INFORME DE INTELIGENCIA OSINT

MARRUECOS, PEGASUS Y CEUTA

SIGINT
HUMINT
GEOINT
CYBER
OSINT

MAR MEDITERRÁNEO

CEUTA

ESTRECHO DE GIBRALTAR

MARRUECOS

ACTIVIDAD DE INTELIGENCIA Y PROYECCIÓN EXTERIOR

Arquitectura de vigilancia, proyección exterior y evaluación analítica de la crisis de Ceuta de 2026

Fecha: 12 de agosto de 2026

Clasificación: Uso analítico / Fuente abierta

Idioma: Español (España)

Síntesis estratégica basada en investigaciones periodísticas, trazabilidad de fuentes y análisis de inteligencia de fuente abierta.

FUENTES ABIERTAS · NO CLASIFICADO

INFORME DE CONTROL
PEGASUS · MARRUECOS · CEUTA

Arquitectura de vigilancia, objetivos exteriores y evaluación de atribución de la crisis de julio de 2026.

CAMPO	DETALLE
Código	INT-OSINT/MA-ES/120826
Fecha de corte	12 de agosto de 2026 · 09:08 CEST (UTC+02:00)
Ámbito	Marruecos · España/Ceuta · Francia · Gabón · ecosistema NSO/contratistas
Disciplina	OSINT · análisis de Inteligencia · evaluación de atribución
Clasificación	NO CLASIFICADO / FUENTES ABIERTAS
Idioma	Español de España; anglicismos sólo cuando son términos técnicos consolidados

NOTA DE INTEGRIDAD DOCUMENTAL

Este informe integra de forma exhaustiva sus hechos, alegaciones, protagonistas, cronologías, datos técnicos y matices, pero no reproduce íntegramente artículos protegidos por derechos de autor. El contenido periodístico se sintetiza y se atribuye a sus fuentes.

ADVERTENCIA DE ATRIBUCIÓN

Las referencias a operaciones de inteligencia, órdenes políticas, espionaje y represalias estatales incluyen afirmaciones periodísticas y testimonios de fuentes anónimas. Cuando no existe corroboración independiente suficiente se marca de forma expresa como ALEGACIÓN o NO CORROBORADO. El informe no convierte una atribución periodística en hecho probado.

Índice de contenidos

1. Resumen ejecutivo y juicios clave

El corpus analizado describe un sistema de vigilancia marroquí por capas: observación física, redes humanas, acceso a telecomunicaciones, explotación de dispositivos, vigilancia de cibercafés, herramientas forenses y, en el extremo de mayor sensibilidad, spyware mercenario de altas prestaciones. El patrón que emerge no es el de una dependencia exclusiva de Pegasus, sino el de una arquitectura escalonada en la que Pegasus funciona como instrumento de acceso remoto de alto valor cuando otros medios se consideran insuficientes. [FS-1; EC-1; GUA-1]

Forbidden Stories y trece socios periodísticos publicaron en julio de 2026 un nuevo paquete de cinco investigaciones sobre Marruecos, apoyado por el Security Lab de Amnesty International, documentos internos inéditos y el testimonio de un antiguo agente de la DGST identificado con el seudónimo “Safir”. El especial amplía el Pegasus Project de 2021 y aporta una narrativa interna sobre adquisición, empleo, responsables, infraestructura y objetivos. [FS-0; FS-1]

La atribución del uso de Pegasus a Marruecos alcanza un nivel de confianza analítica alto dentro de estándares OSINT: concurren testimonios internos, documentos, patrones forenses, infraestructura asociada, datos de litigios y confirmaciones cruzadas de fuentes del sector. Persisten, sin embargo, límites relevantes: Rabat lo niega, no toda inclusión en listas equivale a infección efectiva, y determinadas cadenas de mando o financiación se basan en fuentes que el consorcio no pudo verificar de forma independiente. [FS-1; FS-2; FS-4; GUA-1]

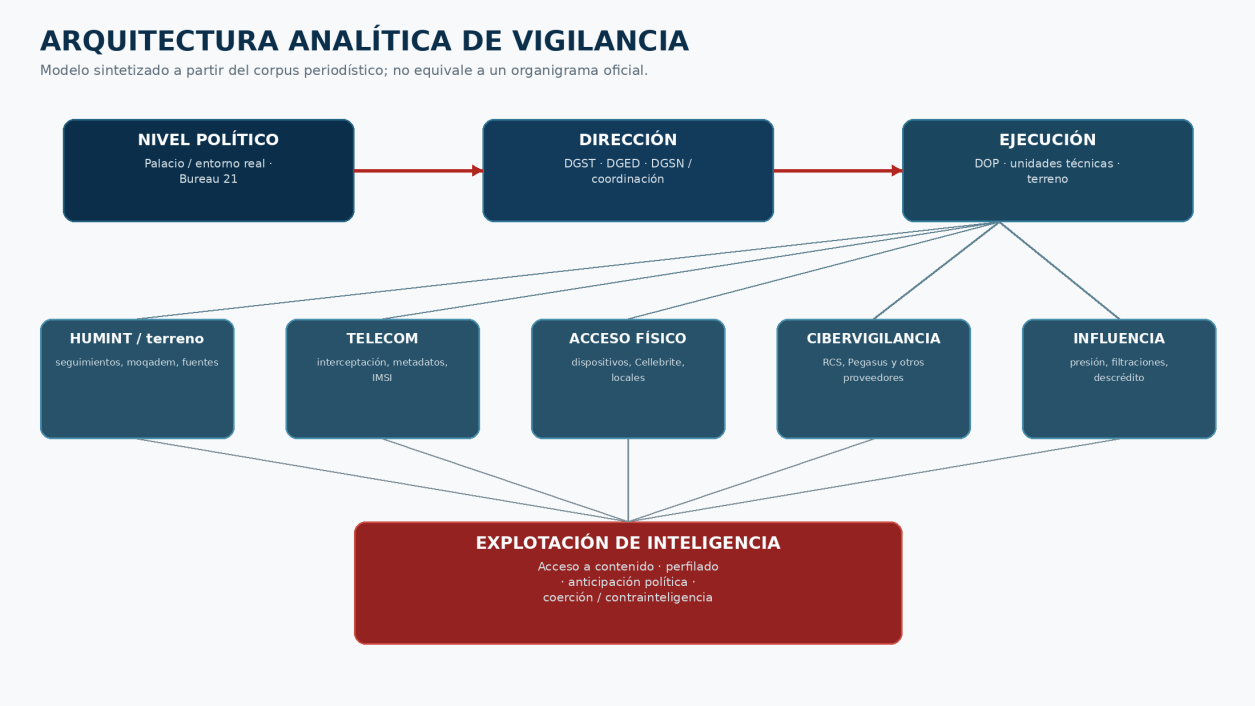


Figura 1. Modelo analítico de la arquitectura de vigilancia descrita por las fuentes. Elaboración propia.

ID	CONFIANZA	JUICIO	BASE
J1	ALTA	La DGST habría operado una arquitectura de vigilancia multicapa que combina seguimiento físico, HUMINT, acceso a telecomunicaciones, herramientas forenses y spyware.	Múltiples documentos, testimonios y corroboraciones cruzadas. [FS-1; EC-1]
J2	ALTA	Marruecos fue cliente/usuario de Pegasus al menos desde 2017 y hasta rastros documentados en 2021; “Morgan” aparece como nombre en clave asociado al cliente marroquí.	Fuentes del sector, documentos litigiosos y testimonios internos. [FS-2; GUA-1]
J3	MEDIA	Un intermediario vinculado al ecosistema emiratí habría facilitado el acceso marroquí a Pegasus; la financiación directa por EAU no está demostrada de forma concluyente.	Testimonios convergentes, pero fuentes ex-NSO no confirman el pago. [FS-2]
J4	ALTA/MEDIA	Altos responsables y funcionarios españoles y franceses quedaron dentro del ámbito de selección o compromiso técnico atribuido a infraestructura ligada a Marruecos.	Forense, listas y expedientes judiciales; la autoría última no está judicialmente establecida en todos los casos. [FS-4; FS-5; GUA-1]

ID	CONFIANZA	JUICIO	BASE
J5	MEDIA	La cooperación Guardia Civil–DGST generó una paradoja contrainteligente: instructores españoles habrían sido observados por el servicio al que formaban.	Documentos filtrados, testimonios y presencia de un alto mando en listas; algunas técnicas concretas no pudieron verificarse. [FS-5]
J6	MEDIA	La selección de figuras gabonesas durante la crisis sucesoria de 2019 sugiere que la vigilancia alcanzó también a aliados, no sólo a adversarios.	Lista de potenciales objetivos; no hay forense de todos los teléfonos. [FS-3]
J7	BAJA/MEDIA	La entrada masiva en Ceuta del 30 de julio de 2026 como represalia directa por las revelaciones Pegasus es plausible, pero NO CORROBORADA.	Dos exagentes y patrón temporal; falta orden documental o confirmación independiente. [EC-4]
J8	MEDIA/ALTA	Si se confirmara intervención estatal en Ceuta, encajaría en un repertorio híbrido que combina presión fronteriza, inteligencia, influencia y cibervigilancia.	Precedentes 2014/2021 y doctrina de instrumentalización; la motivación exacta de 2026 sigue abierta. [FS-5; EC-4]

JUICIO CENTRAL

La pieza de El Confidencial del 12 de agosto de 2026 no debe leerse como “prueba” de que la DGST ordenó la crisis de Ceuta: aporta una hipótesis de atribución sustentada en dos antiguos agentes y en indicios circunstanciales. El informe la mantiene separada de hechos verificados y de hipótesis alternativas.

2. Alcance, metodología y escala de confianza

2.1. Corpus primario

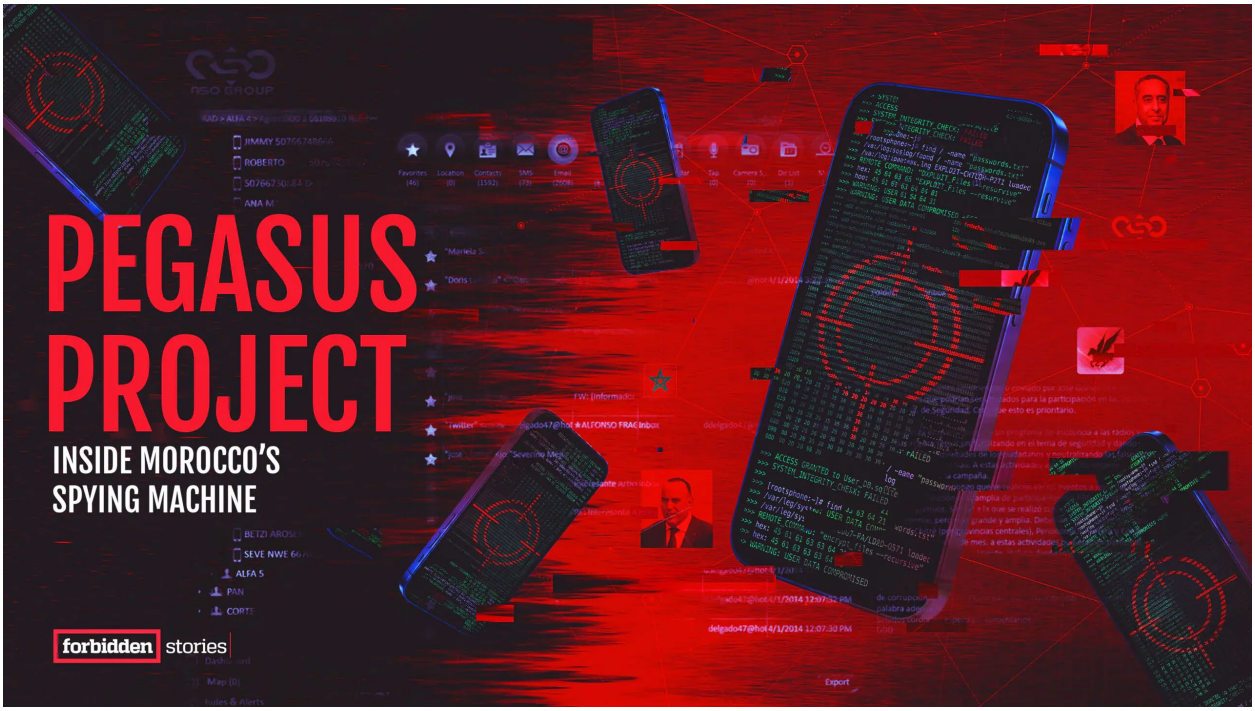


Imagen de apertura del proyecto “Pegasus Project: Inside Morocco’s spying machine”. Fuente: Forbidden Stories, julio de 2026. ©/crédito del medio de origen.

Se ha revisado el proyecto “Inside Morocco’s spying machine” y, dentro de su apartado Investigations, las cinco piezas temáticas publicadas por Forbidden Stories en julio de 2026. Se incorporan además los artículos enlazados de The Guardian y El Confidencial, incluida la pieza del 12 de agosto de 2026 sobre Ceuta. Los enlaces repetidos y la búsqueda de Google se han tratado como rutas de navegación, no como fuentes independientes. [FS-0]

AMPLIACIÓN VISUAL EC-1/EC-17: esta edición incorpora de forma expresa el material gráfico editorial relevante de las piezas de El Confidencial de 16 y 17 de julio de 2026: fotocomposiciones, documento CNI, mapas, capturas cartográficas/celulares, interfaces, las tres infografías de Pegasus y el archivo fotográfico de

la cooperación Guardia Civil–DGST. Cada elemento se integra en el capítulo temático correspondiente con pie, atribución y lectura analítica.

- FS-1 · Vigilancia interior y negación oficial de Pegasus: documentos, testimonio de Safir, caso Omar Radi, teléfonos preinfectados, cibercafés, RCS y estructura DGST.
- FS-2 · Adquisición de Pegasus: demostración en Rabat, nombre en clave “Morgan”, intermediación emiratí, relaciones con NSO e Israel y evolución posterior.
- FS-3 · Gabón: selección de dirigentes y opositores durante la crisis sucesoria de 2019.
- FS-4 · Francia: siete ministros con indicios de compromiso y proceso paralelo de posible compra francesa de Pegasus.
- FS-5 · España: cooperación Guardia Civil–DGST, formación, vigilancia de instructores, selección de un alto mando y contexto 2021–2022.
- EC-1/EC-2/GUA-1 · Ampliación española y técnica del especial: arquitectura, herramientas, cadena operativa, responsables y contexto ibérico.
- EC-4 · Ceuta 2026: hipótesis de represalia por las publicaciones y antecedentes de coerción diplomática/fronteriza.

2.2. Reglas de análisis

ETIQUETA	DEFINICIÓN	TRATAMIENTO
HECHO VERIFICADO	Dato respaldado por documentación pública, forense, registro judicial o múltiples fuentes independientes.	Se formula en indicativo con referencia concreta.
ALEGACIÓN ATRIBUIDA	Afirmación de fuente periodística, exagente, filtración o testimonio no plenamente corroborado.	Se formula con “según”, “habría”, “se atribuye” o equivalente.
INFERENCIA ANALÍTICA	Conclusión derivada de combinar hechos e indicios.	Se identifica expresamente y se acompaña de confianza.
NO CORROBORADO	Atribución sensible con soporte insuficiente para elevarla a hecho.	Se marca en rojo y se confronta con hipótesis alternativas.
VACÍO DE INTELIGENCIA	Información necesaria para discriminar entre hipótesis.	Se incorpora a la colección prioritaria.

2.3. Escala de confianza

La confianza no mide la gravedad de una afirmación; mide cuánto soporte disponible existe para sostenerla. “Alta” exige corroboración fuerte y diversa; “Media” indica evidencia consistente pero incompleta; “Baja/Media” señala una hipótesis razonable que todavía depende de fuentes únicas, anónimas o inferencias. La ausencia de respuesta oficial no se interpreta como confirmación.

LIMITACIÓN DE ACCESO

Una de las páginas de El Confidencial sobre el arsenal técnico aplica restricciones al acceso automatizado. Sus elementos sustantivos se han contrastado con el resto del especial, referencias contemporáneas y antecedentes públicos de proveedores. No se atribuye a esa pieza ningún detalle que no aparezca también apoyado por el corpus convergente.

3. Ecosistema institucional y cadena de decisión

Las fuentes sitúan a Abdellatif Hammouchi en el centro del aparato de seguridad interior: dirige la DGST y la DGSN, lo que concentra inteligencia interior y policía en una misma figura. El especial describe, además, la DGED como servicio exterior y menciona al entorno del Palacio —en particular Fouad Ali El Himma— en decisiones de alto nivel. Esta representación debe entenderse como reconstrucción periodística, no como organigrama oficial completo. [FS-1; FS-5; EC-1]

ACTOR / UNIDAD	FUNCIÓN ATRIBUIDA EN EL CORPUS	OBSERVACIÓN ANALÍTICA
Mohamed VI	Jefatura del Estado y autoridad última del sistema político.	Las fuentes vinculan grandes decisiones de seguridad al entorno real; no toda operación puede atribuirse personalmente al monarca.

ACTOR / UNIDAD	FUNCIÓN ATRIBUIDA EN EL CORPUS	OBSERVACIÓN ANALÍTICA
Fouad Ali El Himma / "Bureau 21"	Canal de alto nivel citado para solicitudes de espionaje estratégico y presión política.	Cadena específica no verificada independientemente por Forbidden Stories en todos los casos.
Abdellatif Hammouchi	Director DGST y DGSN; máxima figura operativa de seguridad interior.	Nodo central de cooperación con España y de la narrativa sobre Ceuta.
Yassine Mansouri / DGED	Inteligencia exterior.	Aparece en el contexto de crisis diplomáticas y coordinación estratégica.
Mohamed Raji / DOP	Dirección de Operaciones, según el especial.	Asociado al empleo operativo y a objetivos de alto nivel.
Abdeljalil Taki / DGEI	Responsable técnico citado; asociado a pruebas iniciales de Pegasus.	Su número habría figurado entre teléfonos usados en pruebas internas.
Abdelaziz Brachmi / ECT	Responsable citado en demostraciones / componente técnico.	Parte del núcleo técnico reconstruido por el consorcio.
FSSYS / Al Fahad / entorno EAU	Intermediación tecnológica y comercial.	El grado exacto de financiación emiratí permanece discutido.

