

APUNTES DE INTRODUCCIÓN

OSINT

Inteligencia de fuentes abiertas
lo esencial

Metodología, marco legal, técnicas, herramientas y glosario

Autor: David M.
davmacsolutions.com

Octubre de 2026

ÍNDICE

1. Qué es OSINT	2
2. Marco ético y legal	2
3. El ciclo de inteligencia	3
4. Seguridad operacional (OPSEC)	4
5. Búsqueda avanzada	5
6. Preservación y documentación	5
7. Verificación de imágenes y vídeos	6
8. Redes sociales	7
9. Dominios e infraestructura	7
10. Empresas y registros públicos	8
11. Diligencia debida de empresas	8
12. Transporte y datos geoespaciales	9
13. Desinformación	10
14. Caso práctico: verificar una noticia viral	11
15. Plantilla de registro de investigación	11
16. Análisis y evaluación de fuentes	12
17. El informe	13
18. Herramientas y recursos	14
19. Errores frecuentes	15
20. Glosario	16

1. QUÉ ES OSINT

OSINT (*Open Source Intelligence*) es la obtención, verificación y análisis de información procedente de *fuentes abiertas*: aquellas a las que cualquiera puede acceder de forma legal, gratuita o de pago, sin recurrir a medios encubiertos ni a accesos no autorizados.

La palabra clave es *inteligencia*. Reunir datos no basta: OSINT consiste en convertir información dispersa en conocimiento verificado, contextualizado y útil para responder a una pregunta concreta.

1.1 Para qué se usa

Ámbito	Ejemplos de uso
Periodismo y verificación	Comprobar si una foto o un vídeo es auténtico, dónde y cuándo se tomó; desmentir bulos.
Ciberseguridad	Conocer la superficie de exposición de una organización; inteligencia de amenazas.
Diligencia debida	Investigar empresas, administradores y proveedores antes de contratar o invertir.
Cumplimiento normativo	Controles de prevención de blanqueo, sanciones internacionales, personas expuestas políticamente.
Derechos humanos	Documentar conflictos y abusos con imágenes de satélite y material publicado en redes.
Investigación académica	Estudio de redes de desinformación, discurso público o fenómenos sociales.

1.2 Disciplinas de inteligencia

OSINT es una de varias disciplinas que se distinguen por el origen de la información:

Disciplina	Fuente
OSINT	Fuentes abiertas: web, prensa, registros públicos, redes sociales, datos abiertos.
SOCMINT	Redes sociales (a menudo se considera una rama de OSINT).
GEOINT / IMINT	Información geoespacial e imágenes (satélite, aéreas, fotografías).
HUMINT	Fuentes humanas: entrevistas, contactos.
SIGINT	Interceptación de señales y comunicaciones (reservada a los Estados).
FININT	Información financiera.

2. MARCO ÉTICO Y LEGAL

ATENCIÓN. Que un dato sea accesible no significa que se pueda usar de cualquier manera. La legalidad y la ética son la primera fase de toda investigación, no un añadido final. Este apartado es orientativo y no sustituye al asesoramiento jurídico.

2.1 Normativa a tener en cuenta

Protección de datos. En la Unión Europea, el RGPD se aplica también a los datos personales que están publicados. Recopilarlos, almacenarlos o cruzarlos es un *tratamiento* y requiere una base legal (por ejemplo, interés legítimo o fines periodísticos), proporcionalidad y minimización. En España lo completa la LOPDGDD y lo supervisa la AEPD; otros países tienen normas equivalentes.

Código Penal. Están tipificados, entre otros, el acceso no autorizado a sistemas informáticos, el descubrimiento y revelación de secretos, el acoso reiterado y la usurpación de identidad.

Términos de servicio. Las plataformas suelen limitar la extracción automatizada de datos y el uso de identidades falsas. Incumplirlos puede suponer la suspensión de cuentas y, en algunos casos, responsabilidad civil.

Propiedad intelectual. Las imágenes y textos encontrados tienen autor; su reproducción puede requerir permiso o ampararse en el derecho de cita.

2.2 Principios de actuación

1. **Finalidad legítima:** una pregunta de investigación justificada (periodística, de seguridad, de cumplimiento...), definida antes de empezar.
2. **Proporcionalidad y minimización:** recoger solo lo necesario para esa finalidad. Datos de terceros no implicados, menores y categorías especiales (salud, ideología, orientación sexual) exigen máxima cautela.
3. **Pasividad:** observar sin interactuar, sin engañar a personas para obtener información y sin acceder nunca a sistemas, cuentas o áreas protegidas.
4. **No causar daño:** valorar las consecuencias de publicar. Exponer el domicilio, la familia o los datos de contacto de una persona (*doxing*) puede ponerla en peligro y suele ser ilegal.
5. **Rigor:** verificar antes de afirmar; un error puede dañar a inocentes.
6. **Trazabilidad:** documentar qué se hizo, cuándo y con qué fuentes.

