caso, con criterios claros y documentados para cada decisión.

3.4 Marco de Decisión — Privacidad vs. Interés Público

P1 **¿La persona es un actor público?**
Losfuncionarios,empresariosconcontratos públicos y figuras con poder social tienen una expectativa de privacidad reducida en el ámbito de su función pública.

P2 **¿La información es relevante para su función pública?**
La vida privada de un funcionario no es de interés público solo por ser funcionario. Debe existir una conexión directa con el ejercicio de su cargo.

P3 **¿El daño a la privacidad es proporcional al beneficio público?**
Usar el mínimo de información privada necesaria para demostrar el hallazgo. Principio de mínima intrusión.

P4 **¿Existen terceros vulnerables involucrados?**
Familiares, menor es de edad, víctimas secundarias. Su privacidad está protegida con mayor rigor, independientemente del caso.

3.5 Responsabilidad Legal del Investigador OSINT

RIESGO LEGAL	ORIGEN	MITIGACIÓN
Difamación	Publicar afirmaciones falsas de hecho sobre personas identificables	Verificar cada afirmación con dos fuentes independientes; derecho a réplica documentado
Violación de datos	Publicar información personal protegida (GDPR, Ley de Datos Ecuador)	Consultar con abogado de privacidad antes de publicar datos sensibles
SLAPP	Demandas estratégicas de silenciamiento por parte de actores poderosos	Documentar metodología exhaustivamente; conservar todo el archivo editorial
Acceso no autorizado	Obtener información mediante engaño o acceso sin autorización	Limitarse estrictamente a fuentes abiertas; documentar el método de acceso a cada fuente

Protección Legal Proactiva
Antes de publicar cualquier investigación sensible, el equipo debe: (1) tener el archivo completo de evidencia con cadena de custodia documentada; (2) tener el borrador revisado por asesor legal especializado en prensa; (3) haber enviado preguntas con suficiente tiempo de respuesta a todos los señalados; (4) tener documentada la decisión editorial de publicar y sus fundamentos.

CAP. 4 — BÚSQUEDA AVANZADA

Google Dorks Avanzados y Técnicas de Búsqueda OSINT

Los "Google Dorks" son combinaciones de operadores avanzados que permiten extraer información de bases de datos públicas que el buscador común no indexa en sus primeras páginas de resultados.

4.5 Dorks para Periodismo de Investigación — Recetas Probadas

OBJETIVO	DORK	QUÉ ENCUENTRA
Contratos públicos Ecuador	site:compraspublicas.gob.ec "nombre empresa" filetype:pdf	Contratos adjudicados con documentación completa
Declaraciones patrimoniales	site:contraloria.gob.ec "declaracion patrimonial" "nombre"	Declaraciones de funcionarios públicos indexadas
Documentos internos expuestos	site:gobierno.ec filetype:xls OR filetype:csv confidencial	Archivos que no debían estar públicos
Cámaras sin contraseña	inurl:"/view.shtml" OR inurl:"/view/index.shtml"	Cámaras IP con acceso abierto (uso periodístico: verificar escenas)
Bases de datos expuestas	intitle:"index of" "database" "backup" site:.gov.ec	Directorios de archivos de bases de datos sin protección
Emails en documentos PDF	site:empresa.com filetype:pdf "@empresa.com" contacto	Listas de contactos internas en PDFs públicos
Historial de precios licitaciones	site:contrataciones.gob filetype:pdf "precio unitario" "oferta"	Comparar precios históricos de contratos similares

4.6 Motores Especializados — Más Allá de Google

Shodan
Motor de búsqueda de dispositivos conectados a internet. Cámaras, servidores industriales, routers. Útil para investigar infraestructura de actores sospechosos.

Censys
Similar a Shodan pero con mejor cobertura de certificados SSL. Permite rastrear infraestructura digital de organizaciones a partir de un solo dominio.

PublicWWW
Buscar código fuente de páginas web. Ideal para encontrar sitios que comparten el mismo código de seguimiento (Google Analytics ID), revelando al operador común.

Carrot2
Agrupa resultados de búsqueda en clusters temáticos. Útil para explorar un tema amplio rápidamente e identificar los ángulos más ricos.

Intelligence X
Motor de búsqueda OSINT con acceso a Tor, I2P, y bases de datos de filtraciones. Para investigadores avanzados.

Ahmia
Motor de búsqueda de servicios Tor. Permite investigar mercados negros y foros sin acceder directamente a cada sitio .onion.

⚠ Aviso sobre Shodan y Censys

El acceso a información de dispositivos conectados mediante Shodan o Censys es legal cuando se hace desde las herramientas (no se accede directamente al dispositivo). Documentar siempre que la información fue obtenida mediante búsqueda en el motor, no mediante acceso directo a la infraestructura del investigado.

4.7 Investigación de Personas — Metodología E3I

La investigación de personas en OSINT debe balancear el derecho público a la información con el respeto a la privacidad. El protocolo siguiente aplica solo a figuras públicas en ejercicio de sus funciones.

▶ PROTOCOLO DE INVESTIGACIÓN DE PERSONA PÚBLICA

1. Registro básico: Nombre completo, variaciones (apellidos, alias conocidos). Cédula de identidad si es pública. Cargo actual y anterior.
2. Presencia corporativa: OpenCorporates + registro local. ¿Aparece como director, accionista o representante legal?
3. Presencia en filtraciones: OCCRP Aleph, Offshore Leaks, Open Sanctions. ¿Aparece en alguna lista?
4. Contratos públicos: NINA, portales de contratación nacional. Montos, contrapartes, fechas.
5. Redes sociales: Buscar perfiles con username similar en múltiples plataformas (Sherlock). Archivar contenido relevante.
6. Propiedades y bienes: Si hay registros catastrales públicos, buscar propiedades a nombre de la persona o empresas asociadas.
7. Red de relaciones: Construir grafo de personas y organizaciones relacionadas en Gephi o draw.io.