El valor analítico de esta estructura es doble. Primero, muestra que la vigilancia descrita no sería un proyecto aislado de una unidad técnica, sino una capacidad conectada con prioridades de seguridad y política exterior. Segundo, explica por qué objetivos domésticos, aliados extranjeros y responsables gubernamentales aparecen en un mismo ecosistema de selección: la utilidad de la información prevalecería sobre la categoría formal de aliado o socio. [FS-1; FS-3; FS-4; FS-5]

Figura 3-A · Fotocomposición editorial del aparato de espionaje marroquí: mandos, objetivos, capturas de vigilancia y material cartográfico. Fuente: El Confidencial, 16/07/2026. Crédito: EC Diseño / pieza original.

Lectura analítica: La composición resume visualmente el núcleo del reportaje: dirección política y operativa, vigilancia territorial, selección de objetivos y explotación tecnológica dentro de una única arquitectura de inteligencia.

3.1. Reconstrucción visual del aparato DGST descrito por la investigación

La pieza de El Confidencial reconstruye una cadena funcional que parte del entorno real para los objetivos de especial sensibilidad y desciende hacia la DGST y, dentro de ella, hacia la Dirección de Operaciones (DOP). El esquema siguiente reproduce esa arquitectura como reconstrucción periodística y analítica; no se presenta como organigrama oficial publicado por Marruecos.

DRS	DLCT	DAFF	DRH	DOP
Inteligencia general	Lucha contra el terrorismo	Asuntos administrativos y financieros	Recursos humanos	Operaciones / núcleo técnico
				Director citado: Mohamed Raji
				SCP · DGEI · DGSO · DAG · DSO · DE · ECT

Dentro de la DOP, la investigación destaca el DGEI (Gestión y Explotación de Internet), asociado a Abdeljalil Taki, y la ECT (Entidad de Coordinación Técnica), asociada a Abdelaziz Brachmi. Ambos aparecen vinculados por las fuentes a las primeras demostraciones de Pegasus. El informe mantiene esta atribución como reconstrucción del consorcio, no como dato orgánico oficialmente confirmado.

JUICIO DE ESTRUCTURA

El material de EC-1 refuerza la tesis de una capacidad institucional y sostenida, no de una operación aislada asociada únicamente a Pegasus. La DOP aparece como el punto de convergencia técnico-operativo de una estructura más amplia en la que la selección de determinados objetivos de alto nivel se atribuye al entorno de la Casa Real y al denominado Bureau 21.

4. Arquitectura de vigilancia: de la calle al dispositivo

4.1. Un embudo de escalada

Safir describe un método incremental: antes de recurrir a Pegasus se explotan técnicas más baratas, discretas o ya integradas en la estructura del servicio. En el caso de Omar Radi, el consorcio relata seguimiento del vehículo, vigilancia de familiares y entorno, micrófonos y cámaras, monitorización de comunicaciones y finalmente acceso al teléfono. La lógica es de “escalada de colección”: sólo si una capa no produce inteligencia suficiente se activa otra de mayor coste, riesgo o sensibilidad. [FS-1; EC-1]

CAPA	CAPACIDADES DESCRITAS	VENTAJA	RIESGO / LIMITACIÓN
1 · Entorno humano	seguimiento, fuentes locales, red de moqadem, observación de contactos	Bajo coste; contexto humano	Detectable; consumo intensivo de personal
2 · Telecomunicaciones	interceptación, metadatos, identificación de terminales, presunto apoyo de operadores	Cobertura amplia	Dependencia de infraestructura y trazabilidad
3 · Acceso físico	teléfonos preinfectados, manipulación de equipos, cibercafés, cámaras	Persistencia / control del entorno	Requiere proximidad y logística
4 · Forense	Cellebrite sobre equipos incautados	Extracción profunda de dispositivos en custodia	Necesita acceso físico o incautación
5 · Spyware remoto	RCS, Pegasus y herramientas equivalentes	Acceso remoto de alto valor	Coste, licencias, exposición técnica y política
6 · Explotación	perfilado, anticipación, presión, campañas de descrédito según fuentes	Convierte datos en efecto	Riesgo legal, reputacional y contrainteligente

4.2. Teléfonos preinfectados y cibercafés

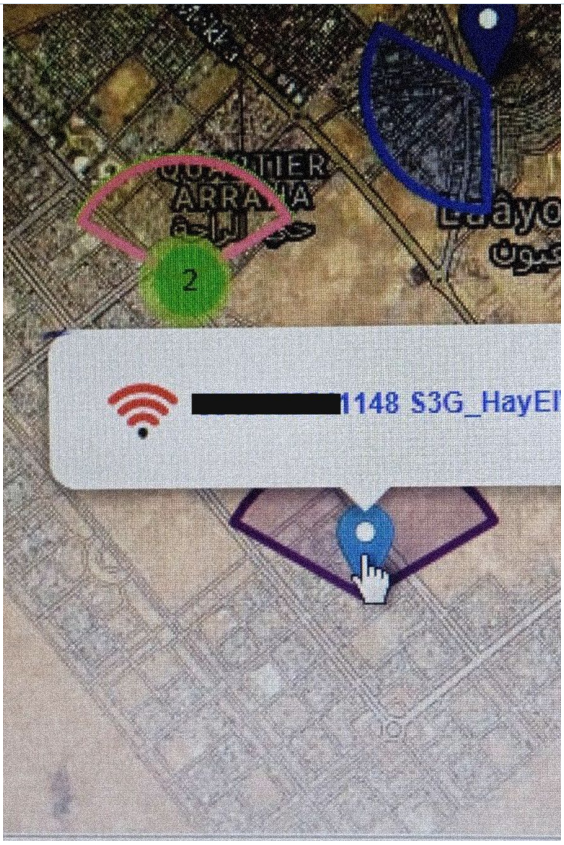
Los documentos internos descritos por Forbidden Stories incluyen la operación “S6_Edge”: alrededor de cincuenta Samsung Galaxy S6 Edge habrían sido adquiridos, infectados con software no identificado como Pegasus y colocados en tiendas del Rif para acabar en manos de activistas. El consorcio localizó a una de las personas fotografiadas en esos materiales, que confirmó haber recibido un terminal nuevo y haber sufrido

problemas de batería compatibles con una carga anómala, aunque ese síntoma por sí solo no prueba infección. [FS-1]

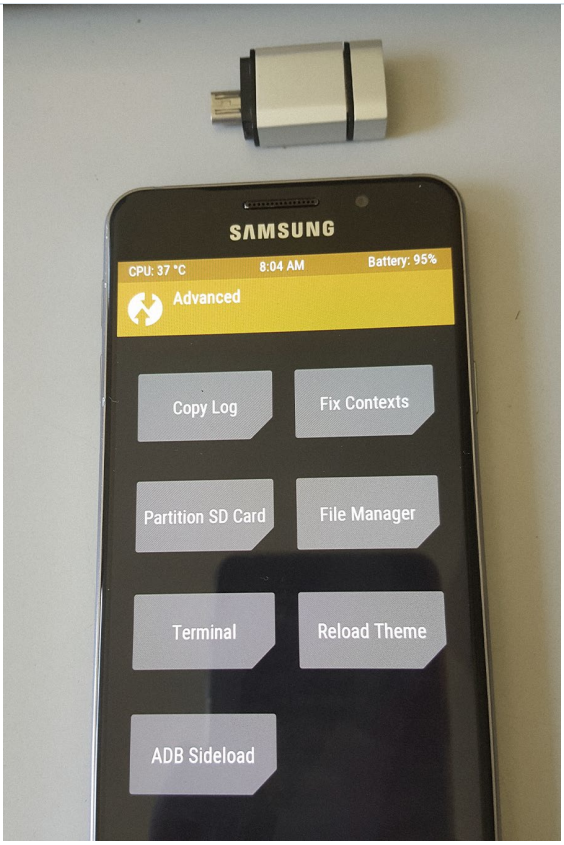
La misma investigación afirma que agentes identificaban los cibercafés frecuentados por objetivos y que ordenadores de esos locales eran comprometidos con Remote Control System (RCS), desarrollado originalmente por Hacking Team. Un antiguo empleado de la compañía recordó preocupaciones internas por el uso marroquí y por la extracción masiva de información. El antecedente es relevante porque demuestra una cultura operativa previa a Pegasus: comprometer el punto de acceso del objetivo cuando atacar directamente su teléfono no era viable. [FS-1]

4.2.1. Evidencia visual publicada sobre vigilancia, terminales y entorno de red

El Confidencial publica dos series de imágenes atribuidas a fuentes de la DGST. El conjunto incluye capturas de seguimiento geográfico/celular, terminales preparados o examinados, comercios y cibercafés, e interfaces empleadas para identificar celdas o puntos de interés. Las fotografías no prueban por sí solas cada operación descrita; sí aportan contexto material coherente con la metodología relatada por las fuentes.



Captura cartográfica/celular publicada como material procedente de fuentes de la DGST.

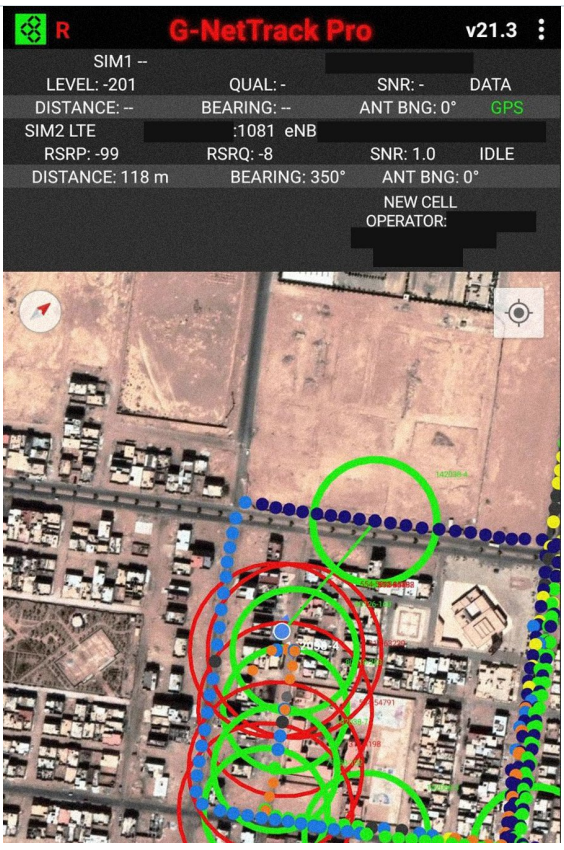


Terminal Samsung mostrado en el material de la investigación; la pieza lo contextualiza dentro de técnicas de acceso y preparación de dispositivos.

Cibercafé fotografiado en el material filtrado; la investigación describe el compromiso de ordenadores de uso público.

Detalle de un Samsung Galaxy S6 con identificadores ocultos en la publicación.

Comercio incluido en el material atribuido a fuentes DGST, relevante para la hipótesis de preposicionamiento de terminales.



Captura de G-NetTrack Pro con cartografía y celdas; contexto de identificación/monitorización de infraestructura móvil.

LECTURA DE COLECCIÓN POR CAPAS

Las imágenes encajan con un modelo que combina HUMINT, observación física, infraestructura celular, acceso a

dispositivos y compromiso de puntos de acceso. El valor analítico reside en la convergencia del material visual con testimonios, documentos y antecedentes técnicos; ninguna imagen aislada debe utilizarse como prueba autosuficiente de una infección concreta.

4.3. Operadores, datos e infraestructura

El especial español añade alegaciones sobre colaboración o acceso privilegiado a datos de operadores de telecomunicaciones, incluidos identificadores de terminal y provisión de tráfico suficiente para evitar que una extracción intensiva agote el bono de datos del objetivo. Estas afirmaciones son sensibles y dependen de fuentes internas; se registran como alegaciones atribuidas, no como hechos regulatoriamente probados. [FS-1; EC-1]

LECTURA DE CONTRAINTELIGENCIA

El patrón no exige que todas las capas estén activas simultáneamente. La ventaja de una arquitectura modular es elegir la combinación menos visible que produzca el dato buscado. Desde la perspectiva defensiva española, el riesgo no se reduce a “tener o no Pegasus”: incluye telecomunicaciones, dispositivos de viaje, redes locales, custodia física y exposición humana.

5. Adquisición de Pegasus y el cliente “Morgan”

5.1. Demostración en Rabat (2017)

Forbidden Stories sitúa una demostración de Pegasus a finales de 2017 en la denominada “Villa FSSYS”, en Rabat. Durante aproximadamente diez días, personal de NSO habría mostrado a altos cargos de la DGST cómo acceder a teléfonos de prueba, activar cámara y micrófono y extraer datos. Safir describe el impacto de la demostración como un salto cualitativo frente a herramientas anteriores. [FS-2]

El punto de transición tecnológica es importante: en 2017 la infección descrita dependía todavía de interacción del objetivo en determinados escenarios; posteriormente, Pegasus incorporó vectores de menor fricción y capacidades “zero-click”. El informe no reproduce procedimientos de explotación ni instrucciones técnicas, porque su interés es de capacidad y atribución, no operativo. [FS-2; GUA-1]

5.2. “Morgan” y la triangulación comercial

Varias fuentes del sector consultadas por el consorcio identifican “Morgan” como nombre en clave de NSO para el cliente marroquí. La pieza relaciona la adquisición con FSSYS/Al Fahad y un entorno empresarial de Emiratos Árabes Unidos. Este intermediario habría permitido una relación comercial menos visible en un momento en que Marruecos e Israel aún no habían normalizado formalmente relaciones. [FS-2]

La afirmación más fuerte —que Emiratos financió directamente el acceso marroquí— no alcanza el mismo nivel de evidencia. Safir y otras fuentes la sostienen, pero antiguos empleados o fuentes de NSO consultados no confirmaron conocer pagos emiratíes por la licencia de Marruecos. Por ello, el informe separa “intermediación probable” de “financiación directa no demostrada”. [FS-2]

5.3. Estado, industria y soberanía tecnológica

La investigación usa documentación judicial y episodios de litigio para mostrar la proximidad entre NSO y el Estado israelí, incluida la intervención gubernamental en procedimientos por razones de secreto de Estado. También relata que Shalev Hulio habría viajado con un pasaporte diplomático israelí, afirmación que el propio Hulio niega en lo relativo a haber poseído tal documento. Este punto debe conservarse como controversia, no como hecho pacífico. [FS-2]

Un memorando francés de inteligencia citado por el consorcio, fechado en diciembre de 2022, señala que decenas de países habían adquirido Pegasus y que Emiratos y Marruecos usaban productos de NSO al menos desde 2017. El mismo análisis consideraba muy probable que el proveedor —y potencialmente autoridades israelíes— pudieran conocer objetivos o información extraída. Es una valoración de riesgo de soberanía, no una demostración pública de acceso efectivo a cada operación. [FS-2; FS-4]

5.4. Dossier gráfico de Pegasus, “Morgan” y la infraestructura de Rabat

La publicación española incorpora material visual que permite documentar tres planos distintos: el entorno físico atribuido a las primeras demostraciones; interfaces históricas del producto Pegasus obtenidas de

filtraciones o procedimientos judiciales; y la capa de explotación posterior a la infección. Se reproducen a continuación los mapas e infografías de la pieza solicitada, con su contexto analítico.

Figura 5-A · Composición editorial de interfaces y material asociado a Pegasus. Fuente: El Confidencial, 16/07/2026.

Lectura analítica: La pieza utiliza este material para mostrar que la capacidad no termina en el acceso inicial: el operador trabaja sobre casos, objetivos, datos extraídos, etiquetas y reglas de explotación.

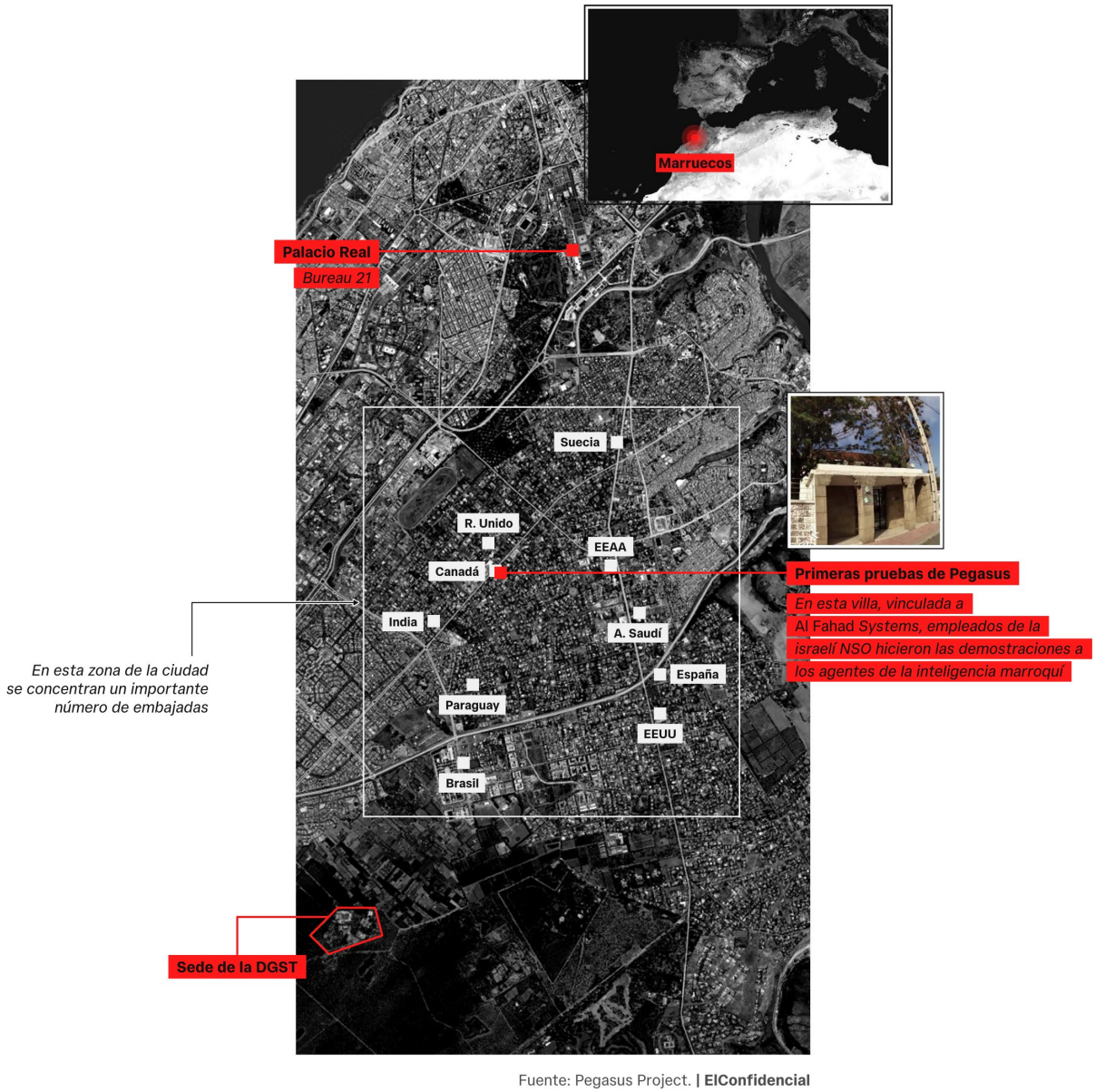


Figura 5-B · Mapa editorial de Rabat: villa vinculada a Al Fahad/FSSYS, embajadas, sede de la DGST y referencia al Palacio Real/Bureau 21. Fuente: Pegasus Project / El Confidencial.