3. EL CICLO DE INTELIGENCIA

Toda investigación sigue, de forma más o menos explícita, un ciclo que se repite hasta responder a la pregunta planteada.

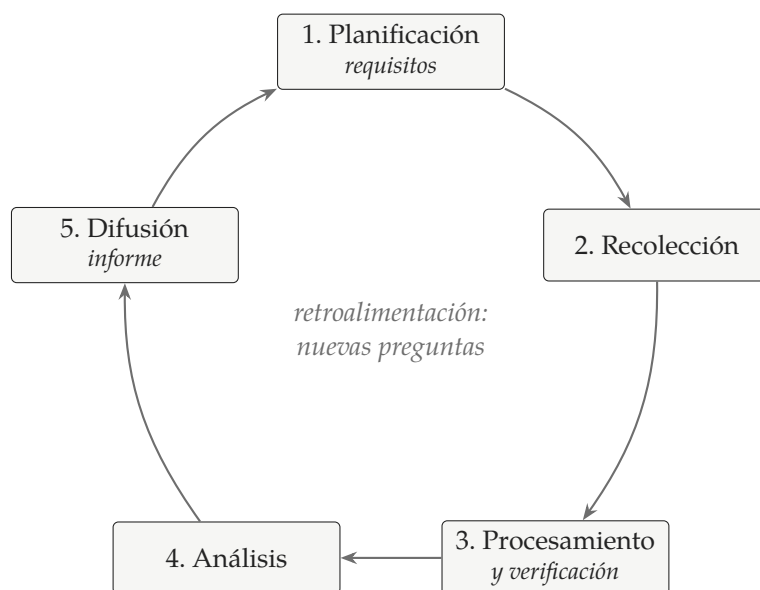


FIGURA 1. Ciclo de inteligencia aplicado a una investigación OSINT.

Planificación. Formular una pregunta precisa (no «todo sobre X», sino «¿quién controla la empresa X y desde cuándo?»), el alcance, los límites legales, el plazo y el formato del resultado.

Recolección. Identificar las fuentes adecuadas y obtener la información, preservándola a medida que se encuentra.

Procesamiento. Ordenar, traducir, extraer datos, eliminar duplicados y, sobre todo, verificar.

Análisis. Relacionar los datos, plantear hipótesis, contrastarlas y valorar la fiabilidad de las conclusiones.

Difusión. Comunicar los hallazgos con claridad, indicando las fuentes y el grado de confianza.

4. SEGURIDAD OPERACIONAL (OPSEC)

Investigar deja rastro: direcciones IP, visitas registradas, búsquedas, cuentas. La OPSEC protege al investigador y a la investigación.

- **Separar entornos:** usar un navegador o perfil dedicado a la investigación, sin sesiones personales iniciadas; para trabajos sensibles, una máquina virtual.
- **Ocultar el origen:** una VPN de confianza evita revelar la ubicación y la red propias a los sitios consultados.
- **No interactuar:** no seguir, no dar «me gusta», no unirse a grupos. Algunas plataformas (LinkedIn, por ejemplo) muestran quién ha visitado un perfil.
- **Cuentas de investigación:** si la plataforma exige iniciar sesión, usar cuentas separadas de las personales, dentro de lo que permiten sus términos de servicio.
- **Cuidar los propios metadatos:** los documentos que se publican o comparten pueden revelar nombre de usuario, software o ubicación.

- **Proteger la información recogida:** almacenamiento cifrado, control de acceso y borrado cuando deja de ser necesaria.

5. BÚSQUEDA AVANZADA

Los buscadores indexan mucho más de lo que se ve con una búsqueda simple. Los *operadores* permiten acotar los resultados.