4.8 Investigación de Redes Sociales — Técnicas Avanzadas

PLATAFORMA	TÉCNICA OSINT	HERRAMIENTA	LIMITACIÓN
Twitter/X	Búsqueda avanzada: from:usuario since:2020-01-01	Advanced Search, Twint (archivado)	API de pago desde 2023; cobertura reducida
Telegram	Buscar canales por keyword; analizar historial de usernames	TGStat, Telemetr.io, búsqueda interna	Canales privados no indexados; requiere acceso
Instagram	Geolocalización por geotag, análisis de seguidores comunes	OSINTgram (con cuenta propia), búsqueda por lugar	API cerrada; scraping viola TOS
Facebook	Graph Search (limitado), análisis de grupos públicos	Who Posted What, Crowdtangle (investigadores)	Datos reducidos post-Cambridge Analytica
LinkedIn	Historial laboral, conexiones en común, empresas asociadas	Búsqueda directa + herramientas de export de perfiles	Bloqueo de scraping; requiere cuenta propia

Sherlock — Rastreo Multi-plataforma de Usernames

Herramienta: Sherlock (código abierto)

Dado un nombre de usuario, Sherlock busca automáticamente en más de 400 plataformas sociales y reporta en cuáles existe un perfil con ese username. **Uso práctico:** cuando se identifica el alias de un sospechoso en una red, Sherlock permite encontrar todos los demás perfiles usando el mismo alias, revelando patrones de comportamiento cross-plataforma.

⚠ Ética del Rastreo de Perfiles

El rastreo de perfiles de personas privadas —no relacionadas directamente con la investigación— puede constituir acoso o vigilancia. La regla E3I: rastrear solo perfiles de personas con función pública relevante para el hallazgo investigado, y documentar la justificación de cada búsqueda.

CAP. 5 — ANÁLISIS DE REDES

Análisis de Redes con Gephi y Herramientas de Grafo

El análisis de redes convierte relaciones complejas en estructuras visuales comprensibles. Para el periodismo de investigación, es la herramienta más poderosa para revelar quién está conectado con quién — y por qué importa.

5.4 Conceptos Fundamentales de Análisis de Redes

CONCEPTO	DEFINICIÓN	IMPORTANCIA PERIODÍSTICA
Nodo (Node)	Un actor en la red: persona, empresa, cuenta de red social, IP	Cada nodo es un posible sujeto de investigación
Arista (Edge)	La relación entre dos nodos: contrato, seguimiento, llamada, transacción	Las aristas son la evidencia de la relación
Grado (Degree)	Número de conexiones de un nodo	Los nodos de alto grado son actores clave; los intermediarios son puentes críticos
Betweenness Centrality	Cuántos caminos cortos entre nodos pasan a través de un nodo	Identifica a los "corredores" o intermediarios que controlan los flujos de información
Clusters (Comunidades)	Grupos de nodos más densamente conectados entre sí que con el resto	Revela organizaciones o redes de amplificación coordinadas
Nodo aislado	Un actor sin conexiones visibles en el grafo actual	Puede indicar que falta información o que el actor opera de forma deliberadamente encubierta

5.5 Flujo de Trabajo Gephi para Investigación Periodística

▶ DE LOS DATOS AL GRAFO PUBLICABLE

1. Preparar los datos: Construir una tabla de nodos (ID, nombre, tipo: persona/empresa/IP) y una tabla de aristas (nodo A, nodo B, tipo de relación, fecha, fuente).
2. Importar en Gephi: File → Import Spreadsheet. Cargar primero los nodos, luego las aristas.
3. Calcular métricas: Statistics → Run: Betweenness Centrality, Modularity (para detectar clusters), Average Degree.
4. Filtrar el grafo: Remover nodos de muy bajo grado si oscurecen la estructura principal. Mantener solo las relaciones verificadas.
5. Layout: Usar Force Atlas 2 para grafos de investigación. Ajustar Gravity y Scaling para separar clusters.
6. Colorear por tipo: Personas en teal, empresas en amber, cuentas sociales en coral. Tamaño de nodo proporcional al Betweenness Centrality.
7. Exportar: Para publicación interactiva, usar sigma.js o Gephi Lite. Para impresión, exportar SVG de alta resolución.

CAP. 6 — FORENSE DIGITAL

Investigación de Infraestructura Digital

Cada sitio web deja huellas digitales: registros WHOIS, certificados SSL, servidores de alojamiento, código de seguimiento publicitario. Leer estas huellas permite identificar al operador real detrás de un sitio anónimo.

6.4 El Mapa Completo de una Infraestructura Web

CAPA	HERRAMIENTA	QUÉ REVELA	URL
Registro del dominio	WHOIS	Registrante, correo, fecha de creación, registrador	whois.domaintools.com
Historial DNS	SecurityTrails	IPs anteriores del dominio, subdominios, cambios de servidor	securitytrails.com
Certificado SSL	crt.sh	Todos los certificados emitidos para un dominio y sus subdominios	crt.sh
IP compartida	VirusTotal / Censys	Otros dominios alojados en la misma IP	virustotal.com
Tecnología del sitio	BuiltWith	CMS, frameworks, widgets de pago, redes publicitarias	builtwith.com
Google Analytics ID	PublicWWW	Sitios que comparten el mismo UA-XXXXXX (operador común)	publicwww.com
Código fuente	Navegador (F12)	Scripts de seguimiento, CDN, metadata de autor, comentarios del código	—

6.5 Técnica del Google Analytics Compartido

📖 TÉCNICA AVANZADA

Un Código de Seguimiento, Cien Sitios de Estafa

Cuando el operador de una red de sitios de desinformación o estafa comete el error de usar el mismo código de Google Analytics en varios de sus dominios, PublicWWW lo revela inmediatamente. Esta técnica fue usada por el Atlantic Council's DFRLab para exponer redes de hasta 200 sitios coordinados.