Lectura analítica: El mapa ubica la villa atribuida a las primeras demostraciones de Pegasus en un entorno diplomático y relativamente próximo a la sede de la DGST. La investigación utiliza esa localización para reconstruir la fase de demostración y la intermediación comercial; no convierte la proximidad geográfica en prueba de una cadena de mando.

Figura 5-C · Composición de listados y documentación asociada a selección de objetivos. Fuente: El Confidencial, 16/07/2026.

Lectura analítica: El material ilustra la diferencia entre selección, intento de compromiso y compromiso confirmado. El informe mantiene esa distinción en todos los casos españoles y extranjeros.

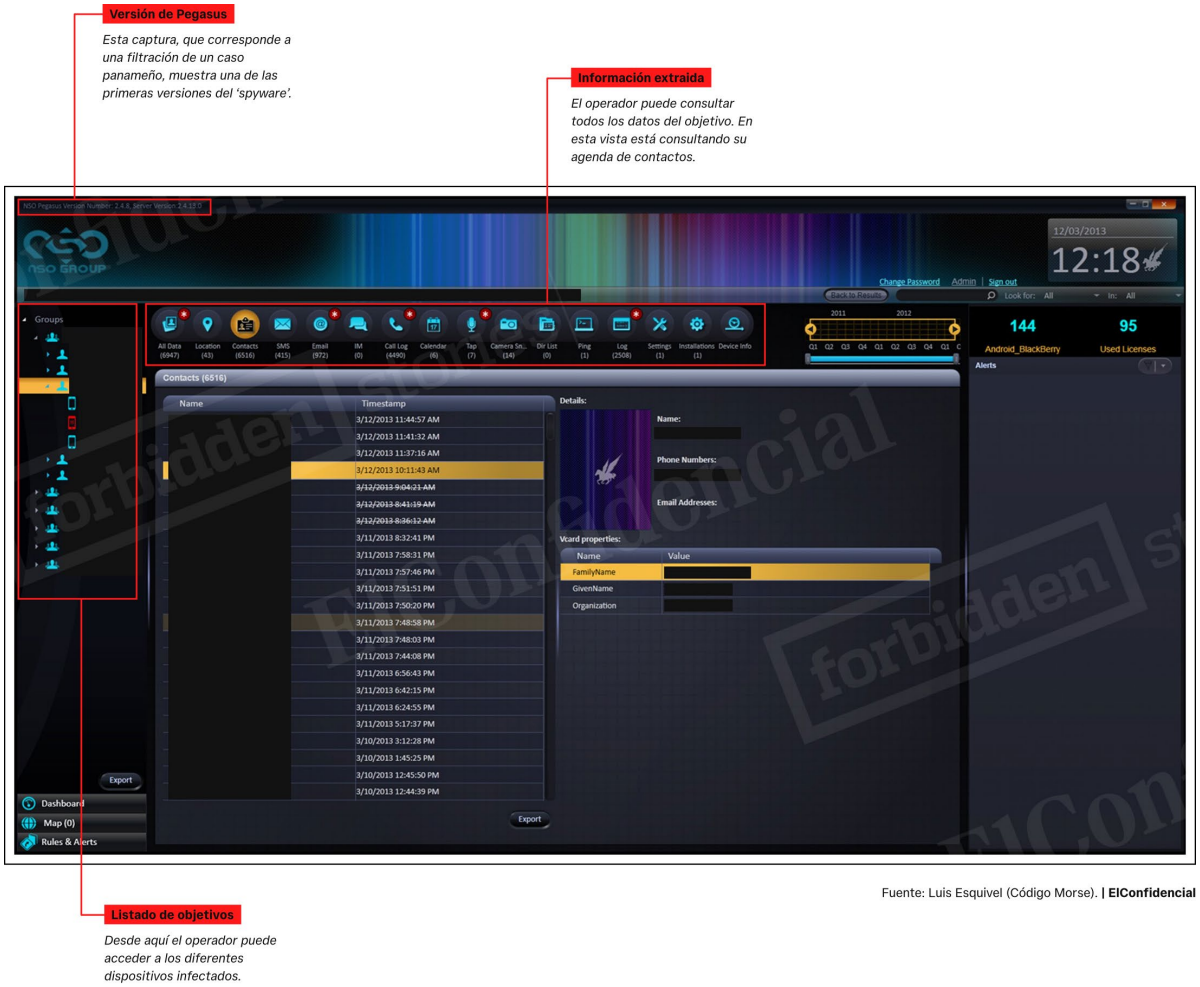


Figura 5-D · Infografía original: interfaz histórica de Pegasus, listado de objetivos y consulta de información extraída. Fuente: El Confidencial / material citado en la pieza.

Lectura analítica: La interfaz muestra la orientación a casos y objetivos y la centralización de datos extraídos. El interés para contrainteligencia reside en la amplitud de información agregable una vez comprometido el dispositivo.

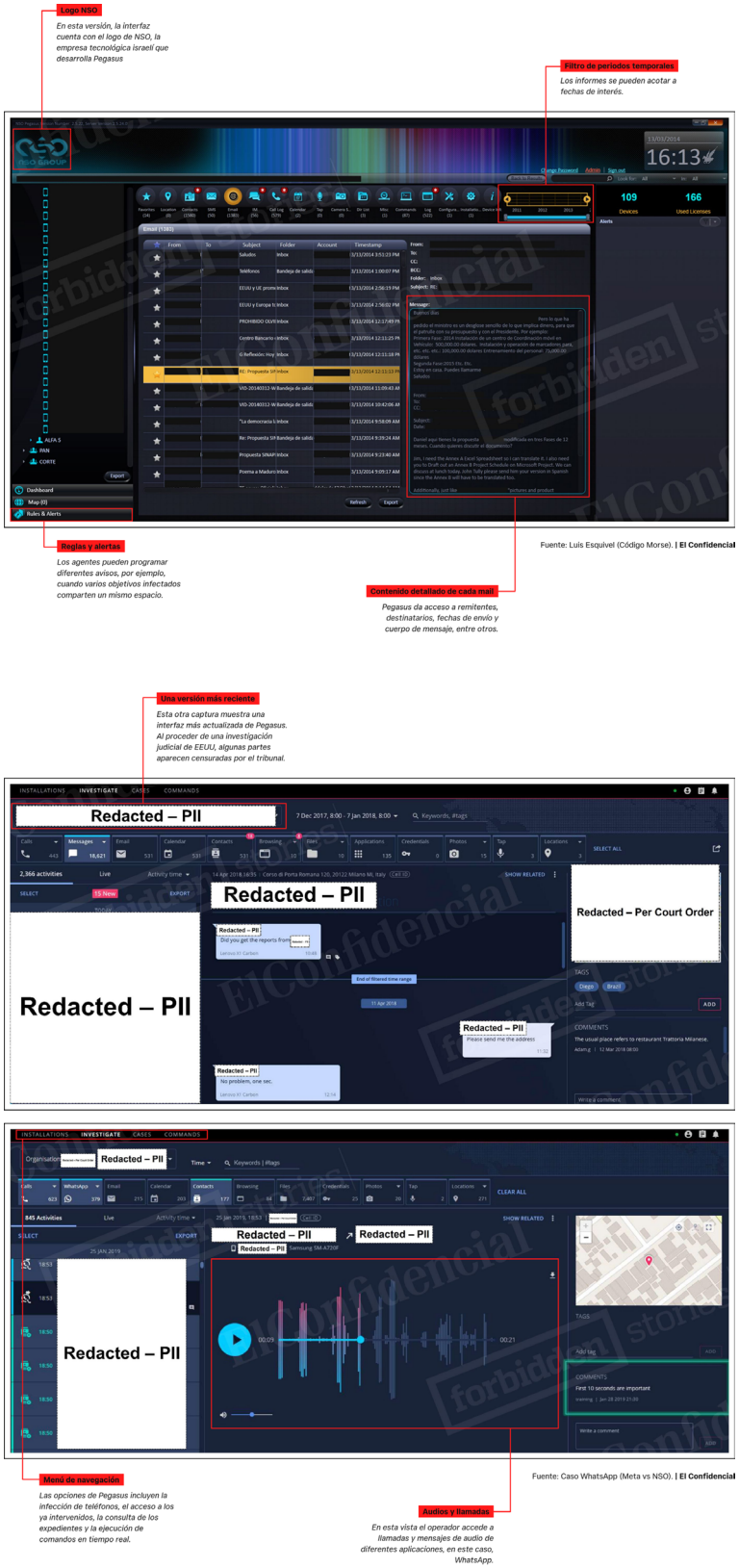
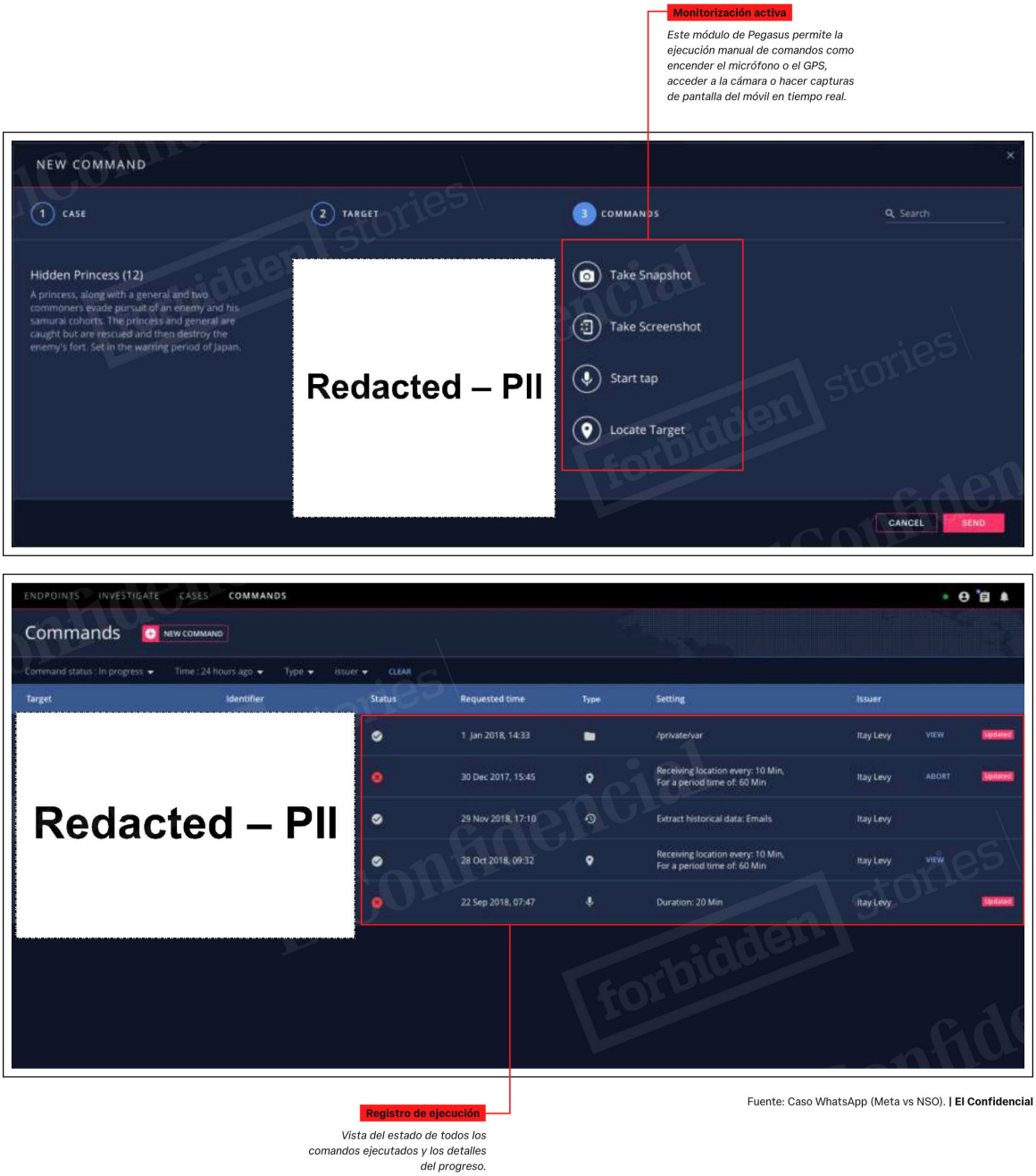


Figura 5-E · Infografía original completa: reglas/alertas, correo, versiones posteriores de interfaz, audio, llamadas y navegación por actividades. Fuente: El Confidencial / documentación judicial citada.

Lectura analítica: La evolución visual entre versiones sugiere una plataforma de explotación integrada: consulta retrospectiva, filtros temporales, mensajería, audio y correlación de actividades. Se reproduce la lámina completa para conservar el contexto editorial de la pieza.



Fuente: Caso WhatsApp (Meta vs NSO). **| El Confidencial**

Figura 5-F · Infografía original: monitorización activa y registro de ejecución de comandos. Fuente: El Confidencial / documentación judicial citada.

Lectura analítica: La lámina documenta el plano de monitorización activa atribuido a Pegasus y el registro de tareas. Desde una perspectiva defensiva, confirma que la protección no puede limitarse al contenido almacenado: sensores y contexto físico del terminal también forman parte de la superficie de riesgo.

SÍNTESIS TÉCNICA DE EC-1

La pieza describe una progresión desde reconocimiento y selección del objetivo hasta compromiso y explotación. Menciona, en términos históricos, vectores con nombres internos como Heaven, Diablo y Dragonfly, así como técnicas de clic, clic cero e inyección de red. El presente informe conserva esos nombres como contexto de evolución tecnológica, pero no reproduce procedimientos de explotación ni instrucciones operativas.

5.5. Cronología de adquisición y empleo

FECHA	HITO	LECTURA
2017 (ago–sep)	Demostraciones y primeras pruebas descritas en Rabat.	Entrada de Pegasus en la caja de herramientas DGST.
sep 2017	Números de agentes DGST usados como pruebas; comienzan selecciones sensibles.	Fase de validación / operacionalización.

FECHA	HITO	LECTURA
2018–2019	Expansión de objetivos nacionales y extranjeros; aparecen Gabón y España.	Consolidación de uso estratégico.
2019–2020	Indicios de compromiso en siete ministros franceses.	Alcance exterior de alto nivel.
2021	Crisis España–Marruecos; teléfonos de ministros españoles comprometidos según investigación judicial.	Pico de relevancia política y judicial.
nov 2021	Últimos rastros citados por el consorcio en Marruecos.	Coincide con mayor presión regulatoria y lista negra estadounidense a NSO.
2022 en adelante	Safir describe presentaciones de proveedores alternativos.	Diversificación y reducción de dependencia de un único spyware.

6. Arsenal técnico más allá de Pegasus

El título de una de las piezas de El Confidencial —"Más allá de Pegasus: el arsenal tecnológico de Marruecos para espiar dentro y fuera del país"— resume la tesis central: Pegasus es sólo la capa más conocida. El corpus menciona productos de extracción forense, interceptación celular, monitorización de redes, vigilancia de cámaras y malware de escritorio. Algunos nombres comerciales proceden de fuentes periodísticas y requieren cautela cuando no existe contrato público o atribución técnica independiente. [EC-2; FS-1; EC-1]

HERRAMIENTA	CLASE	FUNCIÓN ATRIBUIDA	CONFIANZA	NOTA
Pegasus · NSO Group	spyware móvil remoto	Objetivos de alto valor; extracción, sensores y comunicaciones	ALTA/MEDIA	Uso marroquí fuertemente sustentado; cada infección concreta requiere forense.
Cellebrite	forense móvil	Extracción de datos de terminales incautados / en custodia	ALTA	Uso descrito en el caso Radi; herramienta comercial ampliamente conocida.
RCS · Hacking Team / legado Memento	malware de equipos	Compromiso de ordenadores y cibercafés	ALTA/MEDIA	Documentos internos y testimonio de antiguo empleado.
IMSI catchers / Hailstorm	interceptación celular	Identificación, captura de metadatos y simulación de estación base	MEDIA	Alegado en fuentes del especial; detalles operativos concretos no siempre verificados.
Nighthawk / Interionet	vigilancia técnica	Acceso/gestión de cámaras u otros sensores según la pieza española	MEDIA/BAJA	Afirmación periodística; limitada corroboración pública.
Evident / soluciones BAE Systems	monitorización de red	Análisis de tráfico e internet a gran escala	MEDIA	Mencionado en el especial técnico; contratos/detalle requieren más documentación.
FinFisher / FinSpy y antecedentes	spyware	Antecedente histórico de mercado mercenario	MEDIA	Mencionado en contexto de compras anteriores; no equiparar automáticamente a operaciones 2026.