Operador	Función y ejemplo
"..."	Frase exacta: "informe anual 2025"
-	Excluir un término: jaguar -coche
OR	Alternativas: auditoría OR auditoria
site:	Limitar a un dominio: site:boe.es subvención
filetype:	Tipo de archivo: filetype:pdf memoria sostenibilidad
intitle:	Término en el título: intitle:"nota de prensa"
inurl:	Término en la dirección: inurl:transparencia
before:, after:	Fechas de publicación: after:2025-01-01
*	Comodín dentro de una frase: "director * de la empresa"

- **Varios buscadores:** Google, Bing, Yandex, DuckDuckGo o Baidu indexan contenidos distintos y ordenan de forma diferente. Los resultados también varían según el país y el idioma.
- **Buscar en el idioma de la fuente:** un tema local se documenta mejor en la lengua local.
- **Variantes:** nombres con y sin tilde, abreviaturas, transliteraciones de otros alfabetos, faltas de ortografía habituales.
- **Documentos:** informes anuales, memorias, presentaciones y actas publicadas en PDF suelen contener datos que no aparecen en la web principal.

6. PRESERVACIÓN Y DOCUMENTACIÓN

Las páginas cambian y desaparecen. Lo que no se ha guardado no se puede demostrar.

- **Archivos web:** la Wayback Machine (web.archive.org) y archive.today guardan copias públicas de una página y permiten consultar versiones antiguas.
- **Capturas propias:** deben incluir la URL completa y la fecha y hora; mejor en PDF de página completa que en recorte.
- **Herramientas de registro:** extensiones como Hunchly guardan automáticamente cada página visitada durante una investigación.
- **Integridad:** calcular el *hash* (por ejemplo, SHA-256) de los archivos descargados permite demostrar después que no se han alterado.
- **Registro de investigación:** anotar cada paso (fuente, consulta, fecha, resultado). Facilita que otra persona pueda reproducir el trabajo.

7. VERIFICACIÓN DE IMÁGENES Y VÍDEOS

Ante una imagen se plantean cuatro preguntas: ¿es original o se ha manipulado?, ¿quién la tomó?, ¿dónde? y ¿cuándo?

7.1 Búsqueda inversa

Subir la imagen (o un fotograma del vídeo) a varios buscadores inversos: Google Lens, Bing Visual Search, Yandex y TinEye. Ordenando por fecha se encuentra a menudo la publicación más antigua, que suele acercarse al origen. Muchas imágenes «de última hora» resultan ser antiguas o de otro lugar.

Para vídeos, el complemento InVID-WeVerify extrae fotogramas clave, lee metadatos y lanza búsquedas inversas desde el navegador.

7.2 Metadatos

Las fotografías pueden contener metadatos EXIF: fecha, modelo de cámara, ajustes y, a veces, coordenadas GPS. Se leen con ExifTool. Las grandes redes sociales los eliminan al subir la imagen, de modo que suelen estar disponibles solo en archivos originales. Además, se pueden modificar: son un indicio, no una prueba.

7.3 Geolocalización

Consiste en determinar el lugar exacto comparando la imagen con mapas e imágenes de satélite o a pie de calle. Pistas útiles:

- textos visibles (carteles, rótulos, matrículas) y su idioma o alfabeto;
- arquitectura, mobiliario urbano, señalización vial y sentido de la circulación;
- relieve, vegetación, líneas de costa;
- edificios o elementos singulares que puedan buscarse en el mapa.

Herramientas: Google Maps y Street View, Google Earth Pro (incluye imágenes históricas), Bing Maps, Yandex Maps, Mapillary, OpenStreetMap y el Copernicus Browser para imágenes de los satélites Sentinel (sustituye al antiguo EO Browser).

7.4 Cronolocalización

Para estimar *cuándo* se tomó una imagen: longitud y dirección de las sombras (SunCalc calcula la posición del sol para un lugar y una hora), meteorología registrada ese día, estado de obras o comercios comparado con imágenes históricas, o acontecimientos visibles.

Ejemplo 7.1 (flujo de verificación). Circula una foto de una inundación atribuida a una ciudad concreta. (1) Se guarda el mensaje original con su URL y fecha. (2) Búsqueda inversa: aparece publicada dos años antes en otro país. (3) Se localiza la publicación más antigua y su autor. (4) Se geolocaliza la escena con un rótulo visible y Street View. Conclusión: imagen auténtica, pero descontextualizada.

ATENCIÓN. Las imágenes y vídeos generados o alterados con inteligencia artificial son cada vez más convincentes. Ningún detector es infalible: la verificación debe apoyarse en el origen

y el contexto, no solo en el aspecto.

8. REDES SOCIALES

Las redes son una fuente inmediata pero ruidosa. Lo que interesa no es solo el contenido, sino quién lo publica y cómo se difunde.