1. Abrir el código fuente del sitio sospechoso (F12 → Sources)
2. Buscar el patrón "UA-" o "G-" seguido de números (Google Analytics ID)
3. Pegar el ID en PublicWWW → ver todos los sitios que lo usan
4. Mapear la red completa de dominios relacionados en draw.io

6.6 Herramientas de Forense de Imagen — EXIF y Metadatos

ExifTool (CLI)
Extrae todos los metadatos EXIF de imágenes, videos y documentos. Revela GPS, cámara, software de edición y fechas originales.

Jeffrey's Exif Viewer
Versión web de ExifTool. Permite analizar metadatos de imágenes sin instalar software. Ideal para verificación rápida.

FotoForensics (ELA)
Error Level Analysis. Detecta zonas de una imagen que han sido editadas al mostrar diferentes niveles de compresión JPEG.

Forensically
Suite completa de análisis forense visual: ELA, análisis de ruido, clone detection, análisis de histograma. Gratuita y online.

CAP. 7 — FORENSE DE VIDEO

Forense de Video y Análisis Temporal Avanzado

La verificación de video combina análisis de metadatos, cronolocalización solar, análisis de sombras, identificación de referencias geográficas y análisis acústico para confirmar o refutar el contexto declarado de un video.

7.4 Cronolocalización — Convertir el Tiempo en Evidencia

Si se conoce el lugar donde fue tomado un video o foto, SunCalc permite determinar la fecha y hora exactas con alta precisión al calcular el ángulo de las sombras. Este es uno de los métodos más poderosos del arsenal E3I.

▶ PROTOCOLO SUNCALC — PASO A PASO

1. Identificar la ubicación: Geolocalizar el video antes de usar SunCalc. Necesitas las coordenadas exactas.
2. Abrir SunCalc: Navegar a suncalc.org. Introducir las coordenadas identificadas.
3. Medir el ángulodesombra: En el video/foto, medir el ángulo de una sombra larga y clara respecto a su objeto (árbol, poste, edificio).
4. Ajustar lafechaenSunCalc: Modificar la fecha hasta que el ángulo solar en SunCalc coincida con el ángulo medido en la imagen.
5. Confirmar conlahora: La hora en SunCalc también debe coincidir con el contexto declarado del video.
6. Documentar: Captura de pantalla de SunCalc con las coordenadas y la fecha/hora confirmadas. Esta es la evidencia.

7.5 Rastreo de Aviones y Barcos — OSINT de Movimiento

OBJETIVO	HERRAMIENTA	LIMITACIÓN	CASO DE USO
Aviones civiles	Flightradar24, FlightAware	Solo vuelos con transponder ADS-B activo	Rastrear vuelos privados de sospechosos
Aviones militares/sin transponder	ADS-B Exchange (sin filtros)	Cobertura parcial; aviones furtivos no aparecen	Rastrear aeronaves militares rusas pre-invasión Ucrania
Barcos mercantes	MarineTraffic, VesselFinder	Solo barcos con AIS activo; pueden apagarlo	Rastrear barcos de petróleo sancionados
Pesca ilegal	Global Fishing Watch	Actualización con 72h de delay	Detectar pesca en zonas protegidas o sancionadas

🛰️ **Caso Real — Bellingcat y el MH17**

El equipo de Bellingcat usó Flightradar24 y ADS-B Exchange para rastrear los movimientos del lanzador de misiles BUK que derribó el vuelo MH17 en Ucrania en 2014, cruzando datos de avistamientos en redes sociales con registros de movimiento de vehículos militares. El resultado fue admitido como evidencia por el equipo judicial internacional JIT.

CAP. 8 — ESTAFAS DIGITALES

Anatomía de una Estafa con Inteligencia Artificial

Las estafas de inversión con IA siguen un modelo operativo reproducible. Comprender su anatomía es el primer paso para investigarlas y exponerlas.

8.5 Modelo Operativo de una Estafa de Inversión IA — 2026

01 **Impersonación de Marca**
Clonarel diseño visualytipografía de medios confiables (El País, CNN, BBC). Registrar dominios similares: elpais-economia.com, cnn-inversiones.net. Publicar artículos falsos con logotipos reales.

02 **Deepfake de Figura Pública**
Video generado por IA mostrando a un presidente, empresario reconocido o figura de confianza "respaldando" la plataforma de inversión. Distribuido en redes sociales con anuncios pagados.

03 **Plataforma Falsa con "Ganancias"**
Lavíctima ve crecersuinversión enunpanel de control falso. Las "ganancias" son números en una interfaz diseñada para generar confianza. Cuando intenta retirar, se le piden "comisiones" adicionales.

04 **Desaparición del Sitio**
El dominio desaparece antes de que la víctima consulte a autoridades. Los operadores reactivan la estafa en un nuevo dominio con el mismo contenido y nueva impersonación de marca.