Las fuentes también sitúan a empresas y productos anteriores —Amesys, Vupen y Hacking Team— en el historial de adquisiciones de vigilancia de Marruecos. Informes europeos previos ya habían documentado a Marruecos como cliente relevante de Hacking Team. La continuidad histórica reduce la probabilidad de que Pegasus fuese una anomalía: encaja mejor como evolución de una política sostenida de compra de capacidades ofensivas y de vigilancia. [EC-2; antecedentes institucionales europeos]

IMPLICACIÓN DEFENSIVA

La mitigación debe ser "por capas": endurecimiento de dispositivos, control de custodia, separación de terminales sensibles/no sensibles, redes de viaje aisladas, revisión forense cuando existan indicadores y procedimientos contra captación HUMINT. Defenderse únicamente frente a un producto concreto deja abiertas las demás vías de acceso.

7. Caso Omar Radi y vigilancia de opositores / periodistas

El caso del periodista Omar Radi funciona en el especial como ejemplo de cómo se combinan vigilancia física, técnica, social y digital. Forbidden Stories relata que la DGST lo seguía al menos desde 2017; que su domicilio habría sido equipado con micrófonos y pequeñas cámaras; que se vigiló a familiares, amigos y hasta a su vendedor de cigarrillos; y que su vehículo era seguido de forma recurrente. [FS-1]

Radi adaptó su comportamiento: apagaba el teléfono al reunirse con fuentes y cortaba llamadas cuando sospechaba escuchas. Según Safir, esa disciplina obligó a intensificar métodos. En julio de 2020, tras una detención en Casablanca, su iPhone fue incautado. La pieza describe el uso de Cellebrite para extraer datos del terminal y relaciona el caso con infecciones previas de Pegasus documentadas por Amnesty International y el consorcio. [FS-1]

El valor del caso no es sólo biográfico. Muestra un “ciclo de inteligencia” completo: selección del objetivo, cobertura de su entorno, generación de hipótesis, escalada tecnológica, explotación del dispositivo y posterior uso de información en un contexto de presión judicial y mediática. El consorcio recoge alegaciones de que determinadas capacidades se utilizaron también para construir narrativas de descrédito o presionar a personas cercanas. Esas alegaciones requieren mantener una distinción entre vigilancia documentada y finalidad política inferida. [FS-1; EC-1]

Figura 7-A · Composición editorial dedicada al periodista Omar Radi y al seguimiento descrito por la investigación. Fuente: El Confidencial, 16/07/2026.

Lectura analítica: Radi funciona en el corpus como caso de estudio de escalada: vigilancia física, control del entorno, medios técnicos, explotación de dispositivos y posterior presión judicial/mediática. Las finalidades políticas concretas se mantienen como alegaciones atribuidas cuando no existe corroboración independiente.

Ampliación EC-1. La investigación sitúa la vigilancia de Radi en un arco temporal prolongado y describe seguimiento de desplazamientos y contactos, intervención del vehículo y del domicilio, presión sobre personas de su entorno y utilización de medios técnicos cuando las precauciones del periodista reducían la eficacia de las escuchas. También contextualiza la extracción forense de su iPhone mediante Cellebrite durante una

detención. El caso se utiliza como ejemplo de cómo la DGST habría combinado recursos humanos, físicos, forenses y spyware en función del rendimiento de cada capa.

7.1. El Rif y la vigilancia distribuida

Los teléfonos S6 Edge preinfectados y la infiltración de cibercafés aparecen vinculados a la contestación social del Rif. El método reduce la necesidad de atacar individualmente a cada activista: comprometer el canal de acceso o colocar equipos previamente manipulados permite ampliar la cobertura. Desde la perspectiva de inteligencia, es una estrategia de “preposicionamiento” tecnológico. [FS-1]

7.2. Periodistas y defensores de derechos humanos

El corpus incluye periodistas marroquíes y extranjeros, activistas y defensores de derechos humanos. Entre los nombres citados en el especial y sus ampliaciones aparecen Omar Radi, Hicham Mansouri, figuras vinculadas al Sáhara Occidental como Aminatou Haidar y el periodista español Ignacio Cembrero. En todos los casos debe diferenciarse entre estar incluido en una lista de selección, presentar indicadores forenses de compromiso y demostrar qué actor ejecutó la infección. [FS-1; GUA-1]

8. España: cooperación, entrenamiento y exposición de Contrainteligencia

Figura 8-A · Imagen de apertura de “Radiografía de una traición: cómo los agentes marroquíes espiaron a sus instructores de la Guardia Civil”. Fuente: El Confidencial / EC Diseño, 17/07/2026.

Lectura analítica: La composición contrapone la cooperación operativa y el espionaje clandestino, eje central de la pieza: un socio de seguridad puede conservar simultáneamente una misión de colección contra sus interlocutores.

Base documental de la pieza. El reportaje declara apoyarse en documentos y fotografías filtradas y en testimonios de un exagente de la DGST, dos fuentes de Guardia Civil, una de Policía Nacional y otra del CNI. El Laboratorio de Seguridad de Amnistía Internacional habría verificado de forma independiente la autenticidad del material aportado al consorcio. Esta pluralidad mejora la confianza sobre el contexto de cooperación y sobre la existencia del material, pero no convierte cada afirmación operativa de una fuente anónima en hecho probado.

8.1. De la cooperación antiterrorista a una relación de alta confianza

Tras el fin de la actividad armada de ETA, el terrorismo yihadista pasó a ocupar un lugar central en la cooperación de seguridad española. La investigación de Forbidden Stories sitúa desde 2014 una

intensificación de la relación entre la Guardia Civil y la DGST, sobre una cooperación ya existente de Policía Nacional y CNI. Se sucedieron visitas, operaciones antiterroristas y formaciones en ambos países. [FS-5]

La cooperación alcanzó un nivel institucional elevado: altos responsables españoles viajaron a Rabat y Hammouchi fue objeto de reconocimientos oficiales. La pieza señala que el 2 de julio de 2026 recibió a una delegación encabezada por el general Luis Peláez Piñeiro y recuerda que, en noviembre de 2025, el ministro del Interior Fernando Grande-Marlaska le concedió la Gran Cruz del Mérito de la Guardia Civil. [FS-5]

Jefe del Departamento de Sistemas de la DGST durante una visita al Santiago Bernabéu con la Guardia Civil. Fuente/pie: El Confidencial.

Fernando Grande-Marlaska y Abdellatif Hammouchi durante la concesión de la Gran Cruz del Mérito de la Guardia Civil. Fuente: Ministerio del Interior / El Confidencial.

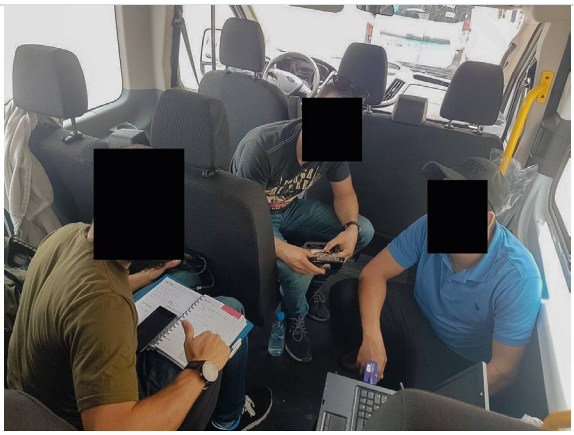
El artículo reconstruye la relación desde 2014: visitas de altos cargos, técnicos del Grupo de Apoyo Operativo (GAO), entrenamientos presenciales, operaciones conjuntas contra yihadismo e inmigración irregular e incluso un grupo conjunto de WhatsApp, según fuentes participantes. La proximidad institucional es relevante porque genera acceso físico, previsibilidad de viajes, conocimiento de rutinas y exposición de dispositivos; es decir, condiciones favorables tanto para cooperación como para colección contrainteligente.

8.2. Formación: capacidades transferidas

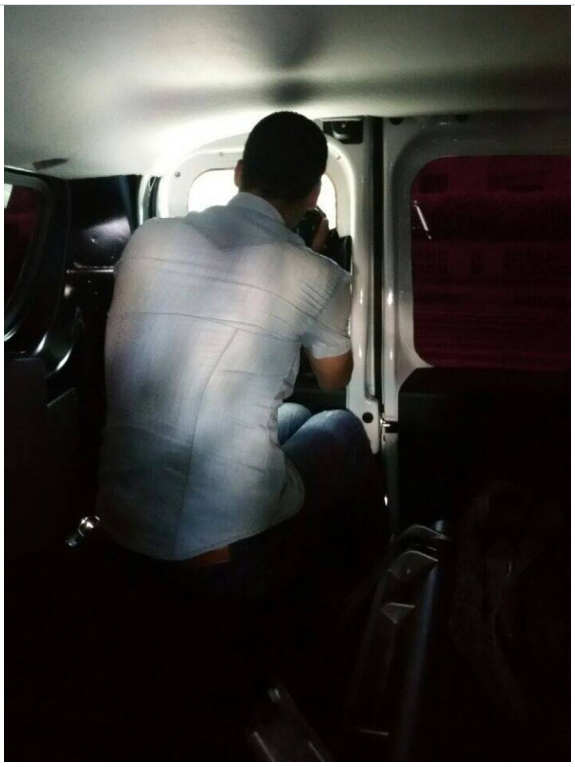
La Guardia Civil habría formado a personal de la DGST en seguimiento, infiltración, técnicas de obtención técnica, ciberinvestigación y otras capacidades. La investigación describe ubicaciones de formación en España —Ceuta, Málaga, Marbella y Madrid— y en Marruecos —Fnideq, Tánger, Rabat, Tetuán, Nador y Marrakech— . Parte de las afirmaciones sobre técnicas concretas procede de fuentes y material filtrado, por lo que no debe confundirse con un programa oficial íntegramente publicado. [FS-5]

La asimetría señalada por las fuentes es relevante: España habría transferido procedimientos a un socio que, al mismo tiempo, mantenía una doctrina de vigilancia de sus propios instructores “por si acaso”. Safir afirma que la DGST observaba a los formadores españoles sin que éstos lo supieran. La pieza añade que determinados mandos de Policía Nacional sí separaban dispositivos sensibles y no sensibles cuando viajaban a Marruecos, mientras que los equipos de Guardia Civil habrían operado con una percepción de confianza superior. [FS-5]

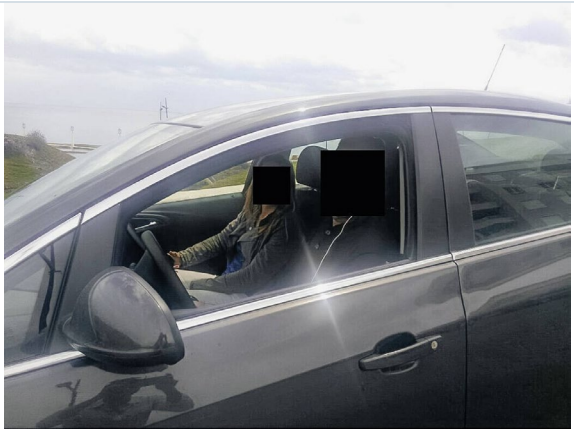
8.2.1. Archivo fotográfico de entrenamientos y vigilancia de los instructores



Ejercicio práctico de Guardia Civil y personal marroquí en Castillejos/Fnideq, junto a la frontera de Ceuta. Fuente/pie: El Confidencial.



Agente de la DGST fotografiando de forma clandestina durante un entrenamiento con la Guardia Civil, según el pie publicado. Fuente: El Confidencial.



Agente de Guardia Civil y agente DGST durante un entrenamiento cerca de Tánger. Fuente/pie: El Confidencial.

Entrenamiento práctico sobre inspección de equipajes durante una operación real, según el pie de la publicación. Fuente: El Confidencial.

Agente veterano de la DGST durante una operación con la Guardia Civil en Castillejos, frontera de Ceuta. Fuente/pie: El Confidencial.

Capacidades transferidas según la pieza. Las fuentes describen formación en seguimiento y vigilancia, acceso discreto a habitaciones de hotel y equipajes, instalación de medios técnicos de obtención de información y compromiso de ordenadores de cibercafés. El reportaje enmarca estas transferencias en la lucha contra el yihadismo, la trata, la inmigración irregular y, posteriormente, el narcotráfico. La alegación de que técnicas aprendidas de España se reutilizaron contra periodistas y defensores de derechos humanos procede esencialmente del exagente marroquí y no se acompaña en la pieza de evidencia documental específica para cada reutilización; por ello se mantiene como alegación de confianza media.

Geografía de la cooperación. La investigación sitúa actividades en España —Ceuta, Málaga, Marbella y Madrid— y en Marruecos —Fnideq/Castillejos, Tánger, Rabat, Tetuán, Nador y Marrakech—. Fuentes de Guardia Civil describen el intercambio de tácticas como esencialmente unidireccional. El artículo añade que algunos ejercicios se convertían en pruebas sobre situaciones reales y atribuye a la cooperación española la introducción temprana de determinados usos de drones por la DGST; esta última afirmación se conserva como testimonio atribuido.

ESPAÑA · ubicaciones citadas	MARRUECOS · ubicaciones citadas
Ceuta · Málaga · Marbella · Madrid	Fnideq/Castillejos · Tánger · Rabat · Tetuán · Nador · Marrakech

Lectura: una red de visitas y entrenamiento repetido aumenta la superficie de exposición HUMINT, física y digital de ambos servicios.

CONTRASTE OPSEC

La pieza describe una diferencia significativa: personal de información de Policía Nacional viajaría con un terminal de uso corriente para la red local y otro configurado para reducir exposición, mientras que efectivos del GAO de Guardia Civil no habrían aplicado medidas equivalentes por no considerar a sus anfitriones una amenaza. Esta asimetría de percepción es uno de los hallazgos contrainteligentes más relevantes del reportaje.

8.3. Alberto Aguilera y la selección de un mando español

Imagen publicada por Forbidden Stories: Fahad (izquierda, camiseta azul) durante una actividad de formación en Marruecos con un agente de la Guardia Civil. Fuente: Forbidden Stories, 17/07/2026.

El número personal de Alberto Aguilera, antiguo agregado de Interior en Rabat y posteriormente responsable de inteligencia de Guardia Civil en Cataluña, aparece cinco veces en la base de potenciales objetivos vinculada al Pegasus Project, con selección iniciada en marzo de 2019 según Forbidden Stories. Estar incluido en esa base demuestra interés de selección, no necesariamente infección exitosa. [FS-5]

Ampliación EC-17/07. La pieza concreta que los intentos de selección asociados al número de Alberto Aguilera comenzarían el 8 de marzo de 2019 y recuerda su etapa como agregado de Interior en la Embajada de España en Rabat (2012–2017) y su papel en el Centro de Cooperación Policial Hispano-Marroquí de Tánger. Después ocupó responsabilidades de información en Cataluña y otros destinos. El propio artículo recoge la opinión de su fuente marroquí sobre el riesgo de contrainteligencia que supone colocar en puestos sensibles a personal con exposición previa prolongada en un servicio extranjero; esta valoración se registra como opinión de fuente, no como incumplimiento probado de un protocolo español concreto.

La misma fuente identifica, mediante iniciales, a responsables de una “Cellule Recherche” de la DGST como participantes en escucha y monitorización de guardias civiles y en operaciones contra periodistas y activistas. Al no publicarse identidades completas ni documentación suficiente para verificar de forma independiente esas atribuciones individuales, el informe mantiene las iniciales y evita elevarlas a hechos nominativos.

PARADOJA CONTRAINTELIGENTE

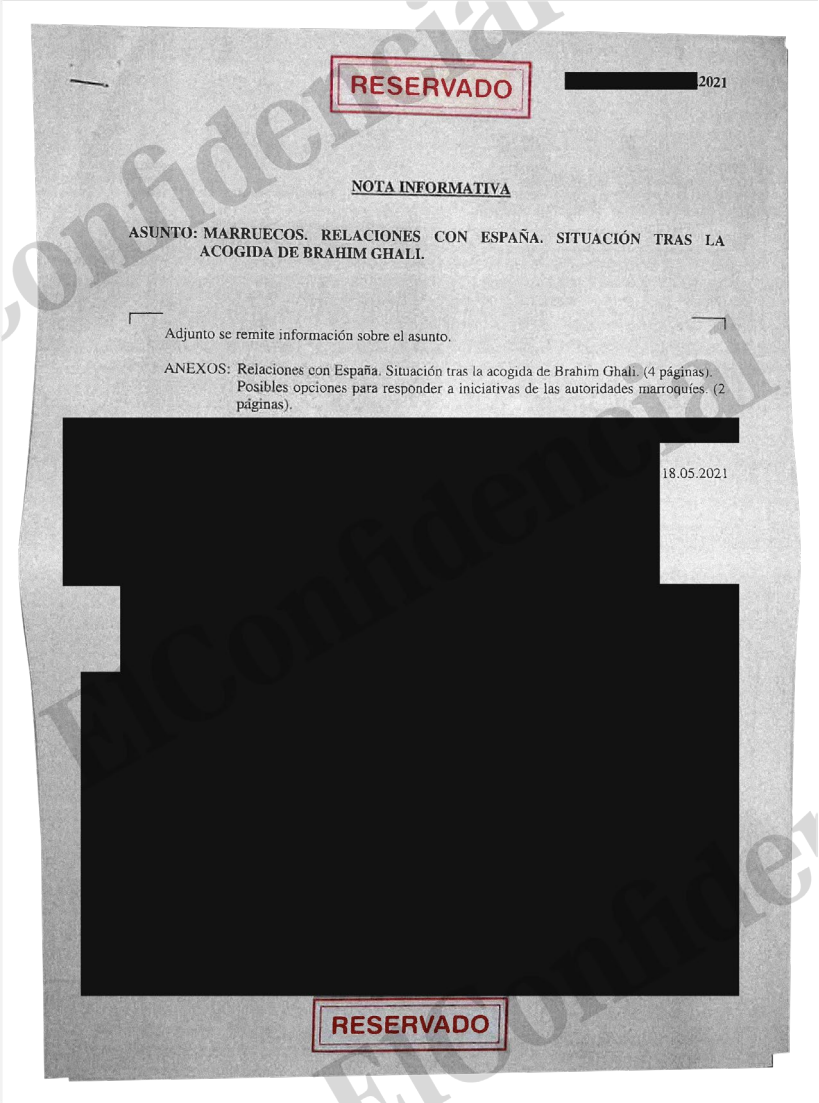
La cooperación operativa genera acceso, confianza y proximidad; esas mismas condiciones incrementan la superficie de captación. Un aliado puede ser simultáneamente socio frente a una amenaza común y objetivo de inteligencia en asuntos diplomáticos, económicos, militares o de política interior.