- **Evaluar una cuenta:** fecha de creación, historial de publicaciones, cambios de nombre, coherencia del perfil, seguidores y seguidos. Una cuenta reciente, con nombre genérico y actividad masiva sobre un único tema merece desconfianza.
- **Comportamiento coordinado:** muchas cuentas que publican el mismo texto a la vez, con imágenes de perfil similares o creadas en las mismas fechas, sugieren una campaña organizada.
- **Búsqueda avanzada propia de cada plataforma:** filtros por fecha, idioma o ubicación cuando existen.
- **Limitaciones:** las plataformas restringen cada vez más el acceso sin cuenta y por API; las herramientas dejan de funcionar con frecuencia. Conviene conocer el método, no depender de una herramienta concreta.

9. DOMINIOS E INFRAESTRUCTURA

Muy útil en ciberseguridad y para investigar sitios web sospechosos (fraudes, desinformación). Todas las técnicas citadas son *pasivas*: consultan información pública sin interactuar con el sistema investigado.

Fuente	Qué aporta
RDAP (antes WHOIS)	Datos de registro de un dominio: registrador, fechas de alta y caducidad, servidores DNS. Desde 2025 RDAP es el protocolo oficial (<code>lookup.icann.org</code>). Los datos del titular suelen estar ocultos por privacidad.
DNS e historial DNS	A qué direcciones IP apunta un dominio y a cuáles apuntó antes; dominios que comparten servidor.
Certificados TLS	Los registros públicos de certificados (<code>crt.sh</code>) revelan subdominios de una organización.
Shodan, Censys	Buscadores de dispositivos y servicios expuestos en Internet: qué tiene publicada una organización.
BuiltWith, Wappalyzer	Tecnologías con las que está construido un sitio; los identificadores de analítica compartidos pueden vincular sitios de un mismo responsable.

ATENCIÓN. Consultar estas fuentes es legal; intentar acceder a un sistema, probar contraseñas o explotar una vulnerabilidad no lo es sin autorización expresa del propietario.

10. EMPRESAS Y REGISTROS PÚBLICOS

Los registros oficiales son fuentes primarias de gran fiabilidad.

Fuente	Contenido
BORME y Registro Mercantil	Constitución de sociedades, nombramientos y ceses de administradores, cambios de domicilio y capital, cuentas anuales (España).
BOE y boletines autonómicos	Normas, subvenciones, sanciones, oposiciones y anuncios oficiales.
Plataforma de Contratación del Sector Público	Licitaciones y adjudicaciones de contratos públicos.
OpenCorporates	Base de datos internacional de sociedades de numerosos países.
EDGAR (SEC)	Información financiera de empresas cotizadas en EE. UU.
Registros de marcas y patentes	Titulares de marcas (OEPM, EUIPO) y patentes (Espacenet).
Listas de sanciones	Sanciones de la UE, la ONU y la OFAC estadounidense.
ICIJ Offshore Leaks	Entidades aparecidas en filtraciones como los Papeles de Panamá o de Pandora.

Observación. Una técnica clave es *pivotar*: usar un dato encontrado (un administrador, un domicilio social, un teléfono corporativo) como punto de partida para descubrir otras sociedades o webs relacionadas.

11. DILIGENCIA DEBIDA DE EMPRESAS

La diligencia debida (*due diligence*) consiste en comprobar quién es realmente una empresa antes de contratarla, invertir en ella o asociarse. Es uno de los usos profesionales más habituales de OSINT.

11.1 Lista de comprobación

1. **Identidad jurídica:** denominación exacta, NIF, forma jurídica, fecha de constitución, domicilio social y objeto social.
2. **Órganos de administración:** administradores actuales e históricos, apoderados y fechas de nombramiento y cese.
3. **Propiedad y control:** socios conocidos, grupo empresarial y titular real cuando esté disponible.
4. **Situación financiera:** cuentas anuales depositadas, evolución de ingresos y resultados, ampliaciones o reducciones de capital.
5. **Situación legal:** concursos de acreedores, embargos, litigios publicados y sanciones administrativas.

6. **Listas de sanciones y prensa adversa:** listas de la UE, la ONU y la OFAC; noticias sobre fraude, corrupción o blanqueo.
7. **Actividad real:** web, presencia comercial, empleados, clientes, contratos públicos, marcas registradas.
8. **Coherencia:** que todo lo anterior encaje entre sí y con lo que la empresa declara de sí misma.

11.2 Señales de alerta

Ninguna de estas señales prueba nada por sí sola, pero varias juntas justifican profundizar.