8.6 Señales de Alerta — Checklist Anti-Estafa

- [ ] ¿El dominio fue creado recientemente (menos de 6 meses)? WHOIS para verificar.
- [ ] ¿Los testimonios usan fotos de stock? Búsqueda inversa en Google Lens.
- [ ] ¿El sitio impersona a una marca reconocida? Verificar el dominio oficial vs. el sospechoso.
- [ ] ¿Hay videos de celebridades o presidentes "respaldando" el producto? Posible deepfake.
- [ ] ¿Piden criptomonedas o transferencias internacionales? Señal clásica de estafa.
- [ ] ¿El sitio no tiene información de contacto física verificable? Señal crítica.

CAP. 9 — IA PRÁCTICA

Prompt Engineering para Periodistas de Investigación

La calidad de la respuesta de un modelo de IA es directamente proporcional a la calidad de la instrucción que recibe. El prompt engineering es una habilidad crítica para el periodista que usa IA como herramienta analítica.

9.3 Plantillas de Prompts — Recetas Verificadas para Investigación

PROMPT #1 — ANÁLISIS DE CONTRADICCIÓN

"Actúa como un abogado defensor y encuentra todos los argumentos que podrían invalidar la siguiente hipótesis periodística: [HIPÓTESIS]. Sé exhaustivo y prioriza los argumentos más sólidos."

PROMPT #2 — CONTEXTO REGIONAL

"Eres un experto en política y economía de Ecuador. Explica el contexto histórico y político que haría que [HALLAZGO] sea especialmente significativo para una audiencia latinoamericana. No incluyas suposiciones no verificables."

PROMPT #3 — SÍNTESIS DE CORPUS DOCUMENTAL

"A partir de los siguientes documentos [adjuntar], identifica: (1) Las tres relaciones más significativas entre personas y organizaciones. (2) Contradicciones internas entre documentos. (3) Preguntas que quedan sin respuesta. Cita la fuente documental para cada afirmación."

PROMPT #4 — VERIFICACIÓN DE CRONOLOGÍA

"Organiza los siguientes eventos en una línea de tiempo cronológica. Para cada evento, indica: fecha exacta o aproximada, fuente que lo documenta, y si existe alguna inconsistencia temporal con otro evento de la lista. [LISTA DE EVENTOS]"

⚠ Limitaciones que Nunca Olvidar

Los modelos de IA no tienen acceso a información en tiempo real (excepto con herramientas web). Pueden alucinar (inventar) hechos que suenan plausibles. Nunca publicar una afirmación basada solo en la respuesta de un modelo de IA sin verificación con fuentes primarias independientes. La IA es un acelerador del análisis, no un reemplazo de la verificación.

CAP. 10 — SEGURIDAD BÁSICA

Higiene Digital para Periodistas

La higiene digital no requiere conocimientos técnicos avanzados. Requiere hábitos sistemáticos aplicados consistentemente. El 90% de los incidentes de seguridad que afectan a periodistas podrían prevenirse con estas prácticas básicas.

10.5 El Modelo de Capas de Seguridad

Capa 1 — Básica (Todo Periodista)
Contraseñas únicas + gestor de contraseñas (Bitwarden) · 2FA con app autenticadora (no SMS) · Actualizaciones automáticas de SO y apps. Cifrado del disco (FileVault en Mac, BitLocker en Windows) · Navegador con adblocker (uBlock Origin)

Capa 2 — Intermedia (Periodistas de Investigación)
Signal para comunicaciones sensibles · VPN de pago (Mullvad o ProtonVPN) · Correo cifrado (Proton Mail) · Dispositivo separado para investigaciones de alto riesgo · Verificar archivos con VirusTotal antes de abrir

Capa 3 — Avanzada (Investigaciones de Máximo Riesgo)
Tails OS en USB cifrado · Sin teléfono presente en reuniones críticas · SecureDrop para recepción de documentos · Comunicaciones solo en persona para información más sensible · Consulta con Access Now Digital Security Helpline

10.6 El Phishing — La Amenaza Más Frecuente

TIPO DE PHISHING	CÓMO RECONOCERLO	QUÉ HACER
Phishing masivo	Remitente desconocido, urgencia artificial, link sospechoso	No hacer clic. Verificar el dominio real del remitente.
Spear-phishing	Remitente que conoces (o parece ser), referencia a algo real y reciente	Llamar al remitente por otro canal para verificar antes de abrir adjuntos
Whaling	Dirigido específicamente al editor o director. Nivel de personalización muy alto.	Contactar a Access Now. Documentar el intento.

💡 **Regla de los 3 Segundos**

Antes de hacer clic en cualquier link en un email: (1) Pasar el cursor por encima para ver la URL real. (2) Verificar que el dominio coincide exactamente con el esperado. (3) Si hay duda, no clic. Pegar la URL en VirusTotal antes de visitar. Tres segundos de verificación pueden evitar meses de comprometimiento.

CAP. 11 — FUENTES HUMANAS

Manejo de Fuentes Humanas y Protección de Informantes

Las fuentes humanas siguen siendo irreemplazables en el periodismo de investigación. Pero la responsabilidad del periodista hacia sus fuentes va más allá de la promesa de anonimato: incluye minimizar el riesgo digital y físico desde el primer contacto.

11.6 El Primer Contacto Seguro — Protocolo

▶ CÓMO RECIBIR UN INFORMANTE DE FORMA SEGURA

1. SecureDrop como primera línea: Configurar SecureDrop en la redacción permite que los informantes envíen documentos de forma completamente anónima, sin dejar rastros digitales en ninguno de los dos extremos.
2. Signal como segunda línea: Si el informante contacta por otros canales, migrar inmediatamente a Signal con mensajes efímeros activados (desaparición de mensajes en 1 semana).
3. Instrucciones de seguridad al informante: Explicar que use Signal desde un teléfono no relacionado con su trabajo, preferiblemente con una SIM de prepago comprada en efectivo.
4. Jamás usar email para información sensible: El email tiene demasiados puntos de intercepción. Signal o SecureDrop para todo lo sensible.
5. Compartimentación editorial: Minimizar el número de personas en la redacción que conocen la identidad de la fuente. El principio de "necesidad de conocer".
6. Acuerdo explícito de riesgo: El informante debe entender claramente qué información será publicada y cómo podría revelar su identidad aunque no se mencione su nombre.