8.4. 2021: crisis diplomática, Ceuta y teléfonos ministeriales

El especial conecta la crisis diplomática de 2021 con la hospitalización en España del dirigente saharaui Brahim Ghali y con la presión marroquí sobre la posición española respecto al Sáhara Occidental. Según El Confidencial y el artículo de Forbidden Stories sobre España, informes secretos del CNI de mayo de 2021 habrían atribuido la planificación de medidas de presión a figuras del entorno real y a los principales responsables diplomáticos y de inteligencia marroquíes. [FS-5; EC-1]

En paralelo, la investigación judicial española confirmó infecciones con Pegasus en teléfonos de Pedro Sánchez, Margarita Robles y otros ministros. The Guardian y Forbidden Stories relacionan determinados indicadores técnicos y cuentas de ataque con infraestructura anteriormente asociada al cliente marroquí. La Audiencia Nacional investigó los hechos, pero la atribución penal a una persona o autoridad concreta quedó limitada, entre otros factores, por la falta de cooperación israelí. Por tanto: compromiso técnico, sí; cadena de autoría estatal completa, no judicialmente cerrada. [FS-5; GUA-1]

8.4.1. Documento CNI, presión diplomática y continuidad del riesgo



RESERVADO

[redacted] 2021

NOTA INFORMATIVA

ASUNTO: MARRUECOS. RELACIONES CON ESPAÑA. SITUACIÓN TRAS LA ACOGIDA DE BRAHIM GHALI.

Adjunto se remite información sobre el asunto.

ANEXOS: Relaciones con España. Situación tras la acogida de Brahim Ghali. (4 páginas).
Posibles opciones para responder a iniciativas de las autoridades marroquíes. (2 páginas).

[redacted]

18.05.2021

[redacted]

RESERVADO

Figura 8-B · Nota informativa del CNI marcada “RESERVADO” sobre las relaciones con Marruecos tras la acogida de Brahim Ghali, tal como fue publicada por El Confidencial. Fecha visible: 18/05/2021. Partes sensibles aparecen ocultas en la publicación.

Lectura analítica: El documento aporta contexto contemporáneo sobre la percepción española de la crisis. La pieza atribuye a informes del CNI una estrategia de presión coordinada por Fouad Ali El Himma con Hammouchi y otros responsables. La publicación de una portada o extracto no permite reconstruir por sí sola el contenido íntegro del informe clasificado.

Figura 8-C · Dos agentes de la DGST frente al Palacio Real en Madrid, según el pie de El Confidencial. Fuente: El Confidencial, 17/07/2026.

Lectura analítica: La imagen refuerza el componente exterior del patrón: la relación de cooperación no excluye presencia operativa o actividades de observación fuera de Marruecos.

Secuencia 2021. El reportaje recuerda que el primer intento de infección detectado en el teléfono de Pedro Sánchez se sitúa en octubre de 2020 y que, en mayo de 2021, la investigación judicial documentó una extracción de 2,57 GB. La proximidad temporal con la crisis de Ceuta y la hospitalización de Brahim Ghali es estratégicamente relevante, pero la correlación temporal no equivale por sí sola a atribución judicial de la operación a Marruecos.

Continuidad 2022–2023 según la pieza. El artículo menciona el viaje secreto de la directora del CNI Esperanza Casteleiro a Rabat en septiembre de 2022 y la posterior difusión por la inteligencia marroquí de fotografías de la reunión con Hammouchi sin consentimiento español, así como una investigación publicada en 2023 sobre el presunto reclutamiento por Marruecos de una familiar directa de un alto responsable de Información de Policía Nacional. Estos episodios se incorporan como ejemplos periodísticos de una relación simultáneamente cooperativa y competitiva; el segundo remite a una investigación separada y no se revalida aquí de forma independiente.

JUICIO CONTRAINTELIGENTE SOBRE ESPAÑA

El hallazgo principal no es que la cooperación deba cesar, sino que la cooperación no debe utilizarse como indicador de ausencia de espionaje. La combinación de entrenamiento, visitas, grupos de coordinación, redes móviles locales y confianza personal crea una superficie de colección excepcionalmente rica. La doctrina defensiva española debería asumir de forma permanente el modelo “socio y colector”.

PERSONA / FUNCIÓN	TIPO DE INDICIO	INTERPRETACIÓN PRUDENTE
Pedro Sánchez · presidente del Gobierno	Infección confirmada en investigación española; extracción de datos citada por el especial.	Compromiso probado; atribución final a Marruecos no equivale a sentencia judicial.
Margarita Robles · Defensa	Infección / infraestructura de ataque asociada en el corpus.	Objetivo de alto valor estratégico.
Fernando Grande-Marlaska · Interior	Objetivo/compromiso citado; infraestructura técnica relacionada.	Interés directo en seguridad y cooperación bilateral.
Luis Planas · Agricultura	Objetivo citado en documentación judicial / periodística.	Amplía el espectro más allá de seguridad estricta.

PERSONA / FUNCIÓN	TIPO DE INDICIO	INTERPRETACIÓN PRUDENTE
Arancha González Laya · Exteriores	Objetivo en contexto de crisis Ghali.	Elevado valor diplomático; cronología políticamente significativa.
Alberto Aguilera · Guardia Civil	Número seleccionado cinco veces desde 2019.	Selección demostrada; infección no confirmada por ese dato solo.

9. Francia: ministros comprometidos y compra frustrada

La investigación francesa muestra una coincidencia estratégica: mientras servicios franceses evaluaban adquirir Pegasus, varios miembros del Gobierno presentaban indicios de compromiso. El revendedor oficial de NSO en Francia describió conversaciones con organismos de seguridad y un posible contrato de entre 60 y 80 millones de euros. La pieza señala que el Elíseo terminó vetando la compra a finales de 2020 por riesgos de soberanía y reputación. [FS-4]

Forbidden Stories identifica siete ministros con “signos de compromiso” compatibles con Pegasus: Jean-Michel Blanquer, Jacqueline Gourault, Julien Denormandie, Emmanuelle Wargon, François de Rugy, Florence Parly y Sébastien Lecornu. Los indicadores técnicos compartían rasgos con infraestructura observada en objetivos anteriormente vinculados al operador marroquí. [FS-4]

La ANSSI documentó identificadores y artefactos técnicos utilizados para correlacionar campañas. La DGSE, en documentación judicial posterior, habría caracterizado determinadas intrusiones como operaciones de espionaje que afectaban a intereses fundamentales franceses y señaló que Marruecos y Emiratos utilizaban productos NSO desde al menos 2017. [FS-4]

El caso ofrece una lección de soberanía: una capacidad puede parecer atractiva para un servicio nacional y, simultáneamente, representar un riesgo contra el propio Estado comprador si el proveedor, el país exportador o terceros clientes mantienen visibilidad sobre metadatos, objetivos, soporte o infraestructura. [FS-2; FS-4]

10. Gabón: vigilancia de un aliado africano

En marzo de 2019, durante la incertidumbre sobre la sucesión de Ali Bongo tras su ictus y un intento fallido de golpe, alrededor de diez figuras gabonesas aparecieron en la lista de potenciales objetivos de Pegasus asociada a Marruecos. Entre ellas se encontraban Noureddin Bongo Valentin, Brice Laccruche Alihanga y opositores como Jean Ping y Dieudonné Minlama Mintogo. [FS-3]

La singularidad del caso reside en la estrecha relación Marruecos–Gabón. Ali Bongo había sido atendido y rehabilitado en Rabat, existían vínculos de seguridad y formación, y Gabón era un socio diplomático relevante para Marruecos en África. Según una fuente de la DGST, la cooperación no impidió la selección de figuras del entorno presidencial. [FS-3]

No se dispone de análisis forense de todos los teléfonos y, por tanto, no puede afirmarse que cada número fuese infectado. La selección, sin embargo, permite inferir interés por anticipar la sucesión, medir lealtades y comprender redes internas de poder. El patrón refuerza el juicio de que la categoría “aliado” no excluye la colección de inteligencia. [FS-3]

11. Ceuta 2021–2026: frontera, coerción e inteligencia

11.1. Ceuta como sensor de la relación bilateral

Ceuta concentra en pocos kilómetros soberanía, migración, cooperación policial, comercio transfronterizo, percepción pública y relación Marruecos–España. Por ello, cambios mínimos en la actuación de fuerzas marroquíes, en las narrativas de redes sociales o en los controles de Fnideq/Tarajal pueden producir efectos políticos inmediatos en España. En términos de inteligencia, la frontera funciona como sensor y como posible palanca. [FS-5; EC-4]

11.2. Precedente de mayo de 2021

En mayo de 2021, aproximadamente diez mil personas cruzaron hacia Ceuta en un episodio que la investigación de Forbidden Stories y El Confidencial vincula a la crisis por Brahim Ghali y a una estrategia de

presión marroquí. Las piezas atribuyen a informes del CNI la idea de que Rabat veía el episodio como instrumento para modificar la posición española sobre el Sáhara Occidental. [FS-5; EC-1]

La coincidencia temporal entre presión fronteriza y compromiso de teléfonos ministeriales alimenta una lectura híbrida: obtención de inteligencia para conocer deliberaciones españolas y presión simultánea en el terreno. Sin una orden pública que una ambos vectores, la relación causal debe formularse como inferencia, no como hecho demostrado. [FS-5; EC-1]

11.3. Precedente de agosto de 2014

La pieza de El Confidencial del 12 de agosto de 2026 recuerda otro antecedente: en agosto de 2014 se produjo una entrada marítima numerosa coincidiendo con una crisis diplomática después de que una patrullera española interceptara por error una embarcación del rey Mohamed VI. El artículo sitúa además una suspensión temporal de cooperación judicial, policial y antiterrorista. El valor del antecedente es analógico: muestra que la cooperación de seguridad puede modularse como señal política. [EC-4]

11.4. Francia 2014 como patrón de represalia institucional

El mismo artículo invoca la crisis franco-marroquí de 2014 tras un intento judicial francés de interrogar a Hammouchi. Marruecos suspendió cooperación y se produjeron filtraciones y campañas informativas. Posteriormente aparecieron filtraciones en sentido contrario sobre documentación marroquí. El episodio ilustra una cultura de represalia y contra-represalia, pero no demuestra automáticamente que el patrón se repitiera con el mismo mecanismo en Ceuta en 2026. [EC-4]

12. Crisis de Ceuta de julio de 2026: análisis competitivo de hipótesis

ATRIBUCIÓN PRINCIPAL: NO CORROBORADA

El 12 de agosto de 2026, Ignacio Cembrero publicó en El Confidencial que la entrada masiva ocurrida a finales de julio habría sido una “venganza” del aparato de seguridad marroquí por las revelaciones del especial Pegasus difundidas por catorce medios. La pieza basa el núcleo de la atribución en dos antiguos miembros de servicios marroquíes exiliados en Occidente y en una secuencia de indicios temporales y conductuales. [EC-4]

Según el artículo, la publicación de las investigaciones entre el 16 y el 18 de julio fue seguida desde alrededor del 20 de julio por un aumento de entradas a nado. El 27 de julio, Ceuta y la Delegación del Gobierno reclamaron una respuesta extraordinaria. El 30 de julio se produjo una entrada masiva cuya magnitud la pieza cifra entre 70.000 y 80.000 personas. Dado lo extraordinario de esa cifra y la existencia de estimaciones diferentes en distintas fuentes, el presente informe la registra como “cifra periodística atribuida”, no como conteo validado. [EC-4]

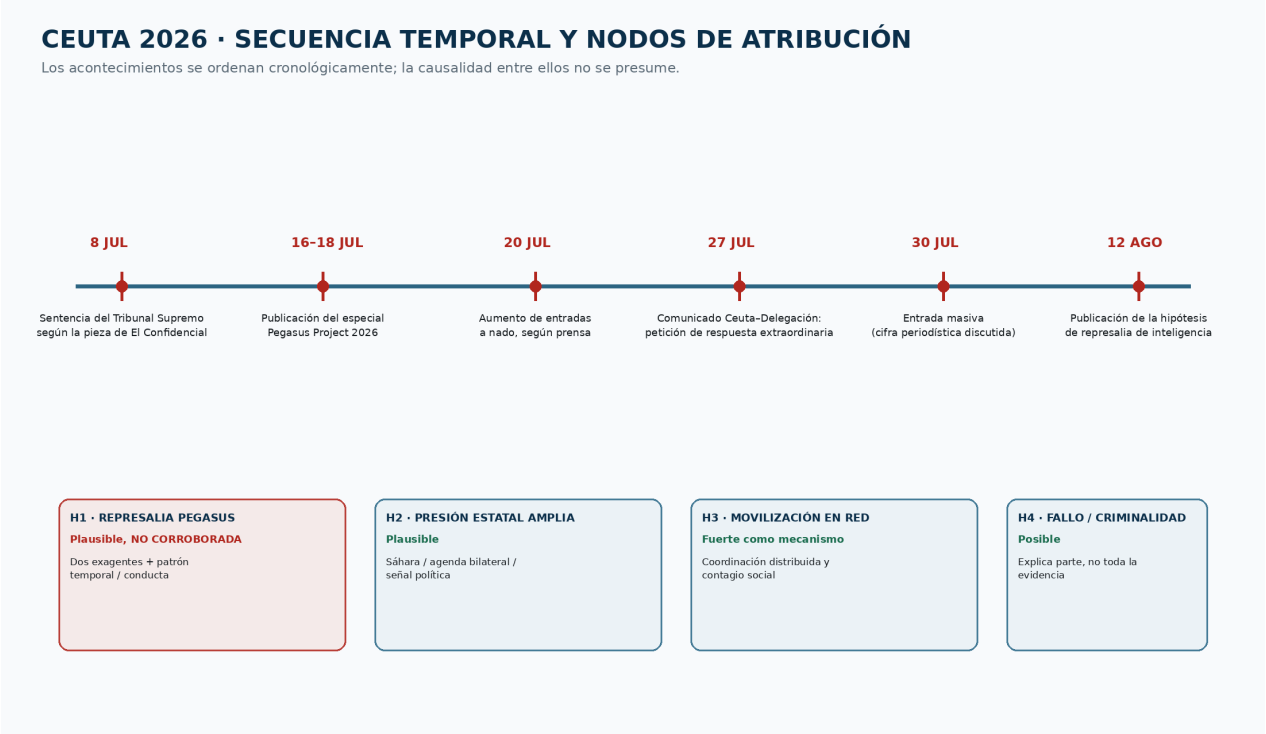


Figura 2. Secuencia temporal de julio–agosto de 2026 y principales hipótesis. Elaboración propia.

12.1. H1 — Represalia por las revelaciones Pegasus

H1 · NO CORROBORADA

La DGST/DGSN habría reducido deliberadamente la presión fronteriza por orden superior para castigar a España y generar un coste político tras las publicaciones sobre Pegasus. Confianza: BAJA/MEDIA.

Indicadores a favor: proximidad temporal entre las publicaciones y el cambio de dinámica fronteriza; testimonios de dos exagentes que atribuyen la decisión a la cúspide de seguridad; alegación de retirada o pasividad de policía y auxiliares en áreas próximas a Tarajal, Fnideq y Belyounech; existencia de precedentes donde Rabat moduló cooperación y presión migratoria durante crisis bilaterales; y la sensibilidad personal/institucional de Hammouchi ante revelaciones que afectan a la DGST. [EC-4]

Indicadores en contra o limitaciones: no se aporta una orden, comunicación interceptada, acta, registro de mando o fuente contemporánea en servicio que documente la cadena de decisión; los dos exagentes pueden disponer de conocimiento general del aparato pero no necesariamente acceso directo a una orden de julio de 2026; la movilización en redes pudo amplificar un gesto inicial hasta un volumen no previsto; y la propia pieza afirma que la situación “se fue de las manos”, lo que debilita la hipótesis de control completo. [EC-4]

12.2. H2 — Presión estatal deliberada por una agenda bilateral más amplia

H2 · PLAUSIBLE

La permisividad fronteriza habría sido una señal estatal, pero motivada por un conjunto más amplio de asuntos —Sáhara Occidental, cooperación, reconocimiento político, mensajes regionales— y no exclusivamente por Pegasus. Confianza: MEDIA.

Esta hipótesis explica mejor una posible decisión de presión sin exigir que el especial Pegasus sea el único desencadenante. Marruecos ha utilizado históricamente la intensidad de cooperación fronteriza como parte de la relación bilateral; las revelaciones podrían haber actuado como catalizador dentro de una acumulación de agravios o mensajes. La debilidad es que la pieza del 12 de agosto atribuye específicamente la motivación a Pegasus, mientras que no se dispone de documentación pública para ponderar otras causas. [EC-4; FS-5]

12.3. H3 — Movilización descentralizada en redes + ventana de oportunidad

H3 · MECANISMO FUERTE

Una red distribuida de cuentas, grupos y coordinadores habría difundido rutas, horarios y expectativas de baja vigilancia; una percepción colectiva de "frontera abierta" habría producido contagio social. Confianza en el mecanismo: MEDIA/ALTA.