Señal	Por qué importa
Domicilio compartido con cientos de sociedades	Puede tratarse de un centro de negocios o de una red de sociedades instrumentales.
Cambios frecuentes de administrador	Puede indicar testaferros o intentos de eludir responsabilidades.
Sociedad muy reciente con contratos o cifras elevadas	Falta de historial que respalde la capacidad declarada.
Cuentas anuales no depositadas	Incumplimiento de una obligación legal; opacidad financiera.
Capital mínimo y estructura en varias capas	Dificulta identificar quién controla realmente la sociedad.
Jurisdicciones de baja transparencia en la cadena de propiedad	Habituales en estructuras para ocultar al titular real.
Web registrada hace pocas semanas o con textos copiados	Posible empresa fantasma o fraude.
Datos de contacto que no coinciden con los registros	Teléfonos, direcciones o nombres incoherentes entre fuentes.
Administradores vinculados a sociedades disueltas o en concurso	Patrón de empresas que se crean y abandonan.

Observación. Los datos de los administradores se consultan en su condición de tales y para la finalidad de la diligencia debida. Su vida privada queda fuera del alcance de la investigación.

12. TRANSPORTE Y DATOS GEOESPACIALES

- **Aviones:** Flightradar24 y ADS-B Exchange muestran posiciones a partir de las señales ADS-B que emiten las aeronaves; se identifican por matrícula o código ICAO.
- **Barcos:** MarineTraffic y VesselFinder usan las señales AIS; los buques se identifican por número IMO o MMSI. Un barco que apaga el AIS deja un hueco significativo en su trayectoria.
- **Mapas abiertos:** OpenStreetMap y su herramienta de consultas Overpass Turbo permi-

ten buscar combinaciones de elementos (por ejemplo, una gasolinera junto a un puente), útil en geolocalización.

13. DESINFORMACIÓN

13.1 Tipos de contenido engañoso

Tipo	Descripción
Sátira o parodia	Sin intención de dañar, pero puede engañar si circula sin contexto.
Conexión falsa	El titular o la imagen no se corresponden con el contenido.
Contenido engañoso	Información real usada de forma sesgada para enmarcar un tema o a una persona.
Contexto falso	Contenido auténtico difundido con fechas, lugares o circunstancias que no son las suyas.
Contenido impostor	Se suplanta a un medio, institución o persona real.
Contenido manipulado	Imagen, vídeo, audio o documento auténtico alterado.
Contenido fabricado	Totalmente falso, creado para engañar (incluidos los generados con IA).

TABLA 1. Clasificación habitual en verificación de datos, de menor a mayor intención de engañar.

13.2 El método SIFT

Un procedimiento rápido para valorar cualquier contenido antes de compartirlo o usarlo:

S — Stop (detenerse). Antes de reaccionar, preguntarse si se conoce la fuente y si el contenido provoca una emoción intensa: la indignación es el combustible de la desinformación.

I — Investigar la fuente. ¿Quién lo publica? ¿Qué trayectoria y qué intereses tiene?

F — Find (buscar mejor cobertura). Comprobar si medios fiables o fuentes oficiales informan de lo mismo.

T — Trazar el origen. Seguir las afirmaciones, citas e imágenes hasta su contexto original.

13.3 Lectura lateral

Los verificadores profesionales no se quedan leyendo la página sospechosa: abren otras pestañas para averiguar qué dicen *otros* sobre esa fuente. Unos minutos de lectura lateral revelan más que un análisis minucioso de un sitio diseñado para parecer creíble.

13.4 Indicios de una campaña coordinada

- Textos idénticos o casi idénticos publicados por muchas cuentas en poco tiempo.
- Cuentas creadas en las mismas fechas, con nombres y fotos de perfil de patrón similar.
- Picos de actividad a horas que no corresponden con la zona horaria declarada.
- Uso repetido de los mismos enlaces, etiquetas o dominios recién registrados.
- Amplificación desproporcionada de cuentas con pocos seguidores reales.

14. CASO PRÁCTICO: VERIFICAR UNA NOTICIA VIRAL

Ejemplo 14.1 (enunciado). Circula en redes una imagen de un edificio en llamas con el texto «Hace una hora: incendio en el ayuntamiento de la ciudad X». Miles de personas la han compartido.