11.7 La Seguridad Operativa del Informante

✕ Lo que puede revelar una fuente

Metadatos de documentos (autor, fecha de modificación, nombre del equipo). Vocabulario especializado único al departamento. Número de personas con acceso al documento. Hora y formato específico de la filtración.

✅ Cómo minimizar el riesgo

Limpiar metadatos con mat2 o ExifTool antes de publicar. Parafrasear en lugar de publicar el documento original cuando sea posible. Verificar que el contenido no es trazable a un único receptor.

11.8 Marco Legal — Protección del Secreto Periodístico

MARCO	COBERTURA	LIMITACIONES
Constitución del Ecuador (Art. 20)	Derecho a la información; protección de periodistas	Interpretación judicial puede variar; insuficiente ante presión estatal
Ley Orgánica de Comunicación (LOC)	Reconoce el secreto de las fuentes periodísticas	Ha sido usada para presionar a medios; no cubre filtradores
Protección internacional (CPJ, RSF)	Documentación, presión diplomática, asistencia legal	No vinculante; dependiente de voluntad política del Estado
Convenios CIDH / ONU	Marco de derechos humanos aplicable a periodistas	Proceso lento; requiere agotar vías internas primero

CAP. 12 — OPSEC AVANZADO

OPSEC Avanzado: Identidades de Cobertura

En investigaciones de crimen organizado, corrupción de alto nivel o vigilancia estatal, el investigador puede necesitar crear identidades de cobertura para acceder a información sin comprometer su seguridad o la de sus fuentes.

12.5 Sock Puppets — Cuentas de Investigación Ética

⚖ Marco Ético de los Sock Puppets

Usar identidades falsas para acceder a información es éticamente justificable solo cuando: (1) la información es de interés público genuino; (2) no existe otra forma de obtener la información; (3) el engaño es mínimo y proporcional; (4) la decisión es tomada con la supervisión editorial de nivel máximo. En ningún caso se usa para dañar a personas o para obtener información irrelevante para el interés público investigado.

▶ CREACIÓN DE UNA IDENTIDAD DE COBERTURA SEGURA

1. Dispositivo dedicado: Un teléfono de prepago comprado en efectivo, nunca vinculado a la identidad real del investigador.
2. Email separado: Crear desde el dispositivo de prepago, usando Tor, un email en Proton Mail sin información real.
3. Identidad coherente: La identidad falsa debe ser internamente coherente: misma región, intereses compatibles, historial de cuenta gradual.
4. Sin cruce con la identidad real: Nunca acceder a cuentas reales desde el dispositivo de cobertura. Nunca mencionar información que solo el investigador real conocería.
5. Limitar la duración: Usar la identidad de cobertura solo durante el tiempo necesario para la investigación específica.
6. Documentar todo: La decisión de usar una identidad de cobertura, sus objetivos, y el período de uso deben estar documentados en el archivo editorial.

12.6 Gestión del Archivo de Investigación

TIPO DE ARCHIVO	DÓNDE ALMACENAR	PERÍODO DE RETENCIÓN	CONTROL DE ACCESO
Evidencia verificada	ProtonDrive cifrado + backup local cifrado	Permanente (relevancia legal)	Solo equipo editorial directo
Comunicaciones con fuentes	Dispositivo cifrado offline	Según acuerdo con la fuente	Solo el periodista responsable
Documentos de trabajo	Drive compartido del equipo (cifrado)	Mientras dure la investigación + 1 año	Equipo de investigación
Archivos publicados	Servidor editorial principal	Permanente	Público

CAP. 13 — NARRATIVA AVANZADA

Narrativa Visual y Comunicación de Evidencia

La pieza OSINT más rigurosa metodológicamente puede fracasar si no logra comunicar su hallazgo de forma comprensible. La narrativa visual es la última milla de la investigación.

13.4 Principios de Visualización de Datos para Periodismo

✅ **Un gráfico, una idea**
Cada visualización debe comunicar exactamente una idea central. Si se necesitan dos ideas, usar dos gráficos. La complejidad visual oculta, no revela.

✅ **Eje Y desde cero**
Nunca truncar el eje Y para exagerar visualmente una diferencia. Es una de las manipulaciones visuales más comunes y menos detectadas.

✅ **Fuente siempre visible**
Toda visualización publicada debe incluir la fuente de los datos, la fecha de acceso, y si corresponde, la metodología de procesamiento.

❌ **Evitar el "spaghetti"**
Los gráficos de línea con más de 5 variables simultáneas son imposibles de leer. Usar facets (paneles múltiples) o seleccionar las variables más significativas.

13.5 Formatos de Publicación para Distintas Audiencias

AUDIENCIA	FORMATO PREFERIDO	PRIORIDAD EN EL CONTENIDO	HERRAMIENTA
Ciudadanía general	Historia narrativa con datos integrados	Impacto humano, claridad, accesibilidad	Datawrapper, Flourish, Canva
Periodistas y editores	Pieza con metodología explícita y datos brutos	Reproducibilidad, fuentes, cadena de custodia	GitHub, repositorios públicos
Organismos judiciales	Informe técnico con estándar Berkeley	Cadena de custodia, hash, admisibilidad	Documentación formal en PDF
Organizaciones internacionales	Policy brief con recomendaciones	Impacto sistémico, comparación regional	Informe ejecutivo estructurado

💡 **La Regla del "Titular Primero"**
Escribir el titular de la investigación antes de escribir la pieza. Si no puedes expresar el hallazgo en una oración de menos de 20 palabras, la investigación aún no está completamente sintetizada. Un buen titular de investigación OSINT responde: quién, qué, evidencia clave, y por qué importa.