La dinámica descrita por fuentes posteriores sobre grupos en redes sociales es compatible con una movilización de tipo enjambre: coordinadores, microdifusores, mensajería privada y amplificación pública. Este mecanismo puede coexistir con H1 o H2. Incluso si una autoridad hubiese relajado controles, la escala final podría haber sido producida por efectos de red que superaron la intención inicial. A la inversa, una movilización descentralizada no demuestra por sí sola que el Estado marroquí la organizara. [fuentes abiertas complementarias; EC-4]

12.4. H4 — Criminalidad organizada / mafias como causa principal

La versión oficial marroquí citada en el artículo atribuye responsabilidad a mafias y redes de migración irregular. El Confidencial discute esa explicación y señala que muchos participantes parecían actuar por oportunidad, curiosidad o contagio social más que mediante un servicio de tráfico estructurado. Desde un enfoque de inteligencia, no conviene eliminar esta hipótesis: redes criminales pueden explotar una ventana sin ser su causa original. Confianza como explicación exclusiva: BAJA. [EC-4]

12.5. H5 — Fallo de control / error administrativo y cascada espontánea

Una combinación de sentencia judicial, expectativas de no devolución inmediata, retirada temporal de efectivos, información falsa o malinterpretada y reacción tardía puede producir una cascada sin una orden estatal de coerción. Esta hipótesis gana plausibilidad si futuras pruebas muestran que las autoridades marroquíes intentaron contener el flujo desde el principio y perdieron capacidad. Pierde fuerza si se confirma una pasividad uniforme y deliberada durante horas en múltiples puntos. Confianza: MEDIA/BAJA. [EC-4]

HIP.	EXPLICACIÓN	CONFIANZA	FORTALEZA	DEBILIDAD
H1	Represalia Pegasus	BAJA/MEDIA	Temporalidad + 2 exagentes + presunta pasividad	Sin orden ni corroboración interna contemporánea
H2	Presión estatal amplia	MEDIA	Precedentes + utilidad estratégica de la frontera	Motivación exacta indeterminada
H3	Movilización en red	MEDIA/ALTA	Mecanismo de coordinación y contagio plausible	No resuelve quién abrió/permitió la ventana
H4	Mafias como causa principal	BAJA	Explicación oficial; capacidad logística existente	No explica por sí sola escala y comportamiento descrito
H5	Fallo + cascada espontánea	MEDIA/BAJA	Puede generar efecto avalancha	Debe explicar presunta retirada/pasividad

SÍNTESIS DE ATRIBUCIÓN

La explicación más robusta, con la evidencia disponible, es un modelo combinado: existió una ventana de oportunidad y una movilización en red; es plausible que la postura de seguridad marroquí contribuyera a esa ventana. Lo que todavía no está demostrado es que la motivación específica y principal fuese "vengarse" por el especial Pegasus. Ese salto causal requiere evidencia adicional.

13. Contradicciones, desmentidos y contranarrativas

13.1. Negación oficial marroquí

Marruecos ha negado históricamente haber utilizado Pegasus. Las investigaciones de 2026 señalan que el Gobierno, la DGST, NSO y otros actores contactados no respondieron a múltiples preguntas o rechazaron determinadas alegaciones. La negación debe formar parte de la matriz; no basta para invalidar una atribución técnica, pero tampoco puede omitirse. [FS-1; FS-2]

13.2. Crítica desde medios alineados con Rabat

Medios cercanos a la narrativa oficial marroquí han cuestionado la investigación alegando que el nombre en clave “Morgan” no identifica inequívocamente a Marruecos, que parte de la infraestructura se atribuye mediante marcos heredados de 2021 y que el anonimato de Safir limita la posibilidad pública de auditar su credibilidad. Son objeciones pertinentes en términos metodológicos —especialmente la necesidad de transparencia sobre cadena de custodia—, aunque algunos textos las mezclan con ataques personales a periodistas y fuentes. [contranarrativa marroquí]

El consorcio responde de facto a esas objeciones mediante corroboración múltiple: cruza números voluntariamente aportados por fuentes DGST con bases filtradas, utiliza indicadores forenses del Security Lab, documentación judicial del litigio WhatsApp–NSO, testimonios de exmiembros del sector y documentos de inteligencia europeos. El peso analítico no recae en un único indicio como “Morgan”. [FS-1; FS-2; FS-4; GUA-1]

13.3. Límites judiciales

Las decisiones judiciales españolas relacionadas con Pegasus muestran un límite frecuente de la atribución cibernética: es posible probar compromiso de terminales sin poder probar en sede penal qué persona, unidad o Gobierno ejecutó materialmente cada operación. La falta de cooperación internacional, la naturaleza opaca de proveedores y la ausencia de logs soberanos completos degradan la atribución jurídica. En consecuencia, “atribución analítica” y “atribución judicial” no son equivalentes. [GUA-1]

Del mismo modo, decisiones judiciales favorables a periodistas frente a acciones promovidas por Marruecos no constituyen por sí mismas una sentencia que declare probado el uso de Pegasus por Rabat. Validan el contexto y la protección de la actividad informativa, no necesariamente cada afirmación técnica del corpus. Esta distinción es esencial para evitar sobreafirmaciones.

14. Implicaciones para España y Ceuta

ÁREA	IMPLICACIÓN / MEDIDA
Contrainteligencia	Tratar la cooperación con Marruecos como relación de “socio y colector” simultáneamente. La confianza operativa no elimina objetivos nacionales divergentes.
Dispositivos oficiales	Aplicar terminales de viaje segregados, mínimos datos en reposo, cuentas temporales y retorno con revisión/reciclado; evitar dispositivos personales en entornos de riesgo.
Formación conjunta	Revisar qué técnicas, herramientas y procedimientos se transfieren; aplicar criterios de necesidad, reciprocidad y riesgo de reutilización contra intereses españoles.
Frontera Ceuta/Melilla	Integrar alerta migratoria, inteligencia de redes sociales, observación de postura de fuerzas marroquíes y señales diplomáticas en un único cuadro de situación.
Soberanía tecnológica	No depender de un único proveedor/indicador de spyware; mantener capacidad forense y telemetría propia para campañas desconocidas.
Protección de altos cargos	Separar comunicaciones políticas, personales y de seguridad; reducir superficie de metadatos; establecer procedimientos de reacción ante indicadores de compromiso.
Comunicaciones estratégicas	Evitar atribuciones públicas prematuras; utilizar niveles de confianza y presentar evidencia por capas para preservar credibilidad.
Diplomacia	Diseñar mecanismos para que desacuerdos políticos no degraden sin aviso la cooperación policial/fronteriza esencial.

Para Ceuta, el riesgo principal no es únicamente una “invasión” física ni un único episodio migratorio; es la capacidad de convertir variaciones rápidas de control fronterizo en un shock político y logístico. La resiliencia requiere capacidad de absorción, mando interadministrativo, información pública rápida, registro forense de lo ocurrido y mecanismos de atribución que no dependan de una sola fuente. [EC-4; FS-5]

15. Indicadores de alerta temprana y recomendaciones defensivas

15.1. Indicadores observables en Ceuta/Melilla

DOMINIO	INDICADOR
Frontera	Reducción abrupta de patrullas o auxiliares en puntos habituales sin explicación operativa pública.
Movilidad	Incremento inusual de taxis, autobuses o desplazamientos hacia Fnideq/Belyounech/Nador y zonas costeras.
Redes sociales	Mensajes coordinados sobre “frontera abierta”, horarios, puntos de entrada, ausencia de devoluciones o convocatorias simultáneas.
Narrativa	Cambio sincronizado en medios alineados: acusaciones contra España, mensajes de soberanía, “lecciones” o amenazas veladas.
Cooperación	Cancelación o ralentización súbita de reuniones, entregas, readmisiones, judicialización o cooperación antiterrorista.
Ciber	Aumento de phishing, intentos de compromiso o indicadores de spyware contra responsables españoles durante una crisis bilateral.
Diplomacia	Incidentes alrededor de Sáhara Occidental, visitas de alto nivel, reconocimiento, Argelia o decisiones judiciales con impacto transfronterizo.
Mando	Señales de actuación excepcional de DGSN/DGST o presencia de altos responsables en el norte de Marruecos.

15.2. Recomendaciones prioritarias

PRIORIDAD	ACCIÓN
R1 · 0–30 días	Crear una célula permanente Ceuta/Melilla de fusión OSINT–frontera–ciber–diplomacia con indicadores compartidos y umbrales de alerta.
R2 · 0–30 días	Auditar exposición móvil de altos cargos y unidades con contacto frecuente con Marruecos; priorizar viajes y periodos de crisis.
R3 · 30–90 días	Formalizar política de “dispositivo de viaje limpio” para personal de seguridad, diplomacia y defensa; separar identidades y datos operativos.
R4 · 30–90 días	Revisar módulos de formación transferidos a DGST/DGSN con una matriz de reutilización adversa y reciprocidad.
R5 · 30–90 días	Establecer procedimiento de preservación de evidencia en crisis fronterizas: vídeo, radio, logs, geolocalización agregada, cronología y decisiones de mando.
R6 · 90–180 días	Mejorar capacidad nacional de análisis forense de spyware mercenario y compartir IOC bajo controles estrictos con socios europeos.
R7 · permanente	Adoptar lenguaje de atribución por niveles: “confirmado / altamente probable / probable / posible / no corroborado”.
R8 · permanente	Mantener canales de cooperación con Marruecos, pero con controles de contrainteligencia equivalentes a los aplicados a cualquier servicio extranjero activo.

PRINCIPIO DE DISEÑO

La respuesta adecuada no es romper cooperación, sino eliminar la suposición de que cooperación equivale a ausencia de espionaje. La política defensiva debe preservar intercambio antiterrorista y fronterizo al tiempo que limita exposición de información sensible.

16. Vacíos de inteligencia y preguntas prioritarias

ID	PREGUNTA	PRIORIDAD
PIR-01	¿Existe una orden, mensaje, registro o testigo contemporáneo que conecte la cúspide marroquí con la reducción de controles del 30/07/2026?	CRÍTICA
PIR-02	¿Qué cifras independientes y trazables existen sobre el número real de entradas y retornos en Ceuta entre el 20/07 y el 05/08?	CRÍTICA
PIR-03	¿Qué unidades marroquíes estaban desplegadas, qué turnos tenían y qué cambios de instrucción recibieron?	ALTA
PIR-04	¿Quién coordinó los principales grupos/cuentas de movilización y qué vínculos financieros, políticos o policiales existen?	ALTA
PIR-05	¿Cuál fue la cadena financiera real de la licencia “Morgan” y qué papel exacto tuvo EAU/FSSYS/Al Fahad?	ALTA
PIR-06	¿Existen indicadores forenses de herramientas sucesoras de Pegasus en Marruecos después de noviembre de 2021?	ALTA
PIR-07	¿Qué número de agentes/instructores españoles fueron seleccionados, comprometidos o vigilados por medios no digitales?	ALTA
PIR-08	¿Qué controles legales internos existen realmente para interceptaciones de DGST y cómo se aplican en práctica?	MEDIA
PIR-09	¿Qué otros aliados africanos o europeos fueron seleccionados durante crisis políticas?	MEDIA
PIR-10	¿Qué proveedores alternativos presentaron capacidades a partir de 2022 y cuáles fueron adquiridos?	MEDIA

ANEXO A. Cronología consolidada 2014–2026

FECHA	EVENTO / RELEVANCIA
2014	Comienza/crece la cooperación Guardia Civil–DGST; antecedente de crisis fronteriza y suspensión temporal de cooperación citado por EC-4.
2017	Documentos sobre S6 Edge y cibercafés; demostraciones de Pegasus en Rabat; primeras pruebas de “Morgan”.
2018	Expansión de selección a activistas y objetivos vinculados al Sáhara; uso internacional en crecimiento.
mar 2019	Figuras de Gabón incluidas como potenciales objetivos durante crisis sucesoria; Alberto Aguilera seleccionado desde marzo.
2019–2020	Indicadores de Pegasus en siete ministros franceses mientras Francia estudia comprar el producto.
jul 2020	Detención de Omar Radi; extracción de su teléfono con Cellebrite según el especial.
may 2021	Crisis de Ceuta por Brahim Ghali; alrededor de 10.000 entradas; teléfonos de altos cargos españoles comprometidos con Pegasus en fechas próximas.
jul 2021	Pegasus Project original publica lista de más de 50.000 números a escala global y atribuciones por clientes; Marruecos niega uso.
nov 2021	Últimos rastros de Pegasus citados por el nuevo especial en Marruecos; NSO entra en lista negra comercial de EE. UU.
mar 2022	España modifica su posición política sobre la propuesta marroquí para el Sáhara Occidental.
jun 2022	Crisis de Melilla/Nador con muertes en la frontera; deterioro de percepción pública.
sep 2022	Reunión secreta citada entre CNI y autoridades marroquíes en Rabat.
2024	Omar Radi es indultado; continúa debate sobre vigilancia y represión.
ene 2026	Caso judicial español Pegasus vuelve a quedar limitado/archivado por falta de cooperación internacional según prensa.
2 jul 2026	Hammouchi recibe delegación española encabezada por Luis Peláez Piñeiro.
16–18 jul 2026	Forbidden Stories y socios publican el nuevo especial de cinco investigaciones.
20 jul 2026	El Confidencial sitúa comienzo de incremento sostenido de entradas a nado.

FECHA	EVENTO / RELEVANCIA
27 jul 2026	Ceuta y Delegación del Gobierno reclaman respuesta extraordinaria, según EC-4.
30 jul 2026	Entrada masiva en Ceuta; cifra exacta discutida entre fuentes.
12 ago 2026	El Confidencial publica la hipótesis de represalia de los servicios marroquíes por el especial Pegasus.

ANEXO B. Entidades y figuras citadas

ENTIDAD	ROL	RELEVANCIA
Abdellatif Hammouchi	DGST/DGSN	Figura central del aparato de seguridad marroquí y cooperación con España.
Fouad Ali El Himma	Entorno real / consejero	Citado por fuentes como nodo de decisiones y “Bureau 21”.
Yassine Mansouri	DGED	Responsable de inteligencia exterior.
Mohamed Raji	DOP / DGST	Responsable operativo citado; asociado a objetivos de alto nivel.
Abdeljalil Taki	DGEI / DGST	Responsable técnico citado; pruebas iniciales Pegasus.
Abdelaziz Brachmi	ECT / DGST	Responsable técnico citado en el entorno de demostraciones.
Safir	exagente DGST, seudónimo	Fuente central del especial 2026; identidad protegida.
Hicham Mansouri	periodista marroquí en el exilio	Investigador y coautor; víctima de Pegasus según el corpus.
Omar Radi	periodista	Caso emblemático de vigilancia multicapa.
Alberto Aguilera	Guardia Civil	Número seleccionado cinco veces según la investigación.
Pedro Sánchez	Presidente del Gobierno de España	Teléfono comprometido con Pegasus según investigación española.
Margarita Robles	Ministra de Defensa	Teléfono comprometido/objetivo citado.
Fernando Grande-Marlaska	Ministro del Interior	Objetivo/compromiso citado; cooperación bilateral.
Arancha González Laya	exministra de Exteriores	Objetivo citado en contexto de crisis Ghali.
Sébastien Lecornu	dirigente francés	Uno de siete ministros con indicios de compromiso citados.
Noureddin Bongo Valentin	figura política gabonesa	Potencial objetivo durante crisis sucesoria 2019.
Brice Laccruche Alihanga	exjefe de gabinete gabonés	Potencial objetivo durante crisis sucesoria 2019.
NSO Group	proveedor israelí	Fabricante de Pegasus.
FSSYS / Al Fahad	intermediario tecnológico	Pieza clave de la hipótesis de triangulación con EAU.
Amnesty International Security Lab	laboratorio forense	Apoyo técnico al consorcio.

ANEXO C. Matriz de hechos, alegaciones e inferencias

AFIRMACIÓN	TIPO	CONFIANZA	BASE
Pegasus fue usado contra teléfonos de altos cargos españoles	HECHO TÉCNICO	ALTA	Investigación forense/judicial española.
Marruecos fue el operador de todas esas infecciones	ATRIBUCIÓN	MEDIA/ALTA	Correlación de infraestructura y contexto; no sentencia penal completa.
“Morgan” es el cliente marroquí de NSO	ATRIBUCIÓN INDUSTRIAL	ALTA/MEDIA	Múltiples fuentes sectoriales + documentos.
EAU pagó la licencia marroquí	ALEGACIÓN	MEDIA/BAJA	Fuentes internas sí; ex-NSO no lo confirman.
DGST preinfectó ~50 S6 Edge para activistas del Rif	ALEGACIÓN CORROBORADA	MEDIA/ALTA	Documentos internos + testimonio + localización de usuario.

AFIRMACIÓN	TIPO	CONFIANZA	BASE
DGST infectó cibercafés con RCS	ALEGACIÓN CORROBORADA	ALTA/MEDIA	Documentos + antiguo empleado Hacking Team.
Guardia Civil entrenó DGST y algunos instructores fueron vigilados	HECHO + ALEGACIÓN	MEDIA/ALTA	Cooperación documentada; vigilancia basada en fuentes y selección de mando.
Marruecos seleccionó figuras de Gabón en 2019	HECHO DE SELECCIÓN	ALTA/MEDIA	Base de potenciales objetivos; infección individual no confirmada.
La crisis de Ceuta 30/07/2026 fue venganza por Pegasus	ALEGACIÓN / INFERENCIA	BAJA/MEDIA	Dos exagentes + secuencia; falta evidencia de mando.
La movilización social amplificó la crisis de Ceuta	INFERENCIA	MEDIA/ALTA	Comportamiento de red y escala de contagio coherentes.
La frontera forma parte del repertorio de presión bilateral	INFERENCIA ESTRATÉGICA	MEDIA/ALTA	Precedentes 2014/2021 y utilidad política recurrente.

ANEXO D. Fuentes y trazabilidad

Las referencias [FS-x], [EC-x] y [GUA-1] utilizadas en el cuerpo remiten a la matriz siguiente. Se priorizan enlaces originales. Las versiones traducidas de Google aportadas por el usuario no se consideran una fuente distinta del original.