1. **Preservar.** Capturar la publicación con URL, fecha y hora; archivarla en la Wayback Machine o archive.today. Descargar la imagen y calcular su *hash*.
2. **Detenerse y formular la pregunta.** ¿La imagen muestra el ayuntamiento de X y fue tomada hoy?
3. **Analizar la cuenta.** Antigüedad, historial, temas habituales y si publica desde la zona. Una cuenta creada la semana pasada que solo difunde alarmas resta credibilidad.
4. **Búsqueda inversa.** Probar Google Lens, Bing, Yandex y TinEye; ordenar por fecha. Supongamos que aparece publicada tres años antes en un medio de otro país.
5. **Localizar el original.** Abrir esa publicación más antigua y comprobar su pie de foto, autor y contexto.
6. **Geolocalizar.** Comparar la fachada con Street View del ayuntamiento de X y del edificio que indica la publicación original. Los elementos arquitectónicos coinciden con el segundo, no con el primero.
7. **Contrastar con fuentes oficiales.** Bomberos, servicios de emergencia y medios locales de X no informan de ningún incendio.
8. **Concluir con grado de confianza.** Imagen auténtica, pero con *contexto falso*. Confianza: casi segura.
9. **Documentar.** Rellenar la ficha de verificación y conservar todas las capturas.

Campo	Contenido de la ficha
Afirmación	Incendio en el ayuntamiento de X «hace una hora».
Contenido analizado	Imagen; URL y captura archivada; <i>hash</i> SHA-256.
Origen identificado	Publicación de un medio extranjero de hace tres años.
Pruebas	Búsqueda inversa, geolocalización, ausencia de avisos oficiales.
Clasificación	Contexto falso.
Confianza	Casi segura.
Fecha y responsable	Fecha de la verificación e iniciales de quien la realiza.

TABLA 2. Ficha de verificación del caso.

15. PLANTILLA DE REGISTRO DE INVESTIGACIÓN

Mantener un registro desde el primer minuto permite reconstruir el trabajo, defenderlo y que otra persona lo reproduzca. Una hoja de cálculo con estas columnas es suficiente:

Columna	Qué anotar
N.º	Número correlativo de la entrada.
Fecha y hora	Momento de la consulta, con zona horaria.
Pregunta o tarea	Qué se buscaba con este paso.
Fuente o herramienta	Sitio, registro o programa utilizado.
Consulta	Términos o parámetros exactos empleados.
Resultado	Qué se encontró (o que no se encontró nada, que también es un dato).
URL	Dirección exacta del resultado.
Evidencia	Nombre del archivo de captura y su <i>hash</i> .
Valoración	Fiabilidad y credibilidad (por ejemplo, B2).
Siguiente paso	Qué pista se abre a partir de aquí.

16. ANÁLISIS Y EVALUACIÓN DE FUENTES

16.1 Fiabilidad y credibilidad

El *sistema del Almirantazgo* (Admiralty o NATO) valora por separado la fuente y la información:

Fiabilidad de la fuente	Credibilidad de la información
A Totalmente fiable	1 Confirmada por otras fuentes
B Normalmente fiable	2 Probablemente cierta
C Bastante fiable	3 Posiblemente cierta
D Normalmente no fiable	4 Dudosa
E No fiable	5 Improbable
F No se puede valorar	6 No se puede valorar

Así, B2 indica una fuente normalmente fiable que aporta una información probablemente cierta.

16.2 Verificar y triangular

- Buscar la **fuentes primaria**: el documento oficial, la publicación original, el autor de la imagen.
- **Triangular**: confirmar cada dato importante con fuentes independientes entre sí (dos medios que copian la misma nota de agencia son una sola fuente).
- Distinguir **hechos** (verificables), **inferencias** (deducciones razonadas) y **opiniones**.

16.3 Sesgos y métodos estructurados

Los errores de análisis más frecuentes no son técnicos, sino cognitivos: el *sesgo de confirmación* (buscar solo lo que apoya la idea inicial), el *anclaje* en la primera hipótesis o ver patrones donde solo hay coincidencias.

El *análisis de hipótesis en competencia* (ACH) ayuda a evitarlos: se enumeran todas las expli-

caciones posibles y se evalúa cada prueba frente a cada una, prestando especial atención a la que *descarta* hipótesis, no a la que las confirma.

16.4 Lenguaje de probabilidad

Para expresar el grado de confianza de forma homogénea, conviene usar términos estimativos con un significado acordado:

Expresión	Probabilidad aproximada
Casi seguro	más del 90 %
Muy probable	75–90 %
Probable	55–75 %
Tan probable como improbable	45–55 %
Improbable	25–45 %
Muy improbable	10–25 %
Casi imposible	menos del 10 %

TABLA 3. Escala orientativa; cada organización define la suya.

17. EL INFORME

Un buen informe OSINT permite al lector entender las conclusiones y comprobarlas.