CAP. 14 — REDES REGIONALES

Redes Periodísticas de Investigación en América Latina

América Latina tiene un ecosistema de periodismo de investigación colaborativo de creciente sofisticación. Conocer estas redes, sus metodologías y sus espacios de colaboración es esencial para el investigador E3I.

14.3 Directorio de Redes y Medios de Investigación — Región

ORGANIZACIÓN	PAÍS/COBERTURA	ESPECIALIDAD	CÓMO COLABORAR
CONNECTAS	Regional (América Latina)	Investigación transnacional, crimen organizado, corrupción	Propuesta de historia a editors@connectas.org
CLIP	Colombia + regional	NINA (contratos públicos), investigación digital	Acceso a NINA para periodistas verificados
Abraji	Brasil	Datos abiertos, acceso a la información, seguridad digital	Membresía; talleres periódicos abiertos
El Faro	Centroamérica	Crimen organizado, corrupción, pandillas, élites	Alianzas para proyectos de investigación regional
IDL-Reporteros	Perú	Corrupción judicial, narcotráfico, política	Intercambio de metodología; alianzas en investigaciones peruanas
Ciper Chile	Chile	Poder político y económico, financiamiento de campañas	Modelo de verificación replicable; datos públicos de Chile
Ojo Público	Perú + regional	Data journalism, visualización, investigación multimedia	Metodología de datos abiertos; proyectos colaborativos
La Nación Data	Argentina	Datos abiertos gubernamentales, visualización avanzada	Repositorios de datos públicos en GitHub

14.4 El Modelo de Cobertura Coordinada — Cómo Funciona

▶ PROTOCOLO DE INVESTIGACIÓN MULTI-REDACCIÓN

1. Identificación de historia transnacional: Un hallazgo que involucra múltiples jurisdicciones. Un actor en Ecuador + empresa en Panamá + cuenta en Malta.
2. Reunión de coordinación inicial: Definir roles, alcance por redacción, calendario y reglas de embargo (fecha de publicación simultánea).
3. Plataforma compartida segura: ProtonDrive o repositorio git privado. Acceso solo para los periodistas asignados por cada redacción.
4. División del trabajo: Cada redacción investiga el componente de su jurisdicción. Reuniones semanales de actualización por Signal.
5. Revisión cruzada: Cada redacción revisa los hallazgos de las otras para detectar inconsistencias antes de la publicación.
6. Publicación simultánea: El embargo se levanta simultáneamente. Mayor impacto mediático; más difícil de ignorar por autoridades locales.
7. Seguimiento compartido: Protocolo para compartir respuestas legales, amenazas y desarrollos posteriores a la publicación.

CAP. 15 — CASO ADICIONAL

Caso de Estudio: El Modelo ICIJ en Filtraciones

Los Pandora Papers (2021) involucraron a más de 600 periodistas de 117 países, 11,9 millones de documentos y más de 330 políticos y líderes mundiales. Su metodología es el modelo de referencia para el periodismo de consorcio.

PANDORA PAPERS — METODOLOGÍA ICIJ 2021

Cómo 617 Periodistas Procesaron 11,9 Millones de Documentos

- F1 Recepción anónima de los archivos mediante SecureDrop. Verificación de autenticidad del corpus antes de invertir recursos.
- F2 Procesamiento masivo con Nuix y motor de búsqueda interno ICIJ. Indexación de entidades (personas, empresas, fechas) en todo el corpus.
- F3 División por jurisdicción: cada redacción recibe acceso solo a los documentos relevantes para su país o región.
- F4 Verificación cruzada multilateral: los hallazgos de cada equipo son revisados por otros dos equipos antes de la publicación.
- F5 Embargo coordinado: publicación simultánea en 117 países el 3 de octubre de 2021. Impacto imposible de suprimir localmente.
- R Resultado: Dimisiones, investigaciones penales en 14 países, reformas legales en 5 jurisdicciones, recuperación de activos documentada en más de 1.000 millones de dólares.

LECCIONES METODOLÓGICAS APLICABLES A CUALQUIER REDACCIÓN

La verificación multilateral es el estándar, no la excepción	El embargo coordinado multiplica el impacto exponencialmente
Ninguna redacción sola puede cubrir una historia global	La seguridad del proceso protege a todas las redacciones involucradas

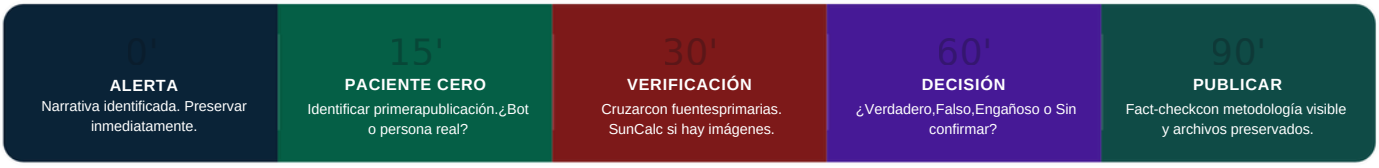
CAP. 15 — CASO 4

Caso de Estudio: Desinformación Electoral en Tiempo Real

Las elecciones concentran la mayor densidad de desinformación en el menor tiempo posible. La metodología E3I en contexto electoral exige protocolos de respuesta rápida sin sacrificar la rigurosidad de verificación.