ID	MEDIO	TÍTULO / FECHA	APORTACIÓN
FS-0	Forbidden Stories	Pegasus Project: Inside Morocco's spying machine · 2026	Página matriz; identifica cinco investigaciones del especial.
FS-1	Forbidden Stories	Morocco Denied Using Pegasus. Documents and Insider Accounts Tell a Different Story · 16/07/2026	Vigilancia interior, Omar Radi, S6 Edge, cibercafés, RCS, Pegasus, responsables DGST.
FS-2	Forbidden Stories	Codename "Morgan": how Morocco accessed Pegasus, involving Israel and the United Arab Emirates · 16/07/2026	Adquisición, Villa FSSYS, "Morgan", NSO, Israel, EAU e intermediarios.
FS-3	Forbidden Stories	How Morocco allegedly spied on an African ally · 16/07/2026	Gabón: crisis sucesoria y potenciales objetivos.
FS-4	Forbidden Stories	While France was considering buying Pegasus, Morocco was spying on its ministers · 16/07/2026	Francia: siete ministros, compra frustrada, DGSE/ANSSI.
FS-5	Forbidden Stories	Moroccan intelligence is believed to have spied on Spanish agents who were training them · 17/07/2026	España: Guardia Civil, formación, selección de mando, crisis 2021.
GUA-1	The Guardian	Morocco intelligence insider reveals widespread use of hacking software Pegasus · 16/07/2026	Corroboración periodística internacional y contexto español.
EC-1	El Confidencial	Pegasus Project: en las entrañas del espionaje marroquí · 16/07/2026	Síntesis española extensa: estructura, técnicas, CNI, España, Omar Radi.
EC-2	El Confidencial	Más allá de Pegasus: el arsenal tecnológico de Marruecos para espiar dentro y fuera del país · 18/07/2026	Arsenal técnico, proveedores e intermediarios. Acceso automatizado parcialmente restringido; contrastado con el corpus.
EC-4	El Confidencial / Ignacio Cembrero	Ceuta fue la venganza de los servicios secretos marroquíes tras ser expuestos por 14 medios de comunicación · 12/08/2026	Hipótesis de represalia, secuencia julio 2026 y precedentes 2014/2021.

Enlaces originales

FS-0 · Forbidden Stories · 2026 · Pegasus Project: Inside Morocco's spying machine

FS-1 · Forbidden Stories · 16/07/2026 · Morocco Denied Using Pegasus. Documents and Insider Accounts Tell a Different Story

FS-2 · Forbidden Stories · 16/07/2026 · Codename "Morgan": how Morocco accessed Pegasus, involving Israel and the United Arab Emirates

FS-3 · Forbidden Stories · 16/07/2026 · How Morocco allegedly spied on an African ally

FS-4 · Forbidden Stories · 16/07/2026 · While France was considering buying Pegasus, Morocco was spying on its ministers

FS-5 · Forbidden Stories · 17/07/2026 · Moroccan intelligence is believed to have spied on Spanish agents who were training them

GUA-1 · The Guardian · 16/07/2026 · Morocco intelligence insider reveals widespread use of hacking software Pegasus

EC-1 · El Confidencial · 16/07/2026 · Pegasus Project: en las entrañas del espionaje marroquí

EC-2 · El Confidencial · 18/07/2026 · Más allá de Pegasus: el arsenal tecnológico de Marruecos para espiar dentro y fuera del país

EC-4 · El Confidencial / Ignacio Cembrero · 12/08/2026 · Ceuta fue la venganza de los servicios secretos marroquíes tras ser expuestos por 14 medios de comunicación

Fuentes complementarias de contraste

El análisis se ha contrastado con información pública sobre litigios NSO/WhatsApp, antecedentes europeos sobre Hacking Team y cobertura contemporánea de medios internacionales. Estas referencias se utilizan para validar contexto y no sustituyen las fuentes primarias del corpus solicitado.

ANEXO E. Glosario técnico e institucional

TÉRMINO	DEFINICIÓN
DGST	Direction Générale de la Surveillance du Territoire; inteligencia interior marroquí.
DGSN	Direction Générale de la Sûreté Nationale; Policía nacional marroquí.
DGED	Direction Générale des Études et de la Documentation; inteligencia exterior marroquí.
DOP	Dirección/estructura de operaciones citada en el especial.
DGEI	Estructura técnica citada por las fuentes; vinculada a Abdeljalil Taki.
CNI	Centro Nacional de Inteligencia (España).
ANSSI	Agence nationale de la sécurité des systèmes d'information (Francia).
DGSE	Direction générale de la sécurité extérieure (Francia).
NSO Group	Empresa israelí fabricante de Pegasus.
Pegasus	Spyware móvil de altas prestaciones para acceso remoto a datos y sensores.
RCS	Remote Control System; plataforma de intrusión asociada históricamente a Hacking Team.
IMSI catcher	Dispositivo que simula/interactúa con estaciones celulares para identificar o interceptar terminales según configuración y marco técnico.
Zero-click	Vector de compromiso que no requiere interacción consciente del usuario.
IOC	Indicator of Compromise / indicador de compromiso.
HUMINT	Inteligencia obtenida de fuentes humanas.
OSINT	Inteligencia de fuentes abiertas.
Atribución analítica	Estimación de responsabilidad basada en evidencia e inferencia; no equivale a una atribución judicial.
Instrumentalización de la migración	Uso deliberado de flujos o presión migratoria como instrumento de coerción política; concepto reconocido en análisis de amenazas híbridas.

Conclusión analítica

El conjunto de investigaciones de julio de 2026 refuerza de manera sustancial la imagen de Marruecos como usuario sofisticado de vigilancia técnica y humana, con capacidad para combinar herramientas comerciales, acceso local, cooperación de seguridad y objetivos de alto nivel. La solidez del corpus es mayor cuando describe capacidades y patrones —Pegasus, RCS, Cellebrite, vigilancia de objetivos y selección de números— que cuando intenta reconstruir decisiones políticas concretas o cadenas de mando no documentadas. [FS-1 a FS-5; GUA-1; EC-1]

España aparece en una posición particularmente delicada: es socio operativo indispensable de Marruecos en seguridad y migración, pero también un objetivo lógico de inteligencia por la intensidad de sus desacuerdos estratégicos y por el valor de anticipar decisiones sobre Sáhara Occidental, fronteras, defensa y política

europea. La evidencia sobre teléfonos comprometidos demuestra que la cooperación bilateral no debe traducirse en relajación contrainteligente. [FS-5; GUA-1]

Respecto a Ceuta en julio de 2026, la hipótesis de represalia por las revelaciones Pegasus merece investigación prioritaria pero no puede elevarse a hecho. Los indicios disponibles permiten sostener que una variación de la postura de control marroquí pudo influir en la ventana de oportunidad; la movilización distribuida en redes explica bien la escalada. Lo que falta es evidencia que conecte de forma trazable la motivación "Pegasus" con una orden concreta. Hasta que aparezca, la formulación profesional correcta es: "atribución plausible, no corroborada, confianza baja/media". [EC-4]

Perspectiva de riesgo a 6–12 meses

ESCENARIO	PROBABILIDAD	IMPACTO	INDICADOR ANALÍTICO
Diversificación de spyware	ALTA	ALTO	Las fuentes describen búsqueda de proveedores alternativos desde 2022; es probable que la capacidad sobreviva a Pegasus como producto concreto.
Nuevos intentos contra altos cargos españoles	MEDIA/ALTA	ALTO	Las crisis bilaterales, defensa, Sáhara y seguridad crean demanda persistente de inteligencia política.
Nueva presión rápida en Ceuta/Melilla	MEDIA	ALTO	La frontera conserva utilidad coercitiva; el detonante y la modalidad concreta son difíciles de anticipar.
Campañas de influencia y descrédito	ALTA	MEDIO/ALTO	Las revelaciones elevan el incentivo para desacreditar fuentes, periodistas y atribuciones técnicas.
Aparición de prueba directa sobre Ceuta 2026	BAJA/MEDIA	MUY ALTO	Una orden, filtración operativa o testimonio contemporáneo podría alterar de forma sustancial la atribución actual.

VALORACIÓN FINAL

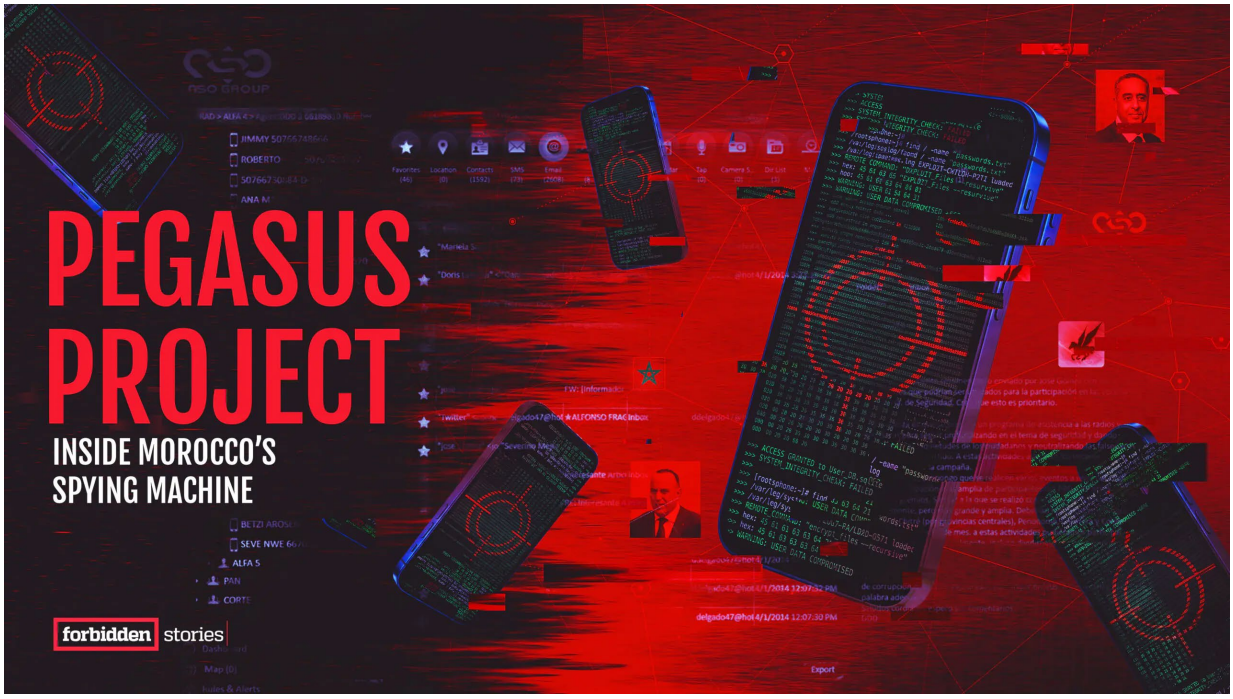
La principal vulnerabilidad española no es una herramienta concreta, sino la combinación de dependencia operativa, proximidad política y exposición técnica frente a un socio con intereses propios. La mitigación exige cooperación con controles, resiliencia fronteriza y disciplina de atribución.

ANEXO F. Dossier documental de publicaciones y explotación analítica

Este anexo reconstruye de forma individualizada cada una de las publicaciones aportadas y las cinco investigaciones enlazadas desde el especial de Forbidden Stories. No reproduce de manera íntegra los artículos protegidos por derechos de autor; integra exhaustivamente sus hechos, protagonistas, cronologías, elementos técnicos, alegaciones, contradicciones y valor analítico, con redacción propia y atribución expresa.

F.1. Forbidden Stories — “Pegasus Project: Inside Morocco’s spying machine”

ID / MEDIO	FS-0 · Forbidden Stories
PUBLICACIÓN	Pegasus Project: Inside Morocco’s spying machine · julio de 2026
TRAZABILIDAD	FUENTE PRIMARIA / PERIODÍSTICA https://forbiddenstories.org/projects_posts/pegasus-project-inside-moroccos-spying-machine/



Visual oficial del especial. Fuente: Forbidden Stories.

La página matriz presenta el proyecto como una continuación, cinco años después, de las revelaciones originales de Pegasus. Forbidden Stories y trece socios periodísticos, con apoyo técnico del Security Lab de Amnesty International, afirman haber trabajado sobre documentos internos previamente inéditos y testimonios de primera mano. El especial articula una tesis de conjunto: la DGST marroquí no dependería de una única herramienta, sino de un repertorio escalonado de seguimiento físico, infiltración de entornos, herramientas forenses y spyware remoto.

- La sección Investigations contiene cinco piezas nucleares: vigilancia interior y caso Omar Radi; adquisición de Pegasus bajo el nombre en clave “Morgan”; Gabón; Francia; y España/Guardia Civil.
- El valor probatorio varía según el elemento: análisis forense y documentación judicial ofrecen mayor robustez que testimonios anónimos o reconstrucciones de cadena de mando.
- El proyecto señala que la inclusión de un número en una lista de selección no equivale por sí sola a una infección efectiva; esta distinción se mantiene en todo el informe.

F.2. “Morocco Denied Using Pegasus. Documents and Insider Accounts Tell a Different Story”

ID / MEDIO	FS-1 · Forbidden Stories
PUBLICACIÓN	Morocco Denied Using Pegasus. Documents and Insider Accounts Tell a Different Story · 16/07/2026
TRAZABILIDAD	FUENTE PRIMARIA / PERIODÍSTICA https://forbiddenstories.org/how-did-morocco-become-addicted-to-tracking-down-its-opponents-with-spyware/

Es la pieza más extensa sobre la arquitectura doméstica de vigilancia. Parte del caso de Omar Radi para mostrar una progresión desde la observación física y la vigilancia del entorno hasta el acceso forense a su iPhone mediante Cellebrite y el uso de Pegasus. La fuente “Safir”, antiguo miembro de la DGST, sostiene que Pegasus se reservaba para objetivos de alto valor cuando los métodos previos no bastaban. La investigación cruza su testimonio con documentos internos, datos del Pegasus Project, análisis de Amnesty International y aportaciones de otros exagentes.

Uno de los episodios centrales es “Op S6_Edge”: documentos internos mostrarían la compra de aproximadamente cincuenta Samsung Galaxy S6 Edge y su preinfección con software distinto de Pegasus antes de ser distribuidos a comercios del Rif para que acabaran en manos de activistas. El consorcio localizó a una persona fotografiada en esos archivos, que confirmó haber recibido un terminal nuevo y haber sufrido sustituciones repetidas de batería. El síntoma de batería, aisladamente, no acredita una infección, pero su testimonio aporta corroboración contextual al material documental.

La misma pieza describe el compromiso de cibercafés con Remote Control System (RCS) de Hacking Team, la explotación intensiva de los equipos y preocupaciones internas de antiguos empleados del proveedor. A finales de 2017 la DGST habría migrado parte de sus objetivos de mayor sensibilidad a Pegasus. La investigación identifica a Abdeljalil Taki y otros responsables técnicos, y señala números de agentes marroquíes usados en pruebas tempranas. También atribuye a Mohamed Raji un papel de primer nivel en el programa de escuchas y recoge la alegación, no verificada independientemente, de que solicitudes especialmente sensibles llegaban desde el entorno de Fouad Ali El Himma y “Bureau 21”.

F.3. “Codename Morgan” — adquisición de Pegasus, Israel y Emiratos

ID / MEDIO	FS-2 · Forbidden Stories
PUBLICACIÓN	Codename “Morgan”: how Morocco accessed Pegasus, involving Israel and the United Arab Emirates · 16/07/2026
TRAZABILIDAD	FUENTE PRIMARIA / PERIODÍSTICA https://forbiddenstories.org/codename-morgan-a-look-back-at-moroccos-acquisition-of-pegasus-involving-israel-and-the-united-arab-emirates/

La investigación reconstruye la fase de adquisición. Sitúa a finales de 2017 una demostración de unos diez días en la denominada “Villa FSSYS” de Rabat, próxima a la avenida Mehdi Ben Barka y a la embajada canadiense. Empleados de NSO habrían mostrado a altos cargos y técnicos de la DGST la infección de terminales de prueba, activación remota de cámaras y micrófonos y extracción de datos. Safir caracteriza el salto tecnológico como radical frente a las técnicas que exigían acceso físico o explotación local.

El consorcio identifica “Morgan” como el nombre en clave utilizado por NSO para el cliente marroquí, a partir de documentación del litigio WhatsApp/Meta contra NSO y de fuentes del sector. La pieza reconstruye además una posible triangulación mediante FSSYS Maroc / Al Fahad, vinculada al ecosistema tecnológico emiratí. El hecho de la intermediación aparece mejor sustentado que la afirmación de que Emiratos Árabes Unidos financiara directamente la licencia: esta última procede de fuentes internas y no fue confirmada por todas las fuentes ex-NSO consultadas.

El artículo incorpora también la dimensión estatal israelí, examinando relaciones entre NSO y autoridades de Israel, así como controversias sobre documentación diplomática y autorizaciones de exportación. Para el análisis español, el punto esencial es que la adquisición de una capacidad comercial se inserta en una red de relaciones políticas y de seguridad que afecta a soberanía tecnológica, trazabilidad del proveedor y posibilidad de conocimiento externo de objetivos.

F.4. Gabón — vigilancia de un aliado africano

ID / MEDIO	FS-3 · Forbidden Stories
PUBLICACIÓN	How Morocco allegedly spied on an African ally · 16/07/2026
TRAZABILIDAD	FUENTE PRIMARIA / PERIODÍSTICA https://forbiddenstories.org/how-morocco-allegedly-spies-on-an-african-ally/

La pieza analiza la crisis sucesoria gabonesa tras el ictus de Ali Bongo en octubre de 2018 y su posterior recuperación en Rabat. En marzo de 2019, alrededor de diez figuras gabonesas aparecen en la lista de potenciales objetivos: entre ellas Noureddin Bongo Valentin y Brice Laccruche Alihanga, además de opositores como Jean Ping y Dieudonné Minlama Mintogo. La selección se habría producido pese a la estrecha relación bilateral y a la cooperación entre aparatos de seguridad.

La conclusión analítica prudente no es que todos los teléfonos fueran infectados, sino que Marruecos habría mostrado interés en conocer la evolución de una sucesión política dentro de un país aliado. El episodio refuerza el patrón general del especial: la condición de socio no elimina el valor de inteligencia de una persona, especialmente cuando existe incertidumbre sobre la continuidad del poder o sobre alineamientos regionales.