1. **Resumen ejecutivo:** la respuesta a la pregunta, en pocas líneas, con el nivel de confianza.
2. **Pregunta y alcance:** qué se investigó, con qué límites y en qué fechas.
3. **Metodología:** fuentes y técnicas empleadas.
4. **Hallazgos:** cada afirmación con su fuente (URL, fecha de consulta y captura archivada).
5. **Análisis:** hipótesis consideradas, valoración de fuentes, lagunas de información.
6. **Conclusiones:** separando lo confirmado de lo probable.
7. **Anexos:** capturas, tablas, registro de investigación.

Incluir solo los datos personales imprescindibles y anonimizar a terceros no relevantes.

18. HERRAMIENTAS Y RECURSOS

Categoría	Herramientas
Búsqueda	Google, Bing, Yandex, DuckDuckGo, Startpage
Archivo y preservación	Wayback Machine, archive.today, Hunchly
Imágenes y vídeo	Google Lens, TinEye, Yandex Imágenes, ExifTool, InVID-WeVerify
Mapas y satélite	Google Earth Pro, Street View, Mapillary, OpenStreetMap, Overpass Turbo, Copernicus Browser, SunCalc
Dominios e infraestructura	ICANN Lookup (RDAP), crt.sh, Shodan, Censys, BuiltWith
Empresas	BORME, OpenCorporates, EDGAR, ICIJ Offshore Leaks
Transporte	Flightradar24, ADS-B Exchange, MarineTraffic, VesselFinder
Relación y visualización	Maltego, SpiderFoot, hojas de cálculo, Gephi

Observación. Las herramientas cambian, se vuelven de pago o desaparecen con frecuencia. Antes de usarlas en una investigación conviene comprobar que siguen disponibles y cómo tratan los datos que se introducen en ellas.

18.1 Para seguir aprendiendo

- **Bellingcat Online Investigations Toolkit:** catálogo colaborativo de herramientas con guías de uso, y la sección de guías y casos de Bellingcat.
- **OSINT Framework** (osintframework.com): mapa de recursos organizados por categoría.
- **GIJN** (Global Investigative Journalism Network): guías de investigación para periodistas.
- **Competiciones:** retos de geolocalización y los CTF de búsqueda de personas desaparecidas de Trace Labs, que aplican OSINT con fines humanitarios y reglas éticas estrictas.

19. ERRORES FRECUENTES

Error	Consecuencia y remedio
Empezar sin pregunta definida	Se acumulan datos sin rumbo. Formular una pregunta concreta y un alcance.
No preservar las fuentes	La página cambia y la prueba desaparece. Archivar a medida que se encuentra.
Confundir coincidencia con identidad	Dos perfiles con el mismo nombre no son la misma persona. Exigir varios elementos independientes.
Fuentes no independientes	Diez artículos que copian la misma nota son una sola fuente. Rastrear el origen.
Sesgo de confirmación	Se ignoran los datos que contradicen la hipótesis. Buscar activamente pruebas en contra.
Fiarse de una herramienta	Los resultados automáticos tienen falsos positivos. Comprobar manualmente.
Descuidar la OPSEC	El investigado detecta la investigación. Entorno separado y sin interacción.
Recoger datos de más	Riesgo legal y ético. Minimizar a lo necesario para la pregunta.
Publicar sin valorar el daño	Exposición de inocentes o de personas vulnerables. Evaluar consecuencias antes de difundir.

20. GLOSARIO

20.1 Siglas

Sigla	Nombre completo	Significado
ACH	Analysis of Competing Hypotheses	Análisis de hipótesis en competencia.
ADS-B	Automatic Dependent Surveillance–Broadcast	Señal con la que los aviones emiten su posición.
AEPD	Agencia Española de Protección de Datos	Autoridad de control de protección de datos en España.
AIS	Automatic Identification System	Sistema de identificación y posición de buques.
AML	Anti-Money Laundering	Prevención del blanqueo de capitales.
API	Application Programming Interface	Acceso programático a los datos de un servicio.
ASN	Autonomous System Number	Identificador de una red en Internet (proveedor u organización).
CTF	Capture The Flag	Competición de retos prácticos.
CTI	Cyber Threat Intelligence	Inteligencia sobre amenazas de ciberseguridad.
DNS	Domain Name System	Sistema que traduce nombres de dominio a direcciones IP.
EXIF	Exchangeable Image File Format	Metadatos de las fotografías.
FININT	Financial Intelligence	Inteligencia financiera.
GEOINT	Geospatial Intelligence	Inteligencia geoespacial.
HUMINT	Human Intelligence	Inteligencia de fuentes humanas.
ICAO / OACI	International Civil Aviation Organization	Organismo que asigna identificadores a aeronaves y aeropuertos.
IMINT	Imagery Intelligence	Inteligencia de imágenes.
IMO	International Maritime Organization	Número único y permanente de un buque.
IOC	Indicator of Compromise	Indicio técnico de un ataque (IP, dominio, hash).
IP	Internet Protocol	Dirección numérica de un dispositivo en la red.
KYC	Know Your Customer	Identificación y verificación de clientes.
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales	Ley española que complementa el RGPD.
MMSI	Maritime Mobile Service Identity	Identificador de las comunicaciones de un buque.
OPSEC	Operations Security	Seguridad operacional del investigador.
OSINT	Open Source Intelligence	Inteligencia de fuentes abiertas.
PEP	Politically Exposed Person	Persona con responsabilidades públicas relevantes, sometida a controles reforzados.