15.4 El Protocolo de Verificación en 90 Minutos

En contexto electoral, la ventana de verificación es estrecha: si una narrativa circula durante 90 minutos sin ser desmentida, tiende a consolidarse en la percepción pública. Este protocolo adapta el modelo E3I a la velocidad electoral.



15.5 Tipos de Desinformación Electoral — Taxonomía

TIPO	DESCRIPCIÓN	SEÑAL	RESPUESTA
Resultado falso	Anunciar ganador antes del cierre oficial	Antes del conteo oficial; sin fuente identificada	Esperar datos del CNE; verificar actas
Foto fuera de contexto	Imagen real de otro evento presentada como del día	Sin metadatos del día; búsqueda inversa positiva	Búsqueda inversa + cronolocalización
Encuesta falsa	Datos de encuesta inventados o de una encuestadora inexistente	Sin metodología pública; encuestadora sin historial	Verificar registro de la empresa; metodología
Irregularidad fabricada	Video o imagen que supuestamente muestra fraude	Difusión súbita coordinada; actores reconocibles	Geolocalización + verificación de fuente

Herramientas Especializadas para Contexto Electoral

First Draft: guías de verificación electoral específicas. **Election Watch:** monitoreo de desinformación electoral coordinado. **WhatsApp Tipline:** sistema de verificación por WhatsApp para audiencias de alto uso de mensajería. **CrowdTangle:** para periodistas con acceso, permite rastrear la difusión de contenido en tiempo real durante la jornada electoral.

CAP. 16 — EJERCICIO 3

Ejercicio 3: Investigación Corporativa Completa

Este ejercicio integra todas las técnicas del manual en una investigación realista. Está diseñado para equipos de 3-4 personas con una semana de trabajo a tiempo parcial.

Escenario Base

🎯 SUPUESTO DE INVESTIGACIÓN

La Empresa de Seguridad y el Contrato Municipal

Una empresa de seguridad privada acaba de obtener un contrato municipal de $4,2 millones de dólares por servicios de vigilancia, siendo la única oferta presentada en el proceso. El director de la empresa aparece en un evento fotográfico junto al alcalde tres meses antes del proceso de licitación.

Tareas del Equipo — Distribución por Pilar E3I

PILAR E3I	TAREA	HERRAMIENTAS	ENTREGABLE
ESCENARIOS	Construir 3 hipótesis: (A) adjudicación legítima, (B) conflicto de interés, (C) empresa fantasma	Análisis documental, árbol de hipótesis	Documento de hipótesis con criterios de falsación
INFORMACIÓN	Buscar toda la información pública sobre la empresa y sus directores	Registro mercantil, OpenCorporates, OCCRP Aleph, portal de contrataciones	Matriz de datos con cadena de custodia
INCIDENCIA	Mapear relaciones entre la empresa, sus directores, el alcalde y su red política	Gephi, registros electorales públicos, declaraciones de interés público	Grafo de relaciones con nodos clave identificados
INTELIGENCIA	Sintetizar la evidencia y determinar si hay base para publicar	Matriz de verificación E3I, lista de chequeo editorial	Informe ejecutivo + solicitud de derecho a réplica

💡 **Criterio de Evaluación del Ejercicio**

El equipo debe ser capaz de responder antes de publicar: ¿Tenemos dos fuentes independientes para cada afirmación central? ¿Hemos intentado falsificar activamente la hipótesis B (conflicto de interés)? ¿Hemos dado derecho a réplica? ¿Podemos mostrar el proceso completo si somos demandados? Si la respuesta es sí a todo, pueden publicar.

CAP. 16 — EJERCICIO 4

Ejercicio 4: Verificación de Desinformación en Salud

La desinformación en salud tiene consecuencias directas en vidas humanas. Este ejercicio aplica la metodología E3I a un escenario de alto impacto donde la velocidad y la precisión son igualmente críticas.

Escenario Base

⚕ SUPUESTO DE VERIFICACIÓN

El "Tratamiento Milagro" que se Viraliza en WhatsApp

Un audio de WhatsApp de 4 minutos, supuestamente grabado por "un médico del Hospital Metropolitano", afirma que un remedio casero cura en 48 horas una enfermedad respiratoria que actualmente tiene a 200 personas hospitalizadas en la región. El audio ya tiene 50.000 reenvíos en 3 horas.

Fase de Respuesta Rápida — Primeros 30 Minutos

▶ PROTOCOLO DE VERIFICACIÓN DE AUDIO VIRAL

1. Preservar el audio (0-2 min): Descargar el archivo de audio. Verificar metadatos con ExifTool: ¿cuándo fue grabado? ¿qué dispositivo?
2. Transcribir (2-8 min): Usar Whisper (OpenAI) para transcripción automática. Identificar afirmaciones de hecho específicas.
3. Verificar la fuente (8-15 min): ¿Existe un médico con ese nombre en el Hospital Metropolitano? Buscar en el sitio oficial del hospital.
4. Verificar las afirmaciones médicas (15-25 min): Consultar UpToDate, PubMed o comunicados de la OPS/OMS sobre la enfermedad mencionada. ¿El "tratamiento" tiene respaldo científico?
5. Rastrear origen (25-30 min): ¿En qué grupo de WhatsApp apareció primero? ¿Hay una versión anterior del mismo audio circulando desde antes?

Fuentes de Verificación para Salud

OPS/OMS
Comunicados oficiales sobre brotes y tratamientos. paho.org para América Latina.

PubMed / Cochrane
Evidencia científica revisada por pares. Para verificar afirmaciones de eficacia de tratamientos.