F.5. Francia — ministros comprometidos mientras París estudiaba comprar Pegasus

ID / MEDIO	FS-4 · Forbidden Stories
PUBLICACIÓN	While France was considering buying Pegasus, Morocco was spying on its ministers · 16/07/2026
TRAZABILIDAD	FUENTE PRIMARIA / PERIODÍSTICA https://forbiddenstories.org/while-france-was-considering-buying-pegasus-morocco-was-spying-on-its-ministers/

Forbidden Stories describe una coincidencia de gran relevancia contrainteligente: durante 2019-2020, organismos franceses evaluaban la compra de Pegasus mientras siete ministros presentaban “signos de compromiso” asociados a infraestructura utilizada contra objetivos vinculados a Marruecos. La investigación cita a Jean-Michel Blanquer, Jacqueline Gourault, Julien Denormandie, Emmanuelle Wargon, François de Rugy, Florence Parly y Sébastien Lecornu.

El revendedor francés Syans habría discutido con organismos de inteligencia y justicia una posible operación de 60 a 80 millones de euros. La Presidencia francesa terminó bloqueando la compra a finales de 2020 por razones de soberanía y reputación, aunque posteriormente se habría vuelto a presentar documentación administrativa para autorizar la comercialización. La pieza también cita documentación de la DGSE y análisis de ANSSI que vinculan determinados artefactos e identificadores a campañas de Pegasus.

El caso francés introduce una advertencia estratégica aplicable a España: una herramienta ofensiva adquirida a un proveedor extranjero puede ser simultáneamente una capacidad deseada y un vector de dependencia. La seguridad no se limita al malware; incluye export controls, soporte, infraestructura, metadatos operativos y posibles relaciones del proveedor con su Estado de origen.

F.6. España — agentes de Guardia Civil que formaban a la DGST y habrían sido vigilados

ID / MEDIO	FS-5 · Forbidden Stories

PUBLICACIÓN	Cómo los servicios de inteligencia marroquíes habrían espiado a los agentes españoles que los formaban · 17/07/2026
TRAZABILIDAD	FUENTE PRIMARIA / PERIODÍSTICA https://forbiddenstories.org/es/como-los-servicios-de-inteligencia-marroquies-habrian-espiado-a-los-agentes-espanoles-que-los-formaban/

Fahad, a la izquierda, en una imagen publicada por Forbidden Stories durante una actividad con la Guardia Civil. Fuente: Forbidden Stories.

Esta pieza es prioritaria para el presente informe. Reconstruye la cooperación formal iniciada en 2014 entre la Guardia Civil y la DGST, sobre una relación previamente dominada por Policía Nacional y CNI. Describe visitas oficiales, operaciones antiterroristas, cooperación sobre migración irregular y sesiones de entrenamiento de personal técnico del Grupo de Apoyo Operativo (GAO), con actividades en Ceuta, Málaga, Marbella, Madrid, Fnideq, Tánger, Rabat, Tetuán, Nador y Marrakech.

La investigación se apoya en documentos y fotografías filtrados y en fuentes que, según Forbidden Stories, participaron directamente en los hechos: un exagente de la DGST, dos agentes de Guardia Civil, un miembro de Policía Nacional y un integrante del CNI. El Security Lab de Amnesty International habría validado material técnico. El núcleo de la alegación es que la DGST mantenía vigilancia sobre instructores españoles “por si acaso”, mientras existía una relación de confianza operativa. La pieza menciona IMSI catchers como posible mecanismo local, pero advierte de que esa descripción concreta no pudo verificarse de forma independiente.

El número personal de Alberto Aguilera, antiguo agregado de Interior en Rabat y posteriormente responsable de inteligencia de Guardia Civil en Cataluña, aparece cinco veces en la lista de potenciales objetivos atribuida al operador marroquí, con selección desde el 8 de marzo de 2019. La pieza resalta una asimetría OPSEC: Policía Nacional habría aplicado terminales separados para información sensible y no sensible durante viajes a Marruecos, mientras miembros de Guardia Civil reconocen que no adoptaron la misma precaución porque no esperaban ser espiados por un socio.

La investigación identifica además a varios agentes marroquíes y funciones atribuidas: Fahad, vinculado según Safir a cámaras ocultas, ataques de tipo man-in-the-middle y NightHawk/Interionet; Khalid, asociado a explotación de información y redes de medios de influencia; Mourad, ligado a operaciones técnicas y al seguimiento de Omar Radi; y Jaouad, señalado como coordinador operativo de vigilancia sobre agentes españoles. Algunas de estas atribuciones se basan en una fuente interna y carecen de documentación pública suficiente para elevarlas a hecho probado.

El elemento estratégico es la paradoja de la cooperación: España transfirió procedimientos de seguimiento, infiltración, obtención técnica y otras prácticas para combatir yihadismo, tráfico de personas y criminalidad; las fuentes sostienen que unidades marroquíes pudieron reutilizar parte de ese conocimiento contra periodistas, activistas y contra los propios formadores. El informe conserva la diferencia entre cooperación documentada y reutilización represiva alegada.

F.7. The Guardian — corroboración internacional y síntesis de la investigación

ID / MEDIO	GUA-1 · The Guardian
PUBLICACIÓN	Moroccan intelligence insider reveals widespread use of Pegasus hacking software · 16/07/2026
TRAZABILIDAD	FUENTE PRIMARIA / PERIODÍSTICA https://www.theguardian.com/news/2026/jul/16/morocco-intelligence-insider-reveals-widespread-use-hacking-software-pegasus

The Guardian sintetiza el corpus internacional y aporta una corroboración editorial independiente dentro del consorcio. Explica que Safir trabajó cerca de una década para la DGST y que su testimonio fue contrastado con materiales filtrados, registros de targeting y análisis forense. Sitúa la adopción de Pegasus en 2017 y describe el empleo previo de HUMINT, cibercafés comprometidos y teléfonos preinfectados. La publicación también recuerda que NSO afirma vender Pegasus a gobiernos para investigación de terrorismo y delincuencia, mientras Marruecos niega haber usado el producto contra críticos.

Para España, The Guardian destaca más de doscientos números españoles seleccionados en los registros atribuidos al usuario considerado marroquí, la infección confirmada de teléfonos de Pedro Sánchez y Margarita Robles en 2021, y posteriores referencias a Fernando Grande-Marlaska y Luis Planas. La pieza señala que una cuenta atacante asignada al sistema marroquí habría sido usada también contra responsables españoles. La investigación judicial española acreditó compromisos técnicos pero no consiguió cerrar judicialmente toda la cadena de autoría, en parte por falta de cooperación israelí.

F.8. El Confidencial — “Pegasus Project: en las entrañas del espionaje marroquí”

ID / MEDIO	EC-1 · El Confidencial
PUBLICACIÓN	Pegasus Project: en las entrañas del espionaje marroquí · 16/07/2026
TRAZABILIDAD	FUENTE PERIODÍSTICA APORTADA; acceso automatizado restringido, contrastada con el corpus del consorcio https://www.elconfidencial.com/mundo/2026-07-16/pegasus-project-entranas-espionaje-marroqui-cbtr_4390628/

Esta publicación española funciona como pieza de integración nacional del especial. El presente informe la utiliza para desarrollar el organigrama funcional de la DGST, el papel atribuido a Hammouchi, Raji, Taki y el entorno de “Bureau 21”, las técnicas empleadas contra periodistas y opositores, el caso Omar Radi y el impacto para España. Los detalles que coinciden con Forbidden Stories, The Guardian y material forense se tratan con mayor confianza; las reconstrucciones de órdenes políticas o funciones personales sin evidencia independiente se mantienen como alegaciones atribuidas.

Su valor añadido es contextualizar la maquinaria de vigilancia dentro de la relación hispano-marroquí: cooperación antiterrorista, crisis por Brahim Ghali, instrumentalización de la frontera, objetivos españoles y evolución de las relaciones posteriores. La versión final del informe separa explícitamente “compromiso técnico”, “selección como objetivo”, “atribución analítica” y “atribución judicial”, evitando que los cuatro conceptos se confundan.

F.8.1. Matriz de cobertura integral de EC-1

EJE	CONTENIDO INCORPORADO	SECCIÓN
Ceuta 2021 y Brahim Ghali	Informes CNI; estrategia de presión; relación con el cambio posterior de posición española.	8.4 · 11 · 12
Bureau 21 / entorno real	Fouad Ali El Himma como nodo atribuido para objetivos de alto nivel.	3 · 8.4
DGST / DOP	Sede, cadena operativa, servidores y departamentos técnicos citados.	3 · 5
Sáhara / MINURSO	Alegaciones de vigilancia física y técnica en El Aaiún.	4 · 14
Vigilancia tradicional	Escuchas, moqadem, seguimientos, cámaras, micrófonos, IMSI/BTS.	4
Teléfonos y cibercafés	Preinfección de terminales, comercios, RCS y ordenadores públicos.	4.2

Pegasus / adquisición	FSSYS Al Fahad, demostraciones 2017, infraestructura y formación.	5
Pegasus / evolución	Selección, fingerprinting, vectores históricos y capacidades de explotación.	5.5
Explotación posterior	Datos, monitorización pasiva/activa, alertas y correlación.	5.5 · 6
DGST / estructura	DRS, DLCT, DAFF, DRH, DOP; DGEI/ECT y responsables citados.	3.1
Omar Radi	Escalada de vigilancia, Cellebrite, Pegasus y presión posterior.	7
Material gráfico	Mapa de Rabat, interfaces, infografías, documentos y fotografías.	3.1 · 4.2.1 · 5.5 · 7 · 8.4

F.9. El Confidencial — arsenal tecnológico más allá de Pegasus

ID / MEDIO	EC-2 · El Confidencial
PUBLICACIÓN	Más allá de Pegasus: el arsenal tecnológico de Marruecos para espiar dentro y fuera del país · 18/07/2026
TRAZABILIDAD	FUENTE PERIODÍSTICA APORTADA; acceso automatizado restringido, contrastada con Forbidden Stories https://www.elconfidencial.com/tecnologia/2026-07-18/marruecos-dgst-espionaje-pegasus-cellebrite-nighthawk-rcs-emiratos_4391801/

La pieza amplía el foco desde Pegasus a un ecosistema de proveedores y métodos. El informe integra Cellebrite para extracción forense de terminales en custodia; Remote Control System de Hacking Team en ordenadores y cibercafés; dispositivos de interceptación celular; y referencias periodísticas a NightHawk/Interionet y otras soluciones de monitorización. También incorpora antecedentes de proveedores y compras previas como evidencia de continuidad histórica del mercado de vigilancia en Marruecos.

La conclusión técnica es que un modelo defensivo centrado únicamente en Pegasus resulta insuficiente. La superficie de riesgo incluye custodia física de dispositivos, estaciones base falsas, redes locales, servicios de telecomunicaciones, herramientas de escritorio, extracción forense y captación humana. En consecuencia, las recomendaciones del cuerpo principal se formulan por capas y no por producto.

F.10. El Confidencial — la “traición” a instructores de Guardia Civil

ID / MEDIO	EC-3 · El Confidencial
PUBLICACIÓN	Pegasus Project: radiografía de la “traición”; agentes marroquíes espiaron a instructores de la Guardia Civil · 17/07/2026
TRAZABILIDAD	FUENTE PERIODÍSTICA APORTADA; contrastada con FS-5 https://www.elconfidencial.com/mundo/2026-07-17/pegasus-project-radiografia-traicion-agentes-marroquies-espiaron-instructores-guardia-civil-cbtr_4391223/

Esta pieza se trata conjuntamente con la investigación de Forbidden Stories sobre los instructores españoles porque ambas describen el mismo núcleo factual. El informe amplía especialmente la lectura contrainteligente: una relación de cooperación profunda produce exposición de identidades, rutinas, dispositivos, técnicas y redes personales. Si el socio mantiene al mismo tiempo una función de colección frente a España, el propio marco de confianza puede convertirse en multiplicador del riesgo.

El caso Aguilera sirve como indicador cuantificable de selección, mientras que las fotografías y notas de entrenamiento aportan contexto de proximidad institucional. La expresión “traición” se conserva como caracterización de fuentes/medio, no como categoría analítica. La formulación profesional utilizada es “asimetría contrainteligente en una relación de cooperación”.

F.10.1. Matriz de cobertura integral de la “Radiografía de una traición”

EJE	CONTENIDO INCORPORADO	SECCIÓN
Inicio de cooperación	Guardia Civil–DGST desde 2014; progresión de confianza y operaciones conjuntas.	8.1
Canales conjuntos	Grupo de WhatsApp y coordinación descrita por fuentes participantes.	8.1
Visitas recíprocas	Madrid, Ceuta, Málaga, Marbella y viajes de altos cargos a Rabat.	8.1

Base probatoria	Documentos/fotos filtrados; fuentes DGST, GC, PN y CNI; verificación técnica de Amnistía.	8
Vigilancia de instructores	Alegación de espionaje sistemático y grupo marroquí de coordinación desconocido por GC.	8.2
IMSI / IMEI / red	Identificación de terminales y acceso atribuido a infraestructura de Maroc Telecom.	4.3 · 8.2
OPSEC comparada	Precauciones de Policía Nacional frente a menor percepción de riesgo del GAO.	8.2.1
Técnicas transferidas	Seguimiento, hoteles/equipajes, medios técnicos, cibercafés; finalidad oficial antiterrorista/criminal.	8.2.1
Geografía	España y seis ubicaciones marroquíes citadas.	8.2.1
Drones	Alegación de aprendizaje inicial a partir de formación española en Málaga.	8.2.1
Cellule Recherche	Atribuciones a J. y M.J.; mantenidas como fuente no plenamente corroborada.	8.3
Alberto Aguilera	Cinco selecciones, inicio 08/03/2019; trayectoria y lectura contrainteligente.	8.3
Crisis 2021	Pegasus, 2,57 GB de Sánchez, Ceuta y contexto CNI.	8.4
Continuidad 2022–2023	Viaje CNI a Rabat, difusión de fotografías y antecedente de captación citado.	8.4.1
Material fotográfico	Hero, Bernabéu, Castillejos, Tánger, inspección de equipajes, vigilancia clandestina y Madrid.	8.1–8.4

F.11. El Confidencial — Ceuta 2026 como posible represalia

ID / MEDIO	EC-4 · El Confidencial / Ignacio Cembrero
PUBLICACIÓN	Ceuta fue la venganza de los servicios secretos marroquíes tras ser expuestos por 14 medios de comunicación · 12/08/2026
TRAZABILIDAD	FUENTE PERIODÍSTICA APORTADA; hipótesis de atribución no corroborada independientemente https://www.elconfidencial.com/espana/2026-08-12/ceuta-venganza-servicios-secretos-marruecos-comunicacion_4404207/

La pieza del 12 de agosto introduce una hipótesis causal distinta de los capítulos técnicos: dos antiguos miembros de servicios marroquíes atribuyen la crisis fronteriza de finales de julio a una represalia por el paquete de revelaciones Pegasus publicado entre el 16 y el 18 de julio. El artículo sitúa un aumento de entradas a nado desde aproximadamente el 20 de julio y una escalada posterior, y la compara con precedentes de 2014 y 2021 en los que la cooperación y la presión fronteriza se habrían modulado durante crisis diplomáticas.

La atribución se mantiene deliberadamente en confianza baja/media. No se dispone públicamente de una orden, registro de mando, comunicación interceptada ni testigo contemporáneo en servicio que conecte de forma trazable la publicación del especial con una instrucción de reducir controles. El análisis competitivo de hipótesis del cuerpo principal mantiene abiertas explicaciones concurrentes: presión estatal por una agenda bilateral más amplia, movilización distribuida en redes, explotación criminal de una ventana de oportunidad y cascada espontánea tras un fallo o relajación inicial.

F.12. Síntesis cruzada de todas las publicaciones

Las publicaciones convergen con mayor fuerza en cuatro puntos: (1) Marruecos desarrolló durante años una arquitectura de vigilancia combinando métodos físicos, humanos, forenses y cibernéticos; (2) existe evidencia sustancial de que fue cliente/usuario de Pegasus y de que el sistema asociado a “Morgan” operó desde 2017; (3) la selección de objetivos se extendió a periodistas, activistas y responsables extranjeros, incluidos españoles; y (4) la cooperación de seguridad con España no anuló la lógica de inteligencia entre Estados. La convergencia es menor cuando se intenta reconstruir la financiación exacta de Pegasus, la cadena de mando de cada operación o la motivación concreta de la crisis de Ceuta de julio de 2026.

El juicio central del documento se mantiene: para España, el riesgo no reside en una única herramienta, sino en la combinación de proximidad institucional, dependencia operativa en materias fronterizas y antiterroristas, exposición técnica durante viajes y cooperación, y divergencia estructural de intereses sobre Sáhara Occidental, Ceuta/Melilla, seguridad regional y política europea.

F.13. Matriz de cobertura: publicaciones solicitadas

PUBLICACIÓN	ESTADO	EXPLOTACIÓN EN EL INFORME

PUBLICACIÓN	ESTADO	EXPLOTACIÓN EN EL INFORME
Forbidden Stories · página matriz	Integrada	5 investigaciones abiertas y desarrolladas
Forbidden Stories · vigilancia interior / Omar Radi	Integrada	Arquitectura, S6 Edge, RCS, Cellebrite, Pegasus, responsables
Forbidden Stories · Morgan	Integrada	Adquisición, FSSYS, EAU, NSO, Israel
Forbidden Stories · Gabón	Integrada	Sucesión 2019, Bongo, Alihanga, opositores
Forbidden Stories · Francia	Integrada	7 ministros, ANSSI/DGSE, compra 60–80 M€
Forbidden Stories · España/Guardia Civil	INTEGRACIÓN PRIORITARIA	GAO, Aguilera, formación, vigilancia, Ceuta, DGST
The Guardian · 16/07/2026	Integrada	Corroboración internacional y objetivos españoles
El Confidencial · 16/07/2026	Integrada y ampliada	Entrañas del espionaje marroquí
El Confidencial · 17/07/2026	INTEGRACIÓN PRIORITARIA	“Traición” / instructores Guardia Civil
El Confidencial · 18/07/2026	Integrada y ampliada	Arsenal tecnológico más allá de Pegasus
El Confidencial · 12/08/2026	Integrada con cautela	Ceuta 2026: hipótesis de represalia
Google Search aportado	Ruta de navegación	No tratado como fuente independiente

FIN DEL INFORME