Sigla	Nombre completo	Significado
PII	Personally Identifiable Information	Datos que identifican a una persona.
RDAP	Registration Data Access Protocol	Protocolo de consulta de datos de registro de dominios; sustituye a WHOIS.
RGPD / GDPR	Reglamento General de Protección de Datos	Norma europea de protección de datos personales.
SIGINT	Signals Intelligence	Inteligencia de señales.
SOCMINT	Social Media Intelligence	Inteligencia de redes sociales.
TLD	Top-Level Domain	Dominio de primer nivel (.es, .com).
TLS	Transport Layer Security	Cifrado de las conexiones web (el candado del navegador).
TTP	Tactics, Techniques and Procedures	Forma de actuar característica de un actor.
UBO	Ultimate Beneficial Owner	Titular real: persona que controla en última instancia una sociedad.
VM	Virtual Machine	Máquina virtual: un ordenador simulado y aislado.
VPN	Virtual Private Network	Red privada virtual que oculta la IP de origen.
WHOIS	—	Antiguo protocolo de consulta de datos de dominios.

20.2 Términos

Archivado. Copia de una página web guardada en un momento dado como prueba.

Atribución. Determinar quién está detrás de una cuenta, un sitio o una acción.

Búsqueda inversa. Buscar a partir de una imagen para encontrar dónde más aparece.

Cadena de custodia. Registro que garantiza que una prueba no ha sido alterada desde su obtención.

Cronolocalización. Determinar la fecha y hora en que se tomó una imagen o vídeo.

Cuenta de investigación. Cuenta separada de la personal que se usa para consultar plataformas; también llamada *sock puppet*, término que en sentido estricto alude a identidades ficticias.

Deepfake. Imagen, vídeo o audio sintético generado con inteligencia artificial para imitar a una persona real.

Desinformación. Información falsa difundida a sabiendas para engañar. Si se comparte sin intención de engañar, se habla de información errónea.

Doxing. Recopilar y publicar datos personales de alguien para exponerlo o acosarlo. Práctica contraria a la ética de OSINT y a menudo delictiva.

Enriquecimiento. Añadir información a un dato inicial a partir de otras fuentes.

Fuente abierta. Fuente accesible legalmente para el público, gratuita o de pago.

Fuente primaria. Origen directo de un dato (documento oficial, autor original); la secundaria lo reproduce o interpreta.

Geolocalización. Determinar el lugar exacto donde se tomó una imagen o vídeo.

Google dorks. Combinaciones de operadores de búsqueda para encontrar información muy concreta.

Hash. Huella digital de un archivo; cualquier cambio en él produce un valor distinto.

Huella digital. Rastro de información que una persona u organización deja en Internet.

Lectura lateral. Comprobar una fuente consultando lo que dicen otras sobre ella, en lugar de quedarse en la propia fuente.

Metadatos. Datos sobre los datos: autor, fecha o ubicación de un archivo.

Pivotar. Usar un dato encontrado como punto de partida para nuevas búsquedas.

Reconocimiento pasivo. Obtención de información sin interactuar con el objetivo.

Scraping. Extracción automatizada de datos de páginas web.

Señal de alerta. Indicio que, sin probar nada por sí solo, justifica profundizar en la investigación (*red flag*).

SIFT. Método de verificación rápida: detenerse, investigar la fuente, buscar mejor cobertura y trazar el origen.

Superficie de exposición. Conjunto de activos de una organización visibles desde Internet.

Titular real. Persona física que en última instancia posee o controla una sociedad.

Triangulación. Confirmar un dato con varias fuentes independientes.

Verificación. Proceso de comprobar la autenticidad, el origen y el contexto de una información.