Full Fact Health
Verificaciones de salud previas. Evitar repetir trabajo ya hecho por otros equipos.

Health Feedback
Red de científicos que verifican contenido de salud. Para casos complejos, contactar a un experto.

SciCheck (FactCheck.org)
Verificaciones de afirmaciones científicas en inglés; metodología replicable.

MSC (Ministerio de Salud)
Boletines epidemiológicos oficiales. Datos de hospitalizaciones y protocolos actuales.

⚠ **Dilema Editorial — Velocidad vs. Precisión en Salud**

Publicar un fact-check incompleto en salud puede hacer más daño que no publicar. Sin embargo, esperar demasiado permite que la desinformación se consolide. La regla E3I: publicar la verificación de cada afirmación verificable, marcando explícitamente qué está confirmado, qué está en proceso y qué no se pudo confirmar. Transparencia sobre el proceso, no silencio hasta tener todo.

APÉNDICE A

Glosario Técnico E3I 2026

Términos técnicos usados en este manual, organizados para su referencia rápida durante investigaciones.

A — C

ADS-B: Automatic Dependent Surveillance-Broadcast. Sistema de rastreo de aeronaves en tiempo real.

Betweenness Centrality: Métrica de grafo que mide el control de un nodo sobre el flujo de información en una red.

CIB: Comportamiento Coordinado Inauténtico. Uso de múltiples cuentas falsas o administradas para amplificar narrativas.

Cronolocalización: Determinación de fecha y hora de una imagen o video mediante análisis de la posición solar (SunCalc).

Cadena de custodia: Registro documentado de quién tuvo acceso a una evidencia y qué hizo con ella.

D — G

Deepfake: Contenido audiovisual sintético generado por IA que muestra a personas reales en situaciones falsas.

EXIF: Exchangeable Image File Format. Metadatos embebidos en imágenes digitales incluyendo GPS, fecha y cámara.

Geolocalización: Proceso de identificar la ubicación geográfica exacta donde fue tomada una imagen o video.

Google Dork: Combinación de operadores avanzados de Google para extraer información específica de fuentes abiertas.

H — O

Hash criptográfico: Huella digital única de un archivo. Garantiza que no ha sido alterado (SHA-256 es el estándar).

Hybrid Fake: Contenido manipulado donde el 95% es real y la falsificación está en un detalle quirúrgico.

MVT: Mobile Verification Toolkit. Herramienta de Amnistía Internacional para detectar spyware como Pegasus.

OPSEC: Operational Security. Prácticas que protegen la investigación y las fuentes de actores adversos.

OSINT: Open Source Intelligence. Inteligencia recopilada de fuentes abiertas y accesibles públicamente.

P — Z

Paciente Cero: La primera publicación verificable de un contenido antes de su viralización masiva.

Protocolo de Berkeley: Estándar metodológico para que evidencia OSINT sea admisible en tribunales internacionales.

SLAPP: Strategic Lawsuit Against Public Participation. Demandas diseñadas para silenciar periodistas o activistas.

Sock Puppet: Cuenta falsa o de cobertura usada en investigaciones periodísticas bajo supervisión editorial estricta.

WHOIS: Protocolo de internet que revela información sobre el registrante de un dominio web.

APÉNDICE B

Directorio de Recursos y Apoyo

SEGURIDAD Y PROTECCIÓN DE PERIODISTAS

- **CPJ (Committee to Protect Journalists):**cpj.org — Asistencia en casos de detención, amenaza y presión legal.
- **RSF (Reporteros Sin Fronteras):**rsf.org — Defensa de la libertad de prensa; índice mundial.
- **Access Now Digital Security Helpline:**accessnow.org/help — helpline@accessnow.org — Asistencia digital 24/7.
- **Fundamedios (Ecuador):**fundamedios.org — Monitoreo de ataques a la libertad de prensa en Ecuador.
- **FLIP (Colombia):**flip.org.co — Protección de periodistas en Colombia; recursos legales.
- **Dart Center for Journalism & Trauma:**dartcenter.org — Apoyo psicológico y recursos sobre trauma vicario.

FORMACIÓN Y DESARROLLO PROFESIONAL

- **Bellingcat Online Investigation Toolkit:**toolkit.bellingcat.com — La mayor colección de herramientas OSINT comentadas.
- **GIJN (Global Investigative Journalism Network):**gijn.org — Recursos, talleres y red global de periodistas de investigación.
- **EFF Surveillance Self-Defense:**ssd.eff.org/es — Guías de seguridad digital en español, actualizadas.
- **First Draft:**firstdraftnews.org — Verificación, desinformación y herramientas para periodistas.
- **European Journalism Centre:**ejc.net — Verification Handbook descargable gratuitamente.

DATOS ABIERTOS — REFERENCIA RÁPIDA

- **OCCRP Aleph:**aleph.occrp.org — Filtraciones masivas y registros internacionales.
- **ICIJ Offshore Leaks:**offshoreleaks.icij.org — Panama Papers, Pandora Papers, Paradise Papers.
- **OpenCorporates:**opencorporates.com — Registros de empresas en 130+ países.
- **OpenSanctions:**opensanctions.org — Personas y empresas bajo sanciones internacionales.
- **NINA (CLIP):**— Contratos públicos en 21 países de América Latina.

Manual OSINT Periodístico — Modelo E3I 2026

Autores: Gabriel Hidalgo Andrade · Yalilé Loaiza

Financiado por: Ministerio para Europa y Asuntos Exteriores de Francia, dentro del proyecto “Comunidad Informada”

Con el apoyo de: UTPL · Fundamedios · Ecuador Chequea